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

Fault-Tolerant Quantum Stabilizer Codes for Improving the Fidelity of Transversal CNOT Gates

by

Rosie Cane
BSc (Hons), MSc

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

September 2021

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

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

Dedicated to the people and horses at the Grange Pony Trekking Centre, Capel-y-ffin.

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

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

Doctor of Philosophy

Fault-Tolerant Quantum Stabilizer Codes for Improving the Fidelity of Transversal CNOT Gates

by Rosie Cane

In support of large-scale practical quantum algorithms Quantum-Error-Correction-Codes (QECC) are designed for mitigating the component errors inherent in quantum circuits. A QECC attaches carefully selected redundancy to quantum information in such a way that the individual qubit errors can be corrected without corrupting the logical qubit state, where the encoding and decoding circuits are built by individual quantum gates. If these components are error-prone, they increase the qubit error probability, hence leading to an even more grave corruption of the data qubits. Therefore constructing QECCs reliant on fault tolerant circuitry is crucial for creating quantum solutions. Fault tolerant QECCs are capable of providing error rate improvements in quantum processors as long as components operate below a certain gate error probability. We start by quantifying the depolarization probability bound, below which the family of transversal QECCs give a better error probability than an uncoded gate. Both a low-complexity repetition code and Steane's 7-bit QECC are characterized. In this context it is observed that the Frame-Error-Rates attained are lower-bounded according to the gate error probability occurring in the non-fault tolerant encoding circuits.

We address this problem by proposing the 'encoderless' quantum code, which replaces the encoder circuit by a fault-tolerant single-qubit gate arrangement. As a further benefit, in contrast to state preparation techniques, our encoderless scheme requires no prior knowledge of the input information, therefore realistic unknown states can be encoded fault-tolerantly. Our encoderless quantum code delivers a frame error rate that is three orders of magnitude lower than that of the corresponding scheme relying on a non-fault-tolerant encoder, when the gate error probability is as high as 10^{-3}.

Next, we consider two practical applications of fault-tolerant QECCs, in quantum communication protocols; Quantum teleportation allows an unknown quantum state to be transmitted between two separated locations. To achieve this the system requires both classical and quantum channel, for communicating a pair of classical bits and an entangled quantum bit from the transmitter to the receiver. It is commonly assumed in the literature that both channels are error free, even though under realistic conditions this is unlikely to be the case. Hence we propose and investigate a secure and reliable

quantum teleportation scheme, when both the classical and quantum channels exhibit errors. It is found that both the security and reliability of the teleportation may be improved, when powerful turbo codes are employed.

Finally, we quantify the fault-tolerance improvements attained by a $[4; 2; 2]$ error detection code in IBM's open-access devices. Up to 100 logical gates are activated in the *Ibmq_Bogota* and *Ibmq_Santiago* devices and we found that a $[4; 2; 2]$ code's logical gate set may be deemed fault-tolerant for gate sequences larger than 10 gates. However, certain circuits did not satisfy the fault tolerance criterion. In some cases the encoded-gate sequences show a high error rate that is lower bounded at $0{:}1$, whereby the error inherent in these circuits cannot be mitigated by classical post-selection. A comparison of the experimental results to a simple error model reveal that the dominant gate errors cannot be readily represented by the popular Pauli error model. Finally, it is most accurate to assess the fault tolerance criterion when the circuits tested are restricted to those that give rise to an output state with a low dimension.

Declaration of Authorship

I, Rosie Cane, declare that the thesis entitled Fault-Tolerant Quantum Stabilizer Codes for Improving the Fidelity of Transversal CNOT Gates 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].

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

Acknowledgements

First of all, I would like to wholeheartedly thank my supervisors Professor Lajos Hanzo and Professor Soon Xin Ng (Michael) for their continuous support and patience throughout the completion of this PhD. I would also like to thank Dr Daryus Chandra, without his kindness and creativity this work would not have been possible. In addition, I would like to extend my gratitude to Mr Yifeng Xiong, Mr Wanwan Xie, and all the members in the Next Generation Wireless Research Group who have inspired and encouraged me throughout this process. I would also like to acknowledge the use of the IRIDIS High-Performance Computing Facility and IBM Quantum services for this work. Finally, I am indebted to the Engineering and Physical Sciences Research Council for providing the financial support that has made this thesis possible.

List of Publications

Accepted Publications:

1. R. Cane, D. Chandra, S. X. Ng, and L. Hanzo, "Mitigation of decoherence-induced quantum-bit errors and quantum-gate errors using steane's code," *IEEE Access*, vol. 8, pp. 3693-–83709, 2020.
   DOI: 10.1109/ACCESS.2020.2991802.

2. R. Cane, D. Chandra, S. X. Ng, and L. Hanzo, "Gate-error-resilient quantum steane codes," *IEEE Access*, vol. 8, pp. 79346-–179362, 2020.
   DOI: 10.1109/ACCESS.2020.3027638.

3. R. Cane, W. Xie and S. X. Ng, ""Turbo-coded secure and reliable quantum teleportation," *IET Quantum Communication*, vol. 1, 2020.

In Review:

4. R. Cane, D. Chandra, S. X. Ng, and L. Hanzo, "Experimental Characterization of Fault-Tolerant Circuits in Small-Scale Quantum Processors," *IEEE Access*, 2021.

Contents

List of Symbols

$\|\ i$	General qubit
$\|\ _1 i$	Control qubit
$\|\ _2 i$	Target qubit
$\|\ ^{0} i$	Error corrupted qubit state
$\|\bar{\ } i$	Encoded state
$\|\tilde{\ } i$	Input state to the encoderless scheme
$[n; k; d]$	Quantum Stabilizer code with parameters $n; k$ and d
$\ ;$	General probability amplitudes
C_1	Pauli group
C_2	Clifford group
C_3	Quantum C_3 gate group
D	D-dimensional quantum system
d	Minimum distance
D	Number of components in circuit
$D_{u;c}$	Experimental uncoded and coded error rate
E	Correctable error
$E(:)$	Quantum channel
E	Quantum hardware
$_1$	Single gate error
$_2$	Two-qubit gate error
E_M	Total measurement error
E_P	Total gate error rate
E_E	Encoder error rate
$_i$	i-components FER scalar
e_i	Corrected i-components FER scalar
	Depolarizing channel probability
FER_3	FER, circuit block output
G_N	N-qubit Pauli group
H	Hadamard gate
h_r	Rayleigh fading channel coefficient
I	Classical simulator

J	Individual operators in the channel
k	Number of information qubits
K	Arbitrary stabilizer
L	Gate sequence length
m	Transmitted classical bit
$\tilde{m}$	Received classical bit
M_i	Measurement operator
M	Measurement circuit element
N	Number of qubits
N^c	Classical bits transmitted
N^c	Number of erroneously received classical bits
N^q	Number of teleported qubits
N^q	Number of erroneously teleported qubits
N_0	Variance of the AWGN
n	Number of physical qubits
p(:)	Probability of .
P_j	Pauli group for the jth qubit
p	Probability of a component error
P_g	Gate error probability
P_e	Channel flip probability
P_{th}	Gate error rate threshold
P_t	Transmit power
P_e^q	Quantum secure error probability for teleportation
$p_i^{u;c}$	Ideal probability distribution
$\tilde{p}_i^{u;c}$	Experimental probability distribution
P	Error rate of physical circuit block
$p_{u;c}$	Theoretical error rate of the uncoded and coded circuit block
P_m	Qubit measurement error
q_0	Physical qubit with index 0 in quantum register
Q_0	Logical qubit with index 0 in quantum register
R	Total number of circuit outputs
R	Quantum code rate
R	Error recovery
S	Quantum S gate
S	Stabilizer set
T	Quantum T gate
t	Error correction capability
U	General quantum gate
$\overline{U}_f$	Transversal gate
$\overline{U}$	General encoded gate
V	Encoder

jv i	Eigenvectors
X	Pauli X Gate
Y	Pauli Y Gate
Z	Pauli Z Gate
	Number of accepted results
	Density matrix
	Eigenvalues
	Kronecker tensor product
y	Transpose conjugate of a matrix
;	Bloch sphere parameters

List of Abbreviations

QECC	Quantum Error Correction Code
NISQ	Noisy-Intermediate-Scale-Quantum
GHZ	Greenberger–Horne–Zeilinger
VQE	Variational quantum eigensolver
QAOA	Quantum-Approximate-Optimization-Algorithm
CNOT	Controlled-NOT Gate
SWAP	Quantum Swap Gate
OR	Classical OR Gate
FER	Frame-error-rate
CSS	Calderbank-Shor-Steane Code
TC	Turbo Codes
QTC	Quantum Turbo Codes
QSDC	Quantum-Secure-Direct-Communication
EPR	Einstein-Podolsky-Rosen
BER	Bit-Error-Ratio
QBER	Quantum-Bit-Error-Ratio
SNR	Signal to Noise Ratio
SISO	Soft-input-soft-output
IBMQ	IBM Quantum
SoA	State-of-the-Art

Chapter 1

Introduction

1.1 Motivation

In the last few years, there have been vast leaps in the practical realisation of quantum computers, with both academia and industry demonstrating a variety of advances in the control, quality and number of programmable qubits [4]. The ever-increasing activities of the field have produced devices processing in excess of 50 qubits, by companies such as Google [5], IBM [6], Rigetti [7] and Ionq [8] along with many smaller devices that are publicly available to the general research community. As the field evolves, these devices will have the capability to implement fully-fledged quantum algorithms with longer gate sequences. Within this framework, a fault-tolerant QECC is needed for mitigating the accumulated component errors in a large-scale quantum circuit. Therefore, characterizing QECC's in new hardware can shed light on the device fidelity that will lead to the realisation of large-scale quantum algorithms.

For a QECC to be fault-tolerant the circuits used for encoding, decoding and error correction must not introduce more errors than the code can correct since the gates of these circuits are imperfect, a single qubit error of a gate can proliferate through subsequent two-qubit gates that may overwhelm the codes' error correction capability. Hence, an encoding circuit built from a large number of realistic noisy gates may introduce too many errors at the start of the computation, making it impossible to achieve an overall coded error rate improvement. Fault-tolerant circuit design aims for mitigating the fundamental component errors inherent in QECC's. Therefore, to assess if a QECC is a viable method of improving the fidelity of a quantum algorithm, the additional circuitry used for implementing the QECC must be designed to be fault-tolerant.

In a fault-tolerant circuit, an error arising from a single component will not overload the QECC, hence incurring zero logical errors after an error-correction step [9, 10]. By contrast, a qubit error introduced by an individual gate of a non-fault-tolerant circuit

can be proliferated to a larger number of errors by the application of noiseless successive gates. This is a consequence of the reversibility of quantum gates, where the dimension of the input and output of the gate are the same. For example, the quantum Controlled-NOT (CNOT) gate takes the two-qubit state $|xy\rangle$ as its input and outputs the two-qubit state $|yz\rangle$, where $z = (x \text{ XOR } y)$ [11]. Therefore, if the control qubit contains a bit-flip error, the output state has two bit-flip errors. In other words, this has the effect of introducing an increased number of qubit errors into the circuit. Therefore, in a highly connected circuit a single qubit error may overwhelm a QECC's error correction capability.

1.2 Brief Historical Perspective

1.2.1 Fault-Tolerant QECC

1956	Von Neuman defined fault-tolerant classical computers [12]
1994	Shor's factoring algorithm [13]
1996	Shor's pioneering contribution to realize a fault-tolerant QECC model [10]
1996	Fault-tolerant state preparation, error correction and measurements [14, 15, 16, 17]
1997	Threshold theorem proves an achievable component error rate $p < P_{th}$ [18, 14, 15, 19]
1997	Kitaev's Toric code is a pre-cursor to surface codes [20]
1999	Fault-tolerant non-Clifford gates [10, 21, 22]
2002	Surface codes as quantum memory [23]
2004	Magic state distillation becomes an efficient way of achieving universality [24]
2007	Raussendorf and Harrington conceive universal gate set for surface codes [25, 26]
2008	3D Colour codes with a transversal T gate [27]
2013	Universal gate set using gauge fixing [28]

Table 1.1: History of Theoretically Fault-Tolerant QECC.

There has been substantial progress in QECC since its inception by Shor in 1995, where he conceived the $\frac{1}{9}$-rate code [29]. This was based on the repetition code, and has the ability to correct both bit and phase-errors. Shor's code motivated the design of Calderbank-Shor-Steane (CSS) codes [30, 31], which exploit the properties of classical linear block codes, providing a more general framework to correct both bit and phase-errors than Shor's code. As a further development, using the $[7, 4, 3]$ Hamming code the

$\frac{1}{7}$-rate Steane code was devised, which can correct a single arbitrary qubit error [31]. This code rate was then further improved in [32, 33], showing that a $\frac{1}{5}$-rate code was the shortest possible codeword length capable of correcting a single qubit error. Gottesman then outlined the quantum stabilizer code formalism in his PhD thesis [34] for providing a general framework for capable of further improving the efficiency of QECCs [35]. The benefit of quantum stabilizer codes is that their construction is not restricted to CSS codes, therefore its inception sparked the development of a wide variety of QECC's (see [36]).

A fault-tolerant quantum circuit must be able to cope with both gate errors as well as proliferated errors. Gate error may impose a qubit error on the circuit, while a perfect gate may still propagate a qubit error. Another scenario is that a poorly located *and* inaccurate gate will be subjected to *both* qubit error and error proliferation at the same time. The invention of fault-tolerant QECCs in [14, 15, 16, 17] addressed this issue by re-thinking the construction of the traditional quantum coding circuits so that single gate errors do not overwhelm the QECC. The work of Aharonov and Kitaev prove that a gate error rate threshold can be found [18, 14, 15, 19] below which the QECC provides improvements to the logical accuracy of a quantum computation. Moreover, when the components of a quantum processor operate below the gate error threshold, fault-tolerant quantum computation is indeed achievable.

The seminal conception of fault-tolerant QECC's by Shor [10] combined with the threshold theorem of Aharonov and Ben-Or [18] provided a proof of concept that quantum computers may execute a quantum algorithm to a reasonable accuracy despite imperfect components. However, such schemes were still impractical because the circuit construction relies on the assumption that there is no restrictions on qubit interactions. Unfortunately, this makes such schemes impractical to implement in hardware. This gave rise first to the Toric code of Kitaev [20] and later to Topologcial codes [23]. These schemes assume a lattice configuration of the qubits, which have interactions amongst the nearest neighbour qubits only. This makes the design of the hardware straightforward and therefore topological constructions have become the most popular methods of practical QECC implementations [37, 38]. The Gottesman-Knill theorem [39, 40] shows that the Clifford gates can be simulated classically [40]. Moreover, there is no code relying on a universal transversal gate set [41, 42]. Magic state distillation is an efficient way of implementing gates within a full gate set [24]. Raussendorf and Harrington [25] also proposed a universal gate set for topological codes by using CNOT gates with magic state distillation [26].

1.2.2 Experimental Current-Day QECC

Now that quantum processors are accessible, the development of powerful QECC's can be based upon experimental results and capable of correcting device specific errors.

2012	$\frac{1}{3}$-repetition code in superconducting qubits without stabilizers [43]
2013	Demonstration of a two-qubit gate in superconducting qubits with fidelity measured via randomized benchmarking finding gate error thresholds [44]
2014	GHZ states using a 5-qubit device [45, 46, 47]
2015	Two parity measurements comprising the stabilizers of the $\frac{1}{3}$-repetition code in 5 qubit superconducting qubits [48]
2015	$\frac{1}{5}$ and $\frac{1}{9}$-rate repetition code with error detection and correction in classical post-processing [49]
2015	Error detection in a two-qubit Bell state by measuring the Z_1Z_2 and X_1X_2 parities with one round of error correction [50]
2016	Testing entanglement in IBMQ 5-qubit device [51]
2016	Non-fault-tolerant error-corrected Rabi oscillation across a logically encoded qubit using a distance-two surface code [52]
2016	Error detection relying on weight-four parity measurements [53]
2017	$\frac{1}{3}$ and $\frac{1}{9}$-qubit repetition code in current-day hardware [54]
2017	Repetition code with protection against bit-flip errors on 16 qubits [55]
2017	Manipulations of a logical qubit encoded in cat states using transmon qubits, where the logical operations in encoded qubits are characterised by process tomography [56]
2017	Preparation of logical qubits using the [4,2,2] code [57]
2018	Error reduction techniques compared in IBMQ and Rigetti devices [58]
2018	Gottesman's criteria of [59] using the [4,2,2] code [60, 61, 62, 63]
2019	Measuring Bell state fidelity [64]

Table 1.2: History of Experimental QECCs.

The fast development of prototype quantum devices has opened up a growing field of research on experimental QECC, as seen in Table. 1.2. Early demonstrations of two-qubit gates [44] paved the way for experiments of entangled two-qubit states in 5-qubit devices [45, 46, 47], along with further advances in testing the entanglement fidelity in small devices [51, 64]. There have been numerous examples of successful experiments demonstrating the repetition code. This includes the $\frac{1}{3}$-repetition code with and without stabilizer measurements [43, 48], as well as the $\frac{1}{9}$-repetition code [49, 54] and even $\frac{1}{16}$-repetition code [55]. The $[4; 2; 2]$ code was recommended in [59] as a starting point for a experimental demonstrations of fault-tolerant QECC. Much work has been undertaken in this line of research, showing that small devices satisfy a simple fault tolerance criterion under certain conditions [60, 61, 62, 63].

There are a number of QECCs that may be suitable for fault-tolerant gates sequences at the current State-of-the-Art (SoA) hardware such as the 5-qubit code [33], the 7-qubit

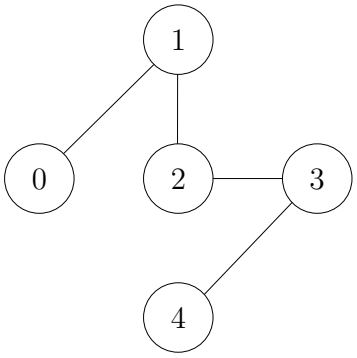

Figure 1.1: 5-qubit *Ibmq Santiago* device layout [6].

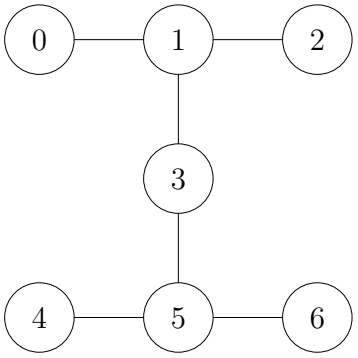

Figure 1.2: 7-qubit *Ibmq Casablanca* device layout [6].

Steane code [31], topological codes [65] or the 9-qubit Shor code [29]. Fault-tolerant versions of these codes are prevalent (see [66, 10]) but since quantum hardware is still in its infancy, the functionality and architecture of the current-day device will determine which of the above schemes can be tested. The requirements of a quantum processor to successfully implement a QECCs experimentally are:

- **Su cient number of available qubits**. Fault-tolerant versions of a QECC often require many more qubits than just those used for encoding the logical qubit [67, 66, 10]. These overheads increase rapidly due to the need for multiple error correction iterations and ancilla check measurements. Therefore, in addition to the redundant qubits required for encoding a logical qubit, the scale of the device must be sufficiently large to provide extra qubits for fault-tolerant error correction and detection operations.

- **Qubit Connectivity**. Figure 1.1 and Figure 1.2 show the device layout for the IBM Quantum (IBMQ) 5-qubit *Ibmq Santiago* the 7-qubit *Ibmq Casablanca* devices [6]. These devices have a general qubit layout with certain two-qubit connections in a two-dimensional architecture. The general architecture of the device determines the possible placement of two-qubit gates in the physical circuit. For example, in Figure 1.1, a CNOT gate is possible between qubits in locations q_0 ! q_1 but it is not possible between q_0 ! q_4. Therefore, in addition to a sufficient number of available qubits, the circuit which applies the QECC in a proposed experiment must also be capable of accommodating the qubit device layout.

- **Quantum measurements mid-computation**. Methods that apply an error correction sub-routine typically require the measurement of a stabilizer or parity check operation to detect the error. Then the outcome of this measurement successively applies the necessary error correction regime. Therefore, to implement a typical measurement-based QECC, the device must have the capability to make a measurement of certain qubits mid-computation. then the outcome of this measurement must become the input of a classically-controlled quantum gate.

- **Highly connected device layout**. Schemes that apply measurement-free error correction require a highly connected device layout with multiple two-qubit gate connections to each qubit. This will enable the code word qubits have nearest-neighbour connections with multiple ancilla qubits. The ancilla qubits (sometimes called auxillary qubits) refer to any additional qubits that are required to carry out a computational task. More formally, the state of an ancilla qubit is not related to that of the information qubits. Most often ancilla qubits are initialized to $|0\rangle$.
- **Multiple ancilla qubits that can be re-initialized**. Error correction routines are supported by many ancilla qubits. So that the device architecture does not demand a disproportionate amount of connections to code word qubits, it may be most efficient if ancilla qubits can be reinitialized multiple times during a circuit execution.

Fortunately, these features are theoretically realisable and there is rapid progress expanding the capabilities of SoA devices. This shows promise that a fully fault-tolerant implementation of a QECC may be possible in the near future[1]. However, in light of these limitations, there is a growing field of research looking to implement optimized quantum algorithms and simulations that achieve a quantum advantage without error correction procedures. This is known as Noisy-Intermediate-Scale-Quantum computing, or the NISQ approach [38]. The aim of this field of research is to perform useful quantum computations directly using uncoded noisy components in order to make the most of the current-day quantum resources that are available. NISQ algorithms rely on quantum simulations, whereby the experimentally controlled quantum hardware is used for simulating a physics problem that is hard to simulate classically [69, 70, 71]. Another example of a NISQ algorithm is constituted by the family of general gate-based algorithms that processes a calculation. This includes rudimentary demonstrations of traditional quantum algorithms, such as the Deutsch–Jozsa, the Grover and the Shor algorithms [72, 73]. Furthermore, hybrid quantum-classical algorithms have been developed, such as the variational quantum eigensolver (VQE), which solves certain classical optimization and quantum chemistry problems [74, 75]. Another example is the Quantum-Approximate-Optimization-Algorithm (QAOA) [76, 77] which applies a quantum machine learning approach to data processing tasks .

Therefore, before the full power of a fault-tolerant error corrected quantum computer is available, NISQ algorithms may provide the proof-of-concept for devices with a 'quantum advantage'. Therefore, the devices in question are capable of outperforming a large classical computer for certain tasks. This has already been shown using less than 100 qubits [78]. Google have recently shown their *Sycamore* device [5] is capable of solving

[1] For example, one of the forthcoming developments in IBMQ devices is the enhanced feature of dynamic quantum circuits, whereby the periodic measurement of a subset of qubits can be carried out repeatedly during the operation of a circuit [68].

a problem faster than their best classical simulation. Explicitly, this experiment demonstrated the sampling of random circuits performed on a 53 qubit processor, showing that within certain hardware constraints quantum advantages can be indeed be measured [79, 80, 81]. With so many fast-moving advances in the field and growing interest from industry, the major technical leaps forward in the development of prototype quantum hardware indicates that error corrected fault-tolerant qubits are just around the corner. The roadmap of experimental QECCs will become clear within the next few years. With these advances, the quest to realize the full promise of quantum computation will be within reach, and the demonstration of an error corrected fault-tolerant circuit are expected to be central to this discovery [82, 83].

1.3 Structure of the Thesis

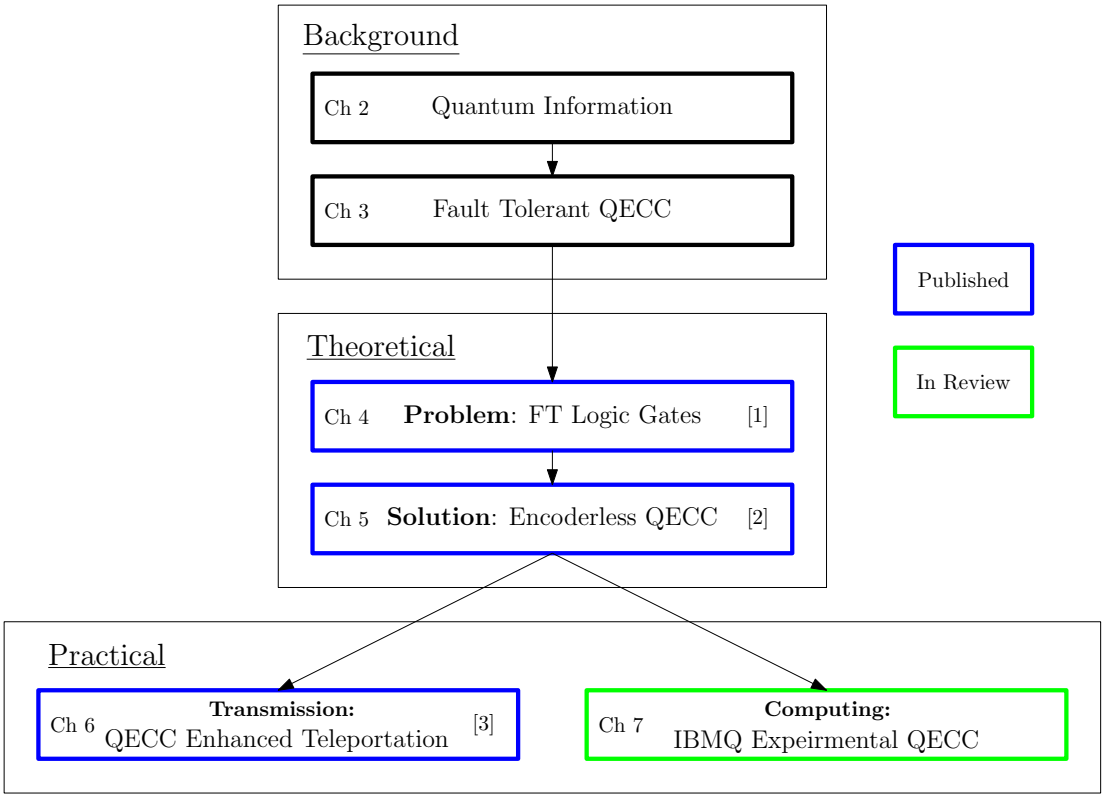

Figure 1.3: Structure of this thesis.

The structure of this thesis is organised as follows, which is also summarized in Figure 1.3.

- **Chapter 2** provides a general introduction to the basic components required for a full quantum circuit. First, the basic unit of quantum computing, the qubit, is introduced in Section 2.2. Then the method to read out the information in a qubit, namely quantum measurement, is detailed in Section 2.2.2. Some popular

quantum gates are presented in Section 2.3, providing a method of processing the information stored in the qubit register. Finally, quantum gate error and quantum Pauli error channels are considered in Section 2.4, completing the necessary foundations before introducing QECCs in the next chapter.

- In Chapter 3, first the basics of QECC and quantum stabilizer codes are explained in Section 3.2. Following from the discussion in Section 1.2.1, general stabilizer codes are introduced in Section 3.2.1. Within this context the $[3; 1; 3]$ repetition code is described in Section 3.2.2, the $[7; 1; 3]$ Steane code in Section 3.2.3. The method of error detection and correction used in QECCs, namely the so-called stabilizer measurements are described in Section 3.2.4, focusing on the circuit implementation. The second half of Chapter 3 defines the method of transforming QECC circuits to fault-tolerant architectures. Fault-tolerant circuit design is defined in Section 3.3. Then the motivation of designing fault-tolerant circuits is described in detail in Section 3.3.1. Then in Section 3.3.2 the phenomenon of error proliferation in circuits is explained. Fault-tolerant circuits are defined in Section 3.3.3, outlining the specifications that QECCs must meet in order to correct all device errors that occurs in a quantum processing task. Finally, in Section 3.3.4 and Section 3.3.5 a detailed example of a fault-tolerant stabilizer measurement is defined, which is a crucial concept for any fault-tolerant QECC. This follows from the work cited in [14, 15, 16, 17] in Table 1.1 (1996).

- In Chapter 4 the simulation results of encoded transversal gates are presented. Transversal gates apply logical operations to encoded states. In Section 4.2 the transversal gate model is defined. Then, the theory of processing information stored in logical qubits is discussed in Section 4.2.2, also found in [14, 15, 16, 17] as seen in Table 1.1 (1996). The system model and simulation parameters are presented in Section 4.3. Then, various FER bounds are derived in Section 4.4 for repetition-encoded transversal CNOT gates and for the Steane code in Section 4.4.3. It is concluded in Section 4.5 that the gate errors inherent in the encoding circuit may become proliferated to an uncorrectable number of qubit errors, which imposes a high error-floor after error correction. These results confirm the theory presented in Chapter 3 and lead to a problem statement to be solved in Chapter 5.

- In Chapter 5 a solution to the impediments of non-fault-tolerant encoding circuits, is presented namely the so-called 'encoderless' codes. First the design of encoderless QECCs is introduced in Section 5.2 for both the repetition code as well as the Steane code. The scheme is described analytically in Section 5.3 and Section 5.4. Then the results of our simulations characterizing imperfect gates are presented in Section 5.4.2. Finally, our encoderless scheme is extended to state preparation protocols in Section 5.5, where the qubit decoherence probability and gate error probability bounds are derived.

- In **Chapter 6** we present the first of two practical applications of fault-tolerant QECCs. This outlines a secure and reliable transmission protocol referred to as quantum teleportation. Quantum teleportation is a communication protocol which exchanges the location of a qubit using quantum entanglement and a classical transmission. First, quantum teleportation over ideal channels is described in Section 6.2, while teleportation over imperfect channels is investigated in Section 6.3 and Section 6.4. A secure teleportation scheme is proposed and investigated in Section 6.5, then our conclusions are offered in Section 6.6.

- In **Chapter 7** we present our experimental results obtained using small-scale devices available from IBMQ. This work follows from that in [60, 61, 62, 63, 57] and Gottesmans criteria [59] as seen in Table 1.2 (2017-18). First, a fault tolerance criterion is defined for our experiments using SoA quantum processors in Section 7.2.1. This is followed by Section 7.2.2, where our IBM-computer experiments are described. Then the $[4, 2, 2]$ code is presented in Section 7.2.4, along with circuit models as well as a method of extracting the relevant error rate metrics. In Section 7.4 we define a simple Pauli-gate error model characterized by its gate and measurement error parameters. Finally, in Section 7.5 this model is compared to the experimental results of the $[4, 2, 2]$-encoded gate sequences, followed by our conclusions.

1.4 Novel Contributions

Against the above background, QECCs must guard against both gate errors and qubit decoherence errors inherent in the encoding, decoding and error correction circuits. It was found that a fault-tolerant circuit design is necessary for reducing the error rate below a certain limit, which is lower-bounded by the gate error rate. Nevertheless, qubit decoherence errors are efficiently mitigated by transversal gate architectures. This work follows from the theory in [66, 84] as well as the simulation results found in [85]. The novel contributions in [1] are presented in Chapter 4 as follows:

1. *The nature of both quantum gate errors and of error proliferation are reviewed and the application of QECCs in these scenarios is explored. We will demonstrate that the transversal gate architecture is capable of reducing the gate error probability.*

2. *We characterize the effects of the propagation of a single gate error in basic QECC encoding circuits and show that a non-fault-tolerant encoding circuit can still provide a Frame-Error-Ratio improvement in conjunction with the fault-tolerant transversal CNOT gate scheme of Figure 4.2*

3. *We present a channel model capable of characterizing both gate errors and individual qubit errors. Finally, the attainable FER improvements are quantified for the transversal CNOT gate using Steane's* $[7; 1; 3]$ *code.*

Based on these conclusions, it was necessary to encode quantum information in a way which circumvents traditional encoding circuits. The 'encoderless' scheme provides a solution to this problem. The concept is comparable to traditional state preparation techniques, which apply a stabilizer measurements in order to prepare a known logical state. Recent work in this area includes [86, 87, 88]. However, our scheme offers the extra benefit that any unknown state can be encoded, akin to the non-fault-tolerant encoding circuit. Additionally, this specification only requires a few extra single qubit gates. Our novel contributions [2] in Chapter 5 are:

1. *We propose a technique of preparing the* n*-qubit encoded version of a* k*-qubit quantum state using imperfect quantum logic gates that are prone to the deleterious effects of decoherence both in repetition codes and in Steanes codes. This scheme has the added benefit that it does not require prior knowledge of the information to be encoded. We demonstrate if provided the gate error probability is below a certain threshold, a reduced gate error probability is attained.*

2. *Our solution is capable of encoding quantum information without the need for encoding circuits, which are inherently error-prone. We achieve this ambitious objective by proposing an additional syndrome decoding step, which prepares a code space containing the same legitimate codewords. This 'encoderless' scheme relies on a fault-tolerant circuit and as a further benefit, it requires fewer gates than the family of common state preparation techniques [66, 9, 88].*

3. *Using the proposed 'encoderless' scheme, upper bounds of the qubit decoherence probability and gate error are derived that define the conditions of constructing an output state having an error rate of* 10^{-5}.

Most simulations of quantum teleportation assume a perfect classical channel. However, to derive the benefit of QECC in a practical transmission scenario it is necessary to simulate the combination of the effects of classical coding alongside the enhanced quantum channel. Additionally, the optimisation of quantum resources is necessary for a secure and reliable application of Quantum Turbo Codes (QTC) [89, 90] in support of teleportation. Teleportation has been widely considered for applications in secure communication and quantum networking, where only the quantum channel is assumed to be imperfect [91, 92, 93, 94, 95]. In this work we consider the effect of an imperfect classical channel on the quantum states transmitted. The novel contributions of [3] are presented in Chapter 6 as follows:

1. *A practical teleportation scheme is investigated, where both the classical and quantum channels exhibit errors. It is shown that classical TCs improve the reliability of teleportation.*

2. *Reliable teleportation with the aid of TC and QTC. QTC improves the security of teleportation by increasing the difference between the QBER in the absence and presence of an eavesdropper. Secure teleportation using QTC is combined with Quantum-Secure-Direct-Communication (QSDC), capable of providing an unconditionally secure quantum channel.*

Finally, we investigate the [4; 2; 2]-encoded gate sequences using the IBM Quantum services. Implementing small-scale QECC experiments in newly available devices provides a straightforward method of verifying that the QECC is constructed of fault-tolerant circuits according to the most realistic noise model in comparison to a result obtained by simulations. Moreover, this might allow us to asses a QECC's potential of enhancing a quantum algorithm without requiring large-scale classical simulations that meet a set of assumptions about the noise model. Previous characterizations of the [4; 2; 2] code have shown error rate improvements for certain gate sequences [96, 57, 63, 97]. Vuillot demonstrated [60] that error-rate improvements can be attained when the highest-quality pair of qubits on the device are targeted. In addition, Wilsch *et. al.* compared various devices in [61] showing that the fault-tolerance criterion was only satisfied when certain types of underlying errors are present in the hardware. Our novel contributions presented in Chapter 7 are:

1. *Using open-access IBMQ experiments, we show that the* [4; 2; 2] *code's state preparation and its encoded logical gates satisfy a fault tolerance criterion for certain logical gate sequences, where the uncoded physical two-qubit gate count is lower than that of its coded counterpart.*

2. *Our experimental results are compared to a simple error model having a small number of parameters for characterizing this QECC, which indicate the pivotal role of fault-tolerant designs in practical circuit construction.*

3. *We observe that the QECC scheme is highly sensitive to errors close to the input of the circuit as well to qubit preparation errors that are proliferated by the encoding circuit. We demonstrate that the fidelity of the Hadamard gate used for initializing the encoded state will lower-bound the error rate performance of the coded scheme, when the CNOT gate error is mitigated by post-selection.*

4. *Our results demonstrate that the trace distance measure only constitutes a reliable metric for certain QECC experiments, where the dimension of the ideal output is the same for all the sampled circuits. Stipulating this idealized experimental condition is necessary in order to maintain a consistent interpretation of the results.*

Chapter 2

Quantum Information Processing and Gate Error

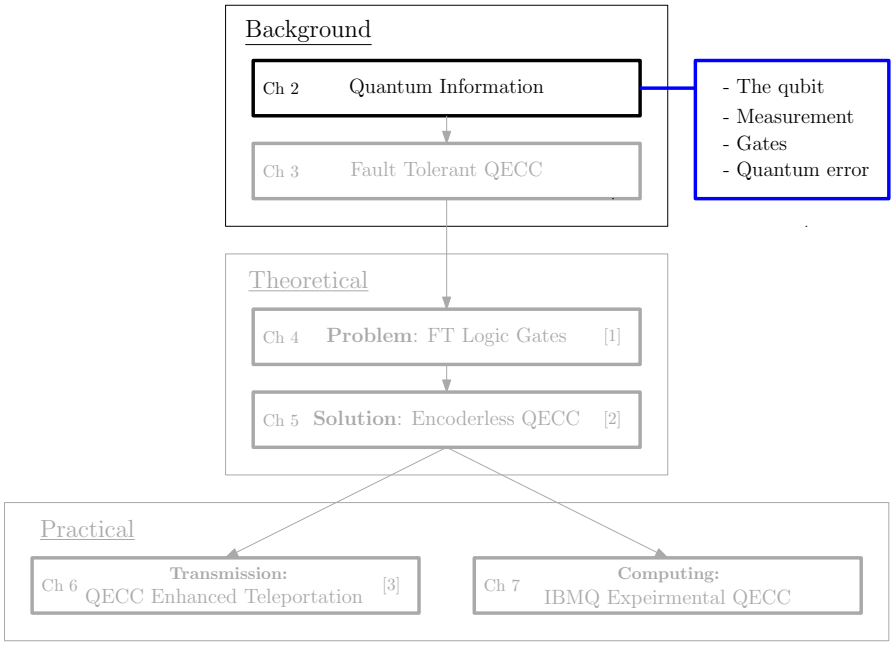

Figure 2.1: The outline of this thesis with the highlight of Chapter 2.

2.1 Introduction

In this chapter we will introduce the basic components of a quantum circuit. To begin, we introduce the qubit in Section 2.2, providing a description of the basic unit of quantum computing. Then quantum measurements are explained in Section 2.2.2, which constitute the method of reading out the information stored in the qubit. Next, we will describe some of the popular quantum gates in Section 2.3, which process the information stored in the qubit register. Using these three fundamental concepts a basic

quantum circuit can be constructed. We round off this chapter in Section 2.4, by the portrayal of quantum gate errors and quantum Pauli error channels, used for modelling the quantum circuit in a realistic noisy scenarios.

2.2 Qubits and Quantum Measurement

2.2.1 The Qubit

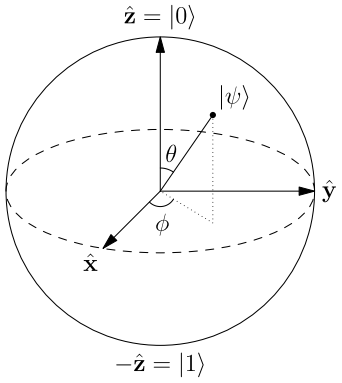

Figure 2.2: The Bloch Sphere representation of a qubit.

The basic unit of quantum computing is the quantum bit (qubit) defined by the vector

$$j \ i = \ j0i + \ j1i = \begin{matrix} ! \\ ; \end{matrix} \tag{2.1}$$

where ; 2 C and

$$j \ j^2 + j \ j^2 = 1; \tag{2.2}$$

where $j \ i$ is described using the so-called *Dirac notation* [9, 98, 99, 36]. The formalism is termed as $j:i$ denotes the *ket* vector and $h:j$ is the corresponding *bra* vector. Therefore, the state in Eq. (2.1) has the row vector $h \ j =$, where indicates the complex conjugation of the coefficients. The qubit in Eq. (2.1) is prepared in the computational basis $fj0i; j1ig$, which is defined by the vectors

$$j0i = \begin{matrix} ! \\ 1 \\ 0 \end{matrix} \qquad j1i = \begin{matrix} ! \\ 0 \\ 1 \end{matrix} : \tag{2.3}$$

The Bloch sphere seen in Figure 2.2 represents a single-qubit system. A specific point on the Bloch sphere defines a qubit in an arbitrary superposition state, described by

$$j \ i = \cos \frac{}{2} j0i + e^{i} \ \sin \frac{}{2} j1i \qquad \begin{matrix} ! \\ \cos \frac{}{2} \\ e^{i} \ \sin \frac{}{2} \end{matrix} ; \tag{2.4}$$

where 0 and 0 2 are real numbers[1]. The definition in Eq. (2.4) is equivalent to Eq. (2.1).

For practical calculations in quantum information processing it is often more convenient to consider the qubit in terms of the density operator notation [9]. This notation is equivalent to the state vector notation in Eq. (2.4) and Eq. (2.1), but represents the qubit using a matrix rather than a vector. The density operator for Eq. (2.4) is defined as

$$= j \; ih \; j = \begin{pmatrix} \cos \frac{}{2} \\ e^{i} \sin \frac{}{2} \end{pmatrix} \begin{pmatrix} \cos \frac{}{2} & e^{\;i} \sin \frac{}{2} \end{pmatrix} = \begin{pmatrix} \cos^2 \frac{}{2} & e^{\;i} \cos \frac{}{2} \sin \frac{}{2} \\ e^{i} \cos \frac{}{2} \sin \frac{}{2} & \sin^2 \frac{}{2} \end{pmatrix} : \tag{2.5}$$

Likewise, the equivalent density matrix of $j \;\; i$ in Eq. (2.1) is given by

$$= j \;\; ih \;\; j = j \;\; i \;\;\; h \;\; j = \begin{pmatrix} j \;\; j^2 & \\ & j \;\; j^2 \end{pmatrix} : \tag{2.6}$$

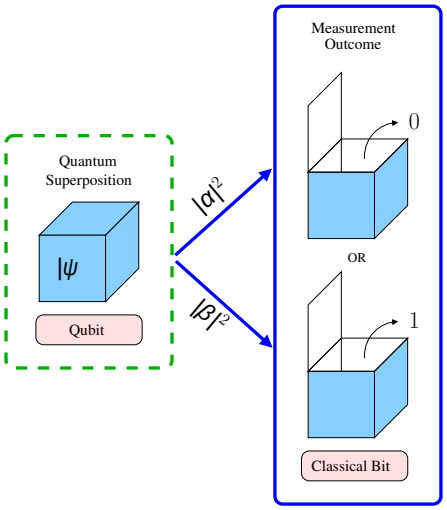

Figure 2.3: Schematic illustration of the quantum measurement of a qubit.

2.2.2 Quantum Measurement

The diagram in Figure 2.3 illustrates the outcome of reading out information or measuring the qubit. Before the quantum measurement the qubit is in a superposition of the quantum states $j0i$ and $j1i$. The probability of measuring the bit value `0` or `1` is given by the modulo squared of the probability amplitudes and in Eq. (2.1). This is illustrated in Figure 2.3. When the qubit is measured there is a probability of $j \;\; j^2$ that a classical bit value of `0` will be recorded. Likewise, there is a probability of $j \;\; j^2$

[1]Note that in Eq (2.4) a phase factor of e^{i} is ignored. We say that $j \;\; i = e^{i} \; j \;\; i$ is equal up to a global phase factor of e^{i}, because the predicted measurement distribution for both states is identical. Therefore, the phase factor e^{i} has no observable e ect.

that a 1 will be measured. Each time the qubit $j\ \ i$ in Eq. (2.1) is prepared and then measured either of the two bit values will be read out. However, for a single instance of the qubit, it cannot be predicted which outcome will be the recorded one.

Let us consider the concept of quantum measurement in more detail [9]. The probability[2] of obtaining the classical bit value 0 can be determined by applying the measurement operator $M_0 = j0ih0j$ to $j\ \ i$ in Eq. (2.1), as follows[3]

$$\mathrm{p}(0) = h\ \ jM_0^y M_0 j\ \ i = j\ \ j^2: \tag{2.7}$$

Likewise, the probability of obtaining 1 is given by applying the measurement operator $M_1 = j1ih1j$. Since and are quantum probability amplitudes, the state must be normalized so that we have $j\ \ j^2 + j\ \ j^2 = 1$. This shows that if the measurement is made in the same basis as the state was prepared in, for example in the computation basis of Eq. (2.3), then orthogonal states can be distinguished. For example, since $h0j1i = 0$ the $j0i$ and $j1i$ states can be distinguished by a measurement along the z-axis in Figure 2.2, according to the computational basis $fj0i; j1ig$ in Eq. (2.3).

The state in Eq. (2.1) is in a *superposition* of the computation basis states. This means that the outcome of the measurement is non-deterministic and therefore the best description of the system is probabilistic. For example, say consider a trivial quantum program that prepares and measures a single qubit in the state $j\ \ i = \frac{1}{\sqrt{2}}(j0i + j1i)$. When the program instructs the quantum computer to measure the qubit, the output of a single run of the program cannot be predicted with certainty. This is because the qubit starts in a superposition. There is a 50 : 50 chance the program will output the bit value 0 or 1. Each time the program is run it will appear to output a 0 or 1 at random. Suppose the program is run at a very large number of times, say 10^6 times. The bits measured will follow the distribution defined by the quantum probability amplitudes defined in the state vector $j\ \ i$, namely $j\ \ j^2 = \frac{1}{2}$ and $j\ \ j^2 = \frac{1}{2}$. Therefore approximately 50% of the runs of the program will output the bit value 1 and 50% will output a 0.

After a quantum measurement the state only gives rise to that which was previously measured. In other words, the measurement operator $M_0 = j0ih0j$ *projects* the qubit into the $j0i$ state. Therefore, after the measurement the qubit is in the state

$$j\ \ _1i = \frac{M_m j\ \ i}{\sqrt{\mathrm{p}(m)}}; \tag{2.8}$$

which can be described as the *collapsed* state vector. For example, if the outcome of measuring the state $j\ \ i = \frac{j0i+j1i}{\sqrt{2}}$ was 0, then after the measurement the qubit is in the state $j\ \ _1i = j0i$. Suppose that $j\ \ _1i$ is then measured again, then the outcome of the

[2] In this section, the probability of obtaining x is denoted by $\mathrm{p}(x)$.

[3] The y symbol represents the transpose of the matrix elements as well as the replacement of each matrix element by its complex conjugate.

second measurement is described by the following probabilities;

$$\mathrm{p}(0) = h\ \ {}_1 j M_0^{y} M_0 j\ \ {}_1 i = 1 \tag{2.9}$$

$$\mathrm{p}(1) = h\ \ {}_1 j M_1^{y} M_1 j\ \ {}_1 i = 0. \tag{2.10}$$

Therefore, the only bit value that is measured is `0` since the probability of obtaining the bit value `1` is now 0. The interaction between the measurement operation and the qubit system corrupted the original state $j\ \ i$, hence the original information it contained is no longer accessible. Alternatively, the original state $j\ \ i$ can be said to have *collapsed* to the $j0i$ state after the first measurement. Therefore, repeated measurements of the same qubit will produce the classical measurement outcome that was obtained from the initial measurement, unless the qubit is re-initialised back to the original state.

2.2.3 Pure and Mixed Quantum States

In the previous section it was noted that if the same state $j\ \ i$ is prepared and measured a large number of times, the probability distribution of the measured bit values follows the values of $j\ \ j^2$ and $j\ \ j^2$ in Eq. (2.1). The example was given for a single qubit quantum program that prepares and measures the state $j\ \ i = \frac{1}{\sqrt{2}}(j0i + j1i)$ and it was stated that the output distribution will be equi-probable between `0` and `1`. For this to be true we must assume that the qubit is in a *pure state*, implying that the system which gives rise to the output distribution is said to be *known*. This is when the experiment prepares exactly the same state $j\ \ i$ each time the program is executed.

However, this appears to be a simplifying assumption, when considering practical quantum systems. It is more realistic to expect that each instance of a similar system varies slightly each time it is prepared. Moreover, the dynamics of a noisy system will give the most accurate description of the experiment. Therefore, most useful calculations in quantum computing will consider composite quantum systems or mixed states [100]. A mixed state is described as an ensemble of quantum states in the set $\{p_i; j\ \ {}_i i\}$ having the density matrix of

$$= \sum_i p_i j\ \ {}_i i h\ \ {}_i j \tag{2.11}$$

where p_i gives the probability that the system is in state $j\ \ {}_i i$. Sometimes p_i is termed as a classical probability (real and positive) for ensuring that it is not confused with a quantum probability amplitude (complex), such as and in Eq. (2.1). Therefore, an important distinction to make is that the mixed state is not a superposition of quantum states, but instead a classical statistical mixture of pure states. Each $j\ \ {}_i i$ in the ensemble may individually be in a superposition defined by its own complex probability amplitudes.

Consider a simple description of a noisy quantum system. Assume that a qubit is in the state $|\ \ i$ with probability $1 \quad p_e$ and in a corrupted state $|\ \ ^0i$ with probability p_e. This system is said to be a *mixed state*, which means that it is a statistical mixture of pure states defined by a real number p_e. Each state $|\ \ i$ and $|\ \ ^0i$ may individually be a superposition characterized by its own complex probability amplitudes, as in Eq. (2.1). Therefore with probability $1 \quad p_e$ the superposition $|\ \ i = \ \ |0i + \ \ |1i$ is measured and with probability p_e a different superposition $|\ \ ^0i = \ \ ^0|0i + \ \ ^0|1i$ is measured. However, both states have the measurement outcome of either `0` or `1`. So the measurement of the qubit will not tell us if the qubit is the perfect $|\ \ i$ or the erroneous $|\ \ ^0i$. This is because there are an infinite number of 'unravellings' of a mixed state. This means that that if we are given a set of measurement results, we cannot work backwards and recover a unique description of the system that gave rise to them [101].

2.2.4 Multi-Qubit Systems

A series of qubits that are not entangled are defined by the tensor product of the individual qubits [9]. The tensor product of $N = 2$ single qubit states gives a 2^N-dimensional two qubit state

$$|\ _1i \quad |\ _2i = |\ \ _1\ \ _2i = a|00i + b|01i + c|10i + d|11i; \tag{2.12}$$

where $a; b; c; d \ 2\ \mathbb{C}$ and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. The notation $|00i$ is equivalent to $|0i \quad |0i$. Alternatively, a system of qubits that *is* entangled cannot be written as a product of qubit states. For example, the state

$$\frac{|00i + |11i}{\sqrt{2}} \tag{2.13}$$

cannot be written as any product such as $|\ _1i|\ _2i$, therefore it is said to be entangled.

2.3 Quantum Gates

So far we have described the qubit, which is the unit of quantum computing as well as quantum measurement, which give us a method to read out the information it contains. In this section we will describe quantum gates, which process the information stored in the qubit register[4]. First, we will describe both single and two-qubit gates and the methods of categorising them. First, in Section 2.3.1 we will describe the Pauli group. This is an important set of single-qubit quantum gates, that also underpins the

[4] A qubit register is the system of qubits in the quantum computer. For example, a 5-qubit quantum computer may have a system of 5 qubits denoted by $q_0q_1q_2q_3q_4$, which can be referred to as the qubit register. Each qubit can be processed individually by single qubit gates, while a two-qubit gate processes a pair of qubits.

description of quantum channels and stabilizer codes. The most common two-qubit gate, the CNOT gate, is presented in Section 2.3.2. Followed by the other common quantum gates in Section 2.3.3.

2.3.1 The Pauli Group

Quantum gates can be classified into three groups, namely the Pauli (C_1), Clifford (C_2) and the C_3 group, together known as the Gottesman-Chuang hierarchy [21]. The Pauli group is the most common one, which consists of the following single-qubit gates [102, 103]

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}: \tag{2.14}$$

The X gate has the effect of a bit-flip or a NOT gate on the qubit. For example,

$$X|i\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix} = \begin{pmatrix} \\ \end{pmatrix} = |1\rangle + |0\rangle: \tag{2.15}$$

Notice that the bit-flip swaps the coefficients and . Similarly, the Z gate has the effect of a phase-flip on the state $Z|i\rangle = |0\rangle - |1\rangle$, which introduces a negative relative phase difference between the basis states. The Y gate acts like both a bit and a phase-flip, since we have $Y = -XZ$. Therefore $Y|i\rangle = i(|0\rangle - |1\rangle)$. Finally, the identity operator leaves the qubit unchanged $I|i\rangle = |i\rangle$.

Then let us define the Pauli group as [9]

$$C_1 = \{e^{P} : P \in \{I, X, Y, Z\}, e \in \{1, i, -1, -i\}\}. \tag{2.16}$$

Let us also define the group G_N as all N-qubit tensor products[5] of the Pauli operators X, Y, Z, I.

$$G_N = \{P_1 \otimes P_2 \otimes \cdots \otimes P_N | P_j \in C_1\}. \tag{2.17}$$

For example, the set G_5 permutes a five-qubit register with 4^5 possible combinations. This contains the operator $XZZXI$, which has the effect of applying a bit-flip to the first and fourth qubit as well as a phase-flip to the second and third qubit.

2.3.2 The CNOT gate

The controlled-NOT gate (CNOT gate) is a two-qubit gate that prepares entanglement between two quantum states [104, 105, 106]. If the control qubit is in state $|1\rangle$, the

[5] Where P_j corresponds to the Pauli group for the jth qubit.

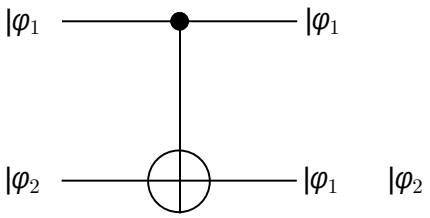

Figure 2.4: CNOT Gate with control qubit $j\ _1i$ and target qubit $j\ _2i$.

CNOT gate applies an X gate (denoted) to the target qubit. The transformation carried out by the CNOT gate is given by the following equations $jABi\ !\ jCDi$

$$j10i\ !\ j11i;\quad j11i\ !\ j10i;\quad j00i\ !\ j00i;\quad j01i\ !\ j01i \tag{2.18}$$

where A and B represent the control and target qubit before the CNOT gate, while C and D represent those after the CNOT gate. Figure 2.4 shows the CNOT gate associated with the control qubit $j\ _1i$ and target qubit $j\ _2i$. The equivalent of an XOR gate is applied to the target qubit. The arbitrary two-qubit state $j\ _1ij\ _2i$, shown in Figure 2.4, can be described by

$$j\ _1ij\ _2i = aj00i + bj01i + cj10i + dj11i = \begin{matrix} 0 & 1 \\ a & \\ b & \\ c & \\ d & \end{matrix} \tag{2.19}$$

where the complex coefficients have the property that $jaj^2 + jbj^2 + jcj^2 + jdj^2 = 1$. The action of the CNOT gate in Figure 2.4 has the following matrix representation

$$CNOT = \begin{matrix} 0 & & & & 1 \\ 1 & 0 & 0 & 0 & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & \\ 0 & 0 & 1 & 0 & \end{matrix}: \tag{2.20}$$

Then the action of the CNOT gate is shown to swap the coefficients in the superposition state in Eq. (2.19) such that $j10i\ \$\ j11i$. This is shown by

$$CNOTj\ _1ij\ _2i = \begin{matrix} 0 & & & & 1\ 0 & 1 \\ 1 & 0 & 0 & 0 & a & \\ 0 & 1 & 0 & 0 & b & \\ 0 & 0 & 0 & 1 & \underline{c} & \\ 0 & 0 & 1 & 0 & \underline{d} & \end{matrix} = \begin{matrix} 0 & 1 \\ a & \\ b & \\ \underline{d} & \\ \underline{c} & \end{matrix} = aj00i + bj01i + \underline{d}j10i + \underline{c}j11i$$

which is in accordance with the transformations listed in Eq. (2.18). The underlined elements highlight where the amplitudes have changed position by the action of the CNOT gate.

2.3.3 Other Gate Sets

When an element of the Pauli group is conjugated by a Clifford gate, it is mapped back to a Pauli gate. This defines the Clifford Group as follows [107]

$$C_2 = \{U : UC_1U^\dagger \in C_1\} \tag{2.21}$$

where U is a general quantum gate. For example, the Clifford group includes the Hadamard, S and CNOT gates

$$HXH^\dagger = Z \quad HZH^\dagger = X \quad HYH^\dagger = -Y \tag{2.22}$$

$$SXS^\dagger = -Y \quad SZS^\dagger = Z \quad SYS^\dagger = -X. \tag{2.23}$$

These gates are defined by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

The Hadamard gate (denoted H) is a common quantum gate that has the following transformation on the computational basis states $(|0\rangle, |1\rangle)$ [9]:

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.24}$$

As we can see, by applying the Hadamard gate the qubit is then in a superposition of the basis states $(|0\rangle, |1\rangle)$.

There is another set of quantum gates exhibiting the property that when a Pauli operator is conjugated by a C_2 Clifford gate, it is mapped back to the Clifford group. The set of gates that have this property belong to what is called the C_3 group [108] defined as:

$$C_3 = \{U : UC_1U^\dagger \in C_2\}. \tag{2.25}$$

The T gate, the Toffoli gate and the controlled-Z gate belong to the C_3 group [9]. For example,

$$TXT^\dagger = SX \quad TZT^\dagger = Z \quad TYT^\dagger = -iSY, \tag{2.26}$$

where the T gate is defined by

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}.$$

2.4 Quantum Gate Error in a Pauli Channel

So far, we have discussed the basic components of a quantum circuit, namely the qubit, quantum gates and quantum measurement. Let us now consider the above elements in a realistic noisy scenario. First, the depolarizing channel is introduced in Section 2.4.1, which is a common worst-case channel model. We then apply this to both single and two-qubit gate errors in Section 2.4.2 and Section 2.4.3.

2.4.1 The Depolarizing Channel

The depolarizing quantum channel may be viewed as a quantum-domain relative of a classical binary symmetric channel [9], where the qubit error[6] can be either a bit-flip (X), a phase-flip (Z) or a combination of both (Y). Each error-events are equally likely, when it is assumed that the channel is symmetric (or unbiased). These errors can be thought of as the application of a Pauli operator (see Section. 2.3.1) to the qubit state. A single-qubit depolarizing channel is characterized by

$$E(\ ; p_e) = (1 \quad p_e) \ + \frac{p_e}{3}(X \ X + Y \ Y + Z \ Z): \tag{2.27}$$

where is the initial quantum state. The qubit remains intact with probability $(1 \quad p_e)$ and it is depolarized with probability p_e, where each type of Pauli error occurs with probability p_e=3. If we substitute $p_e = \frac{3}{4}$ into Eq. (2.27), then we have:

$$E(\ ; \ ) = (1 \quad \frac{3}{4} \ ) \ + \frac{}{4}(X \ X + Y \ Y + Z \ Z); \tag{2.28}$$

which is equivalent to

$$E(\ ; \ ) = \frac{I}{D} \ + (1 \quad) \ ; \tag{2.29}$$

for a D-dimensional quantum system, where $D = 2$ for a single qubit state and $D = 2^N$ for an N-qubit state. This has a slightly different interpretation from Eq. (2.27). It can be interpreted by assuming that the initial state is replaced with the maximally mixed state I=2 with probability and left untouched with a probability $(1 \quad)$, for $p_e \quad \frac{3}{4}$. The totally mixed state describes the state of a system, which is completely corrupted by noise or 'totally randomized'.

A D-dimensional quantum system that is completely mixed is described by

$$\frac{I}{D} = \frac{1}{D} \sum_{i=1}^{D} jiihij; \tag{2.30}$$

[6] See Appendix 9.2, which shows how any arbitrary point on the Bloch sphere can be described in terms of the Pauli matrices.

regardless of its initial state . This has a geometrical interpretation representing the centre of the Bloch sphere, which gives rise to a measurement outcome distribution, where all possible measurement outcomes are equi-probable and the state of the qubit is not known.

2.4.2 Single Qubit Gate Error

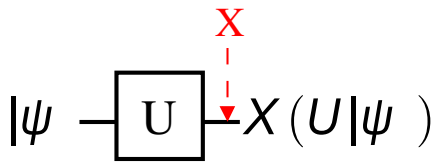

Figure 2.5: Single qubit gate error in the bit-flip channel.

The bit-flip channel affecting a single qubit state applies the X gate from Eq. (2.14) with probability p_e as follows

$$E( ) \; ! \; (1 \quad p_e) \; + p_e X \; X; \tag{2.31}$$

which is analogous to a classical binary symmetric channel. The event of a gate error can be modelled by first applying perfect transformation of the gate U followed by the application of the bit-flip X [109]. This is shown in Figure 2.5 and described by

$$E(U \; U^y) = (1 \quad P_g)U \; U^y + P_g X U \; U^y X: \tag{2.32}$$

In general, where any arbitrary single-qubit gate has a gate error probability of P_g, any arbitrary single-qubit error can be encapsulated by the depolarizing channel in Eq. 2.27. The single-qubit gate error in the depolarizing channel is modelled with the aid of the same methodology as that of a gate error in the bit-flip channel characterized by Eq. (2.32).

2.4.3 CNOT Gate Error

A CNOT gate subjected to the bit-flip channel having a gate error probability P_g may suffer from the error effects of $IX; XI$ and XX with equal probability of $\frac{P_g}{3}$, as seen in Figure 2.6. Let us now assume that $^0 = CNOTj \; ih \; jCNOT^y$ is a two-qubit state evolved by the CNOT gate described by Eq. (2.20). Then a CNOT gate having a gate error probability of P_g in the bit-flip channel is given by

$$E(\; ^0) \; ! \; (1 \quad P_g) \; ^0 + \frac{P_g}{3}(IX \; ^0 IX + XI \; ^0 XI + XX \; ^0 XX): \tag{2.33}$$

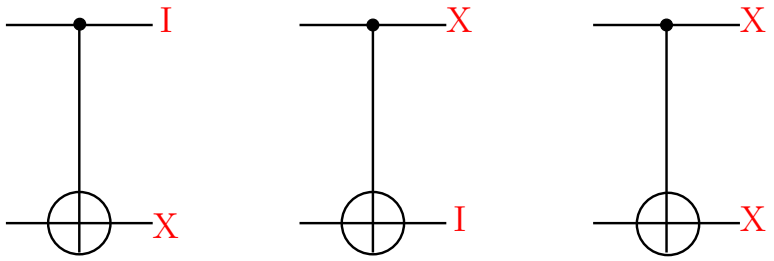

Figure 2.6: A CNOT gate in the bit-flip channel having a gate error probability of P_g suffering from the error effects of $IX; XI; XX$ with equal probability $\frac{P_g}{3}$.

Given an $N = 2$-qubit gate, there are 2^N 1 tensor products of the operators I and X. In general, with J individual operators in the channel and N qubits sent over the channel, there are J^N 1 channel operators excluding the operator associated with N identities[7]. In the case considered here, we have $N = 2$ and $J = 2$, hence there are 3 combinations of I and X in the bit-flip channel, excluding the operator II. These are applied with a probability of P_g=(J^N 1), except in the case of no errors (i.e II), which occurs with a probability of 1 P_g. Therefore the probability of a single error on the control or target qubit is identical to that of a simultaneous error on both the control and target qubit. A CNOT gate error in the two qubit depolarizing channel is the same as that in Eq. (2.33) except that 4^2 1 combinations of the $J = 4$ operators $fI; X; Y; Zg$ are applied, each with probability $\frac{P_g}{15}$. A two-qubit gate with error rate P_g in the depolarizing channel is described by;

$$E(\ ^0) \ ! \ (1 \quad P_g)\ ^0 + \frac{P_g}{15}(IX\ ^0IX + XI\ ^0XI + XX\ ^0XX + IZ\ ^0IZ$$
$$+ZI\ ^0ZI + ZZ\ ^0ZZ + IY\ ^0IY + YI\ ^0YI + YY\ ^0YY + XY\ ^0YX$$
$$+YX\ ^0XY + XZ\ ^0ZX + ZX\ ^0XZ + YZ\ ^0ZY + ZY\ ^0YZ): \qquad (2.34)$$

2.5 Conclusion

This chapter has summarized the three basic operations in a quantum circuit; the qubit, quantum gates and quantum measurements. Next, we describe the noisy version of a general single-qubit gate both in the depolarizing and in the bit-flip channel. We also considered the two-qubit gate error model in terms of the CNOT gate. The discussion of quantum gate errors is a precursor to the next chapter, where we describe the mechanisms behind a gate-error-resilient QECC and how a circuit may satisfy the fault-tolerance criterion.

[7] For example, for $N = 3$ qubits in the bit- ip channel with combinations of $J = 2$ operators $fX; Ig$, there are 2^3 1 = 7 operators excluding III, which are as follows $IIX; IXI; XII; XIX; XXI; IXX; XXX$.

Chapter 3

Fault-Tolerant Quantum Error Correction

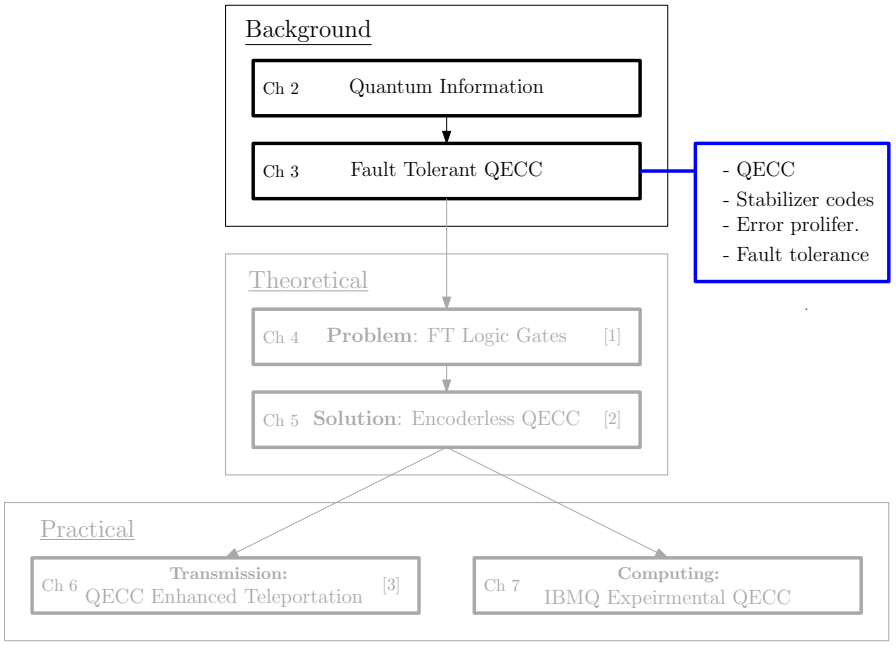

Figure 3.1: The outline of the thesis with the highlight of Chapter 3.

3.1 Introduction

In this chapter we will introduce the fundamental elements of a fault-tolerant QECC, as well as the key definitions required for fault-tolerant circuit design. To begin, the basics of quantum stabilizer codes are introduced in Section 3.2. In this section, general stabilizer codes are introduced giving the background required to introduce QECCs. The $[3; 1; 3]$-repetition code and the $[7; 1; 3]$ Steane code are described in Section 3.2.2 and Section 3.2.3 respectively. The circuits which implement stabilizer measurements

are detailed in Section 3.2.4, highlighting how quantum information can be corrected without direct measurement of the code word qubits.

Then we move on to define fault-tolerance in Section 3.3. We commence with the motivation for fault-tolerant circuit design. This is the phenomenon of qubit *error proliferation*, which is first described in Section 3.3.1 and then further detailed in terms of the CNOT gate in Section 3.3.2. Then a criterion to be satisfied by fault-tolerant circuits is defined in Section 3.3.3 in light of the error proliferation effects. An example of a fault-tolerant circuit design is then provided. This is the fault-tolerant version of the stabilizer circuits of Section 3.2.4, Section 3.3.4 and Section 3.3.5.

3.2 Quantum Error Correction Codes

3.2.1 Stabilizer Codes

A $[n; k; d]$ stabilizer code maps k logical qubits to n physical qubits. Then the code space is a 2^k-dimensional sub-space of a 2^n-dimensional Hilbert space. The stabilizer set $\mathcal{S} = \{K_i\}$ is the n-qubit sub-group of G_n that fixes the code space, when the stabilizers are measured. In this section we use the subscript i of K_i to refer to a specific stabilizer operator in $\mathcal{S}$, while K is used without a subscript, when the stabilizer operator is arbitrary. The legitimate code space is the simultaneous $+1$ eigenspace of $\mathcal{S}$ defined as

$$\{|\bar{j}\rangle \quad \text{s.t.} \quad K|\bar{j}\rangle = |\bar{j}\rangle \quad \forall K \in \mathcal{S}\}. \tag{3.1}$$

A stabilizer group $\mathcal{S}$ is a subgroup of G_N in Eq. (2.17) that is closed under multiplication. The set also has the property that $-I \notin \mathcal{S}$, since we have $(-I)|\bar{j}\rangle = |\bar{j}\rangle$ only when $|\bar{j}\rangle = 0$. All elements of $\mathcal{S}$ commute[1], so there is a simultaneous eigenstate that can be measured for multiple operators. This can then be chosen as the code space and is defined by the set of $n-k$ independent generators of $\mathcal{S}$.

Since the stabilizers are tensor products of Pauli operators, they inherit the properties of the Pauli group, namely that they are unitary ($K^\dagger K = I$) and hermitian ($K = K^\dagger$). This means that the stabilizers will have only ± 1 eigenvalues. Therefore $K|\ \rangle = |\ \rangle$ if $|\ \rangle$ is in the $+1$ eigenspace of K, which means that $|\ \rangle$ is stabilized by K. For example, the $[3; 1; 3]$ repetition code has the encoded states $|\bar{0}\rangle \quad |000\rangle$ and $|\bar{1}\rangle \quad |111\rangle$. This code is stabilized by the operators ZIZ and IZZ. Since $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$, then $ZIZ|000\rangle = |000\rangle$ and $IZZ|111\rangle = |111\rangle$.

[1] Commuting operators satisfy $K_1K_2 = K_2K_1$. Anti-commuting operators satisfy $K_1K_2 = -K_2K_1$.

A correctable error E anti-commutes with the stabilizer, which means that $KE = -EK$ [34]. For example, if $|i\rangle$ is a legitimate code-word, then the stabilizer has the effect [34]:

$$K(E|i\rangle) = -EK|i\rangle = -E|i\rangle: \tag{3.2}$$

Applying the stabilizer operator incurs a -1 phase difference in the data[2]. This is then passed onto the ancilla qubit by a series of CNOT gates, described in Section 3.2.4. A Hadamard gate is then applied to the ancilla qubit so that when it is measured, this returns the bit value of 1. The measurement outcome 1 triggers an error recovery operation, which corrects the error E in the data returning it to the valid codeword state $|i\rangle$, i.e back to a $+1$ eigenstate of K. This allows the stabilizer to detect an error without the need for the data qubits $|i\rangle$ to be measured directly [84].

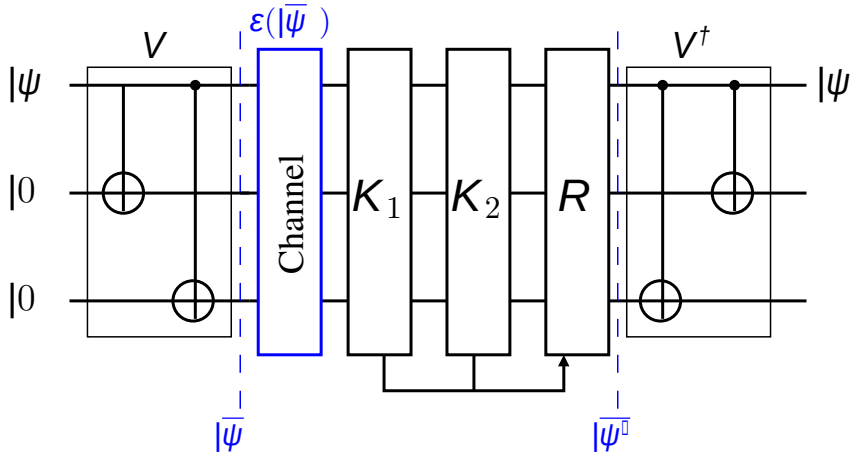

Figure 3.2: $[3; 1; 3]$ Repetition Code with encoding circuit V.

3.2.2 Repetition Code

An example of a stabilizer code is the $[3; 1; 3]$ repetition code [9, 110, 99]. This is a $d = 3$ code and can correct only a single bit or phase-flip error on a single qubit, depending on the design. In this section the specific version that corrects a single qubit bit-flip error is described. However, the results for the phase-flip error are equivalent. The full circuit of implementing the repetition code is shown in Figure 3.2. The traditional $n = 3$ qubit unitary encoding circuit V is applied to the unknown state $|\ i\rangle = \alpha|0\rangle + \beta|1\rangle$ and $(n - k)$ auxiliary qubits in the $|0\rangle$ state as follows [99]

$$|\bar{\ }i\rangle = V(|\ i\rangle \otimes |0\rangle^{\otimes(n-k)}): \tag{3.3}$$

[2] The use of the term `phase difference' refers to a relative phase difference between basis states. For example, the state $|1\rangle$ and $-|1\rangle$ have a relative phase factor of -1, which is physically observable (unlike a global phase factor) [9].

R	$\|\text{data}\rangle\|\text{ancilla}\rangle$
III	$(\|000\rangle + \|111\rangle)\|00\rangle$
IIX	$(\|001\rangle + \|110\rangle)\|01\rangle$
IXI	$(\|010\rangle + \|101\rangle)\|10\rangle$
XII	$(\|100\rangle + \|011\rangle)\|11\rangle$

Table 3.1: Error recovery operators R for the $[3,1,3]$ Repetition code.

This results in the encoded state

$$|\bar{i}\rangle = |\bar{0}\rangle + |\bar{1}\rangle = |000\rangle + |111\rangle. \tag{3.4}$$

The encoded data is corrupted by the bit-flip channel $\mathcal{E}(\ )$ in Eq. (2.31). If $|\bar{i}\rangle$ is corrupted by a single bit-flip error with probability p_e then we have:

$$\mathcal{E}(\ ) = (1 - p_e)\ + \frac{p_e}{3}\ (XII)\ (XII)^\dagger + (IXI)\ (IXI)^\dagger + (IIX)\ (IIX)^\dagger\ ; \tag{3.5}$$

where each error position is equiprobable. This is input to the stabilizers $K_1 = ZZI$ and $K_2 = ZIZ$.

The outcome of the stabilizer measurements is shown in Table 3.1 alongside the required recovery operation R. Since this is a $d = 3$ code, if there are more than a single qubit error then the error recovery may in fact carry out a flawed recovery, hence introduce additional error. Nevertheless, each error recovery operator R in Table 3.1 corrects a single bit flip error inflicted upon the state $|\ i\rangle$ in Eq. (3.4). Finally, the inverse encoder $V^\dagger$ in Figure 3.2 maps the recovered encoded state to an estimate of the initial code word $|\ ^0 i\rangle$. This is the reverse operation of the encoder V, hence n encoded qubits are mapped back to k information qubits.

3.2.3 Steane Code

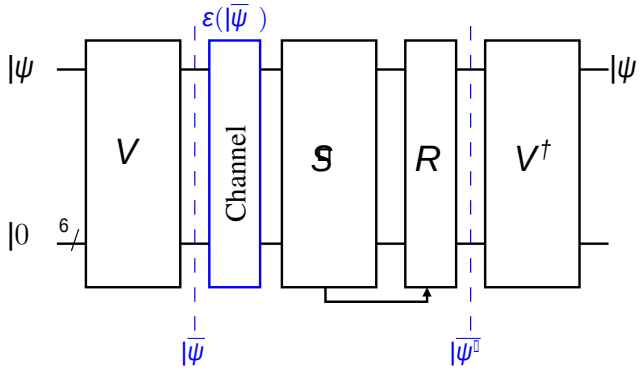

Figure 3.3: Full implementation of Steane's code relying on the encoding circuit V.

Another example of a stabilizer code is the $[7; 1; 3]$ Steane code [31, 111]. The Steane code belongs to the family of CSS code, which is a general construction using a pair of classical linear block codes C_1 and C_2 where $C_2 \quad C_1$. The Steane code is a dual-containing[3] CSS code obeying the property of $C_2 = C_1^{?}$. This is constructed using the $[7; 4; 3]$ classical Hamming code. Since this is a single bit-error correcting code, it leads to a single-qubit error correcting quantum code having the parameters of $[7; 1; 3]$. Therefore a single data qubit is encoded into 7 physical qubits.

The encoded states can be prepared by the traditional Steane encoding circuit[4] V shown in Figure 3.4.

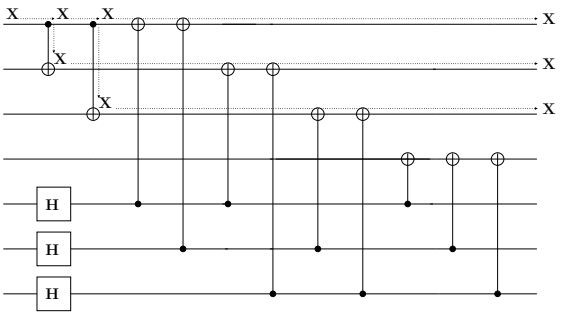

Figure 3.4: Traditional Steane encoding circuit suffering from X error proliferation [85].

The encoded states can be prepared by the traditional Steane encoding circuit V shown in Figure 3.4. As seen in Eq. (3.3), this is applied to the unknown state $j \quad i = \quad j0i + \quad j1i$ and $(n \quad k)$ auxiliary qubits as follows

$$j \bar{} i = V(j \quad i \quad j0i \quad {}^{(n \quad k)}) = \quad j\bar{0}i + \quad j\bar{1}i: \tag{3.6}$$

The full $(n \quad k)$-bit Steane code stabilizer set $\mathcal{S} = fK_i g$ is defined as follows

$$\begin{aligned} K_1 = IIIXXXX; \quad K_2 = XIXIXIX; \\ K_3 = IXXIIXX; \quad K_4 = IIIZZZZ; \\ K_5 = ZIZIZIZ; \quad K_6 = IZZIIZZ: \end{aligned} \tag{3.7}$$

The operation of each stabilizer effectively reduces the 2^7-dimensional space to the 2-dimensional valid code space spanned by the $fj\bar{0}i; j\bar{1}ig$ states. The stabilizer set $K_i \; 2 \; \mathcal{S}$ defines $k = 1$ logical qubit encoded into $n = 7$ physical qubits, and it is applied to the qubit register after the channel, as shown in Figure 3.4. The inverse encoder V^y returns

[3] The notation $C^{?}$ represents the dual pair of C. $C^{?}$ is de ned as a code with a generator and parity check matrix, which is the transpose of that of C.

[4] The ow of time in a quantum circuit diagram is from left to right. The qubit register is represented from top to bottom, where the spatial connectivity required is indicated by the qubits coupled by two-qubit gates. Where the outcome of a circuit block is input to another it is indicated by solid a line and arrows.

the n-qubit code word state based on the recovered k-qubit information state, denoted as $|\tilde{\psi}\rangle$.

The stabilizers are applied via a syndrome extraction circuit, whereby additional ancilla qubits are coupled to the codeword state. This is done by applying a series of two-qubit gates with a pre-determined location according to the operators in Eq. (3.7). The measurement of the ancilla qubit extracts the syndrome outcome, which illustrates the outcome of the relevant parity checks of the physical codeword qubits. Therefore if the data qubits contain a single qubit error, the location of this error will be indicated by the combination of classical bit measurement outcomes. A correction can then be applied in order to return the corrupted word to a legitimate codeword state. Likewise, if the data is error-free, the all zero syndrome will be extracted, indicating that no error correction operation is necessary.

It can be shown that the logical encoded states are

$$|\bar{0}\rangle = \frac{1}{\sqrt{8}} |0000000\rangle + |1010101\rangle + |0110110\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \tag{3.8}$$

and

$$|\bar{1}\rangle = \frac{1}{\sqrt{8}} |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \ ; \tag{3.9}$$

see [112, 9] for the full derivation, as well as Appendix. 9.1.

3.2.4 Non-Destructive Operator Measurement

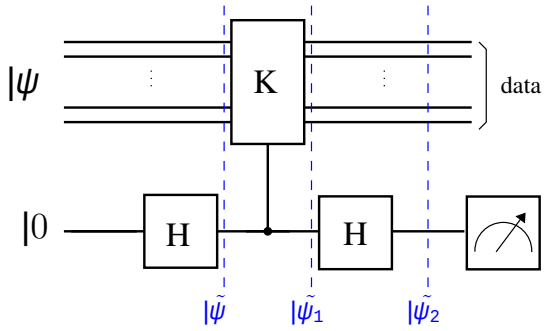

Figure 3.5: Measurement of single stabilizer operator K.

The fundamental task of QECCs is to detect and correct quantum errors. It has been mentioned in Section 3.2.1 that this is done via a quantum stabilizer measurement. Let us explore the circuit construction in a little more detail. This section describes how any error-related information hidden in the data can be extracted with the aid of stabilizer

measurements [34]. Let us discuss how this is possible without directly measuring the data qubits[5] [9]. Figure 3.5 shows the general circuit construction of the measurement of a general single-qubit operator K. Explicitly, a single-qubit operator is considered for the ease of discussion, but in the context of a realistic syndrome decoder this has to be extended to a many-qubit operators, such as the $K_1 = ZZI$ stabilizer of the 3-bit repetition code [9].

The stabilizer is implemented by two Hadamard gates on either side of the control qubit of a controlled-K gate. If the control qubit is in the $|1\rangle$ state, then the gates corresponding to K are applied to the target qubits. This circuit entangles the ancilla and data qubits in such a way that the measurement of the ancilla qubit projects the data into the ± 1 eigenstates of K.

Let us now consider this concept in more detail. Explicitly, consider that the K gate has eigenvectors of $|v\rangle$ with corresponding eigenvalues of $\pm = \pm 1$. Assuming that the input data qubits $|\ \rangle$ are in superposition of the ± 1 eigenstates, we arrive at:

$$|\ \rangle = |v^+\rangle + |v^-\rangle; \tag{3.10}$$

where $$ and $$ are arbitrary probability amplitudes[6] satisfying $|\ |^2 + |\ |^2 = 1$.

Let us describe the evolution of the system at each time-step of the circuit. First, the first Hadamard gate on the ancilla qubit will have the effect of

$$|\ \rangle|0\rangle \xrightarrow{H} |\ \rangle|+\rangle = \frac{1}{\sqrt{2}}\left[|\ \rangle|0\rangle + |\ \rangle|1\rangle\right] = |\tilde{}\rangle. \tag{3.11}$$

Remembering that $H|0\rangle = |+\rangle$ and $|\ \rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$, Eq. (3.11) is the state of the system before the controlled-K gate.

Next, the K gate is only applied to the data when the ancilla is in the $|1\rangle$ state, since this is the control qubit for the controlled-K gate. This has the following effect on Eq. (3.11):

$$\frac{1}{\sqrt{2}}\left[|\ \rangle|0\rangle + |\ \rangle|1\rangle\right] \rightarrow \frac{1}{\sqrt{2}}\left[|\ \rangle|0\rangle + K|\ \rangle|1\rangle\right] = |\tilde{}_1\rangle. \tag{3.12}$$

Substituting Eq. (3.10) into the right hand side of Eq. (3.12) and bearing in mind that $K|v^\pm\rangle = \pm|v^\pm\rangle$, then

$$|\tilde{}_1\rangle = \frac{1}{\sqrt{2}}\left[(|v^+\rangle + |v^-\rangle)|0\rangle + (|v^+\rangle - |v^-\rangle)|1\rangle\right]; \tag{3.13}$$

[5] This example is based on question 4.34 in [9, p. 188] and its extension to stabilizer operators in [9, p. 473]

[6] Note that $|\ \rangle$ is the general case of a superposition of both legitimate and illegitimate code word states, i.e a superposition of ± 1 eigenstates of K. The speci c case where the state is error free is given by $= 0$ where $|\ \rangle = |v^+\rangle$. In this case the outcome of the ancilla is always 0.

which describes the system after the controlled-K gate and before the final Hadamard gate.

The final Hadamard gate again takes the ancilla qubit $|0\rangle \rightarrow |+\rangle$ and $|1\rangle \rightarrow |-\rangle$, therefore we have:

$$|\tilde{\psi}_2\rangle = \frac{1}{2}\Big[(|v^+\rangle + |v^-\rangle)|+\rangle + (|v^+\rangle - |v^-\rangle)|-\rangle\Big]. \tag{3.14}$$

Multiplying this out and simplifying it gives the system before the ancilla measurement formulated as

$$|\tilde{\psi}_2\rangle = |v^+\rangle|0\rangle + |v^-\rangle|1\rangle. \tag{3.15}$$

Eq. (3.15) shows that a $|0\rangle$ is measured in the ancilla qubit with probability[7] $|\alpha|^2$. In this case the data qubits are in the $|v^+\rangle$ eigenvector. Relating this to a stabilizer code, this would indicate that the data resides in a valid code word state [84]. The $|1\rangle$ state is measured in the ancilla qubit with probability $|\beta|^2$, indicating that the data qubits have been projected to the $|v^-\rangle$ eigenvector. The -1 eigenstates of a stabilizer operator constitute the subspace orthogonal to the code space, which means that it is an error that can be corrected [34]. Therefore if a $|1\rangle$ is measured in the ancilla qubit, it indicates that the data contains an error and a recovery operation is required to put the data back into the code space. This is how the quantum stabilizer measurement detects an error without directly measuring the data qubits.

3.2.5 Stabilizer Measurements and Arbitrary Input States

It is useful to determine the effect of an operator measurement for any arbitrary input state $|\psi\rangle$ [110]. Let us describe the transformation of the circuit in Figure 3.5 step-by-step for input state $|\psi\rangle$. The first Hadamard gate in the circuit in Figure 3.5 has the transformation described by Eq. 3.11. The controlled-K gate applies the K operator only when the ancilla qubit is in the $|1\rangle$ state [9]. Therefore the controlled-K gate has the transformation

$$|\tilde{\psi}\rangle \rightarrow \frac{1}{2}\Big[|\psi\rangle|0\rangle + K|\psi\rangle|1\rangle\Big] = |\tilde{\psi}_1\rangle. \tag{3.16}$$

and we arrive at an expression for $|\tilde{\psi}_1\rangle$. After applying another Hadamard gate after $|\tilde{\psi}_1\rangle$ we get

$$\frac{1}{2}\Big[|\psi\rangle|0\rangle + K|\psi\rangle|1\rangle\Big] \rightarrow \frac{1}{2}\Big[|\psi\rangle|+\rangle + K|\psi\rangle|-\rangle\Big] = |\tilde{\psi}_2\rangle \tag{3.17}$$

Expanding Eq. (3.17) gives the state of the system before the ancilla measurement

$$|\tilde{\psi}_2\rangle = \frac{1}{2}\Big[(|\psi\rangle + K|\psi\rangle)|0\rangle + (|\psi\rangle - K|\psi\rangle)|1\rangle\Big]. \tag{3.18}$$

[7] If the same calculation is repeated with the initial state as $|v^+\rangle$, it can be seen that the outcome of the ancilla qubit is always 0.

Let us now describe the effect of this circuit using the simple example of the repetition code. In this case the input state is a superposition of error-free legitimate code word states. Consider the circuit in Figure 3.5 with $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ the stabilizer operator $K_1 = ZZI$. Note that this stabilizer leaves the legitimate code word state $|\psi\rangle$ unchanged, therefore $K_1|\psi\rangle = |\psi\rangle$. Then Eq.(3.18) is shown to be

$$\frac{1}{2}\left[(|\psi\rangle + |\psi\rangle)|0\rangle + (|\psi\rangle - |\psi\rangle)|1\rangle\right] = |\psi\rangle|0\rangle. \tag{3.19}$$

Therefore in the event that a legitimate codeword state is the input, the outcome of the ancilla measurement is 0.

Let us consider the scenario that the input state is a superposition of illegitimate code word states, for example $|\psi\rangle = \alpha|100\rangle + \beta|011\rangle$. This state contains a single qubit error and therefore it can be corrected by the repetition code, so $K_1|\psi\rangle = |\psi\rangle$. Within these restrictions Eq. (3.18) becomes

$$\frac{1}{2}\left[(|\psi\rangle + (-|\psi\rangle))|0\rangle + (|\psi\rangle - (-|\psi\rangle))|1\rangle\right] = |\psi\rangle|1\rangle. \tag{3.20}$$

Therefore in the event that a correctable error is input, then the outcome of the ancilla measurement becomes 1.

In the case where the input state is a superposition of ± 1 eigenstates, the measurement of the stabilizer operator will have the effect of 'projecting' the data into either of the ± 1 eigenstates [9, 110]. The quantum stabilizer measurement is designed so that the data is entangled with the ancilla, and the measurement of the ancilla projects the data into a ± 1 eigenstate of the stabilizer.

Let us now elaborate on a scenario that explains this in more detail. Consider Figure 3.5 when $|\psi\rangle = \alpha|000\rangle + \beta|100\rangle$, namely a superposition of legitimate and illegitimate codewords. When K_1 is applied to this state, the outcome is $K_1|\psi\rangle = \alpha|000\rangle - \beta|100\rangle$. Substituting this into Eq.(3.18) and simplifying it further leads to

$$|000\rangle|0\rangle + \beta|100\rangle|1\rangle. \tag{3.21}$$

if a 1 is measured in the ancilla, we can guarantee the data now resides in the state $|100\rangle$. The ancilla measurement triggers an error correction operation, which then returns the data to a legitimate code word state, in this case $|000\rangle$. Likewise is a 0 is measured in the ancilla it indicates the data now resides in the $|000\rangle$ state. It can be said that the stabilizer measurement 'projects' the input information into a legitimate or illegitimate codeword state [9, 110].

Then referring back to Eq. (3.18), in general when the ancilla qubit of Figure 3.5 is in the state $|0\rangle$, the data qubits are described by

$$|\tilde{\psi}_2\rangle = \frac{1}{2}\left(|\psi\rangle + K|\psi\rangle\right); \tag{3.22}$$

which is the $+1$ eigenstate of K. Likewise, when a $|1\rangle$ is measured in the ancilla, the state of the data qubits is given by

$$\frac{1}{2}\left(|\psi\rangle - K|\psi\rangle\right); \tag{3.23}$$

which is the -1 eigenstate of K. These equations will be referred back to when determining the effect of the measurement of a stabilizer for an arbitrary input state of $|\psi\rangle$ in Section. 5.2.

3.3 Fault-Tolerant Circuit Design

Now that the basics of QECC's have been defined, let us move on to the definition of a fault-tolerant QECC. We begin in Section 3.3.1 by outlining the motivation for fault-tolerant circuit design, with an emphasis on the problem of error propagation and proliferation via two-qubit gates. Then in Section 3.3.3 a criterion for fault-tolerant circuits is defined, before outlining an example of a fault-tolerant stabilizer measurement circuit in Section 3.3.4.

3.3.1 Error Proliferation

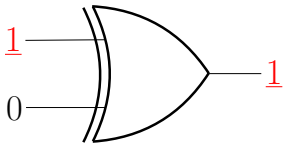

Figure 3.6: Error propagation in classical XOR gate.

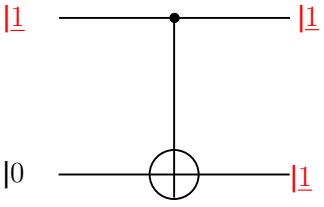

Figure 3.7: error proliferation in quantum CNOT gate.

In this section we distinguish between the occurrence of error *propagation* and error *proliferation* in a circuit. Bit errors that occur in a classical circuit may be input into a logical gate, and subsequently *propagated* to the output of the gate. *Error propagation* is defined as the event where an error is passed on without increasing the number of errors. Let us consider the example of the classical XOR gate in Figure 3.6. This is an irreversible operation, because it has two input bits and one output bit [113]. More explicitly, this gate takes input bits a and b and outputs c (a XOR b). The input

bits a and b are effectively forgotten, when the output is computed and cannot be recovered at the output of the gate. For example, the output bit c = 1 may arise from any of the inputs 01, 10, 11. Therefore the input is not uniquely recoverable after the gate has been applied to the information.

This particular feature of irreversible gates is advantageous, when the input bits suffer from a bit-flip error. Consider for example that the binary input string `ab' contains an error with Hamming weight wt(ab) 1. The output bit c that follows must have an error with wt(c) = 1, since it is a single bit. Therefore the overall number of errors in the circuit either remains the same or it is reduced even when the gate computes an erroneous input[8].

Unfortunately, this is not the case for the quantum CNOT gate, as seen in Figure 3.7. The dynamics of the quantum world are described by unitary transformations, which preserve the dimensions of the system. Therefore quantum gates are reversible, which means that the number of input qubits is the same as the number of output qubits [114]. For example, the quantum CNOT gate takes the two-qubit state $|ab\rangle$ as its input and outputs the two-qubit state $|ac\rangle$, where again we have c (a XOR b). Therefore, if the control qubit contains a bit-flip error, the output state has two bit-flip errors, for example $|\underline{1}0\rangle \rightarrow |\underline{1}\underline{1}\rangle$, as demonstrated in Figure 3.7. Explicitly, underlining indicates the erroneous positions.

Let us now consider this example in more detail, since the data in the control qubit $\underline{a}$ is erroneous, this means that the outcome of $\underline{c}$ = ($\underline{a}$ XOR b) contains an error. This outcome is stored in the target qubit and carried forward to the next gate in the circuit, therefore future gates will further propagate this error. Additionally, the erroneous control qubit $|\underline{a}\rangle$ is not absorbed by the XOR gate. Instead it is preserved in the control qubit, which may impose further degradation at a later time step. In effect, the CNOT gate has proliferated the control bit error to the target qubit and then failed to absorb the error it started with. Hence, a qubit error propagates throughout the circuit, wherever two-qubit gate connections are present. Specifically, an increase in the weight[9] of the error from the input to the output state implies that an error has been proliferated by the gate, potentially giving rise to avalanche-like error proliferation [1].

Note that error proliferation may increase the qubit error ratio even when the CNOT gate itself is perfect. A perfect gate has a gate error probability of $P_g = 0$. Let us now consider the example of the [3,1,3] repetition encoder circuit shown in Figure 3.8. Assuming that the CNOT gates in this circuit are perfect, but a bit-flip error that

[8] Note that when making a comparison to quantum circuits, we may also take into account the inherent binary nature of classical gates. This may also contribute to a classical circuit being less susceptible to avalanche-like circuit error. In addition, a classical circuit comprised of many fan-out gates may also display error proliferation, however this type of circuit is less common in the classical world compared to the quantum case.

[9] The weight wt(S) of a quantum operator S is defined as the number of qubits that differ from the identity operator. Therefore wt(XIZ) = 2.

Figure 3.8: Propagation of a single qubit error to three qubit error.

occurred before the first CNOT gate is proliferated by the subsequent gates results in three individual qubit errors at the circuit's output. Therefore the circuit has increased the qubit error ratio with respect to the input, despite the application of perfect CNOT gates.

3.3.2 Error Proliferation by CNOT Gates

Figure 3.9: X and Z error proliferation in the CNOT gate. X errors are proliferated by additionally passing them from the control to the target qubit, while Z errors are proliferated by additionally passing them from the target qubit to the to control qubit.

In addition to their own intrinsic gate errors, a CNOT gate may increase the error ratio in a circuit by proliferating pre-existing qubit errors. If an X error[10] corrupted the

[10] An X error has the effect of a bit-flip on the qubit, see Eq. (2.15) and Section 2.4.

control qubit before the CNOT gate, then the gate has the effect of copying the control error to the target qubit, as seen in Figure 3.9 (a), which can be represented as [110]

$$CNOT(XI)CNOT^{\dagger} = XX. \tag{3.24}$$

Similarly, the CNOT gate copies an existing phase error (Z) on the target qubit, upwards to the control qubit, as seen in Figure 3.9 (b) and represented by:

$$CNOT(IZ)CNOT^{\dagger} = ZZ. \tag{3.25}$$

3.3.3 Definition of Fault-Tolerant QECC

A fault-tolerant circuit construction mitigates both the gate error and proliferation error probability. Formally, a quantum circuit protected by an $[n, k, d]$ QECC is said to be fault-tolerant, if a single gate error occurring with probability P_g results in less than $t = \lfloor (d-1)/2 \rfloor$ individual qubit errors at the output of a circuit block [10, 84, 66]. A circuit may be constructed by multiple fault-tolerant circuit blocks, whereby each block includes a final error correction step [84]. In other words, for a circuit to be fault-tolerant the proliferation of a single gate error must not overwhelm the QECC used for protecting the quantum circuit. For example, the repetition code's encoding circuit of Figure 3.8 is not fault-tolerant, because a single qubit error may proliferate to $t = 3$ errors. Another example of a non-fault-tolerant circuit is constituted by the Steane encoding circuit, of Figure 3.4, because a single CNOT gate error is proliferated to $t = 3$ qubit errors. Since the Steane code is a $d = 3$ code, this means that there exist single gate errors that cannot be corrected, as exemplified in [99].

The benefit of a fault-tolerant circuit is that it guarantees that the QECC-protected scheme succeeds in achieving an error rate improvement compared to the unprotected scheme. For example, suppose that a component with error probability of P_g is encoded by a circuit having D components. All D components may also be assumed to have an error probability equivalent to that of the uncoded gate, namely P_g. To achieve fault-tolerance, the QECC must be able to correct the qubit error probability for a total of D single gate error scenarios. This guarantees that the final error rate will be upper bounded by $O(P_g^2)$, which is the probability of two gates simultaneously incurring independent errors. Then the inequality characterizing the coded and uncoded scheme by $O(P_g^2) < P_g$ is satisfied, showing that if the qubit error that results from a single gate error can be corrected, it is guaranteed that the QECC scheme will achieve a coded error rate improvement. If any single gate error is left uncorrected, then the coded error rate will be upper bounded by $O(P_g)$ and the QECC protected scheme cannot offer better error rates than the uncoded scheme, namely we have $O(P_g) > P_g$.

3.3.4 Example: Fault-Tolerant Stabilizer

To conceive a fault-tolerant circuit design, let us describe the fault-tolerant construction of a stabilizer measurement, as presented in Section. 3.2.4. This adheres to the de nition of fault-tolerance described in Section. 3.3.3 and it is a fundamental component to any fault-tolerant QECC scheme.

Figure 3.10: Non-fault-tolerant implementation of the Steane code stabilizer $K_1 = IIIXXXX$ [9].

Figure 3.10 shows the circuit construction of the Steane code stabilizer of $K_1 = IIIXXXX$ [115], in which a single bit- ip error on the ancilla qubit is propagated to $t > 1$ errors in the data qubits. This is because the bit- ip error on the control qubit of the rst CNOT gate leads to the application of the NOT gate ($\bar{}$) on the target qubit. Moreover, the control error is not deleted by the action of the logic gate, since the CNOT is a reversible gate. This means that the input information is preserved at the output of the logic gate. Therefore the bit- ip error on the control qubit is input into the second, third and fourth CNOT gates. What began as a single error is spread across the qubit register to $t = 4$ errors. Since the Steane code has a minimum distance of $d = 3$ this circuit construction is not fault-tolerant.

This error-proliferation phenomenon is a general property of all stabilizer circuits obeying the architecture of Figure 3.10. Fortunately, fault-tolerant schemes do exist, such as the one developed by Peter Shor in [10] which is described in this section. However, in most practical cases, a more e cient scheme would be employed such as those in [115, 14, 116], which require reduced qubit overheads [88, 117].

Figure 3.11 shows the fault-tolerant implementation of the $K_1 = IIIXXXX$ Steane code stabilizer. The general idea of the scheme is that the ancilla qubit is replaced by an error-free superimposed state [10]. Replacing the ancilla with a state that is error-free ensures that less qubit errors are propagated to the data qubits by the gates coupling the ancilla and the data. An N-qubit superimposed state is chosen, where N is the same as the number of CNOT gates in the traditional stabilizer. This is equivalent to the

Figure 3.11: Fault-tolerant implementation of the Steane code stabilizer $K_1 = IIIXXXX$ [9].

weight[11] of the stabilizer, so for example we have $N = wt(IIIXXXX) = 4$. Replacing an ancilla qubit by an ancilla state means that the CNOT gates in the stabilizer can be applied to the ancilla relying on the same circuit construction as a transversal CNOT gate. This inherits the fault-tolerant properties of the transversal CNOT gates, see [1, 85]. The transversal construction ensures that there are no scenarios whereby a single qubit error can result in increased-weight errors at the circuit's output. This is because there are no qubits either in the data or in the ancilla state that are connected by more than a single CNOT connection.

The aim of the stabilizer is to copy the error information into the ancilla qubit without directly measuring the data qubits. To do this, the ancilla must be in an equi-probable superposition so that the eigenstate of the data is encapsulated in a ± 1 phase difference. Figure 3.10 shows that a Hadamard gate is applied to the ancilla qubit before the stabilizer. Therefore the stabilizer circuit puts the ancilla qubit into the state $\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$ before applying the controlled-K gate[12]. This state is extended in the fault-tolerant circuit construction to the following N-qubit superimposed state

$$\frac{(|00\ldots00\rangle + |11\ldots11\rangle)}{\sqrt{2}}. \tag{3.26}$$

Then the ± 1 eigenstate in the data is passed to the ancilla state $|00\ldots00\rangle \pm |11\ldots11\rangle$, where the ± 1 phase difference can be detected by a measurement. A fault-tolerant way to do this measurement is to apply a Hadamard gate to all N qubits. This is because

[11] The weight $wt(S)$ of a quantum operator S is defined as the number of qubits that differ from the identity operator. Therefore $wt(XIZ) = 2$.

[12] An arbitrary stabilizer K can be implemented as a controlled-K gate [9].

we see that

$$H^{\otimes N}\frac{(|00\ldots00\rangle + |11\ldots11\rangle)}{\sqrt{2}} = |i\rangle^{\otimes N} \tag{3.27}$$

has an even weight, when the phase difference is positive and odd weight when the phase difference is negative. It is necessary to use a superimposed state in the ancilla rather than simply duplicating the ancilla qubit N times because in this case the ancilla state would be $|+i\rangle^{\otimes N}$, but this will not work because the eigenstate of the data is determined by directly measuring each qubit of the ancilla state.

3.3.5 Superimposed State Preparation

Figure 3.12: Circuit to construct a superimposed state [84].

This section describes how the ancilla state is prepared without an error. The scheme to do this was developed by Shor in [10]. The circuit shown in Figure 3.12 prepares the corresponding superimposed state. This circuit is not itself fault-tolerant, but the superimposed state is part of a fault-tolerant stabilizer implementation [10]. An error-free superimposed state is determined by detecting errors using a parity check and an extra ancilla qubit. For example, an $N = 4$ qubit example of a superimposed state is

$$\frac{(|0000\rangle + |1111\rangle)}{\sqrt{2}}. \tag{3.28}$$

This state represents an equi-probable superposition of equally weighted N-qubit all-zero and all-one vectors. The qubit locations of the parity check CNOT gates should be chosen randomly and repeated until the state can be deemed error-free [10, 107]. For example, let us assume that an XI error is imposed by the CNOT gate connecting qubits (2) and (3) in Figure 3.12. This will result in the following state

$$\frac{(|0100\rangle + |1011\rangle)}{\sqrt{2}}. \tag{3.29}$$

In this case there is an error on qubit (2) which will be detected by a parity check measurement between different circuit locations to that shown in Figure 3.12. A gate

error which results in the state

$$\frac{(|0010\rangle + |1101\rangle)}{\sqrt{2}} \tag{3.30}$$

is detected by another parity check combination. Likewise, other error combinations include

$$\frac{(|1000\rangle + |0111\rangle)}{\sqrt{2}}; \quad \frac{(|1100\rangle + |0011\rangle)}{\sqrt{2}}; \quad \frac{(|0001\rangle + |1110\rangle)}{\sqrt{2}};$$

which can be detected by measuring the parity check ancilla qubit (marked (5) in Figure 3.12). If a qubit error is propagated to all $N = 4$ qubits, the resultant superimposed state remains unaffected. Therefore, the specific location of the parity check in Figure 3.12 will detect the most common error, where the first and last qubits are not similar. If the measurement outcome indicates that the ancilla is in the $|0\rangle$ state, then the superimposed state has been prepared without error. If by contrast a $|1\rangle$ state is measured, this indicates that the state prepared should be thrown away and the process must be re-initialized.

The above-mentioned state construction ensures that there are no X errors in the ancilla qubits, since error detection is used for spotting and throwing away the states with bit-flip errors. Therefore there will be no bit-flip error proliferation imposed on the data qubits. However, there are a pair of scenarios that may results in an incorrect syndrome measurement. A single phase error during the superimposed state preparation results in the phenomenon that the ancilla state $|00...00\rangle - |11...11\rangle$ forces the -1 eigenvalues to switch places. This would result in an incorrect syndrome measurement. The second scenario is that a gate failure in the CNOT gates constructing the syndrome operator would also result in an incorrect measurement outcome.

To combat this problem, the full stabilizer procedure must be repeated for example three times [66, 118]. Then a majority vote is taken to determine the final stabilizer value but the third stabilizer measurement is only necessary when the first two measurement outcomes differ. This means that an incorrect stabilizer result will occur at a probability order of p^2 where p is the probability of a component error, because two of the stabilizer implementations must simultaneously contain a component error for the majority vote to conclude the absence of errors due to a pair of errors. Therefore in the best case scenario, a single syndrome measurement requires an additional 10 ancilla qubits assuming that the superimposed state is prepared without error first time and the first as well as second syndrome measurements match. However, it is possible for this to become more than doubled, because multiple superimposed states may have to be produced to distill a single error free version and this must be done for each repeated stabilizer measurement. Therefore the extent of the qubit overheads is determined by the efficiency of creating an error-free ancilla state. For the full $l = n - k = 6$ Steane code stabilizer set it is not unreasonable to expect more than 60 additional ancilla qubits which is in stark contrast to the 6 required for the non-fault-tolerant scheme.

3.4 Conclusion

In Chapter 2 we introduced the basics of quantum circuits and quantum domain errors. Then QECCs were described, followed by fault tolerant circuit design. In the next chapter another type of fault-tolerant circuit will be introduced, namely the transversal gate, which allows us to fault-tolerantly apply logic gates to encoded qubits. In the subsequent chapter, the so-called `encoderless' scheme will be introduced, which applies the fault-tolerant stabilizer measurement that has just been described. This provides error rate improvements when gate errors are present in the circuit that implement a fault-tolerant QECC scheme.

Chapter 4

Quantum-Gate Errors in Transversal CNOT Gates

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

4.1 Introduction

To recap Chapter 3, a fault-tolerant QECC is by de nition capable of avoiding the proliferation of errors. More explicitly, a $[n; k; d]$ maximum-minimum-distance QECC encodes$k$ logical qubits into n physical qubits and has a minimum distance of$d$, hence it is capable of correcting$t = b(d \quad 1)=2c$ individual physical qubit errors. Our design objective is to ensure that despite using realistic imperfect quantum gates, the prolifera- tion of errors does not lead to exceeding the error correction capability of a fault-tolerant

Figure 4.2: Transversal CNOT gate.

QECC. More formally, a quantum circuit that is protected by an $[n, k, d]$ QECC is fault-tolerant if a single component failure occurring with probability p results in less than $t = \lfloor (d-1)/2 \rfloor$ individual qubit errors at the output of the circuit block [66]. Under this idealistic assumption a physical qubit error introduced by a single gate cannot escalate to an uncorrectable number of errors, given the $[n, k, d]$ QECC considered. Let us assume that the probability of a single gate error is P_g. Hence the probability of two simultaneous gate errors[1] is $O(P_g^2)$, provided that the error events are independent of each other, while $P_g \ll 1$ and $P_g^2 < P_g$.

Unfortunately, a bit-flip error on the control qubit in a CNOT gate will result in a deleteriously applied NOT operation imposed on the target qubit, hence resulting in two erroneous qubits, rather than one. Therefore, an originally correctable number of individual qubit errors escalates to an uncorrectable number of correlated qubit errors even if no additional component failure has occurred.

A fault-tolerant implementation of the CNOT gate relies on a so-called transversal architecture, as seen in Figure 4.2 [85]. The CNOT gate will be discussed in Section 2.3.2 and Transversal Gates in Section 4.2. To elaborate, the left hand side of Figure 4.2 shows the uncoded circuit, whilst the right hand side portrays the fault-tolerantly encoded circuitry, where the $\oplus$ represents a NOT gate and S is a syndrome decoder. For the convenience of our discussions, here we initially portray a simple $R = \frac{1}{3}$-rate repetition code which is capable of correcting one error in each 3-qubit code word. Hence it has a 33% error correction capability. Both the upper and lower syndrome decoders of Figure 4.2 are only capable of correcting a maximum of t errors. We arrange for the logical connection of the ith physical qubit in the control state with the ith qubit in

[1] The magnitude of $O(P_g^2)$ is determined by the number of scenarios, whereby two gates simultaneously endure an error that cannot be corrected.

the encoded target state, as observed in Figure 4.2. For example, a bit- ip error on the second control qubit of the upper syndrome decoder would only interact with the second target qubit seen at the output of the lower syndrome decoder in Figure 4.2. This circuit design limits the propagation of qubit errors, since an error that is corrected by the top syndrome decoder can only propagate to a single error input to the lower syndrome decoder. Since the control and target qubits are encoded separately, the error that has proliferated through the transversal CNOT connection can always be corrected.

Under the fault-tolerant premise, it is assumed furthermore that no adjacent qubit failures occur either spatially or temporally, since they are independent at each segment of the circuit. However, repeated applications of an imperfect gate would be more accurately represented by an error model that includes temporal and/or spatial correlation in the gate failure, since environmental perturbations may a ect a group of components in each others vicinity. Therefore, assuming independence of the component errors constitutes another idealized simplifying assumption.

Furthermore, a common fault-tolerant $[n; k; d]$ encoding technique relies on fault-tolerant stabilizer measurements used for preparing the encoded information [66]. However, this requires knowledge of the state that we wish to encode. More explicitly, in order to prepare an arbitrary state $j\ i = \ j0i + \ j1i$, the coe cients $\ $ and $\ $ must be known to us [9]. This has the drawback that unknown information cannot be encoded. However, encoding unknown information is necessary because in many practical schemes QECC decoding and re-encoding are applied mid-way through the computation, as demonstrated in [119]. Fortunately, there exist unitary encoding circuits, which have the capability of encoding unknown information, but regretfully again these are not fault-tolerant by the above de nition. Having said that, these unitary encoding circuits are still appealing, since they do not require additional ancilla to encode the state.

Fault-tolerant state preparation techniques impose a substantial qubit overhead, since the stabilizer must be repeated multiple times to guarantee that a single error-free outcome can be obtained. In addition to the above complications, the ancilla must be prepared without error, hence potentially requiring the distillation of the error-free states from a larger number of states. Therefore, since the encoding circuit requires only $(n \ \ 1)$ qubits in addition to the unknown information qubit, it is desirable to nd a solution for mitigating the error proliferation inherent in non-fault-tolerant circuits.

The rest of this chapter is structured as follows. In Section 4.2 a transversal gate is outlined, and in Section 4.2.2 the processing of information stored in the encoded qubits is detailed. The system model is detailed in Section 4.3. Then the results characterizing the repetition-encoded transversal CNOT gates are derived in Section 4.4 and for the Steane code in Section 4.4.3.

4.2 QECC Mitigates Quantum Gate Errors

4.2.1 Transversal Gates

Figure 4.3: General transversal single-qubit gate.

The circuits that implement a QECC, such as the encoding circuit, must be themselves fault-tolerant [10]. However, we also wish to implement logical gates in order for our quantum processor to be more useful than just a quantum memory [37]. A fault-tolerant method of improving the error rate of a realistic imperfect quantum gate is the scheme popularly referred to as the transversal gate [34, 85]. More explicitly, a transversal gate allows a logical gate to be applied to an encoded state.

This scheme is characterized by the bit-wise application of the gate to an encoded state [17]. More specifically, to implement a single-qubit gate U transversely it is applied separately to each physical qubit in the n-qubit encoded state, as demonstrated in Figure 4.3 [34]. The left hand side of Figure 4.3 represents a single-qubit gate U applied to an arbitrary uncoded state. The right hand side shows that the transversal gate implementation $\overline{U}$ results in the same logical evolution of the encoded state, as U results in for an uncoded state. The bar above U (giving $\overline{U}$) indicates that this is a transversal gate. Explicitly, the application of $\overline{U}$ to a n-qubit encoded state $|\overline{\ }\rangle$ has the same logical effect of applying the uncoded gate U to a k-qubit uncoded state $|\ \rangle$. For example, the X gate applies a bit-flip to $|\ \rangle$ and $\overline{X}$ applies a bit-flip to $|\overline{\ }\rangle$. This can be viewed as X representing the k-qubit uncoded gate, while $\overline{X}$ is the n-qubit 'encoded' version.

You might wonder, why single-qubit transversal gates are fault-tolerant? If the components introduce errors independently and the information is encoded in a $d = 3$ QECC, then an uncorrectable error may only occur when two independent components fail simultaneously. This happens with the probability of $O(P_g^2)$, therefore achieving a beneficial error-rate improvement compared to the uncoded single gate.

Error proliferation may hence be circumvented by a fault-tolerant gate construction, as shown in Figure 4.2. Specifically, a transversal CNOT gate is applied on a bit-wise basis

from the ith qubit in the encoded control state to the ith qubit in the encoded target state. Figure 4.2 shows that the CNOT gates are specifically arranged in a way so that the qubits are coupled with no more than a single CNOT gate connection. This means that a single error in an encoded block may propagate to no more than a single error in the other. This erroneous scenario can always be corrected by the syndrome decoder, since both the control and target qubits are encoded independently by an $[n, k, d]$ QECC. Therefore, an uncorrectable error may only occur when two CNOT gates simultaneously incur an error with probability $O(P_g^2)$, which satisfies the conditions of fault-tolerance.

4.2.2 Processing QECC-Information by Logic Gates

Logic gates can be applied to QECC-protected data, because the QECC does not treat any permutation of a code word by a legitimate logical gate as an error. Instead, the logical gate has the effect of transforming the data from one legitimate code word to another, provided that the transversal gate is carefully matched to a certain QECC, as described in this section. The discussion in this section follows on from the presentation of stabilizer codes in Section. 3.2.1.

Firstly, what kind of error is detectable by a general stabilizer code? A correctable error E for a stabilizer code $\mathcal{S}$ is constituted by the sub-group of G_n defined in Eq. (2.17) that anti-commutes with $\mathcal{S}$, where we have $KE = -EK$. For example, if $K \in \mathcal{S}$ and $|\bar{\psi}\rangle$ is a legitimate defined code word, then we have:

$$K(E|\bar{\psi}\rangle) = -EK|\bar{\psi}\rangle = -E|\bar{\psi}\rangle; \tag{4.1}$$

where $E \in \mathcal{E}$. The error has the effect of shifting the logical qubit out of the legitimate code space. The negative phase value can be measured by the syndrome measurement and a subsequent recovery operation can be applied to reverse the effect of E.

If the measurement of the stabilizer operator results in an +1 eigenvalue, it is assumed that state $|\bar{\psi}\rangle$ is a legitimate code word satisfying that $K|\bar{\psi}\rangle = |\bar{\psi}\rangle$. However, if an error-corrupted state $|\bar{\psi}'\rangle = E|\bar{\psi}\rangle$ is inserted into this equation, then we arrive at $K|\bar{\psi}'\rangle = -|\bar{\psi}'\rangle$ indicating that the error E cannot be detected by the QECC. If an error commutes with the stabilizer, it has the property of $KE = EK$. Then we have

$$K(E|\bar{\psi}\rangle) = EK|\bar{\psi}\rangle = E|\bar{\psi}\rangle; \tag{4.2}$$

which gives the definition of an error that cannot be corrected by a stabilizer code [34]. This is because the stabilizer measurement results in an +1 eigenvalue, which is interpreted as being in the legitimate code space. More formally, the set of elements in G_n in Eq. (2.17) that commute with the stabilizer $EKE^\dagger = K \;\forall K \in \mathcal{S}$ are the normalizer[2] of $\mathcal{S}$ in G_n, denoted by $N(\mathcal{S})$ [84]. If an error commutes with the stabilizer, it

[2] The set U such that $UG_nU^\dagger = G_n$ is the normalizer of G_n, denoted by $N(G_n)$.

is undetectable, therefore this has the effect of an uncorrectable error E. More formally, $E \in N(\mathcal{S}) \setminus \mathcal{S}$.

A transversal gate $\overline{U}$ has the same properties as an uncorrectable error, because when a valid encoded gate is applied to an encoded state, it will return another legitimate encoded state [107]. In other words, the code will not detect an error, when the gate is applied to the encoded qubits. This reveals the set of transformations that act non-trivially on the code word, yet do not shift the information outside the legitimate code space.

Let us look at this idea from the perspective of applying quantum gates to encoded qubits. A general encoded gate $\overline{U}$ evolves the encoded data according to $|\overline{\psi}_2\rangle = \overline{U}|\overline{\psi}\rangle$. This state would be stabilized by an updated stabilizer $\overline{U}K\overline{U}^{\dagger}$, which has the intended effect

$$\overline{U}K\overline{U}^{\dagger}\overline{U}|\overline{\psi}\rangle = K\overline{U}|\overline{\psi}\rangle = \overline{U}|\overline{\psi}\rangle. \tag{4.3}$$

This is reminiscent of the ordinary stabilizer $K|\psi\rangle = |\psi\rangle$, which leaves a legitimate code word unchanged. Then a transversal gate $\overline{U}$ is chosen for ensuring that

$$\overline{U}K_i\overline{U}^{\dagger} = K_j \; \forall K_{i,j} \in \mathcal{S}, \tag{4.4}$$

where the encoded gate conveniently has no effect on the stabilizer set. How is it justified that certain transversal gates have this property? When S and U commute, then $S\overline{U} = \overline{U}S$. This means that

$$\overline{U}K\overline{U}^{\dagger} = \overline{U}\overline{U}^{\dagger}K = K, \tag{4.5}$$

remembering that $\overline{U}\overline{U}^{\dagger} = I$. Therefore, the transformations $\overline{U}$ carried out by legitimate transversal gates for a given code $\mathcal{S}$ are those, which commute with the stabilizer.

For example, a transversal bit-flip gate corresponds to the bit-wise application of the X gate to each physical qubit, denoted as $\overline{X} = X^{\otimes n}$. For the Steane code, $\overline{X}$ is implemented by applying $n = 7$ X gates directly to the physical qubits of the encoded data. To check that $\overline{X}$ has the intended logical transformation, $\overline{X}$ can be applied to Eq. (3.8) and Eq. (3.9). Then to transform $|\overline{0}\rangle$ to $|\overline{1}\rangle$ we get $\overline{X}|\overline{0}\rangle = |\overline{1}\rangle$ and vice versa. Similarly, $\overline{Z} = Z^{\otimes 7}$ has the effect of the logical phase-flip, where $\overline{Z}|\overline{0}\rangle = |\overline{0}\rangle$ and $\overline{Z}|\overline{1}\rangle = -|\overline{1}\rangle$ can be used for distinguishing whether the logical qubit is either $|\overline{0}\rangle$ or $|\overline{1}\rangle$. Since we have $XZX^{\dagger} = -Z$ and $ZXZ^{\dagger} = -X$, the stabilizer set in Eq. (3.7) remains unchanged. For example, $\overline{X}K_i\overline{X}^{\dagger} = K_j$ and $\overline{Z}K_i\overline{Z}^{\dagger} = K_j \; \forall K_{i,j} \in \mathcal{S}$.

Figure 4.4: General transversal CNOT gate $\overline{U}_f$ scheme.

4.3 System Model

The scheme seen in Figure 4.4 encodes a pair of unknown qubits $|s_1\rangle$ and $|\ _2\rangle$ using the unitary encoding circuit V. The encoding at the top left corner of Figure 4.4 can be described as

$$|\overline{\ _1}\rangle = V(|\ _1\rangle\ |\ 0\rangle^{\otimes(n-k)}): \tag{4.6}$$

The state $|\overline{\ _1}\rangle$ can be stabilized by $\mathcal{S} = \{K_i\}$, which is expressed as

$$K_i|\overline{\ _1}\rangle = |\overline{\ _1}\rangle \quad \forall K_i \in \mathcal{S}: \tag{4.7}$$

In this model $\mathcal{S} = \{K_i\}$ corresponds to the $n-k$ stabilizer operators. By measuring the stabilizers $\mathcal{S}$ the location of an error in the data qubits can be determined. If there is an error, the recovery operation R is applied to the data for returning it to a legitimate code word state.

The encoded control and target qubit are input to the transversal CNOT gate labelled by $\overline{U}_f$, as seen in Figure 4.4. This block represents the logical action of a CNOT gate applied to the encoded qubits. The transversal CNOT gate $\overline{U}_f$ evolves the encoded state $|\ _1\rangle = |\overline{\ _1}\rangle|\overline{\ _2}\rangle$ to $|\ _2\rangle$ as follows:

$$|\ _2\rangle = \overline{U}_f|\ _1\rangle: \tag{4.8}$$

This is stabilized by $\overline{U}_f\mathcal{S}\overline{U}_f^{\dagger}$. Assuming that the transversal CNOT gate represents a legitimate logical transformation for the chosen code, the stabilizer set remains invariant

to the application of $\overline{U}_f$, so that $\$ = K_i \quad K_j$ satisfies $\overline{U}_f \$ \overline{U}_f^{\dagger} = \$$. This allows the intended logical evolution of the encoded information to be preserved and any single qubit error occurring within the data to be corrected.

4.3.1 Frame-Error-Rate

Let us now consider the example of a transversal CNOT gate protected by the $\frac{1}{3}$-rate repetition code of [99]. If more than one qubits in the 6-qubit frame have a bit-flip error at time step $|_3\rangle$ this will be counted as one frame error. This is because, a single qubit error occurring within the top or bottom $n = 3$ qubits after $\overline{U}_f$, i.e. in $|_2\rangle$ seen in Figure 4.4, can be corrected since in this scheme the control and target qubits are encoded individually. For example, two qubit errors, one on qubit 2 and the other on qubit 5, can be fully corrected, hence no frame error is encountered at $|_3\rangle$. This is because qubit 2 is corrected by the upper syndrome decoder and qubit 5 by the lower syndrome decoder. However, a qubit error on the first and second qubit cannot be corrected by the upper decoder, since both qubit errors are processed by the same $d = 3$ syndrome decoder. Therefore, this scenario incurs a frame error at $|_3\rangle$.

The frame-error-rate (FER) is defined by considering all operations involved in the calculation of the error rate at the output of a circuit block, yielding

$$FER = \frac{\text{No. of frame errors}}{\text{Total No. of frames}}. \tag{4.9}$$

The FER is a useful metric because it characterizes the integrity of the transversal CNOT gate and denotes the FER at the output of an error-corrected circuit block.

4.3.2 Quantum Channel Model

In this model seen in Fig. 4.5 each gate of the circuit is assumed to be an independent potential error location with a probability of P_g. Then an independent individual qubit channel is applied after this. The motivation for this hybrid model is that qubit errors may not occur at the gate output as independent events [109], hence the gate errors must also be modelled individually with a probability of P_g. This is because error proliferation results in correlated qubit errors, which systematically spread through the two-qubit gates, as detailed further in Section 3.3.1.

In this hybrid channel model, we assume that each CNOT gate has a gate error rate probability P_g. In addition to gate errors, the qubits may also suffer from decoherence with a probability P_e, which encapsulates the effects of all other circuit errors. Under these assumptions the uncoded circuit has the following FER

$$FER = P_g + 2P_e; \tag{4.10}$$

Figure 4.5: Combined channel model with gate error P_g (blue box) and independent qubit error P_e (red box).

as shown in Figure 4.5. This channel model can also be applied to the coded system model of Figure 4.4. In this case the blocks V and $\overline{U}_f$ have independent gate errors, which may however have a similar P_g. Hence, gate errors occur at gate locations specific to the circuit construction for the particular QECC chosen. Then an independent qubit flip channel is applied at position $|\psi_2\rangle$ of Fig. 4.4. Note that it is assumed that the circuits of $S^\dagger$ and R are fault-tolerant and therefore the gate error probability in these circuits is negligible [66].

4.3.3 Simulation Assumptions

This section makes clear the assumptions made in this simulation:

- It must be that $FER \ll 1$ for a given combination of P_g and P_e. Hence, for this simulation P_g and P_e are considered to be 0.1 or smaller [120, 45, 121].
- In this simulation each of the gate errors and qubit errors are simulated independently. Therefore, all combinations of component errors are encompassed by this simulation, which is run 10^6 times for each data point. The most common scenario is a single-component error, namely a gate error with a probability of P_g or a single qubit error with a probability of P_e.
- The circuit gate error events are modelled by an independent random variable, which determines the qubit error incurred by each gate error. It is necessary to simulate each gate separately in order to encapsulate the effects of error proliferation in subsequent circuit components. Error proliferation within the circuit outputs a pattern of qubit errors specific to the circuit architecture. The simulation results reflect this and the effect of error proliferation on the FER.

Figure 4.6: A $\frac{1}{3}$-rate repetition encoder with Transversal CNOT Gate.

4.4 Frame Error Rate Bounds

In this section we will derive various FER bounds, which are then veri ed by simulations.

4.4.1 Evaluation of Repetition Coding

In this section the method of nding the analytical $FER = e_1 P_g = 2P_g$ is discussed in detail. We commence by considering the accumulated error probability before error correction at $|\ _2\rangle$ and determine how much this is reduced by with the aid of syndrome decoding.

First, let us nd the total accumulated error probability before syndrome decoding, as represented by the FER at $|\ _2\rangle$ in Figure 4.6. The circuit has $D = 7$ CNOT gates, each having gate error probability of P_g. Assuming that the gate errors are independent, the FER at $|\ _2\rangle$ (FER_2) is dominated by the sum of all the single CNOT gate error probabilities. Note that in this example the combinations of two, three, ... gate errors occurring with probability $O(P_g^2); O(P_g^3)$ ... are ignored, since the probability of these scenarios in this channel model is low. Therefore, we have

$$FER_2 = DP_g = 7P_g: \tag{4.11}$$

Naturally, we expect that some error patterns after a single CNOT gate error can be corrected by the syndrome decoders. This means that the nal error rate FER_3 at $|\ _3\rangle$

CNOT Gate	Bit-Flip Error	After Propagation
CNOT 1	$\underline{IX}I$	$I\underline{X}I$
	$\underline{XI}I$	$\underline{XIX}$
	$\underline{XX}I$	$\underline{XXX}$
CNOT 2	$I\underline{IX}$	$II\underline{X}$
	$\underline{XII}$	$\underline{XII}$
	$\underline{XIX}$	$\underline{XIX}$

Table 4.1: Error patterns at the output of the $[3;1;3]$ Repetition code encoder $\mathcal{N}$, as shown in Figure 4.7, after the propagation of a single CNOT gate error in the bit-flip channel. Each scenario has a probability of occurrence $\frac{P_g}{3}$.

will obey:

$$FER_3 = \alpha P_g < 7P_g; \tag{4.12}$$

where α is a scaling coefficient that we have to find by exhaustively considering every error pattern occurring at $|\psi_2\rangle$. If a pattern can be corrected by the syndrome decoders, its probability of occurrence is subtracted from Eq. (4.11) for determining the experimental gate error probability, yielding the final FER_3.

Then the natural question arises, how many different error patterns are accumulated at $|\psi_2\rangle$ in Figure 4.6 after the occurrence of specific single CNOT gate errors? Each CNOT gate in the circuit may suffer from any of the three possible bit-flip error patterns of $IX; XI; XX$ shown in Figure 2.6 with a probability of $\frac{P_g}{3}$. Then in conjunction with $D = 7$ CNOT gates, there are 21 possible error patterns occurring at $|\psi_2\rangle$.

Fortunately, we do not have to consider all 21 error patterns individually. Quantitatively, we will demonstrate later in this section that we only have to analyze 6 patterns. Let us commence by considering the gate error in the transversal CNOT gate section $\overline{U}_f$ of Figure 4.6. This section is constructed from 3 CNOT gates and therefore contributes a total of $3P_g$ to FER_2 in Eq. (4.11). Since the control and target qubit of each CNOT gate is finally input into separate syndrome decoders, any bit-flip error combination $IX; XI$ or XX imposed on the control and target qubit of these gates can be corrected before $|\psi_3\rangle$. This is a benefit of the transversal gate being constructed fault-tolerantly and therefore no error proliferation takes place in this section. Hence we do not have an error event that cannot be corrected [34]. Therefore, Eq. (4.11) may initially be reduced by $3P_g$ so that we have:

$$P_g < 4P_g; \tag{4.13}$$

since any individual error patterns resulting from these gate errors will be corrected.

Now, only the gate error in the top and bottom encoder of Figure 4.6 has to be considered individually. There are four CNOT gates in total, which accounts for FER of $4P_g$ in Eq. (4.13). Let us commence by only considering the top encoder in Figure 4.6, which has two CNOT gates to consider ($2P_g$). This encoder has 6 possible error scenarios in the bit-flip channel. Table 4.1 shows a comprehensive assessment of the error pattern

Figure 4.7: [3; 1; 3] Repetition code encoder V

on the $n = 3$ qubits at the output of the encoder for each bit-flip scenario. Inspection of Table 4.1 shows that 3 out of the 6 error patterns contain only a single bit-flip error. Then the operation of $\overline{U}_f$ in Figure 4.6 copies the same error pattern to the bottom three qubits, which is then entered into the lower syndrome decoder. So a single error entered into the top syndrome decoder will lead to a single error input to the bottom one, both of which can be corrected. Therefore, error proliferation in the subsequent CNOT gates can be avoided. Each scenario occurs with probability $\frac{P_g}{3}$, therefore $3 \frac{P_g}{3} = P_g$ is the probability of frame error after any gate error in the top encoder.

Hence, Eq. (4.13) can be reduced by P_g, giving $P_g < 3P_g$. The only CNOT gates left to consider are those in the lower encoder V_{lower}. This has the same circuit structure as the upper encoder. Therefore, Table 4.1 also describes the probability that the gate error occurring in the lower encoder will lead to an error that can be corrected. Hence the final FER_3 at $|_3\rangle$ of Figure 4.6 after all possible CNOT gate errors will be

$$FER_3 = 2P_g; \tag{4.14}$$

which yields $= 2$ in Eq. (4.12).

4.4.2 Repetition Code Results

Let us first consider the frame error events imposed by pure gate errors in the absence of bit-flip errors. For a circuit block having a total of D components and identical gate error probabilities P_g, we can compute the error floor of the FER before error correction as

$$FER \quad \sum_{i=1}^{D} {}_i P_g^i \quad \text{where} \quad {}_i = \binom{D}{i} : \tag{4.15}$$

where ${}_i$ is given by the binomial coefficient defined by i-combinations of D circuit components. The coefficients ${}_i$ is then reduced to q by the number of i-component failures, resulting in an error pattern corrected by syndrome recovery.

Figure 4.8: $R = \frac{1}{3}$ Repetition code in bit- ip channel with various channel ip probability P_e.

As for the frame error events caused by the pure bit- ip channel having a ip probability of P_e, at the right of Fig. 4.5 the state of having no qubit errors at the output of either the control or the target sub-block occurs with probability $(1 \quad P_e)^3$. A correctable single-qubit error in any position occurs with probability $3\,P_e(1 \quad P_e)^2$. Any uncorrectable error in either sub-block incurs a frame error, therefore the FER after the recovery operation can be calculated as

$$FER = 1 \quad \left[(1 \quad P_e)^3 + 3\,P_e(1 \quad P_e)^2\right]^2 : \tag{4.16}$$

Let us now combine the FER contributions of both the gate errors and bit- ip errors of Eq. (2.15). However, for simplicity, we consider only the dominant term of $i = 1$ in the gate error bound of Eq. (4.15), explicitly this is the dominant term, because having several instantaneous gate errors has a lower probability. Upon computing the decoded FER, we arrive at:

$$FER = 1 \quad \left[(1 \quad P_e)^3 + 3\,P_e(1 \quad P_e)^2\right]^2 + 2\,P_g + \quad 6P_e^2 + 2\,P_g : \tag{4.17}$$

Since the term of $6P_e^2$ in Eq. (4.17) can be deemed negligible, for the coded scheme to o er a FER improvement it is required that $P_g \quad 2P_e$. The repetition coding scheme has

Figure 4.9: $R = \frac{1}{3}$ Repetition code in the Bit- ip channel with various gate error values P_g.

$D = 7$ components, so we have $_1 = 7$ in Eq. (4.15), meaning that $e_1 = 2$ (as detailed in the next section).

In Figure 4.8 we have plotted the FER vs. the gate error probability for both an uncoded CNOT gate as well as for its $\frac{1}{3}$-rate repetition-coded counterpart using dashed and continuous lines, respectively. The FER results are parameterized by the bit- ip probability of our quantum channel model of Figure 4.5. The circles in the gure indicate the speci c P_g values, below which the $\frac{1}{3}$-rate repetition code provides FER reductions. The curves are parameterized by the bit- ip probability P_e de ned in Figure 4.5.

To elaborate further, Figure 4.9 shows that when P_g is smaller, the coded scheme provides more rapid FER improvements, achieving $FER \approx 2P_g$, where $6P_e^2$ is negligible. However, when we have $P_e \gg P_g$, the coded scheme's FER is dominated by the correlated gate error patterns encountered before recovery[3]. Therefore, the FER oor is determined by $2P_g$.

[3] For large $P_g > 0.1$ the discrepancy between the analytical estimation and the simulation results in Figure 4.9 is due to terms according to P_g^2, hence making a signi cant contribution to the nal analytical FER when P_g is large. It may be inferred that the occurrence of simultaneous two-gate errors is not recorded in the Monte Carlo simulation results for the sample size considered.

4.4.3 Transversal CNOT Gate Protected by Steane's Code

Since Steane's encoding circuit V is not fault-tolerant, its FER has an error floor according to

$$FER^{(1)} \quad {}_1P_g: \tag{4.18}$$

where $FER^{(1)}$ gives the FER according to single gate errors alone. The constant ${}_1$ is determined by the specific error patterns produced by single gate errors that cannot be corrected. This process is demonstrated in Fig. 3.4, where the error imposed on the first CNOT gate leads to a larger number of errors at the circuit output, causing error proliferation. Subsequent CNOT gates copy this error throughout the circuit. Therefore, the proliferation of the error resulting from the initial single gate failure results in multiple qubit errors that cannot be corrected at the circuit output. Since the initial CNOT gate failure occurred with probability P_g, this error event will add a term of $O(P_g)$ to the FER.

The independent gate error is modelled by assuming an error location at each two-qubit CNOT connection in the circuit. Each gate failure is simulated as a perfect gate followed by Pauli operators acting on the individual qubits defined by the statistics corresponding to the depolarizing channel [109]. All other component errors are modelled by a single-qubit depolarizing channel after the block labelled $\overline{U}_f$, as seen in Figure 4.4. This incurs a frame error rate of

$$FER^{(2)} \quad {}_2P_e^2; \tag{4.19}$$

where ${}_2$ is the number of two qubit error combinations in the block that cannot be corrected by the upper and lower syndrome decoder of Figure 4.6. Therefore, the $FER^{(2)}$ is the FER according to simultaneous two-qubit errors that cannot be corrected.

The coded scheme provides frame error rate improvements, when the resultant error rate is lower than that of the uncoded scheme, namely when $FER^{(1)} + FER^{(2)} < P_g + 2P_e$. Rearranging this gives the gate error threshold $P_g < P_{th}$, which is the gate error rate below which coded improvements are possible. This is defined by a condition for P_g and P_e in conjunction with one another. Therefore, the gate error threshold is given by

$$P_{th} = \frac{2P_e \quad {}_2P_e^2}{{}_1 \quad 1}; \tag{4.20}$$

which is the point at which the coded scheme starts to have a better FER than the uncoded scheme.

A drawback of this scheme is that the FER is improved in line with a reduction of $P_g < P_{th}$, as indicated in Fig. 4.10. Fig.3.4 shows that the proliferation of qubit errors by CNOT gates in Steanes code leads to the correlation of qubit errors at the output of the Steane encoding circuit. Therefore, a set of error patterns occurring with probability $O(P_g)$ consisting of $t > 1$ individual qubit errors accumulate before the transversal

Figure 4.10: FER of a transversal CNOT gate vs. the gate error probability P_g parameterized by various depolarizing probabilities P_e.

Figure 4.11: FER of a transversal CNOT gate vs. the depolarizing probability P_e parameterized by various gate error probabilities P_g. Analytical is determined by Eq. (4.20).

CNOT gate. Hence, the application of Steane's code introduces more errors than the uncoded scheme has, when the gate error probability is high. The e ects of error proliferation overloading the decoder are seen in Figure 4.11, where the resultant FER is lower-bounded at $20P_g$.

However, our results demonstrate that coding is indeed bene cial, when the statistically independent qubit decoherence probability P_e is approximately an order of magnitude higher than P_g for counteracting the e ects of correlated errors. This is due to the fact that Steane's code is capable of correcting statistically independent individual qubit errors, since it has a minimum distance of $d = 3$. More speci cally, Figure 4.10 shows that an uncoded system would su er from an FER oor at $2 \quad 10^{-3}$, when the qubit decoherence error probability is $P_e = 10^{-3}$. However, a Steane code assisted system is capable of reducing the FER below $2 \quad 10^{-3}$, provided that the gate error probability is lower than $P_{th} = 1:1 \quad 10^{-4}$.

4.5 Conclusion

Practical quantum circuits experience both gate-induced qubit errors with a probability of P_g as well as qubit errors imposed by the decoherence probability of P_e. We found that improved logical qubit reliability can be attained using non-fault-tolerant QECC's when P_e is an order of magnitude higher than P_g. However, this imposes a strict condition on our quantum channel model, where the channel parameters have to obey the speci c conditions unveiled in this treatise.

In this chapter, it has been shown that the gate errors inherent in non-fault-tolerant encoding circuits proliferated to an uncorrectable number of qubit errors, hence resulting in a high error oor at the circuit output according to Eq. (4.18). The results presented in Chapter 5 o er a solution to this problem by relying on `encoderless' QECCs, where the non-fault-tolerant encoding circuit is eliminated and replaced by a fault-tolerant alternative. This scheme allows information to be encoded with the aid of a fault-tolerant circuit, therefore reducing the error oor.

Chapter 5

Gate-Error-Resilient Quantum Steane Codes

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

5.1 Introduction

A QECC must be implemented by a fault-tolerant circuit that is capable of avoiding avalanche-like error-proliferation[1] in quantum gates. More explicitly, a fault-tolerant circuit limits the effects of a single gate error to a correctable number of qubit errors [66]. However, unfortunately many traditional encoding circuits are not fault-tolerant

[1] We define error-proliferation as the event when a single error in icts more than one error. This is in contrast to error-propagation, which passes on the same number of errors as its input. See Section 3.3.1.

[66, 9, 1]. This is because these circuits have two-qubit CNOT gate connections which have the property that a single qubit error propagates to many qubits, hence proliferating the errors [107]. In the previous Chapter, it was shown that this overwhelms the error correction capability of the $[n; k; d]$ QECC. Hence, more errors are inflicted by the circuit than are corrected, where n is the number of encoded physical qubits, k is the number of original information qubits, d is the minimum distance and t is the error correction capability where $t = b(d - 1)/2c$ for the family of maximum-minimum distance codes. Therefore, rather than satisfying our original objective of improving the error rates, the QECC failing to rely on a fault-tolerant architecture prepares encoded states that have a higher error rate than the original uncoded information [1].

To mitigate these problems, we present an alternative scheme that prepares encoded quantum states without applying non-fault-tolerant encoding circuits. More explicitly, this outputs an encoded state with a FER that is lower than that of the uncoded information[2], even when the gate error probability is high. This is achieved by using a circuit, which is entirely comprised only of single-qubit gates. Hence the resultant circuit has a fault-tolerant arrangement, in which no error proliferation can occur. Rather than directly encoding the information using a quantum error correction encoder, this `encoderless' scheme first prepares an n-qubit state that is a superposition of legitimate codewords or correctable error patterns. The resultant encoded state is carefully chosen so that any error patterns within the code's correction capability can be corrected by the syndrome decoder. As a benefit, following the action of the syndrome decoder, only valid codewords are created which represent the n-qubit encoded version of the k-qubit input information. Again we refer to our proposed method as the 'encoderless scheme'.

This approach is reminiscent of quantum state preparation techniques [10]. Further investigations of Steane code state preparation were presented in [122, 123, 109], where the logical states such as $|\bar{0}\rangle$ and $|\bar{+}\rangle$ are prepared fault-tolerantly. Improvements that minimize the ancilla qubit overheads required for Steane code state preparation were provided in [88]. In addition, methods of preparing the encoded states of longer codes were conceived in [124] for circumventing the employment of complex encoding circuits. Finally, state preparation assuming a local 2D-architecture was designed in [125].

The scheme presented here has the added benefit that it can be applied to unknown input information, implying that we have no prior knowledge of the state before encoding. In this paper, what is referred to as a 'known state' $|\psi\rangle$ is one whereby we do have prior knowledge of the value of the complex probability amplitudes α and β in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Therefore, with no knowledge about the value of α and β the state is said to be 'unknown'.

[2] See Section 4.3.1 for a definition of FER. A frame error event is defined as the occurrence of more than the number of correctable errors t.

Unitary encoding and decoding circuits are prone to the proliferation of errors, because the circuits are not fault-tolerant and therefore they in ict more errors than the QECC can correct [9, 107, 10]. The scheme presented in this paper o ers fault-tolerant encoding of unknown states with the aid of a single stabilizer measurement and two extra Hadamard gates. The ability to encode states with no prior knowledge of the information qubits will be necessary for systems relying on multiple networked devices. Another bene t of this scheme is that it has a simpler circuit than the state preparation schemes for certain known states [126]. This is advantageous in NISQ processors having limited qubit coherence times and error-infested circuit components [38]. However, the cost of this scheme is that it needs clean all-zero ancilla qubits in order to achieve fault-tolerance. In addition, this scheme relies on a full stabilizer measurement, which is costly compared to the non-fault-tolerant unitary encoding circuit in terms of qubit overheads[3] [1, 85]. Nevertheless, if the architectural assumptions of the stabilizer circuit are met by the processor, the `encoderless' scheme imposes no further connectivity constraints on the device. Therefore, the implementation is likely to be applicable to a number of state-of-the art devices, where the stabilizer measurements can be easily implemented.

The scheme operating in the face of combined gate error and quantum bit error channel model presented in [1] requires the gate error P_g to be an order of magnitude lower than the quantum bit decoherence probability P_e. This is the limitation imposed by the gate error in the encoding circuit. The error rate of the encoding circuit has an error oor according to single gate errors, therefore introducing an error rate on the order of $O(P_g)$ after syndrome decoding. This section presents a scheme which does not require encoding circuits, therefore reducing the probability of gate error in the encoder the order of $O(P_g^2)$ that can nevertheless encode an unknown state.

By simulating this scheme we can determine the e ect it may have on the error oor according to the gate error probability P_g. Therefore, we do not consider the e ects of the qubit depolarizing error probability P_e, as seen in Chapter 4. However, the combined error channel is considered, when simulating various state preparation techniques and comparing these to the encoderless scheme. These results show the e ect of an error on the input qubits according to P_e.

The rest of this chapter is structured as follows. First the design of `encoderless' QECCs is introduced in Section 5.2. This discussion follows from the fault-tolerant implementation of a stabilizer measurements detailed in Section 3.3.4 as well as from the non-destructive operator measurements associated with arbitrary input states discussed in Section 3.2.5. The analytical background for the scheme is detailed in Section 5.3 and Section 5.4, showing its resilience to individual gate error locations in each block of the

[3] For example, it is expected that an additional 60 ancilla qubits may be required for implementing a single Steane code stabilizer measurement fault-tolerantly. See Section 3.3.5 for a full explanation of this calculation.

Figure 5.2: Encoderless [3, 1, 3] Repetition Code.

circuits implementation. Then the simulation results of imperfect gates are presented in Section 5.4.2. Finally, in Section 5.5 the scheme is extended to specific state preparation protocols.

5.2 Encoderless QECC

State preparation techniques[4] are a scheme whereby a known state can be prepared without the application of the traditional encoder [110]. However, it is not yet understood if this approach can be pursued for encoding an unknown state [37], which we have no prior information concerning the probability and before encoding. This section proposes a scheme for solving this problem. In practice traditional unitary encoding circuits must be applied for encoding an unknown state.

5.2.1 Encoderless Repetition Code

Quantum information can be protected without an encoding circuit by preparing a legitimate and illegitimate codeword states in a superposition and then applying syndrome decoding to transform this to valid codeword states. A general outline of this concept can be found in Section 3.2.5. Let us now explore this idea in more detail with respect to the repetition code, first presented in Section 3.2.2. Firstly, let us compare the repetition encoded state[5] of

$$|\bar{\psi}\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle = \alpha|000\rangle + \beta|111\rangle, \tag{5.1}$$

to the state produced by the circuit that replaces the encoder by a pair of Hadamard gates, as shown in Figure 5.2. After applying both Hadamard gates to the unknown

[4] See Section 5.5 for a detailed explanation of these schemes.
[5] This is Eq. (3.4) in Section 3.2.2 reproduced here for convenience.

$\hat{R}^{(b)}$	$\|data\rangle\|ancilla\rangle$
III	$(\|000\rangle + \|111\rangle)\|00\rangle$
IIX	$(\|001\rangle + \|110\rangle)\|01\rangle$
IXI	$(\|010\rangle + \|101\rangle)\|10\rangle$
IXX	$(\|011\rangle + \|100\rangle)\|11\rangle$

Table 5.1: Error recovery operators $\hat{R}^{(b)}$ for the encoderless $[3,1,3]$ Repetition code.

input state of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the system is in the state

$$|\tilde{\psi}\rangle = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right). \tag{5.2}$$

Expanding this gives

$$|\tilde{\psi}\rangle = \frac{1}{8}\left(\underline{|000\rangle} + |001\rangle + |010\rangle + |011\rangle + \underline{|111\rangle} + |110\rangle + |101\rangle + |100\rangle\right). \tag{5.3}$$

The vectors that overlap with the state shown in Eq. (5.1) are underlined.

The vectors that are not underlined must be corrected to one of the valid code word states in Eq. (5.1). Additionally, the coefficients α or β have to be consistent with the encoded state of $\alpha|0\rangle + \beta|1\rangle$. For example, the vector $|100\rangle$ must be corrected to $|111\rangle$. This can be done by measuring the traditional repetition code stabilizers $K_1 = ZZI$ as well as $K_2 = ZIZ$ and then carrying out the recovery operations shown in Table 5.1. To elaborate these operations are similar to those based on the traditional repetition code (see [99]) except that when the ancilla qubits are in state $|11\rangle$, the bit flip correction is applied to both the second and third data qubits X_2X_3 ensuring that

$$\alpha|011\rangle + \beta|100\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle. \tag{5.4}$$

This is necessary because if the traditional single qubit correction X_1 was made, this would result in the state $\alpha|111\rangle + \beta|000\rangle$. In this case the coefficients are the wrong way around therefore the result is not consistent with Eq. (5.1). The aim of the scheme in Figure 5.2 is to ensure that $|\tilde{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle$.

Let us now describe the operations in Table 5.1 is discovered. The input state of Eq. (5.3) evolves under the measurement of the stabilizers K_1 and K_2 according to Eq. (3.22) and Eq. (3.23), this yields

$$|\tilde{\psi}_2\rangle = \frac{1}{2}|\psi\rangle + K|\psi\rangle \qquad |\tilde{\psi}_2\rangle = \frac{1}{2}|\psi\rangle - K|\psi\rangle. \tag{5.5}$$

Let us consider the example that a $|0\rangle$ is measured in both the ancilla qubits each described by Eq. (3.22). First, $|\tilde{}\rangle \to |\tilde{}_1\rangle$ when K_1 of Figure 5.2 is measured, given by

$$|\tilde{}_1\rangle = \frac{1}{2}\,|\tilde{}\rangle + ZZI\,|\tilde{}\rangle = |000\rangle + |001\rangle + |111\rangle + |110\rangle.$$

This state is then input to the measurement of the K_2 stabilizer. A $|0\rangle$ is also measured in the second ancilla qubit, giving

$$|\tilde{}_2\rangle = \frac{1}{2}\,|\tilde{}_1\rangle + ZIZ\,|\tilde{}_1\rangle = |000\rangle + |111\rangle. \tag{5.6}$$

This shows that the encoded state $|\bar{}\rangle$ is recovered without having to apply an error correction operation R.

Let us now check the effect of measuring the $|01\rangle$ ancilla states. After the K_1 stabilizer is applied, the system is in the same state, as described in Eq. (5.6). Then the second measurement of the K_2 stabilizer results in the $|1\rangle$ state in the ancilla qubit. This is described by Eq. (3.23), so in this case we have

$$|\tilde{}_2\rangle = \frac{1}{2}\,|\tilde{}_1\rangle - ZIZ\,|\tilde{}_1\rangle = |001\rangle + |110\rangle \tag{5.7}$$

and a bit flip recovery operation X_3 will return the state to $|\bar{}\rangle$. The same calculation can be done for the other two scenarios listed in Table 5.1.

Let us see the effect of measuring the $|10\rangle$ ancilla states. After the K_1 stabilizer is applied the system is in

$$|\tilde{}_1\rangle = \frac{1}{2}\,|\tilde{}\rangle - ZZI\,|\tilde{}\rangle = |010\rangle + |011\rangle + |101\rangle + |100\rangle. \tag{5.8}$$

The $|0\rangle$ state is measured in the second ancilla qubit, giving

$$|\tilde{}_2\rangle = \frac{1}{2}\,|\tilde{}_1\rangle + ZIZ\,|\tilde{}_1\rangle = |010\rangle + |101\rangle. \tag{5.9}$$

hence the $R = IXI$ correction operation recovers $|\bar{}\rangle$. Similarly, if the $|11\rangle$ ancilla state is measured, we have

$$|\tilde{}_2\rangle = \frac{1}{2}\,|\tilde{}_1\rangle - ZIZ\,|\tilde{}_1\rangle = |011\rangle + |100\rangle \tag{5.10}$$

and the $R = IXX$ correction operation recovers $|\bar{}\rangle$.

Furthermore, any single Hadamard gate error acts trivially on the state $|\tilde{}\rangle$. So even though at this step in the circuit the state is not strictly encoded in the state $|\bar{}\rangle$, the scheme is still robust against the gate errors of its preparation circuits. For example,

Figure 5.3: Encoderless transversal CNOT using the [3,1,3] Repetition Code.

a Hadamard gate error on the middle qubit can be described by IXI for the bit-flip channel $E(\cdot)$. The channel output is described by

$$E(|\tilde{\psi}\rangle) = IXI\,|\tilde{\psi}\rangle = |\tilde{\psi}\rangle; \tag{5.11}$$

where $|\tilde{\psi}\rangle$ is given by Eq. (5.3). This error takes one vector state in the superposition state $|\tilde{\psi}\rangle$ to another and preserves the coefficients α and β. Similarly a Hadamard gate error on qubit (3) has the same effect, namely $IIX\,|\tilde{\psi}\rangle = |\tilde{\psi}\rangle$. In fact, two simultaneous Hadamard gate errors occurring with probability P_g^2 is also trivial, since we have $IXX\,|\tilde{\psi}\rangle = |\tilde{\psi}\rangle$. Therefore, no possible gate error combination suffers from an error that cannot be corrected by the measurement of $\hat{S}$.

Note that the error correction operations must still be applied. Since the state in Eq. (5.3) consists of only $+1$ eigenstates of $\hat{S}$, the application of $\hat{R}$ results in $|\tilde{\psi}\rangle \to |\bar{\psi}\rangle$, as seen in Figure 5.2. In simple terms, the input state $|\tilde{\psi}\rangle$ is in a superposition of the code word states and correctable errors. This state is carefully designed in such a way that the unknown coefficients α and β are preserved after $\hat{R}$. So the unknown state $|\psi\rangle$ effectively ends up in the encoded state $|\bar{\psi}\rangle$ by the application of $\hat{S}$ and $\hat{R}$.

5.2.2 Encoderless Transversal CNOT Gate

The `encoderless' scheme depicted in Figure 5.3 applies the transversal CNOT gate $\overline{U}_{\text{CNOT}}$ to the control and target qubits $|\psi_1\rangle$ and $|\psi_2\rangle$. Both qubits are separately prepared in the partially encoded state in Eq. (5.3) with the addition of $n - k = 2$ ancilla qubits.

In this scheme the original repetition code recovery operation R is applied, therefore FER improvements are expected with the aid of R. This scheme applies the following transformation

$$\bar{U}_f(|\psi_1\rangle|\psi_2\rangle + |\psi_3\rangle|\psi_4\rangle + \cdots) \xrightarrow{S;R} \bar{U}_f(|\bar{\psi}_1\rangle|\bar{\psi}_2\rangle); \tag{5.12}$$

so that after syndrome decoding the control and target states $|\bar{\psi}_1\rangle$ and $|\bar{\psi}_2\rangle$ are encoded as well as transformed by the CNOT gate. Syndrome decoding is applied after the transversal CNOT gate since $\bar{U}_f$ commutes with S, see [1].

5.3 FER without Encoder

The FER before decoding at position $|\psi_2\rangle$ of Figure 5.3 is

$$FER_2 = 7P_g + 21P_g^2 \tag{5.13}$$

More explicitly, since this circuit construction is fault-tolerant, the term $7P_g$ can be ignored as any single gate error can be corrected by the syndrome decoders. Therefore, it is only necessary to consider the proportion of errors occurring owing to a pair of simultaneous gate errors. Given 4 Hadamard gates and 3 CNOT gates in the circuit there are 21 combinations of two simultaneous gate errors, so Eq. (5.13) can be re-written as

$$FER_2 = \alpha P_g^2 < 21P_g^2. \tag{5.14}$$

Therefore the upper bound[6] of the FER marked with a triangle in Figure 5.7 is

$$FER^{UPPER} = 21P_g^2. \tag{5.15}$$

The value of α in Eq. (5.13) is found by considering the probability that two simultaneous gate errors can be corrected, and subtracting this probability from $21P_g^2$.

There are three general categories that the 21 combinations of two simultaneous gate errors may take:

- Two simultaneous Hadamard gate errors (6 combinations),
- Two simultaneous CNOT gate errors (3 combinations),
- Simultaneous CNOT gate and Hadamard gate error (12 combinations),

These will be considered in each subsection that follows.

[6] This does not account for two simultaneous gate errors. In this case the errors will either cancel each other or be corrected, therefore reducing the final error rate.

CNOT 1	CNOT 2	Correctable
IX	IX	N
IX	XI	Y
IX	XX	N
XI	IX	Y
XI	XI	N
XI	XX	N
XX	IX	N
XX	XI	N
XX	XX	N

Table 5.2: Combinations of two simultaneous CNOT gate error in the bit- ip channel.

5.3.1 Two Simultaneous Hadamard Gate Errors

Let us start with analyzing the six combinations of two simultaneous Hadamard gate errors, which contributes $6P_g^2$ to FER_2. Firstly, a single qubit gate objected to the bit ip channel simply incurs an X error with a probability of P_g (namely the gate error). Therefore, more than qubit errors will be encountered, only when two Hadamard gates in the same encoded block impose an error in either the top or the bottom syndrome decoder of Figure 5.3. This only occurs in 2 out of the 6 two-Hadamard gate error combinations. Then two simultaneous Hadamard gate errors can be corrected with a probability of $4P_g^2$ giving $P_g^2 < 17P_g^2$.

5.3.2 Two Simultaneous CNOT Gate Errors

Figure 5.4: IX error on both CNOT 1 and CNOT 2 resulting in two qubit error input into the bottom encoder.

Furthermore, there are only three scenarios, where a pair of CNOT gates have an error simultaneously, which contributes a probability of $3P_g^2$ to FER_2. When we consider the two-qubit gate bit- ip error event of (IX , XI , XX) two CNOT gates su er from

an error, this gives 9 combinations, each occurring with a probability of $\frac{P_g}{3}\ \frac{P_g}{3}$. Each combination is listed in Table 5.2 and visualized in Figure 5.4. There are only two combinations that result in a single qubit error being input into the top and bottom syndrome decoder in Figure 5.4. Therefore, each time when two CNOT gates have an error simultaneously this may be corrected with a probability of $\frac{2P_g^2}{9}$. Then accounting for all three `two-simultaneous-CNOT-gate-error' combinations gives $P_g^2 < 16{:}3P_g^2$.

5.3.3 Simultaneous CNOT Gate and Hadamard Gate Error

Figure 5.5: A scenario where one error event cancels another. A Hadamard gate incurs an X error that is subsequently input to the control qubit of a CNOT gate, which itself has incurred an IX error.

Next there are twelve scenarios, where a Hadamard and a CNOT gate have an error simultaneously. There are two ways this could happen. Let us start with the simplest case namely which a Hadamard gate error is input to the CNOT gate, as shown in Figure 5.5. In this case there may be no more than one error entered into each syndrome decoder in Figure 5.5. This is because the transversal CNOT gate will not proliferate the input error to more than one error. Additionally, the CNOT gate error cancels the propagated Hadamard gate error. There are four scenarios, where a Hadamard gate is applied to a qubit before it is input to a CNOT gate - therefore we have $P_g^2 < 12{:}3P_g^2$.

Figure 5.6: X error imposed on a Hadamard gate occurring in the same encoded block as the control qubit error of a CNOT associated with an XI error.

H	CNOT	Correctable
X	IX	Y
X	XI	N
X	XX	N

Table 5.3: Combinations of a Hadamard gate error in the same encoded block as the target qubit of a simultaneous CNOT gate error in the bit ip channel. See Figure 5.6.

Figure 5.7: Transversal CNOT gate in the bit- ip channel with $[3;1;3]$ repetition code with and without the traditional encoding circuit.

The last 8 scenarios are where the Hadamard gate error is at a location that is either in an encoded block, but its output is not entered into that speci c CNOT gate, which has a simultaneous gate error, as shown in Figure 5.6. Table 5.3 shows that with a probability of $\frac{P_g^2}{3}$ this combination will not incur a $[3;1;3]$ frame error. This is valid for all 8 combinations. Hence the total associated probability is $\frac{8P_g^2}{3}$. Therefore, nally we get $P_g^2 < 9{:}7P_g^2$, which gives $9{:}7$ in Eq. (5.13). Consequently the lower bound marked with a circle in Figure 5.7 is given by

$$FER^{LOWER} = 9{:}7P_g^2. \tag{5.16}$$

Figure 5.7 shows the upper and lower bound of the FER to be derived in this section for the `encoderless' scheme with a channel model, whereby each CNOT and Hadamard gate is a potential source of error location with a gate error probability of P_g. Having

Figure 5.8: Encoderless Steane Code with three Hadamard Gates.

introduced the basis of the `encoderless' scheme, let us now focus our attention on the more practical Steane code in the next section.

5.4 Encoderless Steane Code

The scheme of Figure 5.8 replaces the traditional $n = 7$ qubit unitary encoding circuit V seen in Figure 3.4 in Section 3.2.3. Ordinarily, the encoder V is applied to both the unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and to $(n - k)$ auxiliary qubits as follows[7]

$$|\bar{\psi}\rangle = V(|\psi\rangle |0\rangle^{(n-k)}). \tag{5.17}$$

This achieves the encoded state,

where we have:

$$\begin{aligned}|\bar{\psi}\rangle = & \frac{\alpha}{\sqrt{8}}|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ & + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle + \\ & \frac{\beta}{\sqrt{8}}|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ & + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle : \end{aligned} \tag{5.18}$$

Let us compare this to the state produced by the circuit that replaces the encoder by three Hadamard gates, as shown in Figure 5.8. After applying the Hadamard gates

[7] This is Eq. (3.3) in Section 3.2.3, reproduced here for convenience.

Figure 5.9: Full Scheme of the Transversal CNOT gate with the `encoderless' Steane code.

below the unknown input state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the system is found in the state

$$|\tilde{\psi}\rangle = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|000\rangle. \tag{5.19}$$

Expanding this gives

$$\begin{aligned}|\tilde{\psi}\rangle = \frac{\alpha}{\sqrt{8}}[&|\underline{0000000}\rangle + |0010000\rangle + |0100000\rangle + |0110000\rangle \\ &+ |0001000\rangle + |0011000\rangle + |0101000\rangle + |0111000\rangle] + \\ \frac{\beta}{\sqrt{8}}[&|\underline{1110000}\rangle + |1000000\rangle + |1010000\rangle + |1100000\rangle \\ &+ |1001000\rangle + |1011000\rangle + |1101000\rangle + |1111000\rangle].\end{aligned} \tag{5.20}$$

The underlined vectors represent those that overlap with the conventionally encoded state shown in Eq. (5.18). The vectors that are not underlined represent errors that can be corrected. Then by the same reasoning as for the repetition code of Section 5.2.1, the encoded state in Eq. (5.18) is fixed after the application of the stabilizer operators in Eq. (3.7).

Figure 5.10: Encoderless Steane Code with two Hadamard Gates.

Then the vectors that are not underlined are corrected by the syndrome decoder of Figure 5.9. This is shown by Eq. (3.22). We can readily see that the encoded state in Eq (5.18) can be recovered by the following calculations

$$
\begin{aligned}
|\tilde{\underline{1}}\rangle &= \frac{1}{2}(|\tilde{i}\rangle + K_1|\tilde{i}\rangle) \\
|\tilde{\underline{2}}\rangle &= \frac{1}{2}(|\tilde{\underline{1}}\rangle + K_2|\tilde{\underline{1}}\rangle) \\
|\tilde{\underline{3}}\rangle &= \frac{1}{2}(|\tilde{\underline{2}}\rangle + K_3|\tilde{\underline{2}}\rangle) \\
|\tilde{\underline{4}}\rangle &= \frac{1}{2}(|\tilde{\underline{3}}\rangle + K_4|\tilde{\underline{3}}\rangle) \\
|\tilde{\underline{5}}\rangle &= \frac{1}{2}(|\tilde{\underline{4}}\rangle + K_5|\tilde{\underline{4}}\rangle) \\
|\tilde{\underline{6}}\rangle &= \frac{1}{2}(|\tilde{\underline{5}}\rangle + K_6|\tilde{\underline{5}}\rangle) = |\bar{i}\rangle ; \qquad (5.21)
\end{aligned}
$$

where K_1 to K_6 corresponds to the Steane code stabilizers in Eq. (3.7). Therefore, the `encoderless' schemes can be readily combined with transversal gates in the same way, as described for the repetition code of Section 5.2.2. The full scheme is shown in Figure 5.9.

5.4.1 Further Improvements

The number of Hadamard gates in the scheme seen in Figure 5.9 can be reduced to as few as two, which is shown in Figure 5.10. Let us elaborate on this scenario by using the same method as that in the previous section. If we have $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$, the top encoded qubit of Figure 5.10 can be described by

$$|\tilde{\psi}\rangle = |0\rangle \quad (\alpha|0\rangle + \beta|1\rangle) \; |0\rangle \quad \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \; |0\rangle \quad \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) |0\rangle. \tag{5.22}$$

This may be expanded to give

$$\begin{aligned} |\tilde{\psi}\rangle = \frac{\alpha}{\sqrt{8}}[\underline{|0000000\rangle} + |0000010\rangle + |0001000\rangle + |0001010\rangle] + \\ \frac{\beta}{\sqrt{8}}[\underline{|0101010\rangle} + |0101000\rangle + |0100010\rangle + |0100000\rangle], \end{aligned} \tag{5.23}$$

where the underlined vectors overlap with the conventionally encoded state in Eq. (5.18). After the application of the syndrome decoder, the encoded state in Eq. (5.18) can be recovered as shown in Eq. (5.21).

This methodology can also be applied to other codes, where the positioning of Hadamard gates and of the original information qubit $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ are arranged for ensuring that a single vector belonging to the logical $|\bar{0}\rangle$ appears with an $\frac{\alpha}{\sqrt{2}}$ coefficient. Likewise, a single vector belonging to the logical $|\bar{1}\rangle$ state appears with an $\frac{\beta}{\sqrt{2}}$ coefficient. Therefore, where the code satisfies the property that $|\bar{1}\rangle = X^{\otimes 7}|\bar{0}\rangle$ the vectors with the smallest (classical) weight indicate the position of the smallest number of Hadamard gates. Then the application of the stabilizer measurements projects this expansion to the correctly encoded state $|\bar{\psi}\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$. Therefore, it is feasible that the broad class of QSC may exhibit `encoderless' properties, provided that stabilizer measurements can be implemented fault-tolerantly.

5.4.2 Simulation Results & Discussions

Figure 5.11 shows that the FER upper bound of the `encoderless' scheme is $FER = 78P_g^2$ which is derived by the probability of two simultaneous gate errors of Figure 5.9 by Eq. (4.15) in Section 4.4. To recap, this is

$$FER \leq \sum_{i=1}^{D} \alpha_i P_g^i \quad \text{where} \quad \alpha_i = \binom{D}{i}. \tag{5.24}$$

Observe in Figure 5.11 that the simulation results appear to be better than the estimated `upper bound' indicating that there are certain simultaneous two-gate errors that actually impose qubit error that can be corrected by the syndrome decoder. The gate

Figure 5.11: Encoderless scheme comparing the systems of Figure 5.9 (3H) and Figure 5.10 (2H). The analytical circle represents the upper bound. The analytical results marked by squares is calculated according to Section 4.4.3

.

error rate below which the scheme o ers an CNOT gate accuracy better than an uncoded gate is seen to be $P_{th} = 0.024$. Naturally we aim for $P_g < P_{th}$. Furthermore, to achieve a FER less than 10^{-4} this scheme requires individual components having a gate error probability lower than 10^{-3}, as seen in Figure 5.11.

The encoderless scheme provides better-than-uncoded FER performance for both the bit- ip and depolarizing channel, as seen in Figure 5.11. This is because the scheme dispenses with the non-fault-tolerant traditional encoding circuits, which increase the qubit error probability owing to error proliferation. Therefore, the encoderless scheme of Figure 5.10 provides a compelling proof-of-concept for implementing QECCs fault-tolerantly without any initial assumption about the information being computed. Moreover the encoderless scheme provides a FER improvement for Steane's code even when constructed from imperfect gates.

QECCs constructed based on traditional encoding circuits have the advantage that they are capable of encoding unknown information. However, these circuits are not fault-tolerant [66]. Hence techniques of encoding known information without a traditional encoding circuit have been investigated in [9, 110, 127] for example. However, these schemes have the drawback that only certain simple quantum states can be encoded. By contrasting the scheme presented here circumvents these issues by using stabilizer

measurements for encoding unknown states. This means that an additional error correction step is required, which has a substantial qubit overhead, when implemented fault-tolerantly, as described in Section 3.3.4. Nevertheless, these results provide a proof-of-concept for the family of the techniques that are capable of encoding any arbitrary information without the need for non-fault-tolerant encoding circuits.

5.5 State Preparation

Figure 5.12: Preparing the known state $|\bar{0}\rangle$ encoded by the Steane code using the stabilizer measurements of K_1, K_2 and K_3 in Eq. (3.7).

This section investigates how the known state $|\psi\rangle = |0\rangle$ can be encoded by applying certain Steane code stabilizers to a specific input state [9]. This circumvents the application of the traditional unitary encoding circuit characterised by Eq. (3.6) albeit with the drawback that the state that is being encoded must be known [66]. The basic idea is that the stabilizers K_1, K_2 and K_3 in Eq. (3.7) are applied to the all-zero qubit input state $|\tilde{\psi}\rangle = |0\rangle^{\otimes 7}$, as shown in Figure 5.12. This gives $|\bar{\psi}\rangle = |\bar{0}\rangle$ in Eq. (3.8), which is the encoded version of $|\psi\rangle = |0\rangle$. It is not necessary to apply the full stabilizer set, because $|\tilde{\psi}\rangle = |0\rangle^{\otimes n}$ is already a +1 eigenvalue of K_1, K_2 and K_3 [110].

Let us consider the most straightforward scenario, whereby the measurement of the stabilizers K_1, K_2 and K_3 in Eq. (3.7) results in the $|0\rangle$ state in the ancilla, as described by Eq. (3.23). If the measurement of $K_1 = IIIXXXX$ results in $|0\rangle$ in the ancilla, the system is in the state of

$$|\tilde{\psi}_1\rangle = \frac{1}{2}\left(|\tilde{\psi}\rangle + K_1|\tilde{\psi}\rangle\right) = |0000000\rangle + |0001111\rangle. \tag{5.25}$$

This state is input to the $K_2 = XIXIXIX$ stabilizer, which is also measured in the $|0\rangle$ state. Then $|\tilde{\psi}_2\rangle$ describes the system after this measurement

$$|\tilde{\psi}_2\rangle = \frac{1}{2}\left(|\tilde{\psi}_1\rangle + K_2|\tilde{\psi}_1\rangle\right) = |0000000\rangle + |0001111\rangle + |1010101\rangle + |1011010\rangle. \quad (5.26)$$

Finally the $|0\rangle$ state is measured in the ancilla, when the $K_3 = IXXIIXX$ stabilizer is applied to the state in $|\tilde{\psi}_2\rangle$. This gives

$$|\tilde{\psi}_3\rangle = \frac{1}{2}\left(|\tilde{\psi}_2\rangle + K_3|\tilde{\psi}_2\rangle\right) = |0000000\rangle + |0001111\rangle + |1010101\rangle + |1011010\rangle + |0110011\rangle + |0111100\rangle + |1100110\rangle + |1101001\rangle = |\bar{0}\rangle; \quad (5.27)$$

which is the Steane encoded $|\bar{\psi}\rangle = |\bar{0}\rangle$ in Eq. (3.8).

Once the encoded $|\bar{0}\rangle$ state is prepared, it becomes possible to prepare the encoded version of any arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, provided that we know the value of α and β [9]. This is possible as long as the processor has an encoded universal gate set as de ned in [128]. This will mean that any arbitrary gate operation can be applied to the encoded data allowing the encoded zero state to be transformed to any arbitrary superposition of code word basis states. For example, we might like to prepare the encoded state $|\bar{\psi}\rangle = |\bar{1}\rangle$, where $\alpha = 1$. This can be done by preparing the $|\bar{0}\rangle$ state as outlined above and then applying the transversal bit- ip gate as follows

$$\bar{X}|\bar{0}\rangle \rightarrow |\bar{1}\rangle; \quad (5.28)$$

therefore preparing $|\bar{\psi}\rangle = |\bar{1}\rangle$. Similarly, to prepare the encoded version of the equi-probable superposition state of

$$|\bar{\psi}\rangle = \frac{|\bar{0}\rangle + |\bar{1}\rangle}{\sqrt{2}} = |\bar{+}\rangle; \quad (5.29)$$

the same method is employed. First the encoded $|\bar{0}\rangle$ state in Eq. (3.8) is prepared, followed by the application of the transversal Hadamard gate,

$$\bar{H}|\bar{0}\rangle \rightarrow \frac{|\bar{0}\rangle + |\bar{1}\rangle}{\sqrt{2}}. \quad (5.30)$$

Likewise, the encoded $|\bar{-}\rangle$ state is prepared using Eq. (5.28) as follows;

$$\bar{H}|\bar{1}\rangle \rightarrow \frac{|\bar{0}\rangle - |\bar{1}\rangle}{\sqrt{2}} = |\bar{-}\rangle. \quad (5.31)$$

Figure 5.13: With traditional Steane encoder.

Figure 5.14: Without an encoder using 3 Hadamard gates.

Figure 5.15: Preparing the unknown Steane encoded $|\bar{\psi}\rangle$.

5.5.1 System Model

In this system the encoded version of various single qubit states is encoded by the Steane code, therefore in general this system has the transformation $|\psi\rangle \rightarrow |\bar{\psi}\rangle$. This is seen in 5.14, 5.13 and Figure 5.18, where any unknown state is prepared.

Figure 5.16: Preparing $|\bar{0}\rangle$

Figure 5.17: Preparing $|\bar{1}\rangle$

The known state preparation constituted a specific case of these schemes, as seen in Figure 5.16, 5.17 and 5.19. For example in Figure 5.16 we can see that $|0\rangle \rightarrow |\bar{0}\rangle$. The encoded $|\bar{1}\rangle$ described in Eq. (5.28) is shown in Figure 5.17.

Moreover, the encoded $|\bar{+}\rangle$ described in Eq. (5.30) is shown in Figure 5.19. Each scheme is simulated in the face of gate errors as well as qubit decoherence error probability of P_e before the syndrome decoder in Figure 5.16, 5.17 and 5.19. Therefore, Figure 5.19 has an additional syndrome decoder, meaning that the $|0\rangle$ state is prepared to achieve the transformation seen in Eq. (5.30). There may be circuit implementations that have a reduced number of syndrome decoding steps, reminiscent of the approach taken in Section 5.2.2. However, this is not explored here. Since a single qubit state is encoded (not a quantum gate) the uncoded scheme has an error rate of $FER = P_e$.

Figure 5.18: Preparing the unknown Steane encoded $|\overline{-}\rangle$ state without encoder using two Hadamard gates.

Figure 5.19: Preparing the Steane encoded $|\overline{+}\rangle$ state.

Summary of Fig. 5.20-5.25			
Fig.	P_g	P_e	FER
5.20-5.21	$5 \quad 10^{-3}$	10^{3}	10^{4}
5.22-5.23	10^{2}	10^{4}	10^{4}
5.24-5.25	10^{3}	$5 \quad 10^{4}$	10^{5}

Table 5.4: Table summarising the results in Figure 5.20-5.25 for the 2H encoderless scheme.

Figure 5.20: FER vs. P_g for State Preparation aided Steane encoded states at $P_e = 10^{-2}$.

Figure 5.21: FER vs. P_g for State Preparation aided Steane encoded states at $P_e = 10^{-3}$.

Figure 5.22: FER vs. P_g for State Preparation aided Steane encoded states at $P_e = 10^{-4}$.

5.5.2 Results and Discussion

In this simulation we assume that both the stabilizer and the error recovery circuits of Figure 5.16, 5.17 and 5.19 are fault-tolerant (see Section 3.3.4) and incur a negligible error rate. Therefore, the FER associated with preparing the encoded $|\bar{0}\rangle$ state has an error floor according to $\frac{7}{2} P_e^2$. The scheme shown in Figure 5.18 demonstrates the best FER performance of encoding an unknown input state. See Table 5.4 for a summary of results of this scheme in Figures 5.20-5.25. This is due to the low complexity of its circuit, which helps in limiting the error proliferation. For example, when $P_e = 0.01$ (Figure 5.20) and $P_g = 0.005$ the scheme relying on a traditional encoding circuit has a FER 386% higher than the encoderless scheme using two Hadamard gates. To achieve $FER \approx 10^{-5}$, a gate error probability of $P_g = 5 \times 10^{-5}$ and $P_e = 10^{-3}$ are required, as shown in Figure 5.21. In this case the encoderless 2H scheme achieves a FER almost two orders of magnitude lower than that of the uncoded scheme. Where the gate error probability is $P_g > 10^{-3}$, then $FER < 10^{-4}$ can be achieved, provided that the qubit decoherence is below ($P_e = 10^{-4}$), as seen in Figure 5.22.

When the gate error probability is as high as $P_g = 0.01$, the encoderless scheme achieves only a modest improvement on the uncoded scheme, namely a 24% reduction in FER at $P_e = 10^{-4}$, as seen in Figure 5.23. However, Figure 5.24 shows that when the gate error probability is $P_g = 10^{-3}$, then a qubit decoherence at $P_e = 5 \times 10^{-4}$ can be tolerated,

Figure 5.23: FER vs. P_e for State Preparation aided Steane encoded states at $P_g = 10^{-2}$.

Figure 5.24: FER vs. P_e for State Preparation aided Steane encoded states at $P_g = 10^{-3}$.

Figure 5.25: FER vs. P_e for State Preparation aided Steane encoded states at $P_g = 10^{-4}$.

while still achieving $FER < 10^{-5}$. In this case the `Three Hadamard Gate Encoderless scheme' reduces the error rate by three orders of magnitude compared to the scheme using the traditional encoder. This is because the circuit in Figure 3.4 is not fault-tolerant and therefore the gate error probability dominates the FER. For even further improvements a smaller gate error is required, as seen in Figure 5.25, where $P_g = 10^{-4}$.

5.6 Conclusion

The encoderless scheme achieves better FER performance since the complexity of the circuit it reduced. The arrangement of fewer single qubit gates means that the circuit is fault-tolerant leading to a FER crossover with the uncoded scheme, where $P_g < P_{th}$. However, the scheme relies on the application of a fault-tolerant stabilizer measurement. The implementation of this is described in Section 3.3.4, where it is shown that additional ancilla qubits and repeated circuit blocks are required for a fault-tolerant design, meaning that this scheme may require further resources to be implemented practically. The results presented in this chapter also show that this can be applied to state preparation where the encoderless quantum codes outperform the preparation of $|\bar{1}\rangle$, $|\bar{+}\rangle$ and $|\bar{-}\rangle$ states. However, the simplicity of the preparation of the $|\bar{0}\rangle$ state means that this

achieves the best FER performance. These schemes o er signi cant improvements on the traditional encoder which cannot o er a FER better than the uncoded scheme.

Future research may seek to apply this scheme in SoA quantum processors to obtain an experimental estimate of the practical error-rate improvements according to a noise model of interest. For this to be possible, the encoderless circuit of Steane's code requires a speci c qubit layout associated with a su cient number of qubits. In addition, to apply the stabilizer measurements, the processor must have the capability carrying out measurements mid-computation as well as of applying classically controlled quantum operations. This functionality is indeed feasible on near-term devices.

Chapter 6

Turbo-coded Secure and Reliable Quantum Teleportation

Figure 6.1: The outline of this thesis with the highlight of Chapter 6.

6.1 Introduction

Quantum teleportation is a communication protocol that transmits the information using an arbitrary and unknown quantum bit (qubit) without the physical transmission of that speci c qubit [129]. The single qubit state can be represented by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$, as described in Section 2.2. This qubit can be teleported from the transmitter to the receiver by using the transmission of classical information and with the aid of an additional entangled pair of qubits. Without the transmission of

the qubit $|\psi\rangle$ itself, the teleportation protocol reconstructs a replica of the original qubit at the receiver using the classical information communicated over the classical channel as well as one of the pre-shared entangled qubit that was communicated over the quantum channel. Hence, a quantum teleportation system has a dual classical-quantum channel. More explicitly, information about the qubit $|\psi\rangle$ is extracted at the transmitter by a Bell measurement and the outcome is then communicated to the receiver over the classical channel. This information determines the appropriate application of single-qubit gates on the pre-shared qubit for reproducing the original state $|\psi\rangle$ of the teleported qubit at the receiver. Note that before the measurement, the quantum channel was used for sharing one of the entangled qubits from the transmitter to receiver.

However, the teleportation protocol is only effective provided that there is a low level of noise in the implementation hardware and both the classical and quantum transmissions are error free. Hence, quantum error correction must be incorporated for protecting the transmission of the pre-shared entangled qubit. Similarly, classical error correction is also needed for reliable transmission of the measurement results from the transmitter to the receiver. It is also necessary to ensure the security of the transmission, especially in the quantum channel.

Error in either the classical or quantum channel (or both) can reduce the fidelity of the final teleported qubit. It is often assumed that channel error can be negligible in the teleportation protocol. However, this assumption must be removed when the teleportation scheme is implemented practically. On one hand, teleportation has been widely considered for applications in secured communication, quantum networking and quantum repeaters, as well as some conceptual applications in quantum information theory [130]. Further advances in Quantum communications are available at [91, 92, 93, 94, 95].

However, practical investigation of error correction aided practical teleportation scheme is still lacking. Against this backdrop, this chapter investigates a practical teleportation scheme, where both the classical and quantum channels exhibit errors. The effect of channel errors is investigated with the aid of both classical Turbo Codes (TC) [131] and Quantum Turbo Codes (QTC) [132]. Then, secure quantum teleportation protocols are explored by authenticating entangled qubit pairs via a trusted third-party and with the aid of Quantum-Secure-Direct-Communication (QSDC) [133] scheme.

This chapter is organized as follows. The results disseminated in [3] are discussed in terms of the enhanced error rate attained by the application of turbo codes to both the classical and quantum information transmitted. The basic philosophy of quantum teleportation protocol is described in Section 6.2, where the channel is assumed to be perfect. Teleportation over imperfect channels is then investigated in Section 6.3 and Section 6.4, while a secure teleportation scheme is proposed in Section 6.5 using QSDC and QTC. Finally our conclusions are offered in Section 6.6.

6.2 Teleportation over Perfect Channels

Figure 6.2: Quantum teleportation protocol [129].

In this section, the Quantum Teleportation (QT) protocol [129] is described based on error-free classical and quantum channels. The aim of teleportation is to send the information of an arbitrary unknown qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ from the transmitter to the receiver without the transmission of the qubit itself. The circuit that can achieve teleportation is shown in Figure 6.2.

As seen in Figure 6.2, the protocol begins with three qubits. First of all, qubit 1 is the qubit for the teleportation, which is in an arbitrary unknown state $|\psi\rangle$. Secondly, qubits 2 and 3, which are in the zero state, will be entangled and they will be shared between the transmitter and the receiver. This initial state can be described as follows:

$$|\psi\rangle|0\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle = \alpha|000\rangle + \beta|100\rangle. \tag{6.1}$$

To recap, the Hadamard gate[1] has the following transformation on the computational basis states $\{|0\rangle, |1\rangle\}$:

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{6.2}$$

reproduced from Eq. (2.24). Applying a Hadamard gate to the second qubit in Eq. (6.1) would give:

$$\begin{aligned} \alpha|00\rangle + \beta|10\rangle &\xrightarrow{H} \alpha\frac{|00\rangle + |01\rangle}{\sqrt{2}} + \beta\frac{|00\rangle - |01\rangle}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|001\rangle + \beta|100\rangle - \beta|101\rangle). \end{aligned} \tag{6.3}$$

Then, a CNOT gate is applied between qubit 2 and qubit 3. If a control qubit (qubit 2) is in the $|1\rangle$ state the CNOT gate applies a NOT gate to the target qubit (qubit 3), as exempli ed in Eq. (2.18), reproduced here for convenience:

$$\begin{aligned} |10\rangle &\xrightarrow{CNOT} |11\rangle \qquad |00\rangle \xrightarrow{CNOT} |00\rangle \\ |01\rangle &\xrightarrow{CNOT} |01\rangle \qquad |11\rangle \xrightarrow{CNOT} |10\rangle. \end{aligned} \tag{6.4}$$

[1] See Section. 2.3.3.

Hence, the application of the CNOT gate to qubits 2 and 3 in Eq. (6.3) would give:

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|000\rangle + |010\rangle + |100\rangle + |110\rangle) \xrightarrow{\text{CNOT}} \\ &\quad \frac{1}{\sqrt{2}}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) \\ &\quad = (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned} \tag{6.5}$$

At this point qubits 2 and 3 are entangled in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, known as the Einstein-Podolsky-Rosen (EPR) pair [134]. At this point, qubit 3 of the entangled EPR pair can be transmitted to the receiver over an error-free quantum channel, while qubit 2 will be retained at the transmitter.

Next, a bell state measurement [135] will be applied to qubit 1 and 2, where qubit 1 is the unknown qubit for teleportation. To make a bell-state measurement, the CNOT and Hadamard gates are applied between qubits 1 and 2, as seen in Figure 6.2, before the measurement [9]. The CNOT gate evolves Eq. (6.5) as follows:

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) \xrightarrow{\text{CNOT}} \\ &\quad \frac{1}{\sqrt{2}}(|000\rangle + |011\rangle + |110\rangle + |101\rangle); \end{aligned} \tag{6.6}$$

while a Hadamard gate on qubit 1 would further transform Eq. (6.6) to:

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|000\rangle + |011\rangle + |110\rangle + |101\rangle) \xrightarrow{H} \frac{1}{\sqrt{2}}\left[\frac{|000\rangle + |100\rangle}{\sqrt{2}} \right. \\ &\quad \left. + \frac{|011\rangle + |111\rangle}{\sqrt{2}} + \frac{|010\rangle - |110\rangle}{\sqrt{2}} + \frac{|001\rangle - |101\rangle}{\sqrt{2}}\right]: \end{aligned} \tag{6.7}$$

After collecting the terms with the same values in the first and second qubits in Eq. (6.7), we obtain:

$$\begin{aligned} &\frac{1}{2}(|000\rangle + |001\rangle) + (|011\rangle + |010\rangle) + (|100\rangle - |101\rangle) + (|111\rangle - |110\rangle) \\ &\quad = |00\rangle\frac{|0\rangle + |1\rangle}{2} + |01\rangle\frac{|1\rangle + |0\rangle}{2} |10\rangle\frac{|0\rangle - |1\rangle}{2} + |11\rangle\frac{|1\rangle - |0\rangle}{2}; \end{aligned} \tag{6.8}$$

which gives the system before the measurement at the transmitter. The measurements of qubits 1 and 2 could be in any of the following combinations: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. These measurements can then be communicated over a classical channel to the receiver as seen in Figure 6.2. Note that after the measurement, qubit 1 has been destroyed.

If the measurement bits are given by 10, then the state of the pre-shared qubit 3 has been changed to $\frac{1}{2}(|0\rangle - |1\rangle)$. It is possible to transform qubit 3 to the state of qubit 1 (before measurement) based on the lookup table of Table 6.1, where X and Z refers to

the bit and phase- ip gates de ned by the X and Z Pauli operators [9]. More speci cally, when the measurement results are $;1$0, the receiver should apply the$Z$ gate to qubit 3. This will transform qubit 3 to the original state of qubit 1 as follows:

$$j0i \quad j1i! \overset{Z}{} \quad j0i + \quad j1i = j \quad i: \tag{6.9}$$

The corresponding lookup table mapping all possible measurement results to quantum gate operations is given in Table 6.1.

Table 6.1: Gate operation applied to qubit 3 according to the measurement results.

State	Measurement	Qubit 3 state	Gate Correction
$j00i$	0,0	$j0i + j1i$	I
$j01i$	0,1	$j1i + j0i$	X
$j10i$	1,0	$j0i \quad j1i$	Z
$j11i$	1,1	$j1i \quad j0i$	XZ

6.3 Teleportation over Imperfect Classical Channel

Figure 6.3: Reproduction of Figure 6.2 with imperfect classical and quantum channel.

In this simulation an unknown arbitrary qubit $j \ i$ is teleported based on a perfect quantum channel but an imperfect classical Rayleigh fading channel. As described in the previous section, the classical bits determine the activation of the$X$ and Z gates at the receiver. The correctly applied combination of gates is essential in order to accurately resurrect the state of qubit 1 $j \ i$ at the receiver.

The classical bits m_1 and m_2 of Figure 6.3 can take four combinations, namely 00, 01, 10 and 11. However, only when both m_1 and m_2 are transmitted perfectly can the X and Z gates be enabled or disabled properly at the receiver. For example, if qubit 1 is in the state $j0i + j1i$ the measurement result for transmission would be 00. In this case, the identity gate$I$ gate is applied at the receiver (see Table 6.1) to obtain the nal state $j \ i$. However, if the corrupted classical bit sequence 01 is received instead, then

an X gate is mistakenly applied as follows:

$$|0\rangle + |1\rangle \xrightarrow{X} |1\rangle + |0\rangle \neq |\psi\rangle; \tag{6.10}$$

which produces a quantum bit-flip error in the reconstructed qubit 1. Therefore, an error in the classical channel can induce a quantum error on the teleported qubit 1.

Note that a single error on either m_1 or m_2 as well as simultaneous error, on both m_1, m_2, will result in only a single quantum error on the teleported qubit. For example, if the erroneous bit combination $m_1 = 0, m_2 = 1$ is applied at the receiver to the qubit in the previous example, then

$$|0\rangle + |1\rangle \xrightarrow{XZ} |1\rangle - |0\rangle \neq |\psi\rangle; \tag{6.11}$$

however this will be counted as only a single qubit error[2].

6.3.1 Bit-Error-Ratio

If N^c classical bits are transmitted and N^c is the number of erroneously received classical bits then the Bit-Error-Ratio (BER) is given by:

$$BER = N^c/N^c. \tag{6.12}$$

Likewise, the Quantum-Bit-Error-Ratio (QBER) is given by:

$$QBER = N^q/N^q; \tag{6.13}$$

where N^q is the total number of teleported qubits and N^q is the total number of erroneously teleported qubits.

More specifically, the teleportation of N^q number of qubit 1 (as shown in 6.2) requires the transmission of $N^c = 2N^q$ classical bits for conveying the two measurement results from the transmitter to the receiver. If there are N^c classical bit errors, the worst case[3] would be when only one error occurs in each of the two measurement results, giving rise to $N^q = N^c$ qubit errors. Hence, the corresponding QBER upper bound would be given by $QBER = N^q/N^q = N^c/(0.5N^c) = 2\,BER$.

Figure 6.4: QBER/BER versus SNR performance when communicating over Rayleigh fading channel using uncoded BPSK, 4QAM, 8PSK, 16QAM and 64QAM schemes.

6.3.2 Classical Turbo Coded Teleportation

Recall that for each recovered teleported qubit, two classical bits $(m_1; m_2)$ must be accurately received. Figure 6.4 shows the QBER/BER versus Signal to Noise Ratio (SNR) performance when communicating over Rayleigh fading channel using uncoded modulation schemes.

The SNR is defined as $SNR = E[h_r^2]P_t/N_0$, where h_r is the Rayleigh fading channel coefficient, P_t is the transmit power and N_0 is the variance of the additive white gaussian noise.

The effect on QBER is consistent with the relationship explained previously, which is given by:

$$QBER \quad 2BER : \tag{6.14}$$

TCs [131] are popular classical channel coding scheme for mitigating the effect of channel fading and channel noise. TCs were first proposed in [131] and they showed a remarkable error correction performance under certain conditions, with only 0.7 dB disparity [136] compared to the Shannon limit, which was regarded as impossible before the invention of TCs. TCs take advantage of parallel-code concatenation at the encoder, having

[2] Note that classically-induced errors are different from those imposed by the imperfect quantum channel. This is denoted by P_e^q in Figure 6.3 and it is discussed further in Section 6.4

[3] For example, a single error imposed on either of the pair of classical bits, as well as a simultaneous error on both classical bits, will result in a single quantum error. Therefore, the `worst case' is a single bit error, since this is all that is necessary to cause a qubit error.

Figure 6.5: QBER/BER versus SNR performance when communicating over Rayleigh fading channel using uncoded BPSK and TC-4QAM having 1, 2 and 8 decoding iterations.

an interleaver between the two component codes. At the decoding side, an iterative decoder based on two soft-input-soft-output (SISO) decoders is invoked for exchanging soft extrinsic information between the two component decoders.

Figure 6.5 shows that the QBER of the teleportation protocol can be improved by introducing TC in the classical transmission. Furthermore, an increased number of decoding iterations would allow the soft information from each decoder to be exchanged more effectively, leading to a more accurate bit recovery. However, to achieve a BER level of 10^{-5} the performance of the 4-iteration and 8-iteration based schemes are relatively close[4]. As a good trade-off between performance and complexity, the 4-iteration based TC scheme is chosen for our study[5].

6.4 Teleportation over Imperfect Quantum and Classical Channels

6.4.1 Quantum Depolarizing Channel

We have shown that errors in the classical channel lead to quantum errors in the teleported qubits and that this can be improved by classical turbo coding. In this section we consider errors in both the classical and quantum channels. Depolarizing error probability P_e^q is the probability having a quantum error in the quantum channel over which

[4] Monte Carlo simulation considered is 10^7 samples.

[5] $\frac{1}{2}$-rate TC with generator polynomial [G_0 = (111), G_1 = (101)], 1200 bits per frame.

qubit 3 is transmitted, as shown in Figure 6.3. The quantum depolarizing channel [137] is characterized by three possible error events, namely the quantum bit- ip error, the phase ip error, and the combination of the two (the simultaneous occurrence of both bit and phase ip errors). Explicitly, a bit- ip error is equivalent to the transformation using a NOT gate (or Pauli X gate) and is similar to a classical bit- ip. For example, a bit- ip error has the e ect that $|0\rangle \$ |1\rangle$ on the computational basis states. On the other hand, a phase- ip error is equivalent to the transformation using the Z gate, where $|1\rangle \$ -|1\rangle$ while $|0\rangle \$ |0\rangle$ is left unchanged. Additionally, the bit-and-phase ip error is equivalent to the transformation using both X and Z gates, for example $|0\rangle \rightarrow -|1\rangle$. The probability each of these error events occurring is assumed to be equivalent in the standard quantum depolarizing channel, i.e. each occurs with a probability of $P_e^q/3$.

Figure 6.3 shows that the pre-shared qubit 3 (denoted as $|\$_{tx}\rangle$) may arrive corrupted at the receiver (denoted as $|\$_{rx}\rangle$) due to the quantum depolarizing channel. Let us consider this scenario in more details, assuming that $|\$_{tx}\rangle = -|1\rangle + |0\rangle$ has a quantum bit- ip (X) error occurs during the transmission, then

$$|1\rangle + |0\rangle \xrightarrow{X} |0\rangle + |1\rangle. \tag{6.15}$$

This would lead to an error to the transported qubit 1 (denoted $|\ \rangle$).

Let us now further describe the quantum channel error probability as P_e^q. For example, $P_e^q = 10^{-1}$ is equivalent to 1 corrupted qubit in ten pre-shared corrupted qubit 3 at the receiver, i.e. $|\$_{rx}\rangle \neq |\$_{tx}\rangle$. Let us de ne the total number of transmitted pre-shared qubits as N^q and the total number of corrupted transmitted qubits as $\overline{N}^q$. Then the QBER at the quantum channel is given by

$$P_e^q = \overline{N}^q / N^q. \tag{6.16}$$

6.4.2 TC-Teleportation over Imperfect Quantum Channel

As described in Section 6.3.1, the QBER is approximately twice of the BER, when the quantum channel is error free. With the addition of the imperfect quantum channel, the upper bound of the QBER is now given by:

$$QBER \leq 2BER + P_e^q. \tag{6.17}$$

This is an upper bound since there are certain scenarios where the classical and quantum channel errors cancel each other. Figure 6.6 shows various P_e^q values and the corresponding BER varying from 0.5 to 10^{-6}. The QBER follows the trend of Eq. (6.14), when P_e^q is small, as expected. For example, when the quantum channel error probability is

Figure 6.6: QBER versus BER curves of the turbo coded 8PSK assisted scheme when communicating over the Rayleigh fading channel. The qubit depolarizing probability considered are $P_e^q = (10^{-1}; 10^{-2}; 10^{-3}; 10^{-4}; 10^{-5}; 0)$.

Figure 6.7: QBER versus SNR performance of the turbo coded 8PSK assisted scheme when communicating over the Rayleigh fading channel. The qubit depolarizing probability considered are $P_e^q = (10^{-1}; 10^{-2}; 10^{-3}; 10^{-4}; 10^{-5}; 0)$.

given by $P_e^q = 10^{-4}$, we have $QBER \approx 2BER$ for $BER > 10^{-4}$. In this case, the classical channel error dominates the QBER at the region of $BER > 10^{-4}$. However, when $P_e^q > BER$, the QBER converges to the P_e^q value in the form of an error floor. This is because the quantum error is now dominating the QBER, according to Eq. (6.17).

Figure 6.7 shows the QBER versus SNR performance of the turbo coded 8PSK assisted scheme when communicating over the Rayleigh fading channel. Since the BER of the classical channel reduces as SNR increases, we notice that the QBER has an error floor at P_e^q at high SNR region, as expected.

6.5 Quantum Turbo Coded Secure Teleportation

As seen previously in Figure 6.2, teleportation requires an entangled qubit pair (qubits 2 and 3), which are prepared at the transmitter and then one of them (qubit 3) is communicated to the receiver over the quantum channel. This section describes an alternative method whereby an EPR pair is distributed via an authentic third party, where each qubit in the entangled pair is communicated to the transmitter and receiver, separately. This way the teleportation protocol is applied at the transmitter without any knowledge of the location of the receiver. This adds a layer of security to the generation of the entangled qubits and the transmission of the EPR pairs. The only drawback of this approach is that a quantum memory is required to store the EPR pair before its distribution. However, this arrangement is more secure compared to that in Figure 6.2.

When the entangled qubits are shared securely then the quantum teleportation can be considered absolutely secure. This is because the measurement results are only beneficial to the eavesdropper, when the transmitted qubit 3 is in the eavesdropper's possession. The addition of an authentic third-party means that quantum teleportation can be used as a one-time-pad scheme and therefore can be employed for secure quantum communications [138]. Explicitly, an entangled qubit pair can be considered as a key for each teleportation. Once security of the key is certified, then the transmission process can be deemed to have unconditional security [139].

However, provided that the EPR pairs are transmitted from an authenticated third party there exists a risk that the qubits can be exploited by an eavesdropper. The security of the EPR pair that is distributed via the quantum channel can be examined based on the characteristics of quantum entanglement [140]. On the one hand, any measurements of either of the qubits in an entangled pair disturbs the entanglement state, which ultimately results in an equivalent pure state. If the eavesdropper intercepts the transmission of the EPR pairs, it could therefore be discovered immediately. On the other hand, if the eavesdropper first intercepts the transmission of either qubit and resends it after some manipulations, the whole structure of the original entanglement is

altered. Nevertheless, this attack can be detected if the transmitted and received qubit in the EPR pair are measured and the outcomes are compared [141].

For example, consider the transmission of the EPR pair $|AB^{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where qubit A is kept at the transmitter and qubit B is transmitted to the receiver. If the eavesdropper prepares the same EPR pair, namely $|CD^{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and then captures the qubit $|B\rangle$, then the system can be described by [142]:

$$|AB^{00}\rangle|CD^{00}\rangle = \frac{1}{2}(|AC^{00}\rangle|BD^{00}\rangle + |AC^{01}\rangle|BD^{01}\rangle + |AC^{10}\rangle|BD^{10}\rangle + |AC^{11}\rangle|BD^{11}\rangle); \quad (6.18)$$

where

$$|i^{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|i^{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$
$$|i^{11}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle): \quad (6.19)$$

Eq. (6.18) shows that if the eavesdropper measures $|BD^{00}\rangle$ then the other qubits are in the state $|AC^{00}\rangle$. Therefore, the original entangled state $|AB^{00}\rangle$ is no longer valid and the qubits $|A\rangle$ and $|B\rangle$ are no longer entangled. When the qubits are no longer entangled, its measurement outcomes can no longer determine the measurement result of the other qubit. In other words, the QBER will be very high when the eavesdropper is present and this phenomenon can be used for secure quantum transmissions as explained in Section 6.5.1.

6.5.1 Secure and Reliable Teleportation

Figure 6.8: QTC aided Quantum-Secure-Direct-Communication.

In this section a secure and reliable quantum teleportation based on the Quantum Turbo Code (QTC) of [132] and the Quantum-Secure-Direct-Communication (QSDC) of [133] is investigated. Provided that the security of pre-shared entangled qubit pairs has been ensured, the teleportation process would be unconditionally secure and therefore the protocol only concentrates on the security of the quantum channel. Furthermore, the QTC-decoded entangled pairs are more reliable compared to the uncoded scheme. Our proposed secure and reliable teleportation protocol seen in Figure 6.8, can be explained below:

1. Prepare n pairs of EPR qubits
   Half of these qubits are to be communicated from the transmitter and to the receiver via a quantum depolarizing channel[6]. To do this the each of the n EPR pairs is prepared in the state $|\Phi^{00}_{tx,rx}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

2. Prepare m dummy EPR pairs
   These qubits are to be inserted to the original EPR qubit pairs at secret locations. The dummy EPR pairs are in the state $|\Phi^{01}_{tx,rx}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. This protocol becomes more precise for a larger value of m, as the dummy EPR pairs are used to detect the eavesdropper.

3. Encode with QTC
   There are now $(n + m)$ EPR pairs, which are encoded with a $\frac{1}{2}$-rate QTC to produce $2(n + m)$ qubit pairs in total.

4. Decode with QTC
   The corresponding QTC decoding process is implemented at the receiver[7] and is based on the error syndromes [143, 144]. If the syndrome indicates that a qubit is erroneously bit flipped, an X gate correction is applied at the receiver. Then after QTC decoding, $(n + m)$ qubits are restored at the receiver.

5. Measure m dummy qubits
   The measurement of the decoded dummy qubits can be used to determine the severity of eavesdropping that may have occurred. The location of the dummy qubits is communicated to the receiver. These qubits are measured at the receiver and the results are sent back to the transmitter. If there is no eavesdropper in the quantum channel, then the results obtained at the receiver should be opposite to that at the transmitter (since the dummy qubits are in state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, when the quantum channel is error-free.

6. Evaluate the secure error ratio
   The quantum communication is deemed secure if the QBER of the dummy qubits

[6] If a third party is used to prepare these EPR qubit pairs, then half of the EPR pairs will be communicated to the transmitter and the other half to the receiver [138].

[7] QTC decoding at the transmitter is also needed, if the EPR pairs are prepared by a third party [138].

is below a certain chosen security threshold (this threshold will be explained in Section 6.5.2). When the QBER of the dummy qubits is below the threshold, then the n pairs of pre-shared EPR qubits (qubits 2 and 3 of Figure 6.2) are considered secure. Then the decoded EPR pairs can be used for teleportation. However, if the QBER of the dummy bits is higher than the threshold, then this indicates that the transmission has been intercepted and the whole transmission process should be discarded and the protocol should restart from step 1.

7. Teleportation of information qubits
   When the EPR pairs are secure and reliable, then the teleportation of information qubits (qubit 1 in Figure g:teleportation) based on classical measurement bits, as described in Section 6.2 can proceed correspondingly.

Figure 6.9: Channel depolarizing error probability P_e^q (uncoded) versus QTC-decoded error probability $P_e^q(QTC)$. The QTC of [144] was considered.

Note that dummy entangled qubit pairs are used in QSDC, while random entangled qubit pairs are also needed for the Bell inequality testing in the device-independent QKD. Hence, it is a good future research to compare the performance of these systems, in terms of the e ciency in using these entangled qubit pairs.

6.5.2 Secure Error Ratio Threshold with QTC

Step 6 in the previous section requires a secure error ratio threshold to compare with the error ratio of the dummy qubits in order to establish if an eavesdropper was present during the qubit transmission. This must be determined carefully with the aid of the QTC. The secure error ratio can be speci ed from Figure 6.9, where the x-axis P_e^q

corresponds to the depolarizing error probability in the quantum channel, while the y-axis shows the corresponding error ratio (denoted as $P_e^q(QTC)$) after applying the QTC.

Suppose that the channel depolarizing probability without eavesdropping is given by $P_e^q = 0:31$. It is reasonable to assume that eavesdropper would introduce at least further 10% of error to the channel depolarizing probability. This would make the overall channel-plus-eavesdropper depolarizing probability to be $P_e^q > 0:41$ As we can see from Figure 6.9 that after the application of the QTC of [144], say, with an interleaver length of 6000 qubits the corresponding QBERs are $P_e^q(QTC) = 7 \quad 10^{-6}$ for $P_e^q = 0:31$ and $P_e^q(QTC) > 0:4$ for $P_e^q < 0:41$. Hence, without QTC, the 10% additional error introduced by the eavesdropper may be hard to detect when the quantum channel has a high depolarizing error probability. However, with the aid of QTC, the QBER di erence between the cases for having no eavesdropper ($P_e^q(QTC) = 7 \quad 10^{-6}$) and with eavesdropper ($P_e^q(QTC) > 0:4$) is signi cantly larger. In other words, the employment of QTC would make the detection of the eavesdropper easier. The reliability of the pre-shared qubits is also signi cantly improved from $P_e^q = 0:31$ to $P_e^q(QTC) = 7 \quad 10^{-6}$, when the eavesdropper is not present. Interested readers are referred to [144] for details of QTC.

To determine this threshold, it is assumed that the eavesdropper will impose a further 10% error contribution to the channel error rate. Let us elaborate brie y on this assumption. For example, if all $n + m$ qubits are intercepted by an eavesdropper in a perfect quantum channel in icting no errors, due to the process of detecting an error in the transmitted EPR pairs, only half of the corrupted qubits will be detected [133]. Note that this is an ine ciency of the simple QSDC scheme considered here, which can be improved upon by implementing a variation on QSDC, such as those in [145, 146, 147, 148].

For many theoretically investigated schemes the security proof may assume a perfect quantum channel. However, a noisy quantum channel can either reduce the e ciency of detecting the eavesdropper or make this impossible altogether, since the error rate of the dummy qubits determines if an eavesdropper is deemed to be present in the channel [149]. Therefore, the approach presented here provides a method of improving the security of a QSDC protocol in noisy channel conditions by introducing QTC. In this case, the detection probability of the eavesdropper is improved when $P_e^q = 0:31$. In di erent channel conditions the same approach can be pursued, by considering the error contributed by an eavesdropper according to the speci c version of QSDC that has been implemented, and by adjusting the parameters of the QTC according to P_e^q. Therefore, a secure error rate threshold can be obtained that is relevant to the speci c transmission scenario.

6.5.3 Reliable Quantum Teleportation

Based on the discussions so far, it is clear that both classical TC and QTC can be used to improve the reliability of the teleportation scheme. More explicitly, when QTC is employed, the over QBER of teleported qubits (qubit 1 of Figure g:teleportation) given in Eq. (6.17) can be rewritten as:

$$QBER = 2BER + P_e^q(QTC) ; \tag{6.20}$$

where $P_e^q(QTC)$ is the QBER of the QTC-aided transmission of the pre-shared qubits over the quantum channel. If the BER is controlled to a relatively low level using the classical TC, then the QBER error oor can be reached with lower SNR in the classical channel as seen in Figure 6.6.

As seen in Figure 6.6, in order to attain $QBER < 10^{-4}$ the corresponding BER must also be $BER < 10^{-4}$. Figure 6.7 shows that this condition can be met with an SNR higher than 8dB. In addition, with the implementation of QTC, $P_e^q(QTC) = 10^{-4}$ is achieved when the depolarizing probability is $P_e^q = 0:327$ with the application of a 6000-bit interleaver, as shown in Table 6.2. A larger depolarizing probability of $P_e^q = 0:334$ can be tolerated if the interleaver length is doubled to 12000. Hence, the stronger the encoding scheme, the more reliable and secure the teleportation system become.

Table 6.2: Tolerated quantum channel depolarizing probability (P_e^q) as a function of the turbo interleaver length and the target QTC-decoded QBER ($P_e^q(QTC)$). This is based on Fig. 6.9.

$P_e^q(QTC)$	Intlv. 3000	Intlv. 6000	Intlv. 12000
10^{-2}	0.331	0.336	0.339
10^{-3}	0.326	0.332	0.336
10^{-4}	0.321	0.327	0.334
10^{-5}	0.281	0.321	0.331

6.6 Conclusion

We have investigated the performance of a TC and QTC aided quantum teleportation scheme, when communicating over a Rayleigh fading channel and an imperfect quantum channel. The upper bound of the quantum error ratio was derived, which depends on the quality of both classical and quantum channels.

A QTC-aided secure transmission of pre-shared entangled qubits based on the QSDC protocol was investigated. More explicitly, the employment of QTC was found to be very useful for detecting eavesdroppers when the quantum channel is imperfect, as explained in Section 6.5.2.

More quantitatively, the proposed secure and reliable quantum teleportation scheme can achieve $QBER = 10^{-4}$ when the quantum channel depolarizing probability is as high as $P_e^q = 0.327$, if a QTC having an interleaver length of 6000 qubits is invoked for the transmission of the pre-shared qubits, while a classical TC is invoked to protect the classical transmission of the measurement results, as shown in Table 6.2.

Chapter 7

Experimental Characterization of Fault-Tolerant Circuits

Figure 7.1: The outline of this thesis with the highlight of Chapter 7.

7.1 Introduction

There are a number of QECC's that may be suitable for constructing fault-tolerant gate sequences at the time of writing. The family of attractive short QECC's includes the 5-qubit code of [33], the 7-qubit Steane code [31], topological codes [65] and the 9-qubit Shor code [29]. Fault-tolerant versions of these codes are prevalent [66, 10], but since the quantum hardware is still in its infancy, the functionality and architecture of the devices limits the choice of which QECC scheme can be tested. Fault-tolerant versions of

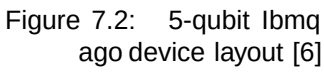

Figure 7.2: 5-qubit Ibmq Santiago device layout [6].

Figure 7.3: 7-qubit Ibmq Casablancadevice layout [6].

a QECC often require many more qubits than just those used to encode a logical qubit. These overheads increase rapidly due to the need for multiple error correction iterations and ancilla check measurements. These processes often require a device that has multiple re-initialised ancilla qubits, as well unique qubit connectivity and classically controlled quantum operations. Therefore, experimental demonstrations of a fully fault-tolerant QECC with all the necessary steps such as repeated error detection and correction are still in the early stages of testing.

There are a few considerations when selecting a quantum error correction code for experiments run on small-scale openly accessible state-of-the-art (SoA) devices. Figure 7.2 and Figure 7.3 show the device layout for the IBM Quantum (IBMQ) 5-qubit ibmq_santiago mode and for the 7-qubit ibmq_casablancadevice[1], respectively [6]. These devices have a general qubit layout with certain two-qubit connections in a two-dimensional architecture. The general architecture of the device determines the possible placement of two-qubit gates in the physical circuit. For example, in Figure 7.2, a CNOT gate may be placed between $q_0 ! q_1$, but is not possible between $q_0 ! q_4$. Therefore, in addition to having a su cient number of available qubits, the circuit which applies the QECC in the proposed experiment must also be able to accommodate the speci c qubit layout.

The limited functionality of SoA devices may also impose limitations on the extent to which error correction and detection can be applied. Methods that apply an error correction sub-routine typically require the measurement of a stabilizer or parity check operation to detect the presence of errors. Then the output of this measurement is successively forwarded to the necessary error correction regime. Therefore, to implement a typical measurement-based QECC the device must have the capability of carrying out a measurement during a particular computation and then input the result to a classically-controlled quantum gate. In addition, schemes that apply measurement-free error correction typically require a speci cally-crafted device layout, whereby the code word qubits have nearest-neighbour connections with multiple ancilla qubits. Furthermore, this type of scheme is supported by ancilla qubits that can be reinitialized multiple

[1] Figure reproduced from Section 1.2.2.

times during a circuit's execution, so that the device architecture does not require an excessive number of connections to codeword qubits. Nevertheless, these features are theoretically realisable and there is rapid progress in expanding the capabilities of open-access devices underpinning the promise that a fully fault-tolerant implementation of a QECC may be possible in the near future.

Given these limitations of the existing hardware, the $[[4, 2, 2]]$ QECC is chosen for this study, as a bene t of its straightforward implementation relying on low qubit overheads requiring only 4-5 qubits. This is because the fault-tolerant version only requires a single additional ancilla qubit [10]. Moreover, it is an error-detection code that relies on post-selection, which can be ful lled in classical post-processing, circumventing multiple ancilla measurements in support of their circuit-based application.

7.1.1 State-of-the-Art Experiments

Previous characterizations of the $[[4, 2, 2]]$ code have shown that the preparation of an encoded state and small-scale gate sequences o er an overall logical error rate improvement compared to its uncoded counterpart in the same device [96, 57]. In [57], arti- cially in icted errors were inserted, showing that indeed fault-tolerant circuit designs are robust to error proliferation. Vuillot demonstrated [60] that small-scale encoded logical gates relying on error detection capability succeed in providing error-rate improvements, when the highest quality pair of qubits on the device are targeted. The comparison between non-fault-tolerant and the equivalent fault-tolerant circuits showed that the fault-tolerant design will have a lower logical error rate. It was also shown that the error rate of the circuit was in uenced by the choice of the state sampled at the circuits output, observing that Pauli gate errors had less dramatic e ct on the output distribution, when sampling from an equi-probable superposition of logical states.

Wilsch et. al. compared various devices [61], showing that the fault-tolerance criterion was only satis ed when certain types of underlying errors are present in the hardware, such as preparation and measurement errors of the IBM devices. However, the dominance of decoherence errors in the spin qubit device meant that it failed to demonstrate fault-tolerance, despite applying a similar scheme. Further investigations in [63, 97] conclude that the overall performance improvement attained by the QECC coded scheme can be explained by the low circuit overheads involved in applying the most error-prone gates, namely two-qubit gates, in the logical code space.

Against this backdrop, the results to be presented in this chapter show that the $[[4, 2, 2]]$ code satis es the fault-tolerance criterion, because the uncoded scheme contains a larger number of two-qubit gates. However, we observe that the error rate of the coded scheme should still be signi cantly lower than what is observed and should also scale with the gate sequence length. Therefore, it is concluded that Pauli gate errors do not constitute

the most important source of error in terms of quantifying the ultimate delity of the circuit. It will also be shown that post-selection may fail to x certain proliferated qubit preparation errors. Furthermore, the encoding circuit may be very sensitive to those gate errors, which cannot be represented by the pure Pauli gate error model or to those that cannot be mitigated by post-selection[2].

The structure of this chapter is as follows. First, a fault-tolerance criterion is de ned for our experiments using current-day quantum processors in Section 7.2.1, against the traditional de nition presented in Chapters 4 and 5. This is followed by Section 7.2.2, which outlines the system design for SoA quantum experiments. The $[4,2,2]$ error detection code is presented in Section 7.2.4 as well as the reasoning for its suitability for these experiments. In Section 7.4 we de ne a simple Pauli-gate error model, which is compared to the experimental results of the $[4,2,2]$-encoded gate sequences in Section 7.5.

7.2 Experiment Design Using the [4,2,2] Code

7.2.1 Quantum Fault-Tolerance Criterion

In Section 7.2.1.1 we will recap a traditional de nition of fault-tolerant circuits as described in Section 3.3.3 [9]. Then in Section 7.2.1.2 we de ne a fault-tolerance criterion more speci cally suited to small-scale near-term experiments [59].

7.2.1.1 Fault Tolerant Circuit Design

Accordingly, we say that in a fault-tolerant circuit, an error from a single component will not overload the QECC, hence incurring zero logical errors after an error-correction step [9, 10]. By contrast, a qubit error introduced by an individual gate of a non-fault-tolerant circuit can be proliferated to a larger number of errors by the application of noiseless successive gates[3]. In other words, this has the e ect of introducing an increased number of qubit errors into the circuit (see Section 3.3.1). For example, when a single bit ip error XI is imposed on the control qubit of a CNOT gate, it will be copied to the target qubit and consequently the higher weight error of XX will be output. Therefore, in a highly connected circuit having numerous independent qubits a single qubit error may overwhelm a QECC's error correction capability. More explicitly, a quantum circuit protected by an $[n,k,d]$ QECC is only deemed fault-tolerant if a single component error results in less than $t = \lfloor (d-1)/2 \rfloor$ individual qubit errors at the output of the circuit,

[2] An over-rotation (or under-rotation) of the Hadamard gate in the encoding circuit may introduce an error that cannot be corrected in post-selection. Furthermore, the non-fault-tolerant encoding circuit implemented in this experiment may proliferate an error occurring during the preparation of the initialised qubit register. See Section 7.5.2 for further discussion.

[3] Note that this example and de nition assumes a simple error model relying on interdependent component errors. De nitions relying on more practical assumptions can be found in [18, 150, 123].

where the code is capable of correcting t errors upon using hard decisions.

De nition 1 . A QECC is said to be fault-tolerant if an error occurring in a single circuit component results in either t or less than t individual qubit errors at the output of the circuit block [9].

This general de nition can be veri ed either numerically or by simulation. For example, if a single component error occurs with probability p, the simulated error rate of the coded circuit block[4] is $p_c = O(p^2)$, provided that the probability of a component error is independent. This is because all single component errors occurring with a probability order of $O(p)$ proliferate to qubit errors that can be corrected during an error correction step when the circuit design is fault-tolerant. However, eliminating the error from a single gate error will not remove circuit error entirely. The qubit error that cannot be corrected will occur from any con guration of two or more simultaneous gate errors. Nevertheless, a circuit that satis es this de nition of fault-tolerance will exhibit an error rate improvement over the corresponding uncoded circuit, i.e. $p_c < p_u$, because the uncoded scheme has an error rate with probability $O(p)$.

There are many fault-tolerant circuit designs satisfying De nition 1 [9, 37]. This framework has historically been veri ed using simulations, which rely on analytical error models that are assumed to imitate a real quantum processor. Using these models, diverse component error rate thresholds have been derived [150, 123]. Therefore, it has been shown that an arbitrarily long computation becomes possible, provided that the components operate below the maximum tolerable error rate [19, 151]. The value of this speci c error rate threshold depends both on the noise model assumed, as well as on the particular choice of the fault-tolerant technique employed, and on whether the model has been determined analytically or by simulation. Simple versions of these models rely on an unbiased depolarizing channel su ering from independent single-qubit errors [9] or from correlated errors using a general Hamiltonian framework [18, 150, 123].

Given that several quantum processors are accessible in the cloud, it is possible to include experimental results in the process of developing fault-tolerant QECC's for characterizing device-speci c errors. Naturally, it is desirable for the noise within the real device to be accurately characterised for the model obtained. This model may be limited to the parameters that de ne the most likely error patterns that occur in the device, hence making the calculations simple enough for an e cient classical simulation. The response of the fault-tolerant protocol to these parameters would also have to be known, and then the QECC can be speci cally designed for the particular device considered. At this point

[4] Therefore, within this circuit block, two simultaneous component errors occur with probability $O(p^2)$, provided that the probability of a component error is independent.

a benchmark component error rate may be derived and bespoke hardware improvements can be recommended.

However, we have to strike a trade-o between the complexity and accuracy of the classical simulation of the noise model. In this context, it is quite challenging to infer the error rate in icted by an individual noise source in an interconnected circuit [152]. For example, repeated activation of a speci c gate may incur its own nuanced interaction or there may be multiple ways a gate incurs an error. In some cases, the gate error rates determined using the randomized benchmarking technique of [153] may exclude certain types of gate-coherence errors[5].

7.2.1.2 Criterion for Small-Scale Experiments

Therefore, the prediction of how a QECC will in uence the estimated error phenomena rate occurring in a real device may be most straightforwardly carried out by a full experimental implementation of a QECC, which characterizes all sources of circuit errors. The methodology of [59] provides a starting point for de ning fault-tolerance within the constraints of near-term devices. An experiment conducted using a prototype quantum processor may be said to demonstrate fault-tolerance when:

(a) the error rate of the encoded circuit D_c is shown to be lower than that of its uncoded counterpart D_u;

(b) it is a complete circuit implementation, which includes the initial state preparation and nal measurement;

(c) the output distribution of the encoded circuit is equivalent to that of the uncoded circuit;

(d) both the encoded and uncoded experiments are run on the same device.

For example, if the scheme satis es $D_c < D_u$, it is deemed to be fault-tolerant as long as the experimental assumptions (b)-(d) are upheld. The error rate of the circuit output $D_{u;c}$ is quanti ed in terms of the trace distance metric of the experimental outcome with respect to the ideal outcome de ned in more detail in Section 7.3.

De nition 2 A QECC demonstrates fault-tolerance in a small-scale quantum experiment when it satis es $D_c < D_u$ [59].

[5] A coherence error can be thought of as something like a calibration error [154]. This is an over or under-rotation of the gate each time the gate is called. See Section 7.5.2 and Appendix 9.3.

Directly characterizing fault-tolerant QECCs on an experimental quantum processor has a number of bene ts. The results characterize the response of the QECC to the total noise model of the device [155]. Therefore, the experimental results incorporate both gate errors as well as qubit preparation and measurement errors, plus the e ects of repeatedly activating components without any simplifying assumptions concerning the independence or correlation of error sources. The drawback of this however is that some coarse assumptions are required concerning the most likely source of error at the hardware level in order for the fault-tolerant protocol to be speci cally optimised for the particular device at the software level. Nevertheless, the resultant bene t is that a speci c characterization of the device appears to be unnecessary for this approach. Therefore, the combination of experimental results with a simpli ed classical simulation may be the most convenient process of advancing the understanding of fault-tolerance in QECCs for practical purposes.

7.2.2 Experiments Relying on Open Quantum Software

Figure 7.4: Schematic of the experiments design where $\mathcal{M}$ denotes a quantum measurement. Furthermore, the red boxes indicate that the outcome is derived classically and the blue boxes represent a quantum experimental result. Finally, I and E are the ideal and the experimental outcome distribution, respectively, while P-S denotes classical post-processing.

The results presented in this Chapter are obtained from the IBM Quantum cloud-based platform [6]. Figure 7.4 represents a schematic of the methodology used for classifying a

Figure 7.5: Example of the uncoded version of a $L = 2$ gate sequence according to Figure 7.4 in IBMQ [6]. This includes the logical gate sequence $H_0 H_1$ SWAP$_{0;1}$; cz$_{0;1}$ $Z_0 Z_1$ and a final measurement.

Figure 7.6: Example of the coded version of the same $L = 2$ gate sequence as Figure 7.5. This includes the initial $|\bar{0}\bar{0}\rangle$ state preparation circuit (non-fault-tolerant version) followed by logical gate sequence $H_0 H_1$ SWAP$_{0;1}$; cz$_{0;1}$ $Z_0 Z_1$ and a final measurement.

[4; 2; 2]-encoded circuit as fault-tolerant by comparing the uncoded and the corresponding encoded version of a gate sequence. The gate sequence length L refers to the number of successive logical gates in the circuit that is being tested. For example, in the scenario of a QECC-protected quantum algorithm, the sequence length L would correspond to the number of gates in the circuit. The total circuit depth is given by the number of physical gates required for the implementation of the QECC applied to the qubit register plus that of the required logical gates. To elaborate, this encompasses both the encoding circuit as well as the physical gates that implement each individual logical gate. Therefore, the total physical gate count of the circuit corresponds to the circuit that is directly implemented in the hardware.

Accordingly, a unique gate sequence is generated for a sequence length L and the corresponding physical circuit is then constructed for both the uncoded and encoded scheme. The encoded version includes both the encoding circuit and the final measurement (denoted by M in Figure 7.4). The separate uncoded and encoded circuits are then implemented by the same hardware sequentially, represented by the pair of dashed boxes in Figure 7.4. The uncoded circuit is realized both by a classical simulator (denoted I) as well as by the quantum hardware (denoted E) to obtain the uncoded error rate D_u. Likewise, the encoded circuit is realised by both the classical and quantum hardware to obtain the coded error rate D_c. An example of the full circuit for an equivalent $L = 2$ uncoded and coded gate sequence is shown in Figure 7.5 and Figure 7.6 respectively.

The circuit shown in Figure 7.5 is represented by the dashed box at the left of Figure 7.4. Likewise, Figure 7.6 is represented by the dashed box at the right of Figure 7.4.

The $L = 2$ gate sequence in Figure 7.5 is the $H_0H_1 \quad SWAP_{0;1}$ gate[6] followed by the $cz_{0;1} \quad Z_0Z_1$ gate (see Table 7.1 in Section 7.2.5 for the de nition). The uncoded circuit in Figure 7.5 shows each gate separated by circuit barrier, with a measurement at the end of the circuit (black squares). The corresponding encoded version of the circuit is shown in Figure 7.6. The rst section of the circuit is the encoding circuit (see Section 7.2.4). This is followed by the equivalent encoded version of the $H_0H_1 \quad SWAP_{0;1}$ and $cz_{0;1} \quad Z_0Z_1$ gates. The circuit is then terminated with a measurement operation applied to each of the four physical qubits.

The general routine seen in Figure 7.4 is then applied to a selection of gate sequences, which form a sub-family that is representative of all possible gate sequences derived from the $[4; 2; 2]$-code's gate set. The complete set of gate sequences can be de ned as all possible combinations of gates from a single one up to a length of d gates. If the sub-family of typical gate sequences that are representative of the complete set satis es the fault-tolerance criterion, then it can be assumed that the QECC is fault-tolerant for any circuit [59].

Both the uncoded and encoded circuits investigated rely on the same IBMQ device to keep the underlying source of error as similar as possible. The submission of the jobs to the IBMQ cloud-based platform is batched so that the encoded and uncoded versions are run one after another to our best ability. Each device is re-calibrated and all the jobs submitted for an experiment are within the same IBMQ calibration cycle. There are however user-speci c restrictions both on the number of circuits and jobs according to the user access rights and the device chosen, as well as depending on the demand for the IBMQ device at a certain time.

7.2.3 Post-Selection

The $[4; 2; 2]$ code of [59] provides a method whereby a pair of logical qubits Q_0Q_1 are encoded using four physical qubits $q_0q_1q_2q_3$, as seen in Figure 7.6. The $[4; 2; 2]$ code's logical states[7] are [59]:

$$|\overline{00}\rangle \; ! \quad (|0000\rangle + |1111\rangle)/\sqrt{2} \tag{7.1}$$

$$|\overline{01}\rangle \; ! \quad (|1100\rangle + |0011\rangle)/\sqrt{2} \tag{7.2}$$

$$|\overline{10}\rangle \; ! \quad (|1010\rangle + |0101\rangle)/\sqrt{2} \tag{7.3}$$

$$|\overline{11}\rangle \; ! \quad (|0110\rangle + |1001\rangle)/\sqrt{2}. \tag{7.4}$$

[6] The notation for the $H_0H_1 \quad SWAP_{0;1}$ gate is written according to the circuit transformation (see Figure 7.11) rather than to its mathematical form of $SWAP_{0;1}[(H_0 \quad H_1)|Q_0Q_1\rangle]$.

[7] Logical states and operations are denoted with an overbar; $\overline{x}$.

The [4; 2; 2] code is an error detection code, therefore a codeword that is found to contain an error is discarded rather than corrected. To implement this scheme in small-scale experiments, error detection is carried out with the aid of classical post-processing. Explicitly, the logical qubits Q_0Q_1 can be measured in the computational basis by direct measurement of the physical qubit register $q_0q_1q_2q_3$. The operation of detecting an erroneous state by the classical post-processing is straightforward, because if the outcome of the measurement is a bit-string containing an even number of 1, then it can be decoded into one of the four legitimate codeword, of Eq. (7.1)-(7.4). If by contrast the measurement outcome corresponds to a bit-string with an odd parity; namely we have 1000, 0111, 0100, 1011, 0010, 1101, 1110 and 0001, then an error has occurred, hence the corresponding results can be discarded in post-selection. Therefore, if is the number of accepted legitimate results and R is the total number of circuit outputs, then the post-selection retention ratio r is de ned by

$$r = \frac{}{R}; \tag{7.5}$$

where is equivalent to the number of outputs having even parity.

7.2.4 [4,2,2]-Encoded State Preparation

Figure 7.7: Fault-tolerant circuit to prepare the [4 ; 2; 2]-encoded logical state $|\overline{00}\rangle$. After the dashed line a parity check of $(q_0; q_3)$ is determined by measuring the ancilla in q_4. To make this circuit fault-tolerant post-selection is also applied to q_0 to q_3.

There are several methods of ensuring that the logical state is encoded using a circuit relying on a theoretically fault-tolerant design, as presented in Section 7.2.1.1. To recap, if a single gate error proliferates through subsequent gates to an increased number of qubit errors that are not detectable according to the speci c detection capability of the QECC, then the circuit design must not be deemed to be fault-tolerant [9]. For example, if a certain CNOT gate in the [4; 2; 2] code's encoding circuit has an erroneous output and this error in turn proliferates to an even number of qubit errors in the output state,

then this error cannot be detected and the circuit is not fault-tolerant, as it will be briefly exemplified below.

Figure 7.7 shows the circuit[8] that prepares the $[4,2,2]$-encoded states q_0, q_1, q_2, q_3 representing the logical state $|\overline{00}\rangle$ in Eq. (7.1). This circuit has a fault-tolerant design for two reasons. Firstly, the gate errors that proliferate to an odd number of errors at the output of the encoding circuit will be discarded in the post-selection operation presented in Section 7.2.3. For example, if the CNOT gate between (q_1, q_0) incurs an XI Pauli error, the X error on the control qubit will be proliferated by the following two CNOT gates between both (q_1, q_2) as well as (q_2, q_3). Hence, the output state q_0, q_1, q_2, q_3 will be $(|0111\rangle + |1000\rangle)/\sqrt{2}$. Since this contains an odd number of errors in each 4-tuple, the state will be discarded during the classical post-selection.

Secondly, there are some gate errors that proliferate to an even number of qubit errors and therefore cannot be detected by the classical post-selection. To detect these gate errors an additional parity check is appended between (q_0, q_3) using an ancilla qubit in location q_4. If the result is 1 when the ancilla qubit is measured, it indicates that the intended encoded state $|\overline{00}\rangle$ has not been prepared and the run should be discarded. For example, an IX due to a fault in the CNOT gate between (q_1, q_2) will produce the output state $(|0011\rangle + |1100\rangle)/\sqrt{2}$. This error will not be picked up during post-selection, since the number of errors is even and the state corresponds $|\overline{01}\rangle$. However, it can be spotted by the ancilla measurement. Therefore, this ancilla measurement combined with classical post-selection would render the encoder fault-tolerant, according to Definition 1 of Section 7.2.1.1. Note that the circuit in Figure 7.7 prepares only the $|\overline{00}\rangle$ encoded state. See Appendix 9.4 for circuits that directly prepare alternative encoded states.

7.2.5 Encoded Gates

In this section we will describe the method of protecting logical gates by the $[4,2,2]$ encoder. In classical communications the FEC encoded bits are modulated and may be corrupted by the channel at the output of the demodulator, which is then corrected by the FEC decoder. By contrast, in a quantum computer, the faulty logical gates inflict errors, which can be modelled by a quantum decoherence channel. To demonstrate an error detection-aided quantum computation process, rather than merely a protected quantum memory, it is necessary to apply the $[4,2,2]$ code to their logical gates. There exists a set of logical gates[9] whose error-free operation may be detected by the $[4,2,2]$ scheme. These logical gates carry out certain logical transformations between the four legitimate encoded states of Eq. (7.1)-(7.4). Each logical operation is implemented by a set of physical gates carrying out the desired logical transformation.

[8] See Section 3.3.5 for discussion of a similar circuit.
[9] For quantum gate definitions see [9].

Figure 7.8: X_1 Circuit

Figure 7.9: Z_1 Circuit

The equivalent encoded and uncoded gate circuits are shown in Table 7.1. The $[[4,2,2]]$-encoded version of the gates has a physical circuit implementation that is fault-tolerant according to Section 7.2.1.1. For example, applying a logical X gate to the Q_1 qubit in the encoded state $|\overline{00}\rangle$ is readily shown to be equivalent to applying two X gates directly to the physical qubits q_0 and q_1 of the $[4,2,2]$-encoded state,[10] which is shown as follows

$$\overline{X}_1|\overline{00}\rangle \rightarrow X_0X_1(|0000\rangle + |1111\rangle) = |\overline{01}\rangle; \tag{7.6}$$

where $\overline{X}_1$ corresponds to the logical counterpart of an X gate applied to the logical qubit Q_1. The circuit representing this gate is shown in Figure 7.8. Additionally, the equivalent uncoded circuit is implemented by simply applying an X gate to the uncoded qubit q_1.

Table 7.1: Encoded and uncoded circuits according to the $[[4,2,2]]$ code logical gate set. For the definitions of quantum gates see [9].

Uncoded	Coded
X_0	X_0X_2
X_1	X_0X_1
Z_0	Z_0Z_1
Z_1	Z_0Z_2
$cz_{0,1}$ Z_0Z_1	$S_0S_1S_2S_3$
H_0H_1 $SWAP_{0,1}$	$H_0H_1H_2H_3$

The circuit of the logical Z_1 gate is shown in Figure 7.9. This is similar to the X_1 gate, but it is implemented by applying a Z gate to qubits q_0 and q_2 in the $[4,2,2]$-encoded state. The logical single qubit gates X and Z have different physical gate implementations, depending on which qubit in the logical state is being targeted, as seen in Table 7.1.

The gate referred to as $cz_{0,1}$ Z_0Z_1 is shown in Figure 7.10. This gate is applied between (Q_0, Q_1) and the uncoded version consists of a controlled-Z (cz) gate followed by a Z gate acting upon both qubits. The logically equivalent coded gate can be constructed

[10] The logical gates may be applied after the fault-tolerant encoding scheme described in Section 7.2.4. Therefore, the state $|\overline{00}\rangle$ is deemed error-free and the ensuing legitimate logical transformation applied to the code-word state will not result in error.

Figure 7.10: $cz_{0;1}$ Z_0Z_1 Circuit

Figure 7.11: H_0H_1 $SWAP_{0;1}$

by applying four of the single-qubit S gates to the qubits $q_0; q_1q_2; q_3$. This has the advantage of implementing a logical two-qubit controlled-Z gate by single-qubit gates[11] which has the e ect of a low number of physical two-qubit gates in the encoded circuit.

Figure 7.11 shows the e ect of applying four physical Hadamard gates to the encoded state. This is the physical circuit that implements the logical gate referred to as H_0H_1 $SWAP_{0;1}$ in Table 7.1. This gate has the following transformation on the uncoded qubits $Q_0; Q_1 = j00i$, giving the output:

$$\frac{1}{2} \; j00i + j01i + j10i + j11i \quad : \tag{7.7}$$

The uncoded circuit of Figure 7.11 is constituted by a pair of Hadamard gates H_0H_1 followed by a SWAP gate applied to $(Q_0; Q_1)$. The SWAP gate has the e ect of exchanging the position of two qubits $jxyi ! j \; yxi$ and is implemented using three CNOT gates [9].

There are several ways of applying a CNOT gate to the qubits $(Q_0; Q_1)$ for the $[4; 2; 2]$ code [59]. Applying a SWAP gate between qubits $(q_0; q_1)$ in the encoded state has the e ect of a logical CNOT gate, but this is not a fault-tolerant circuit according to Section 7.2.1.1. A way around this is to apply a virtual SWAP gate between $(q_0; q_1)$ by switching the qubit positions in post-processing. Finally, with the aid of an additional ancilla qubit it is possible to use SWAP gates, but the excessive overheads of this circuit makes it less practical.

7.3 Circuit Error Rate Evaluation

The error rate of the circuit output is determined by quantifying the trace distance between the non-ideal experimental results and the ideal outcome distribution [59]. This is the most practical metric that may be determined experimentally since it is operationally

[11] The $cz_{0;1}$ gate can be implemented alone by applying the Z gates to the coded scheme with the physical gates $S_0S_1S_2S_3 \quad Z_1Z_2$.

e cient, when the scale of the experiment is restricted by the number of available circuit activations. The trace distance is obtained by measuring the nal state at the circuit output in the computational basis. This gives a non-ideal noisy probability distribution, which is then compared to a classically simulated ideal distribution for the same circuit. Therefore, a low trace distance is desirable, since this corresponds to a circuit having a lower error rate. This procedure is repeated separately for both the encoded and equivalent uncoded scheme. This allows the error rates to be compared and the fault-tolerance criterion $D_c < D_u$ to be evaluated for that particular circuit, following De nition 2 of Section 7.2.1.2.

Let p be the ideal output distribution extracted from a classical circuit simulator and $\tilde{p}$ be the direct measurement outcome gleaned from the IBMQ device. For the uncoded scheme let the ideal probability distributions be denoted by p^u. This is the probability distribution over the set of possible outputs, when the qubits Q_0Q_1 are measured, namely $00, 01, 10, 11$. The error-prone experimental circuit produces a di erent probability distribution $\tilde{p}^u$ over the same possible outcomes $00, 01, 10, 11$. Then the error rate D_u of the circuit output for the uncoded scheme is given by

$$D_u = \frac{1}{2} \sum_i |p_i^u - \tilde{p}_i^u|; \tag{7.8}$$

where i is the index of the set of possible outcomes. The error rate D_c for the encoded scheme is given by the same method:

$$D_c = \frac{1}{2} \sum_i |p_i^c - \tilde{p}_i^c|; \tag{7.9}$$

where p^c and $\tilde{p}^c$ are the ideal and non-ideal experimental results respectively, over the 16 possible outcomes for $q_0q_1q_2q_3$.

7.4 Experimental Parameters

It is anticipated that two-qubit gates will have a more signi cant contribution to the overall error rate of the circuit, which is currently re ected in the benchmarked device metrics [156]. Therefore, we seek to investigate whether the fault-tolerance criterion is satis ed, because there is a larger number of two-qubit gates in the uncoded scheme [63, 97]. It will only become clear which the most critical parameters are after assessing the overall device noise e ects. Nevertheless, in this section we assign dedicated parameters to the single gate error $_1$ and to the two-qubit gate error $_2$ as well as to the measurement error P_m using a simple Pauli error model [9, 66].

7.4.1 Error Rate Associated with a Single Parameter

The associated measurement error can be accounted for by an independent qubit error channel having a single parameter. Let us consider the measurement error in a two-qubit register reminiscent of the uncoded scheme. Let us denote the probability of a single qubit read-out error by $0 < P_m < 1$. If the intended measurement outcome is 00 but instead either 01 or 10 are measured, then we can say that a single qubit is measured incorrectly with probability $P_m(1 - P_m)$. Likewise, the measurement outcome is 11 with probability P_m^2 since two qubits are simultaneously read out incorrectly. Then the total error rate becomes:

$$E_M = 1 - (1 - P_m)^2 = 2P_m - P_m^2. \quad (7.10)$$

By the same reasoning, the corresponding encoded scheme will have an error rate according to the measurement of 4-qubit strings followed by the action of post-processing. All the odd numbers of qubit errors will be spotted and discarded by the post-selection. Therefore, $[4, 2, 2]$-encoded scheme incurs an error rate of $P_m^2(1 - P_m)^2$ after post-selection according to the associated simultaneous two-qubit errors.

7.4.2 Encoder Gate Error

Unless the error in the encoding circuit can be perfectly corrected or the run may be discarded, the error rate of the encoded scheme will be lower bounded by the residual encoder error. The ancilla measurement between (q_0, q_3) of Figure 7.7 does not have a straightforward implementation based on the device layouts shown in Figure 7.2 and Figure 7.3. Therefore, the ancilla measurement is excluded how the experiments presented in the next section. This means that the encoding circuit implemented does not have a fault-tolerant design satisfying Definition 1 of Section 7.2.1.1.

Let us assume that the error imposed by each gate may be modelled by a symmetrical Pauli error channel. A CNOT gate modelled by a two-qubit depolarizing channel outputs $IX, YI, YX, ZZ, \ldots$ after the normal functioning of the gate (see Section 2.4.1 and Section 2.4.3). Each error has a probability of $\epsilon_2/15$, since there are 15 combinations of $\{X, Y, Z, I\}$ excluding II representing the identity operation that has no effect. The resultant gate error rate of the encoding circuit seen in Figure 7.7 is $E_E = \epsilon_1 + 3\epsilon_2$ before post-selection.

Let us consider the effect of each gate separately. Any X, Y, Z error occurring after the Hadamard gate with probability $\epsilon_1/3$ will be proliferated by the following CNOT gates to a state with the outcome distribution of $|\overline{00}\rangle$ in Eq. (7.1). Therefore, this error can be ignored. Let us assume that the first CNOT gate between (q_1, q_0) of Figure 7.7 has error probability of ϵ_2. The phase flip errors IZ, ZI, ZZ occurring with probability $3\epsilon_2/15$ can be ignored, since an odd-weight Z error is not detectable in the $|\overline{00}\rangle$ state

during post-selection and an even weight-2 error will cancel one another. In addition, all other depolarizing error combinations on this gate will result in an odd number of qubit errors, which will be discarded during post-selection or return the state to $|\overline{00}\rangle$.

Therefore the final error rate of the encoding circuit will be determined by that of the CNOT gates connecting (q_1, q_2) and (q_2, q_3). Any of the IX, IY, ZX, ZY errors after the (q_1, q_2) CNOT gate will result in an even number of errors, namely in the $|0011\rangle + |1100\rangle$ state, therefore the error arising from this gate that cannot be detected occurs with a probability of $4\epsilon_2/15$. Any other error combinations applied to this gate will result in an odd number of errors that can be removed by post-selection. Likewise, the (q_2, q_3) CNOT gate of Figure 7.7 will also contribute $4\epsilon_2/15$ to the final error rate. Therefore, when considering gate errors modelled by the depolarizing channel it is expected that the encoding circuit will contribute $8\epsilon_2/15$, when the additional ancilla measurement is not implemented. Note that if the device layout is suitable for realizing the fully fault-tolerant circuit of Figure 7.7 (which includes the ancilla parity check), then theoretically all possible gate errors occurring in the circuit are detectable and the above lower bound would not be applicable.

7.4.3 Circuit Gate Error

Table 7.2: Gate error probabilities according to the physical gate count for the circuits of Table 7.1.

Gate	Uncoded	$[4, 2, 2]; r = 1$
X_0, X_1, Z_0, Z_1	ϵ_1	$2\epsilon_1 + \frac{2}{3}\epsilon_1$
$cz_{0,1}$ $Z_0 Z_1$	$2\epsilon_1 + \epsilon_2$	$4\epsilon_1 + 6\frac{2}{3}\epsilon_1$
$H_0 H_1$ $SWAP_{0,1}$	$2\epsilon_1 + 3\epsilon_2$	$4\epsilon_1 + 6\frac{2}{3}\epsilon_1$

Let us assume that the circuit is modelled by a sequence of temporally uncorrelated noisy channels and consists of spatially uncorrelated physical gates, where P denotes the overall error rate of each physical circuit block that implements a logical gate in the sequence. Furthermore, there are L gates in the sequence, each having an error rate P. According to these idealized simplifying assumptions, the overall error rate E_P of the gate sequence is given by

$$E_P = \sum_{i=1}^{L} \binom{L}{i} P^i = 1 - (1 - P)^L \tag{7.11}$$

and LP is the largest term corresponding to the probability of a single logical gate block in the sequence operating with an error. Let us denote the physical single-qubit gate count by n_1 and the two-qubit gate count by n_2. Furthermore, the average physical single-qubit gate error probability is denoted by ϵ_1, regardless of the specific type of the individual gate applied. Likewise, the average two-qubit gate error probability is ϵ_2. For

example, a logical Z_0 gate is implemented using $n_1 = 2$ physical Z gates, each having an error rate of $_1$. Then the total gate error probability attributed to each circuit block is $P = \sim_1 + \sim_2 + \sim_1\sim_2$, where we have

$$\sim_1 = \sum_{i=1}^{n_1} \binom{n_1}{i} {}_1^i, \quad \sim_2 = \sum_{i=1}^{n_2} \binom{n_2}{i} {}_2^i. \tag{7.12}$$

Table 7.2 shows the expected error rate of a circuit block implementing both the uncoded as well as the $[[4, 2, 2]]$-encoded scheme and the post-selected coded scheme. For example, the X_0 gate contains a single X gate for the uncoded implementation, therefore we have $P = _1$. The corresponding encoded version requires $n_1 = 2$ physical X gates. Before post-selection ($r = 1$) this circuit block will have an error rate of $\sim_1 = 2 _1 + {}_1^2$. After post-selection ($r < 1$) the odd numbers of qubit errors are removed, so it is expected that we have $P = {}_1^2$. Since this circuit contains only single qubit gates, no qubit errors may proliferate to a larger number of errors through two-qubit gates. Additionally, the gate counts are the same for the single qubit encoded gates and $_1$ represents the error probability of all individual physical gates, so by the same reasoning as that for the X_0 gate, the expected error rate attributed to the implementation of the X_1, Z_0, Z_1 gates can be derived.

7.5 IBMQ Experimental Results Associated with a Simple Error Model

In this section we introduce three experiments. Each experiment relies on random sequences from the $[[4, 2, 2]]$-encoded gate set $\{X_0, X_1, Z_0, Z_1, cz_{0,1}, Z_0Z_1, H_0H_1, SWAP_{0,1}\}$. The first experiment in Section 7.5.2 shows the results of implementing Figure 7.4 for random sequences of a reduced gate set that excludes the H_0H_1 $SWAP_{0,1}$ gate. In the second experiment, sequences of the H_0H_1 $SWAP_{0,1}$ gate alone are considered and the results are discussed. This gate prepares an output state that is 4-dimensional therefore there are some considerations when deriving the error rate compared to an ideal state. The final experiment in Section 7.5.4 shows the results of random sequences of the full gate set. Before we discuss the experiment results, let us consider the trace distance bounds in a `worst case' circuit noise scenario.

7.5.1 Trace Distance Bounds

Consider the scenario where the only source of circuit error is the depolarizing channel. In the `worst case' scenario the probability of error is $= 1$ meaning that the

experimental circuit output is always the totally mixed state [9]

$$\frac{I}{4} = \frac{1}{4}\sum_{i=1}^{4} |i\rangle\langle i|. \tag{7.13}$$

This can be thought of as a randomized output, where the desired state has been totally corrupted by circuit error. In this case, the uncoded experimental output distribution p^u is of the form:

$$p_j^u = \frac{1}{4} \quad \forall \; j = \{00, 01, 10, 11\}, \tag{7.14}$$

where each measurement outcome is equi-probable.

First let us compare this to the class of circuits, where the ideal circuit output is 1-dimensional, so $p_i^u = 1$ for any $i = \{00, 01, 10, 11\}$. The dimension of the output state is determined by the selected gate sequence, namely by the specific state which that particular set of gates gives rise to.

For example, if the circuit prepares $Q_0 Q_1 \; |00\rangle$ and then applies the gate X_1, the output becomes:

$$|00\rangle \rightarrow |01\rangle. \tag{7.15}$$

In this case the ideal noiseless output generated by the classical simulator is

$$p_{01}^u = 1, \quad p_i^u = 0 \quad \forall \; i = \{00, 10, 11\}. \tag{7.16}$$

When the ideal circuit output is given by Eq. (7.16) but Eq. (7.14) is the measured experimental distribution, the error rate becomes

$$D_u = \frac{1}{2}(|p_{01}^u - p_j^u| + 3|p_i^u - p_j^u|) = 0.75 \tag{7.17}$$

by Eq. (7.8).

Consider now logically equivalent scenario for the $[[4, 2, 2]]$-encoded scheme. This is the encoded equivalent to the circuit in Eq. (7.15) and generates the output state $|\overline{01}\rangle = (|1100\rangle + |0011\rangle)/\sqrt{2}$ given in Eq. (7.2). Therefore, the ideal output of the noiseless classical simulation is

$$p_{1100,0011}^c = \frac{1}{2}, \quad p_i^c = 0$$
$$\forall \; i = \{0000, 1111, 0101, 1010, 0110, 1001\}. \tag{7.18}$$

When = 1, the experimental circuit output is of the state I =16. After post-selection, we have

$$p_j^c = \frac{1}{8} \quad 8 \quad j = \{0000, 1111, 0101, 1010, 0110, 1001, 1100, 0011\}; \tag{7.19}$$

where the probability of each legitimate codeword is identical and it is normalised by the post-selection ratio of $r = 1/2$. Then according to Eq. (7.9) the upper bound for the error rate of the encoded scheme is the same as that of the uncoded version, namely

$$D_c = \frac{1}{2}(2|p_{1100,0011}^c \quad p_j^c| + 6|p_i^c \quad p_j^c|) = 0.75. \tag{7.20}$$

7.5.2 Experiment 1: Reduced Gate Set

Figure 7.12: Experimental results based on the Ibmq_Bogota device characterizing random sequences of the $[4, 2, 2]$-encoded gates along with those of the corresponding uncoded gate for sequence lengths . Model parameters: samples = 60, device = ibm bogota, date= 26.05.2021, gate set= $\{X_0, X_1, Z_0, Z_1, CZ\}$, $P_m = 0.02$, $_1 : _2 = 1 : 40$, $3 \quad 10^{-3} < _1 < 5.5 \quad 10^{-3}$

Figure 7.12 shows the results of random $[4, 2, 2]$-encoded gate sequences of length 1 L 100 after the initialisation of the $|\overline{00}\rangle$ encoded state, which were run on the Ibmq_Bogota device according to the method shown in Figure 7.4. Let us compare this to a simple model having as few as three parameters; namely the single and two-qubit gate error as well as another parameter representing the measurement error de ned in Section.7.4. The error rate for each circuit block P is taken to be the average gate error evaluated over the chosen gate set. In this section the results refer to random combinations of the gate set $\{X_0, X_1, Z_0, Z_1, cz_{0,1} \quad Z_0Z_1\}$. In this scenario, the error rate at the circuit

output for the uncoded scheme can be approximated analytically by

$$D_u = E_P + E_M = \frac{L}{5}\left[6\,\epsilon_1 + \epsilon_2\right] + 2P_m - P_m^2; \tag{7.21}$$

which is the sum of the largest term in Eq. (7.11) and of the measurement error in Eq. (7.10). The parameters applied in Figure 7.12 are approximated by the device's same specific calibration metrics provided by IBMQ [6] for the device within the calibration cycle the experiment was run in. These metrics are taken as general guide, but they must be applied with some caution [157]. Moreover, the fitting of the model to the experimental results does not represent an accurate calibration of the device noise, since the model is incomplete. For example, the parameter P_m may encompass some state preparation error in this model, therefore it does not accurately represent the scale of measurement error in the device.

Nevertheless, the uncoded model gives a reasonable approximation of the increase in error rate with the gate sequence length. Therefore, it may be reasonable to assume that two-qubit gates constitute the dominant source of the uncoded error, and therefore it may be deemed plausible that the fault-tolerance criterion $D_c < D_u$ is satisfied by the post-selected scheme associated with $\eta < 1$ for sequence lengths of $L > 10$.

The $[4,2,2]$-encoded scheme operating without post-selection[12] and represented by $r = 1$ includes the gate errors of the encoding circuit (without post-selection) as well as both the gate and measurement errors. Under these assumptions, and upon considering the largest terms, the analytical error rate of the output becomes:

$$E_E + E_P + E_M = \epsilon_1 + 3\,\epsilon_2 + L\left[\frac{12}{5}\,\epsilon_1 + 2\,\epsilon_1^2\right] + 4P_m - 6P_m^2; \tag{7.22}$$

which applies the same metrics as the uncoded scheme. The upper bound gives a reasonable approximation of the experimental results. However, it is clear that the model of the post-selected ($\eta < 1$) scheme is overly optimistic for comparison with the results obtained from the Ibmq_Bogota device. The $[4,2,2]$-encoded scheme relying on post-selection is approximately characterized by:

$$D_c = \frac{8\,\epsilon_2}{15} + L\,2\,\epsilon_1^2 + 6P_m^2; \tag{7.23}$$

which is lower-bounded by the post-selected encoder error, namely by $E_E \approx 8\,\epsilon_2/15$, as described in Section 7.4.2. This error floor is owing to the residual two-qubit gate errors in the encoding circuit that cannot be detected during post-selection. However, this assumption is not consistent with the experimental results in Figure 7.12, which exhibit an error rate that is almost an order of magnitude higher than this, closer to $D_c \approx 0.07$.

[12] The $[4,2,2]$-encoded scheme without post-selection is considered here to compare the error rate before and after error detection, as well as to evaluate the error model proposed.

It is not unexpected that the experimental results will deviate from this simple model, since we can assume that many parameters are required for accurately characterising the time-variant behaviour of the device during each consecutive circuit execution. Additionally, both temporal and spatial independence has been assumed for all circuit components, which represents a simplistic model of a real device. Nevertheless, since the error rate of the $[4, 2, 2]$-encoded gate sequence does not increase with the gate sequence length L, it may be surmised that the error of the encoding circuit outweighs that of the encoded gate sequence. In addition, the encoding circuit may contain more significant errors than just two-qubit gate errors. Let us consider this interpretation further.

However, this model excludes qubit preparation errors, which may occur before the circuit is activated, while initializing the qubit register. A qubit preparation error occurring before the encoding circuit will be proliferated by the subsequent CNOT gates to a logical error that cannot be detected in the post-selection phase implemented in this scheme. For example, an X error imposed on q_2 before the encoding circuit seen in Figure 7.6 would result in the preparation of the $|\overline{01}\rangle$ state, rather than the intended $|\overline{00}\rangle$. If the preparation error P_p was modelled as a single-parameter channel as described in Section 7.4.1, this error would contribute a term on the order of $O(P_p)$ to the encoded error rate, hence resulting in an excessive lower-bound according to . In addition, the uncoded scheme will also have an error rate on the order of $O(P_p)$. Note that it is expected that this error would be discarded, if the full circuit of Figure 7.7 is implemented.

This model also excludes detuning or gate-coherence errors. A simple calibration error can be thought of as an inaccurate rotation of the gate's output state, effectively imposing the same error each time the gate is activated. Since this error is systematic, it will rapidly escalate if the gate is used repeatedly. This raises the dilemma whether it could be mitigated by re-calibrating the gate rotation. Alternatively, it may be hypothesized that there is a random fluctuation in the gate output's rotation within a certain range and therefore re-calibration of the gate may only have a limited effect. Note that the average error rate of the Hadamard gate ($_1$) does not represent the contribution of a gate-coherence error to the final error rate, because it is not encompassed by the Pauli error model considered here. See Appendix 9.3 for a further explanation of errors that may not be accounted for in the error model considered here.

It is quite plausible that this affects the weighting of the superposition of the encoded state $|\overline{00}\rangle$, rather than influencing an individual qubit error detectable in post-selection. Therefore, when determining the statistical distance between the non-ideal experimental results and an ideal output distribution of quantifying the error rate, the weighting of the superposition in the experimental encoded state must be close to the ideal one, otherwise the difference of the two distributions would cause a high error floor. This

Figure 7.13: Experimental results based on the ibmq_Santiago device characterizing the [4; 2; 2]-encoded H_0H_1 $SWAP_{0;1}$ gate repeated for the gate sequence length Ls. The final state at the circuit output is either $|00\rangle$ (1-dimensional) or $|{+}{+}\rangle$ (4-dimensional), which are both denoted by different symbols.

may be straightforwardly resolved by user-calibrated gate pulses relying on a hybrid classical-quantum algorithm without the need for fully characterizing the circuit noise.

7.5.3 Experiment 2: Single Gate

Figure 7.13 portrays the trace distance for the output states vs. the gate sequence length L, where the H_0H_1 $SWAP_{0;1}$ logical gates are applied L times after the initialisation of the $|\overline{00}\rangle$ [4; 2; 2]-encoded state. When an even number L of gates is applied, the output state generated is

$$[H_0H_1 \quad SWAP_{0;1}]^{L}|00\rangle \rightarrow |\quad 00\rangle; \tag{7.24}$$

since the effect of an even number of the same gate results in the identity operation. An odd number of the H_0H_1 $SWAP_{0;1}$ gates will prepare the equi-probable 4-dimensional state

$$[H_0H_1 \quad SWAP_{0;1}]^{L}|00\rangle \rightarrow \frac{1}{2}\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,: \tag{7.25}$$

This is denoted by $|{+}{+}\rangle$ in Figure 7.13. The figure shows that the circuits, which produce the output state $|00\rangle$ have an increasing trace distance vs. the gate sequence length L and the circuits that generate the 4-dimensional state of Eq. (7.25) have a gently decreasing trace distance with the gate sequence length.

Let us consider the trace distance for a 4-dimensional output state in the depolarizing channel, as described previously for the 1-dimensional output state in Section 7.5.1. The

circuit of Eq. (7.7) generates a 4-dimensional ideal output state, given by

$$p_i^u = \frac{1}{4} \quad 8 \quad i = f00; 01; 10; 11g: \tag{7.26}$$

The trace distance between this state and the totally mixed state of Eq. (7.14) is

$$D_u = \frac{1}{2}(4jp_i^u \quad p_j^u j) = 0: \tag{7.27}$$

To interpret this e ect in more detail, since the ideal state in Eq. 7.26 and the totally corrupted `worst case' noisy state in Eq. (7.14) are identical, the statistical trace distance between these states is zero. Therefore, when the ideal state is 4-dimensional, the error rate tends to $D_u \; ! \; 0$, if the depolarizing noise a ecting the experimental state obeys $\; ! \; 1$. This explains the unexpected trend as to why the error rate may decrease even though the system error tends to become more prevalent. This trend is also seen for the logical 4-dimensional state in the encoded scheme.

Again, these trends are speci c to the 4-dimensional output state. However, in general, the dimension of the output state will determine the upper bound of the trace distance. For example, consider a circuit where the 2-dimensional superposition state$j1(0i + j01i)=\sqrt{2}$ is output, described by

$$p_{01;10}^u = \frac{1}{2}; \quad p_i^u = 0 \quad 8 \quad i = f00; 11g: \tag{7.28}$$

Let us employ the same reasoning to that in Eq. 7.27. When the depolarizing channel[13] noise has its `worst case' values associated with = 1, the measured experimental outcome is the totally corrupted state described by Eq. (7.14). Then, in the noisiest scenario the uncoded error rate of Eq.(7.8) becomes;

$$D_u = \frac{1}{2}(2jp_{01;10}^u \quad p_j^u j + 2jp_i^u \quad p_j^u j) = 0:5: \tag{7.29}$$

Therefore, when the ideal state is 2-dimensional, the error rate tends to$D_u \; ! \; 0:5$ as the depolarizing noise increases. Therefore, according to Eq. 7.27 and Eq. 7.29, the dimension of the circuit output should be carefully considered, when assessing whether the fault-tolerance criterion is satis ed.

Figure 7.13 demonstrates that the dimension of the output state will a ect whether the circuit can or cannot satisfy the fault-tolerance criterion. For example, the fault-tolerance criterion of $D_c < D_u$ is only satis ed, when an even number of theH_0H_1 $SWAP_{0;1}$ gates are applied and the output state is 1-dimensional. The uncoded version of this gate has a SWAP operation, which is implemented with the aid of 3 CNOT gates, while its $[4; 2; 2]$-encoded version is implemented with the aid of single qubit gates, as shown in Table 7.1. Therefore, Figure 7.13 shows the trend that$D_u \; ! \; 0:75$ as$L \; ! \; 100$

[13] See Section 2.4.1.

Figure 7.14: Experimental results based on the ibmq_Santiago device characterizing random sequences of the $[[4,2,2]]$-encoded gates and the corresponding uncoded gate for sequence lengths L. Model parameters: samples = 58, date= 14.02.2021, gate set= $[X_0, X_1, Z_0, Z_1, cz_{0,1}\ \ Z_0Z_1, H_0H_1\ \ SWAP_{0,1}]$, $P_m = 0.025$, $_1 : _2 = 1 : 20$, $5\ \ 10^{-3} < _1 < 6\ \ 10^{-3}$

only for even L, where the circuit output is $|00\rangle$. The corresponding encoded scheme has an error rate, which satisfies $D_c < D_u$, since the encoded circuit predominantly consists of single-qubit gates. However, when the output state is 4-dimensional, the reverse trend is observed. Since the uncoded scheme contains a large number of the noisiest gate, namely CNOT gates, the output state becomes more corrupted. However, this has the effect of mitigating the error rate [14] as intimated in Eq. (7.27). The logically equivalent state of the encoded scheme contains only single qubit gates, yet we have $D_c > D_u$. Therefore, for the fault-tolerance criterion to be assessed, the gate sequences may be modified for ensuring that each circuit outputs a 1-dimensional state.

7.5.4 Experiment 3: Full Gate Set

Figure 7.14 and Figure 7.15 show the results of random gate sequences of the full $[[4,2,2]]$-encoded gate set $\{X_0, X_1, Z_0, Z_1, cz_{0,1}\ \ Z_0Z_1, H_0H_1\ \ SWAP_{0,1}\}$, which also includes the $H_0H_1\ \ SWAP_{0,1}$ gate introduced in Section 7.2.5. In contrast to the trends of the previous section, both figures show that the uncoded error rate does not increase as expected according to the model of Section 7.5. This is due to the inclusion of the $H_0H_1\ \ SWAP_{0,1}$ gate in the random gate sequence generated. As the sequence length increases, it is more common for an odd number of this gate to be included in the random gate sequence. In this case the final output state is a 4-dimensional equi-probable superposition, which results in a reduction of the total error rate. This

[14] This is because the ideal output state is 4-dimensional, therefore it is expected that $D_u \ ! \ 0$ when the experimental state sampled is totally corrupted.

Figure 7.15: Experimental results based on the Ibmq_Bogota device characterizing random sequences of the $[4,2,2]$-encoded gates and the corresponding uncoded gate for sequence lengths L. Model parameters: samples = 60, date= 15.04.2021, Gate set= $[X_0, X_1, Z_0, Z_1, cz_{0,1}\ \ Z_0Z_1, H_0H_1\ \ SWAP_{0,1}]$, $P_m = 0.04$, $_1 : _2 = 1 : 50$, $3\ \ 10^{-3} < _1 < 5\ \ 10^{-3}$

Table 7.3: Summary of results in Figure 7.12, Figure 7.14 and Figure 7.15. D_u is the error rate for random gate sequences of length L and D_c is the corresponding $[4,2,2]$-encoded gate sequence with post-selection m (1).

	$L = 10$		$L = 100$	
Fig.	D_u	D_c	D_u	D_c
7.12	0.08	0.06	0.34	0.09
7.14	0.11	0.07	0.25	0.07
7.15	0.13	0.06	0.29	0.10

is because the ideal state is indistinguishable from a totally mixed state and therefore the average states become the same, despite being produced from two very different scenarios [158].

7.6 Conclusion

The results of Section 7.5.4, do not lead to consistent conclusions, when grouping together circuits with ideal output states of different dimensions upon using the trace distance for evaluating the fault-tolerance criterion. Despite this, $[4,2,2]$-encoded gate sequences satisfy the fault-tolerance criterion for the full gate set due to the inclusion of a larger number of the noisiest gates in the uncoded scheme. The encoded performance may be further improved, when aiming for mitigating either state preparation or gate-coherence errors by the post-selection mechanism. This may leave space for a combined classical and quantum machine learning approach, whereby the device errors are estimated and mitigated for circumventing the need for a comprehensive characterization of

the device. Therefore, the experimental characterization of a fault tolerant QECC may provide a method of discovering powerful QECCs without the need for a complete noise model.

An accurate noise model that encompasses all sources of errors will require many parameters, especially for numerous qubits and long gate sequences considering a range of di erent coherent and incoherent errors. However, such a noise model may become excessively complex, in particular, when it encompasses unique correlated error patterns. In conclusion, the results of Figure 7.12, Figure 7.14 and Figure 7.15 are summarized at a glance in Table 7.3.

Chapter 8

Summary and Future Research

In this thesis we have outlined the fundamental theory of fault-tolerant QECC for mitigating the component errors inherent to quantum circuits and transmissions. In the first two chapters we outlined the basics of quantum information and the fundamentals of fault-tolerant QECC. In Chapter 4 we presented results which showed that despite implementing a fault-tolerant logical gate construction, the non-fault-tolerant encoding circuit will impose a high error- oor in a quantum depolarizing channel according to the gate error inherent to the encoding circuit. This was shown for both the repetition codes and the Steane code. In Chapter 5 a solution to this problem was presented, whereby the non-fault-tolerant encoding circuit is replaced by the `encoderless' scheme. This method prepares an initial state that can be transformed to the encoded state by a fault-tolerant stabilizer measurement. The simulation results showed this scheme can be e ective to reduce the circuit error rate by three orders of magnitude when the gate error is as high as 10^{-3}.

The final two chapters presented practical applications for a fault-tolerant QECC. The first, in Chapter 6, we proposed that TC and QTC can be employed in both a noisy classical and quantum transmission to improve the security and reliability of the protocol. Finally, in Chapter 7 we presented the experimental results of logical gate sequences based on IBMQ small-scale devices, where we classi ed the fault-tolerance of circuits according to an experimental de nition. In this concluding chapter, we start by summarizing our conclusions in Section 8.1, then a range of possible future research directions will be discussed in Section 8.2.

8.1 Summary

For the practical realisation of reliable large-scale quantum algorithms, fault-tolerant QECC will be necessary to mitigate the deleterious e ects of component error inherent

to quantum circuits. In addition, the encoding, decoding and error correction circuits of a QECC must also have a fault-tolerant construction de ned by a gate error rate threshold P_{th}. Moreover, the recent advancement of quantum hardware opens up the possibility of the practical development of fault-tolerant QECC alongside theoretical proposals. Against this background, this thesis aimed for

(a) De ning the construction of fault-tolerant circuits for QECC that are capable of mitigating component errors inherent to quantum circuits.

(b) Utilizing fault-tolerant QECC in practical scenarios, not only for the secure and reliable transmission of quantum information, but also for improving circuit error inherent to current-day quantum processors.

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 for applying fault-tolerant QECC to suppressing circuit component error in quantum computers. In Section 1.2.1 we proceeded with the history of important milestones in the theoretical development of fault-tolerant QECC. Then in Section 1.2.2 we outlined the SoA experiments activated in current-day devices and the challenges faced when designing fault-tolerant QECC experiments. Finally, the outline of the thesis was presented in Section 1.3 and the novel contributions of the thesis in Section 1.4.

(b) Chapter 2 . In this chapter we provided a general rudimentary introduction to quantum information and quantum circuits. The unit of quantum computing, namely the qubit, was introduced in Section 2.2. Then quantum measurement and quantum gates were presented in Section 2.2.2 and Section 2.3 respectively. This provided the theoretical background to read-out and process the information stored in the qubit. Finally, quantum Pauli error channels were introduced in Section 2.4, providing all the necessary background to introduce fault-tolerant QECC in the next chapter.

(c) Chapter 3 . This chapter was split into two parts. First the basics of QECC and quantum stabilizer codes were explained in Section 3.2, followed by the general de nition of fault-tolerant circuit design. General stabilizer codes were described in Section 3.2.1, covering the $[3,1,3]$ repetition code in Section 3.2.2 and then the $[7,1,3]$ Steane code in Section 3.2.3. Then the circuit construction for stabilizer measurements was described in detail in Section 3.2.4, which forms the basis of many fault-tolerant QECC techniques. The motivation for fault-tolerant circuits, namely error proliferation, was described in detail in Section 3.3.1 and Section 3.3.2. Then the criterion for circuits to be deemed fault-tolerant was de- ned Section 3.3.3. This was demonstrated with the example of a fault-tolerant stabilizer measurement in Section 3.3.4 and Section 3.3.5.

(d) Chapter 4 . In this chapter, we presented encoded transversal gates in the presence of both gate errors with probability P_g and qubit depolarization error P_e. In Section 4.2 the transversal gate scheme was outlined providing a method of applying logical gate transformations to encoded quantum information. The theory of processing information stored in encoded qubits was further explained in Section 4.2.2 providing the background for fault-tolerant logical gates. The system model and assumptions for the scheme were explained in Section 4.3. It was shown in Section 4.4 and Section 4.4.3 that the reliability of logical gates can be improved when P_e is an order of magnitude higher than P_g. However, this imposed a strict condition on the quantum channel model, where the channel parameters obeyed a certain gate error rate threshold P_{th} lower bounded by the gate error inherent to the non-fault-tolerant encoding circuit. Therefore, a limitation of this scheme is that P_{th} may only be relevant for certain restricted channel conditions, whereby the gate error probability is su ciently low. In future work it would be bene cial to determine the speci c gate error rate thresholds whereby the value of P_e is not restricted.

(e) Chapter 5 . In this chapter, the `encoderless' scheme was presented, providing a solution to encode unknown quantum information under realistic channel impairments. The methodology of the scheme was explained in Section 5.2, and then described analytically in Sections 5.3 and 5.4. The resilience of the circuit construction to gate error events at circuit component locations was quanti ed in terms of FER. It was then shown in Section 5.4.2 that the scheme can tolerate a gate error probability of $P_g = 10^{-3}$ and qubit decoherence of $P_e = 5 \quad 10^{-4}$, achieving a $FER < 10^{-5}$. For further improvements to the FER, it was observed that a smaller gate error, such as $P_g = 10^{-4}$ is required. Finally in Section 5.5 the scheme was extended to protocols directly preparing known encoded states demonstrating the possible application of the scheme in speci c quantum processing tasks. A limitation of this scheme is that a fault tolerant stabilizer measurement requiring a high resource overheads is necessitated for implementing the scheme in full. Future work may seek to assess the trade-o between the qubit overheads required for the fault tolerant scheme and the reduction in error rate it may achieve. This can be achieved by comparing fault tolerant and non-fault tolerant stabilizer measurements.

(f) Chapter 6 . In this chapter, we presented the secure and reliable transmission of quantum information via the QTC and TC-aided quantum teleportation protocol. To start, the basic quantum teleportation protocol under perfect channel assumptions was explained in Section 6.2 and then with an imperfect channel in Section 6.3 and Section 6.4. The security of the scheme was discussed in Section 6.5 and shown to be improved in with the addition of QTC which made QBER differences due to the presence of an eavesdropper signi cantly larger and therefore

easier to detect. As well as this, QTC improved the reliability of the pre-shared qubits from $P_e^q = 0:31$ to $P_e^q(QTC)$ 10^{-6}. A limitation of this scheme is that it is determined for the speci c channel conditions of $P_e^q = 0:31$ as well as a simple QSDC scheme. In future work alternative secure error rate thresholds can be determined by considering further combinations of QTC and improved QSDC schemes.

(g) Chapter 7 . In this chapter we moved on to present the experimental results of the $[4; 2; 2]$-code activated in IBM's quantum hardware. These results provide a practical classi cation of a fault-tolerance criterion against the theoretical background de ned in Chapters 3,4 and 5. First, an experimental fault-tolerance criterion was de ned in Section 7.2.1 and the SoA experiment design in Section 7.2.2. Then the $[4; 2; 2]$-encoded gate sequences was explained in detail in Section 7.2.4. We de ned a simple Pauli-gate error model in Section 7.4, characterized by its gate and measurement error parameters, which was then compared to the experimental results extracted from IBMQ hardware in Section 7.5. Three experiments of different gate sets were presented in Section 7.5 . These results showed that circuits with outputs should not be grouped together as these lead to inconsistent circuit error rates. In addition, most encoded circuits which contained a smaller number of two-qubit gates compared to the uncoded scheme demonstrated fault-tolerance. However, it was also discussed that the error rate of the encoded scheme should still be signi cantly lower than what is observed. In addition, it is expected it should scale with the gate sequence length which is not observed in the experiment results. It is concluded in Section 7.5.2 that post-selection may fail to x certain proliferated qubit preparation errors. Furthermore, the encoding circuit may be very sensitive to those gate errors, which cannot be represented by the pure Pauli gate error model. These limitations may be addressed in future work by conducting experiments that directly quantify the e ects of coherent errors in the encoding circuit. This may lead to a better understanding of the source of the high error oor seen in the coded results. The problem may be addressed by considering encoded state preparation without gate sequences and tested for a variety of QECCs that are applicable to the devices available.

8.2 Future Research

There are many exciting avenues for future re-design of QECC according to real-life error models and device architectures that may pave the way for quantum-classical hybrid-QECC. A full experimental demonstration of a resource-e cient theoretically fault-tolerant logical qubit appears to be on the horizon. Surface codes have a number of advantages, the main one being their low gate error rate thresholds and a device layout that has nearest neighbour connections [159, 26]. There are also a range of methods for

implementing a universal set of logical gates with the aid of surface codes, such as magic state distillation and code deformation techniques [21, 160]. The drawback of surface codes is that e cient decoding algorithms are still to be fully developed [161]. Therefore, the choice of the most appropriate codes to be used by the quantum hardware of the future are yet to be discovered. The inclusion of experimental results in the process of code-discovery may open up new avenues to explore. In this section we will brie y discuss two potential future research directions.

Figure 8.1: Steane encoding circuit for device layout shown in Figure 8.2.

1. IBMQ experiment of the non-fault-tolerant Steane Code. The experiment method of Figure 7.4 in Section 7.2.2 of Chapter 7 may be extended to the $[7, 1, 3]$ Steane code of Section 3.2.3. The encoding circuit in Figure 8.1 prepares the $[7, 1, 3]$-encoded zero state (reproduced from Eq. 3.8):

$$|\bar{0}\rangle = \frac{1}{\sqrt{8}} |0000000\rangle + |1010101\rangle + |0110110\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle . \quad (8.1)$$

   This circuit in Figure 8.1 is a modi cation of the optimized Steane encoding circuit in [162, 88] that is suitable for a more simple device layout than that required by the traditional encoding circuit in Figure 3.3. This circuit may not be fault-tolerant according to the de nition in Chapter 3, nevertheless future research may classify the circuit according to the experimental fault-tolerance criterion in Chapter 7. The bene t of this circuit is that it is designed according to realistic device layouts such as the depreciated 16-qubit `ibmq_Melbourne` device [6]. The required device layout is shown in the circuit in Figure 8.2. In addition, it may be possible to classify the fault-tolerance of sequences of $[7, 1, 3]$-encoded logical single qubit gates implemented transversely according to Section 4.2.

2. Quantum-classical machine learning for estimating encoding parameters. The results in Chapter 7 show that the $[4, 2, 2]$-encoded gate sequences are fault-tolerant according to a simple criterion, however the error inherent to the

Figure 8.2: Qubit layout suitable for the circuit in Figure 8.1.

real-hardware may not be completely encompassed by the Pauli error model simulated in Chapter 4 and Chapter 5. In Appendix 9.3, it is shown in Figure 9.1 and Figure 9.2 that by adjusting the value of an user-de ned rotation gate located after the Hadamard gate in the encoding circuit (see Figure 9.3), may cause uctuations of the lower bound of the error rate D_c of the encoded scheme. Future work may seek to nd the optimum value of this parameter to minimise D_c. This may be done through an iterative quantum-classical machine learning approach that mitigates the deleterious conditions in the device within a certain calibration cycle. The bene t of this approach is that it may reduce the lower-bound of the error rate of the encoded gate sequence without the need to have full knowledge of the speci c noise model in the device at the time of the circuit activation.

Chapter 9

Appendix

9.1 Deriving the Steane Encoded Logical State

The Steane code is an example of a CSS code constructed from the Hamming (7,4,3) code. It is constructed from the $C_1(7,4)$ and $C_2(7,3)$ codes such that $C_2 \subset C_1$ [9]. This results in a $(n, k_1 - k_2) = (7, 1)$ CSS code that can correct up to $t = 1$ qubit error.

To derive the Steane encoded logical states the classical counterparts C_1 and C_2 are used. The generator matrix[1] for the $[7,4,3]$ Hamming code is given by [9]

$$G(C_1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}. \tag{9.1}$$

Lets define x as a column vector with k information bits and y the n-bit codeword mapping. Then y is found by

$$y = Gx \tag{9.2}$$

[1] Note that in this case we are using the definition for G found in [9] which is different from that in [112], both are equivalent.

multiplication is modulo-2 [163]. For example, if $x = [0101]^T$ then

$$y = Gx = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}: \tag{9.3}$$

9.2 Density Matrix in terms of Pauli Matrices

A single qubit state on the Bloch sphere can be described by

$$|\ i\rangle = \cos\frac{}{2}|0\rangle + e^{i}\ \sin\frac{}{2}|1\rangle \qquad \begin{pmatrix} \cos\frac{}{2} \\ e^{i}\ \sin\frac{}{2} \end{pmatrix} \tag{9.4}$$

where 0 and $0\ \ 2$ are real numbers and de ne a state on the Bloch sphere in Figure 2.2. A non-observable global phase factor e^{i} is omitted from this equation.

The density operator is de ned as

$$= |\ i\langle\ | = \begin{pmatrix} \cos\frac{}{2} \\ e^{i}\ \sin\frac{}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{}{2} & e^{\ i}\ \sin\frac{}{2} \end{pmatrix} = \begin{pmatrix} \cos^2\frac{}{2} & e^{\ i}\ \cos\frac{}{2}\sin\frac{}{2} \\ e^{i}\ \cos\frac{}{2}\sin\frac{}{2} & \sin^2\frac{}{2} \end{pmatrix} \tag{9.5}$$

Using Eulers formulae and the following trigonometric identities $\cos(2\ ) = 2\cos^2(\ )\ \ 1 = 1\ \ 2\sin^2(\ )$ and $\cos\frac{}{2}\sin\frac{}{2} = \frac{1}{2}\sin(\ )$ then

$$= \frac{1}{2} \begin{pmatrix} 1 + \cos & \cos\ \sin\ \ i\sin\ \sin \\ \cos\ \sin\ + i\sin\ \sin & 1\ \ \cos \end{pmatrix}: \tag{9.6}$$

This can be expressed in terms of the Pauli matrices $\{I; X; Y; Z\ g$ as follows

$$= \frac{1}{2}\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \cos\ \sin \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \sin\ \sin \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + \cos \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right] \tag{9.7}$$

$$= \frac{1}{2}\left[I + \cos\ \sin X + \sin\ \sin Y + \cos Z \right] = \frac{1}{2}(I + r \cdot v) \tag{9.8}$$

where

$$r = (r_x; r_y; r_z): \tag{9.9}$$

9.3 Coherent Error Insertion

Figure 9.1: Experimental results from the Ibmq_Jakarta device showing random sequences of the $[4,2,2]$-encoded gates and of the corresponding uncoded gate for sequence lengths L. A rotation error θ is inserted after the Hadamard gate in the encoding circuit. 30 samples 21.06.2021

Figure 9.2: Experiment results from Ibmq_Bogota (same as Figure 7.12) with a rotation error θ inserted after the Hadamard gate in the encoding circuit.

What are the most critical parameters when assessing a noise model? A tangible hypothesis is that rather than encountering a symmetric depolarizing noise channel, the device error is biased towards phase-flip errors (Z) rather than bit-flip errors (X) [164, 36, 99]. This is because the physical process of a phase-flip error is in a more direct interaction with the environment [165]. However, there may be many parameters that accurately characterize a qubit that are not accounted for by the Pauli error model.

For example, a simple calibration error may be viewed as an over-rotation (or under-rotation) of a gate which has the same value each time the gate is activated. When this is systematic, the error is accumulated if the gate is used repeatedly and in theory can be resolved by improving the accuracy of the calibration of the gate rotation. Another type of gate error is constructed by dephasing errors. This varies randomly between each activation of the gate and it tends to be dependent on the time required to complete the associated operation. A leakage error is incoherent. This occurs when a qubit is relaxed from $|0\rangle$ to $|l\rangle$ at a probability of p. Crosstalk errors occur in two-qubit gates, which occur owing to the interactions between the target system connecting systems and they are also excluded from a traditional model of independent component errors [156].

Figure 9.3: Coherent error insertion.

Figure 9.1 and Figure 9.2 show the results of inserting a rotation error in the encoding circuit before a random sequence of coded gates. This is demonstrated by the circuit shown in Figure 9.3. Figure 9.1 shows that as the rotation is increased, the error oor of the coded scheme is also increased. The opposite trend is seen in Figure 9.2. Therefore it may be concluded that this experiment is not robust to an over-rotation (or under-rotation) of the gate in the location shown in the circuit of Figure 9.3. Additionally, this error cannot be signi cantly mitigated by post-selection.

9.4 Other Encoded States

Figure 9.4: Encoder for $|\overline{0+}\rangle$

Figure 9.5: $|\overline{-+}\rangle$

Apart from the circuit in Figure 7.7, other states that can also be directly prepared using the $[4,2,2]$ code, which are:

$$|\overline{0+}\rangle = (|\overline{00}\rangle + |\overline{01}\rangle)/\sqrt{2} \tag{9.10}$$

$$|\overline{-+}\rangle = (|\overline{00}\rangle + |\overline{11}\rangle)/\sqrt{2}. \tag{9.11}$$

The circuit preparing the $|\overline{0+}\rangle$ state in Eq. (9.10) is shown in Figure 9.4. In this circuit there are two possible scenarios if either of the CNOT gates impose an error. Either it will result in a single qubit error, which can be picked up by post-selection, or the error will not affect the correctly prepared state. For example, an XX Pauli error after the CNOT gate between (q_2, q_3) has no effect on the output distribution;

$$|\overline{0+}\rangle = |0000\rangle + |1111\rangle + |1100\rangle + |0011\rangle)/2, \tag{9.12}$$

since $|0000\rangle$ and $|0011\rangle$ are interchangeable. The circuit preparing the $|\overline{-+}\rangle$ state shown in Figure 9.5 is also fault-tolerant following a similar reasoning to that for Figure 9.4.

We also see that the class of circuits that generate a 2-dimensional superposition state at the circuit output have an upper bound on the trace distance that is 0.5 in the depolarizing channel. For example, consider the circuit which prepares initial state $q_0q_1 \; |-+\rangle$ from Eq. (9.11) and then applies an X_0 gate. The transformation of the X_0 gate has the effect[2]

$$|-+\rangle = |00\rangle + |11\rangle \xrightarrow{X_0} |10\rangle + |01\rangle \tag{9.13}$$

and therefore the superposition state $(|10\rangle + |01\rangle)/\sqrt{2}$ is generated by the gate sequence. This can be described by

$$p^u_{01;10} = \frac{1}{2}, \quad p^u_i = 0 \quad \forall \; i = \{00, 11\}. \tag{9.14}$$

When the experimental outcome is totally corrupted the measured is that in Eq. (7.14). In this case, by Eq.(7.8), the uncoded error rate is

$$D_u = \frac{1}{2}(2|p^u_{01;10} - p^u_j| + 2|p^u_i - p^u_j|) = 0.5 \tag{9.15}$$

when the depolarizing channel noise is $= 1$.

The corresponding encoded circuit has the same upper bound. This circuit has the transformation

$$|\overline{-+}\rangle \xrightarrow{\overline{X}_0} |\overline{10}\rangle + |\overline{01}\rangle \tag{9.16}$$

[2] Normalization is omitted.

so the ideal output state is

$$p^c_{0101;1010} = p^c_{1100;0011} = \frac{1}{4}; \tag{9.17}$$
$$p^c_i = 0 \; 8 \quad i = f\,0000;\,1111;\,0110;\,1001g:$$

When experimental outcome is that in Eq. (7.19), by Eq.(7.9), the error rate upper bound is also

$$D_c = \frac{1}{2}(4jp^c_{0101;1010} \quad p^c_j j + 4\,jp^c_i \quad p^c_j j) = 0:5: \tag{9.18}$$

Bibliography

[1] R. Cane, D. Chandra, S. X. Ng, and L. Hanzo, \Mitigation of decoherence-induced quantum-bit errors and quantum-gate errors using steane's code,"IEEE Access, vol. 8, pp. 83693{83709, 2020.

[2] R. Cane, D. Chandra, S. X. Ng, and L. Hanzo, \Gate-error-resilient quantum steane codes,"IEEE Access, vol. 8, pp. 179346{179362, 2020.

[3] R. Cane and S. Ng, \Turbo-coded secure and reliable quantum teleportation," IET Quantum Communication, vol. 1, April 2020.

[4] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, \Superconducting qubits: Current state of play," Annual Review of Condensed Matter Physics, vol. 11, pp. 369{395, 2020.

[5] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al., \Quantum supremacy using a programmable superconducting processor,"Nature, vol. 574, no. 7779, pp. 505{510, 2019.

[6] IBM Quantum. Available at https://quantum-computing.ibm.com/ , accessed 2021-03-31.

[7] Rigetti. Available at https://www.rigetti.com/ , accessed 2021-03-31.

[8] Ionq. Available at https://ionq.com/resources , accessed 2021-03-31.

[9] M. A. Nielsen and I. Chuang, Quantum computation and quantum information. Cambridge University Press, UK, 2010.

[10] P. W. Shor, \Fault-tolerant quantum computation," in Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on, pp. 56{65, IEEE, 1996.

[11] C. H. Bennett and D. P. DiVincenzo, \Quantum information and computation," nature, vol. 404, no. 6775, pp. 247{255, 2000.

[12] J. Von Neumann, \Probabilistic logics and the synthesis of reliable organisms from unreliable components," Automata studies, vol. 34, pp. 43{98, 1956.

[13] P. W. Shor, \Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM review, vol. 41, no. 2, pp. 303{332, 1999.

[14] A. Y. Kitaev, \Quantum error correction with imperfect gates," in Quantum Communication, Computing, and Measurement, pp. 181{188, Springer, 1997.

[15] A. Y. Kitaev, \Quantum computations: algorithms and error correction," Russian Mathematical Surveys, vol. 52, no. 6, pp. 1191{1249, 1997.

[16] J. Cirac, T. Pellizzari, and P. Zoller, \Enforcing coherent evolution in dissipative quantum dynamics," Science, vol. 273, no. 5279, pp. 1207{1210, 1996.

[17] W. H. Zurek and R. La amme, \Quantum logical operations on encoded qubits," Physical review letters, vol. 77, no. 22, p. 4683, 1996.

[18] D. Aharonov and M. Ben-Or, \Fault-tolerant quantum computation with constant error rate," SIAM Journal on Computing, 2008.

[19] E. Knill, R. La amme, and W. H. Zurek, \Resilient quantum computation," Science, vol. 279, no. 5349, pp. 342{345, 1998.

[20] A. Y. Kitaev, \Fault-tolerant quantum computation by anyons," Annals of Physics, vol. 303, no. 1, pp. 2{30, 2003.

[21] D. Gottesman and I. L. Chuang, \Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," Nature, vol. 402, no. 6760, pp. 390{393, 1999.

[22] X. Zhou, D. W. Leung, and I. L. Chuang, \Methodology for quantum logic gate construction," Physical Review A, vol. 62, no. 5, p. 052316, 2000.

[23] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, \Topological quantum memory," Journal of Mathematical Physics, vol. 43, no. 9, pp. 4452{4505, 2002.

[24] S. Bravyi and A. Kitaev, \Universal quantum computation with ideal Cli ord gates and noisy ancillas,"Physical Review A, vol. 71, no. 2, p. 022316, 2005.

[25] R. Raussendorf and J. Harrington, \Fault-tolerant quantum computation with high threshold in two dimensions," Physical review letters, vol. 98, no. 19, p. 190504, 2007.

[26] R. Raussendorf, J. Harrington, and K. Goyal, \Topological fault-tolerance in cluster state quantum computation," New Journal of Physics, vol. 9, no. 6, p. 199, 2007.

[27] H. Bombin and M. Martin-Delgado, \Topological computation without braiding," Physical review letters, vol. 98, no. 16, p. 160502, 2007.

[28] A. Paetznick and B. W. Reichardt, \Universal fault-tolerant quantum computation with only transversal gates and error correction," Physical review letters, vol. 111, no. 9, p. 090505, 2013.

[29] P. W. Shor, \Scheme for reducing decoherence in quantum computer memory," Physical review A, vol. 52, no. 4, p. R2493, 1995.

[30] A. R. Calderbank and P. W. Shor, \Good quantum error-correcting codes exist," Physical Review A, vol. 54, no. 2, p. 1098, 1996.

[31] A. M. Steane, \Error correcting codes in quantum theory," Physical Review Letters, vol. 77, no. 5, p. 793, 1996.

[32] 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, p. 3824, 1996.

[33] R. La amme, C. Miquel, J. P. Paz, and W. H. Zurek, \Perfect quantum error correcting code," Physical Review Letters, vol. 77, no. 1, p. 198, 1996.

[34] D. Gottesman, Stabilizer codes and quantum error correction. California Institute of Technology, 1997.

[35] D. Gottesman, \Class of quantum error-correcting codes saturating the quantum hamming bound," Physical Review A, vol. 54, no. 3, p. 1862, 1996.

[36] 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.

[37] E. T. Campbell, B. M. Terhal, and C. Vuillot, \Roads towards fault-tolerant universal quantum computation," Nature, vol. 549, no. 7671, p. 172, 2017.

[38] J. Preskill, \Quantum computing in the nisq era and beyond," Quantum, vol. 2, p. 79, 2018.

[39] D. Gottesman, \The heisenberg representation of quantum computers," Conference: Group theoretical methods in physics, 1998.

[40] S. Aaronson and D. Gottesman, \Improved simulation of stabilizer circuits," Physical Review A, vol. 70, no. 5, p. 052328, 2004.

[41] B. Eastin and E. Knill, \Restrictions on transversal encoded quantum gate sets," Physical review letters, vol. 102, no. 11, p. 110502, 2009.

[42] X. Chen, H. Chung, A. W. Cross, B. Zeng, and I. L. Chuang, \Subsystem stabilizer codes cannot have a universal set of transversal gates for even one encoded qudit," Physical Review A, vol. 78, no. 1, p. 012353, 2008.

[43] M. D. Reed, L. DiCarlo, S. E. Nigg, L. Sun, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, \Realization of three-qubit quantum error correction with superconducting circuits," Nature, vol. 482, no. 7385, pp. 382{385, 2012.

[44] R. Barends, J. Kelly, A. Megrant, D. Sank, E. Je rey, Y. Chen, Y. Yin, B. Chiaro, J. Mutus, C. Neill, et al., \Coherent josephson qubit suitable for scalable quantum integrated circuits," Physical review letters, vol. 111, no. 8, p. 080502, 2013.

[45] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Je rey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, et al., \Superconducting quantum circuits at the surface code threshold for fault tolerance," Nature, vol. 508, no. 7497, pp. 500{503, 2014.

[46] J. M. Chow, J. M. Gambetta, E. Magesan, D. W. Abraham, A. W. Cross, B. Johnson, N. A. Masluk, C. A. Ryan, J. A. Smolin, S. J. Srinivasan, et al., \Implementing a strand of a scalable fault-tolerant quantum computing fabric," Nature communications, vol. 5, no. 1, pp. 1{9, 2014.

[47] O.-P. Saira, J. Groen, J. Cramer, M. Meretska, G. De Lange, and L. DiCarlo, \Entanglement genesis by ancilla-based parity measurement in 2d circuit qed," Physical review letters, vol. 112, no. 7, p. 070502, 2014.

[48] D. Riste, S. Poletto, M.-Z. Huang, A. Bruno, V. Vesterinen, O.-P. Saira, and L. DiCarlo, \Detecting bit- ip errors in a logical qubit using stabilizer measurements," Nature communications, vol. 6, no. 1, pp. 1{6, 2015.

[49] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Je rey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Y. Chen, et al., \State preservation by repetitive error detection in a superconducting quantum circuit," Nature, vol. 519, no. 7541, pp. 66{69, 2015.

[50] A. D. Corcoles, E. Magesan, S. J. Srinivasan, A. W. Cross, M. Ste en, J. M. Gambetta, and J. M. Chow, \Demonstration of a quantum error detection code using a square lattice of four superconducting qubits," Nature communications, vol. 6, no. 1, pp. 1{10, 2015.

[51] D. Alsina and J. I. Latorre, \Experimental test of mermin inequalities on a ve-qubit quantum computer," Physical Review A, vol. 94, no. 1, p. 012314, 2016.

[52] S. J. Devitt, \Performing quantum computing experiments in the cloud," Physical Review A, vol. 94, no. 3, p. 032329, 2016.

[53] M. Takita, A. D. Corcoles, E. Magesan, B. Abdo, M. Brink, A. Cross, J. M. Chow, and J. M. Gambetta, \Demonstration of weight-four parity measurements in the surface code architecture," Physical review letters, vol. 117, no. 21, p. 210505, 2016.

[54] I. Sohn, S. Tarucha, and B.-S. Choi, \Analysis of physical requirements for simple three-qubit and nine-qubit quantum error correction on quantum-dot and superconductor qubits," Physical Review A, vol. 95, no. 1, p. 012306, 2017.

[55] J. R. Wootton and D. Loss, \Repetition code of 15 qubits," Phys. Rev. A, vol. 97, p. 052313, May 2018.

[56] R. W. Heeres, P. Reinhold, N. Ofek, L. Frunzio, L. Jiang, M. H. Devoret, and R. J. Schoelkopf, \Implementing a universal gate set on a logical qubit encoded in an oscillator," Nature communications, vol. 8, no. 1, pp. 1{7, 2017.

[57] M. Takita, A. W. Cross, A. Corcoles, J. M. Chow, and J. M. Gambetta, \Experimental demonstration of fault-tolerant state preparation with superconducting qubits," Physical review letters, vol. 119, no. 18, p. 180501, 2017.

[58] B. Pokharel, N. Anand, B. Fortman, and D. A. Lidar, \Demonstration of delity improvement using dynamical decoupling with superconducting qubits," Physical review letters, vol. 121, no. 22, p. 220502, 2018.

[59] D. Gottesman, \Quantum fault tolerance in small experiments," arXiv preprint arXiv:1610.03507, 2016.

[60] C. Vuillot, \Is error detection helpful on ibm 5q chips?," Quantum Information and Computation, vol. 18, no. 11, p. 0949, 2018.

[61] D. Willsch, M. Willsch, F. Jin, H. De Raedt, and K. Michielsen, \Testing quantum fault tolerance on small systems," Physical Review A, vol. 98, no. 5, p. 052348, 2018.

[62] J. Ro e, D. Headley, N. Chancellor, D. Horsman, and V. Kendon, \Protecting quantum memories using coherent parity check codes," Quantum Science and Technology, vol. 3, no. 3, p. 035010, 2018.

[63] R. Harper and S. T. Flammia, \Fault-tolerant logical gates in the ibm quantum experience," Physical review letters, vol. 122, no. 8, p. 080504, 2019.

[64] C. K. Andersen, A. Remm, S. Lazar, S. Krinner, J. Heinsoo, J.-C. Besse, M. Gabureac, A. Wallra , and C. Eichler, \Entanglement stabilization using ancilla-based parity detection and real-time feedback in superconducting circuits," npj Quantum Information , vol. 5, no. 1, pp. 1{7, 2019.

[65] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, \Topological quantum memory," Journal of Mathematical Physics, vol. 43, no. 9, pp. 4452{4505, 2002.

[66] J. Preskill, \Fault-tolerant quantum computation," in Introduction to quantum computation and information, pp. 213{269, World Scienti c, 1998.

[67] D. Gottesman, \Fault-tolerant quantum computation with constant overhead," Quantum Info. Comput., vol. 14, p. 1338{1372, Nov. 2014.

[68] A. D. Corcoles, M. Takita, K. Inoue, S. Lekuch, Z. K. Minev, J. M. Chow, and J. M. Gambetta, \Exploiting dynamic quantum circuits in a quantum algorithm with superconducting qubits," Physical Review Letters, vol. 127, 2021.

[69] I. Buluta and F. Nori, \Quantum simulators," Science, vol. 326, no. 5949, pp. 108{111, 2009.

[70] G.-S. Paraoanu, \Recent progress in quantum simulation using superconducting circuits," Journal of Low Temperature Physics, vol. 175, no. 5, pp. 633{654, 2014.

[71] A. M. Dalzell, A. W. Harrow, D. E. Koh, and R. L. La Placa, \How many qubits are needed for quantum computational supremacy?,"Quantum, vol. 4, p. 264, May 2020.

[72] L. DiCarlo, J. M. Chow, J. M. Gambetta, L. S. Bishop, B. R. 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, pp. 240{244, 2009.

[73] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, et al., \Computing prime factors with a josephson phase qubit quantum processor,"Nature Physics, vol. 8, no. 10, pp. 719{723, 2012.

[74] N. Moll, P. Barkoutsos, L. S. Bishop, J. M. Chow, A. Cross, D. J. Egger, S. Filipp, A. Fuhrer, J. M. Gambetta, M. Ganzhorn, et al., \Quantum optimization using variational algorithms on near-term quantum devices," Quantum Science and Technology, vol. 3, no. 3, p. 030503, 2018.

[75] A. Montanaro, \Quantum algorithms: an overview," npj Quantum Information, vol. 2, no. 1, pp. 1{8, 2016.

[76] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, \Quantum machine learning," Nature, vol. 549, no. 7671, pp. 195{202, 2017.

[77] V. Akshay, H. Philathong, M. E. Morales, and J. D. Biamonte, \Reachability de cits in quantum approximate optimization," Physical review letters, vol. 124, no. 9, p. 090504, 2020.

[78] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, \Characterizing quantum supremacy in near-term devices,"Nature Physics, vol. 14, no. 6, pp. 595{600, 2018.

[79] Y. Zhou, E. M. Stoudenmire, and X. Waintal, \What limits the simulation of quantum computers?," Physical Review X, vol. 10, no. 4, p. 041038, 2020.

[80] S. Bravyi, D. Gosset, R. Koenig, and M. Tomamichel, \Quantum advantage with noisy shallow circuits," Nature Physics, vol. 16, no. 10, pp. 1040{1045, 2020.

[81] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, et al., \Quantum computational advantage using photons," Science, vol. 370, no. 6523, pp. 1460{1463, 2020.

[82] M. H. Devoret and R. J. Schoelkopf, \Superconducting circuits for quantum information: an outlook," Science, vol. 339, no. 6124, pp. 1169{1174, 2013.

[83] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. Girvin, L. Jiang, et al., \Extending the lifetime of a quantum bit with error correction in superconducting circuits," Nature, vol. 536, no. 7617, pp. 441{445, 2016.

[84] D. Gottesman, \An introduction to quantum error correction and fault-tolerant quantum computation," in Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics, vol. 68, pp. 13{58, 2010.

[85] D. Chandra, Z. Babar, H. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, \Quantum topological error correction codes are capable of improving the performance of Cli ord gates," IEEE Access, 2019.

[86] S. Huang and K. R. Brown, \Constructions for measuring error syndromes in calderbank-shor-steane codes between shor and steane methods," Physical Review A, vol. 104, no. 2, p. 022429, 2021.

[87] C. Chamberland and M. E. Beverland, \Flag fault-tolerant error correction with arbitrary distance codes," Quantum, vol. 2, p. 53, 2018.

[88] H. Goto, \Minimizing resource overheads for fault-tolerant preparation of encoded states of the steane code," Scienti c reports , vol. 6, p. 19578, 2016.

[89] 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.

[90] 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.

[91] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, \Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 881{919, 2019.

[92] L. Gyongyosi, S. Imre, and H. V. Nguyen, \A survey on quantum channel capacities," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1149{1205, 2018.

[93] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, \Secure quantum communication technologies and systems: From labs to markets," Quantum Rep., vol. 2, no. 1, pp. 80{106, 2020.

[94] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirnadola, and M. Razavi, \Long-distance continuous-variable quantum key distribution with quantum scissors," IEEE Journal of Selected Topics in Quantum Electronics, vol. 26, no. 3, pp. 1{12, 2020.

[95] Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, and L. Hanzo, \Measurement-device-independent quantum secure direct communication,"Science China Physics, Mechanics & Astronomy, vol. 63, no. 3, p. 230362, 2020.

[96] N. M. Linke, M. Gutierrez, K. A. Landsman, C. Figgatt, S. Debnath, K. R. Brown, and C. Monroe, \Fault-tolerant quantum error detection," Science advances, vol. 3, no. 10, p. e1701074, 2017.

[97] A. Kole and I. Sengupta, \Resource optimal realization of fault-tolerant quantum circuit," in 2020 IEEE International Test Conference India, pp. 1{10, IEEE, 2020.

[98] N. D. Mermin, Quantum computer science: an introduction Cambridge University Press, 2007.

[99] 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.

[100] D. Aharonov, A. Kitaev, and N. Nisan, \Quantum circuits with mixed states," in Proceedings of the thirtieth annual ACM symposium on Theory of computing pp. 20{30, 1998.

[101] J. Preskill, Lecture Notes for Physics 229:Quantum Information and Computation. CreateSpace Independent Publishing Platform, 2015.

[102] D. P. DiVincenzo, \Quantum gates and circuits," Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 454, no. 1969, pp. 261{276, 1998.

[103] D. P. DiVincenzo, \The physical implementation of quantum computation," Fortschritte der Physik: Progress of Physics, vol. 48, no. 9-11, pp. 771{783, 2000.

[104] W. K. Wootters, \Entanglement of formation of an arbitrary state of two qubits," Physical Review Letters, vol. 80, no. 10, p. 2245, 1998.

[105] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, \Quantum entanglement," Reviews of modern physics, vol. 81, no. 2, p. 865, 2009.

[106] G. Vidal and R. F. Werner, \Computable measure of entanglement," Physical Review A, vol. 65, no. 3, p. 032314, 2002.

[107] D. Gottesman, \Theory of fault-tolerant quantum computation," Physical Review A, vol. 57, no. 1, p. 127, 1998.

[108] G. Nebe, E. M. Rains, and N. J. Sloane, \The invariants of the Cli ord groups," Designs, Codes and Cryptography, vol. 24, no. 1, pp. 99{122, 2001.

[109] E. Knill, \Quantum computing with realistically noisy devices," Nature, vol. 434, no. 7029, p. 39, 2005.

[110] S. J. Devitt, W. J. Munro, and K. Nemoto, \Quantum error correction for beginners," Reports on Progress in Physics, vol. 76, no. 7, p. 076001, 2013.

[111] A. Steane, \Multiple-particle interference and quantum error correction," Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 452, no. 1954, pp. 2551{2577, 1996.

[112] D. Chandra, Z. Babar, H. 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. 11557{11581, 2017.

[113] R. Landauer, \Irreversibility and heat generation in the computing process," IBM journal of research and development, vol. 5, no. 3, pp. 183{191, 1961.

[114] V. Vedral and M. B. Plenio, \Basics of quantum computation," Progress in Quantum Electronics, vol. 22, no. 1, pp. 1{39, 1998.

[115] A. M. Steane, \Active stabilization, quantum computation, and quantum state synthesis," Physical Review Letters, vol. 78, no. 11, p. 2252, 1997.

[116] D. P. DiVincenzo and P. W. Shor, \Fault-tolerant error correction with e cient quantum codes," Physical review letters, vol. 77, no. 15, p. 3260, 1996.

[117] R. Chao and B. W. Reichardt, \Quantum error correction with only two extra qubits," Physical review letters, vol. 121, no. 5, p. 050502, 2018.

[118] L. Egan, D. Debroy, C. Noel, A. Risinger, D. Zhu, D. Biswas, M. Newman, M. Li, K. Brown, M. Cetina, et al., \Fault-tolerant operation of a quantum error-correction code," Bulletin of the American Physical Society, 2021.

[119] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. Nguyen, S. X. Ng, and L. Hanzo, \Quantum error correction protects quantum search algorithms against decoherence," Scienti c reports , vol. 6, p. 38095, 2016.

[120] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, \Validating quantum computers using randomized model circuits,"Physical Review A, vol. 100, no. 3, p. 032328, 2019.

[121] C. Ballance, T. Harty, N. Linke, M. Sepiol, and D. Lucas, \High- delity quantum logic gates using trapped-ion hyper ne qubits," Physical review letters, vol. 117, no. 6, p. 060504, 2016.

[122] C.-Y. Lai, Y.-C. Zheng, and T. A. Brun, \Fault-tolerant preparation of stabilizer states for quantum calderbank-shor-steane codes by classical error-correcting codes," Physical Review A, vol. 95, no. 3, p. 032339, 2017.

[123] P. Aliferis, D. Gottesman, and J. Preskill, \Quantum accuracy threshold for concatenated distance-3 codes,"Quantum Info. Comput., vol. 6, p. 97{165, Mar. 2006.

[124] A. Paetznick and B. W. Reichardt, \Fault-tolerant ancilla preparation and noise threshold lower bounds for the 23-qubit golay code,"Quantum Information and Computation, vol. 12, p. 1034, 2012.

[125] K. M. Svore, D. P. Divincenzo, and B. M. Terhal, \Noise threshold for a fault-tolerant two-dimensional lattice architecture," Quant. Inf. Comp., vol. 7, no. 4, p. 297, 2007.

[126] A. M. Steane, \Overhead and noise threshold of fault-tolerant quantum error correction," Physical Review A, vol. 68, no. 4, p. 042322, 2003.

[127] Y. S. Weinstein, \Fidelity of an encoded [7,1,3] logical zero,"Phys. Rev. A, vol. 84, p. 012323, Jul 2011.

[128] A. Y. Kitaev, \Quantum computations: algorithms and error correction," Russian Mathematical Surveys, vol. 52, no. 6, pp. 1191{1249, 1997.

[129] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, \Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," Physical review letters, vol. 70, pp. 1895{1899, 04 1993.

[130] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, \Advances in quantum teleportation," Nature Photonics, vol. 9, no. 10, pp. 641{652, 2015.

[131] C. Berrou, A. Glavieux, and P. Thitimajshima, \Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," inIEEE International Conference on Communications, vol. 2, (Geneva), pp. 1064{1070 vol.2, May 1993.

[132] D. Poulin, J. Tillich, and H. Ollivier, \Quantum serial turbo codes," IEEE Transactions on Information Theory, vol. 55, no. 6, pp. 2776{2798, 2009.

[133] 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, p. 042317, Oct 2003.

[134] A. Einstein, B. Podolsky, and N. Rosen, \Can quantum-mechanical description of physical reality be considered complete?,"Phys. Rev., vol. 47, pp. 777{780, May 1935.

[135] N. Pisenti, C. P. E. Gaebler, and T. W. Lynn, \Distinguishability of hyperentangled bell states by linear evolution and local projective measurement,"Phys. Rev. A, vol. 84, p. 022340, Aug 2011.

[136] B. Sklar, Fundamentals of Turbo Codes Prentice Hall, USA, March 2002.

[137] E. Knill, \Quantum computing with realistically noisy devices," Nature, vol. 434, no. 7029, pp. 39{44, 2005.

[138] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, \Quantum cryptography," Reviews of Modern Physics, vol. 74, pp. 145{195, March 2002.

[139] X. Li, N. Wan, and D. Zhang, \Quantum determined key distribution scheme using quantum teleportation," in WRI World Congress on Software Engineering, vol. 1, (Xiamen, China), pp. 431{434, 2009.

[140] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, \Puri cation of noisy entanglement and faithful teleportation via noisy channels," Physical review letters, vol. 76, no. 5, p. 722, 1996.

[141] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, \Entangled state quantum cryptography: Eavesdropping on the ekert protocol," Phys. Rev. Lett., vol. 84, pp. 4733{4736, May 2000.

[142] S. Schauer and M. Suda, \Security of entanglement swapping qkd protocols against collective attacks," in The Sixth International Conference on Quantum, Nano and Micro Technologies (ICQNM) , (Rome, Italy), 2012.

[143] 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, p. 146{176, 2015.

[144] 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.

[145] F.-G. Deng and G. L. Long, \Secure direct communication with a quantum one-time pad," Phys. Rev. A, vol. 69, p. 052319, May 2004.

[146] M. Lucamarini and S. Mancini, \Secure deterministic communication without entanglement," Phys. Rev. Lett., vol. 94, p. 140501, Apr 2005.

[147] G. Fei, L. Song, W. Qiao-Yan, and Z. Fu-Chen, \A special eavesdropping on one-sender VersusN-receiver QSDC protocol,"Chinese Physics Letters, vol. 25, pp. 1561{1563, may 2008.

[148] M. Zhong-Xiao and X. Yun-Jie, \Improvement of security of three-party quantum secure direct communication based on GHZ states,"Chinese Physics Letters, vol. 24, pp. 15{18, jan 2007.

[149] A. Wojcik, \Eavesdropping on the \ping-pong" quantum communication protocol," Physical Review Letters, vol. 90, Apr 2003.

[150] H. K. Ng and J. Preskill, \Fault-tolerant quantum computation versus gaussian noise," Physical Review A, vol. 79, no. 3, p. 032318, 2009.

[151] E. Knill, R. La amme, and W. H. Zurek, \Resilient quantum computation: error models and thresholds," Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 454, no. 1969, pp. 365{384, 1998.

[152] Y. R. Sanders, J. J. Wallman, and B. C. Sanders, \Bounding quantum gate error rate based on reported average delity," New Journal of Physics, vol. 18, no. 1, p. 012002, 2015.

[153] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout, \What randomized benchmarking actually measures," Phys. Rev. Lett., vol. 119, p. 130502, Sep 2017.

[154] D. Greenbaum and Z. Dutton, \Modeling coherent errors in quantum error correction," Quantum Science and Technology, vol. 3, no. 1, p. 015007, 2017.

[155] P. Iyer and D. Poulin, \A small quantum computer is needed to optimize fault-tolerant protocols," Quantum Science and Technology, vol. 3, no. 3, p. 030504, 2018.

[156] J. M. Gambetta, A. D. Corcoles, S. T. Merkel, B. R. Johnson, J. A. Smolin, J. M. Chow, C. A. Ryan, C. Rigetti, S. Poletto, T. A. Ohki, et al., \Characterization of addressability by simultaneous randomized benchmarking,"Physical review letters, vol. 109, no. 24, p. 240504, 2012.

[157] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout, \What randomized benchmarking actually measures,"Physical review letters, vol. 119, no. 13, p. 130502, 2017.

[158] O. Oreshkov and J. Calsamiglia, \Distinguishability measures between ensembles of quantum states," Physical Review A, vol. 79, no. 3, p. 032336, 2009.

[159] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, \Surface codes: Towards practical large-scale quantum computation,'Phys. Rev. A, vol. 86, p. 032324, Sep 2012.

[160] T. Jochym-O'Connor and R. La amme, \Using concatenated quantum codes for universal fault-tolerant quantum gates," Physical Review Letters, vol. 112, Jan 2014.

[161] A. G. Fowler, \Minimum weight perfect matching of fault-tolerant topological quantum error correction in average o(1) parallel time," Quantum Info. Comput., vol. 15, p. 145{158, jan 2015.

[162] R. Cleve and D. Gottesman, \E cient computations of encodings for quantum error correction," Physical Review A, vol. 56, no. 1, p. 76, 1997.

[163] 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.

[164] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, \Fifteen years of quantum LDPC coding and improved decoding strategies,"IEEE Access, vol. 3, pp. 2492{ 2519, 2015.

[165] L. M. Vandersypen, M. Ste en, 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.