Suppression and characterization of decoherence in practical quantum information processing devices

by

Marcus Palmer da Silva

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2008

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public

M. Silva

Abstract

This dissertation addresses the issue of noise in quantum information processing devices. It is common knowledge that quantum states are particularly fragile to the effects of noise. In order to perform scalable quantum computation, it is necessary to suppress effective noise to levels which depend on the size of the computation. Various theoretical proposals have discussed how this can be achieved, under various assumptions about properties of the noise and the availability of qubits. We discuss new approaches to the suppression of noise, and propose experimental protocols characterizing the noise.

In the first part of the dissertation, we discuss a number of applications of teleportation to fault-tolerant quantum computation. We demonstrate how measurement-based quantum computation can be made inherently fault-tolerant by exploiting its relationship to teleportation. We also demonstrate how continuous variable quantum systems can be used as ancillas for computation with qubits, and how information can be reliably teleported between these different systems. Building on these ideas, we discuss how the necessary resource states for teleportation can be prepared by allowing quantum particles to be scattered by qubits, and investigate the feasibility of an implementation using superconducting circuits.

In the second part of the dissertation, we propose scalable experimental protocols for extracting information about the noise. We concentrate on information which has direct practical relevance to methods of noise suppression. In particular, we demonstrate how standard assumptions about properties of the noise can be tested in a scalable manner. The experimental protocols we propose rely on symmetrizing the noise by random application of unitary operations. Depending on the symmetry group use, different information about the noise can be extracted. We demonstrate, in particular, how to estimate the probability of a small number of qubits being corrupted, as well as how to test for a necessary condition for noise correlations. We conclude by demonstrating how, without relying on assumptions about the noise, the information obtained by symmetrization can also be used to construct protective encodings for quantum states.

Acknowledgments

I cannot emphasize how much I have learned from my colleagues at IQC over the last four years. It has been a great opportunity to be around so many talented people, and the experience has undoubtedly enriched my academic career. I owe a lot to Raymond Laflamme, Frank Wilhelm and Hamed Majedi, for their support and guidance, and the many opportunities they provided me with. I am grateful to the Natural Sciences and Engineering Council of Canada, the Bell Family Fund, and the University of Waterloo for their financial support.

I find that one of the highlights of my doctorate has been working with my collaborators. I thank Joseph Emerson, Elham Kashefi, David Kribs, Martin Laforest, Easwar Magesan, Osama Moussa, Bill Munro, Casey Myers, Kae Nemoto, Harold Ollivier, Martin Rötteler and Colm Ryan for all that I have gained from our discussions. I hope that in the future we have more chances to work together.

I have had a number of great teachers during my stay at Waterloo, without whom the path towards finishing the doctorate would have been much more arduous. I thank Daniel Gottesman, Joseph Emerson, Michel Gingras, Eric Poisson, and Achim Kempf for all the effort they put in their lectures, and for the insights they shared.

I thank all my IQC colleagues including Jonathan Baugh, J. C. Boileau, Jamie Batuwantudawe, Jeremy Chamilliard, Mike Ditty, Chris Erven, Rolf Horn, Adam Hubbard, Aziz Kara, Chandrashekar Madaiah, Camille Negrevergne, Tim Reid, and Lana Sheridan for making my stay enjoyable and stimulating. I also thank Judy McDonnell, Wendy Reibel, Lorna Schmalz, Mary Lyn Payerl, and all other staff members who make UW and IQC work.

I thank my friends and family for all their support and understanding over the last few months of hermitage. I owe Lu, Laura, Osama and Ben at least a few beers, and probably a whole lot more. I especially thank my sister Andrea and her husband Phil for introducing me to little Samuel.

Finally, I thank Wenting for her love, strength, and patience.

Esta tese é dedicada ao meu pai, Luis, e à minha mãe, Carol.

Contents

Preface **1**

Overview 1

Notation 5

Additional information for the examiners of this thesis 6

I Fault-tolerance and quantum error correction **9**

1 Fault-tolerant computation via measurements **11**

1.1 Introduction 11

1.2 Teleportation and one-way quantum computation 13

1.3 One-way quantum computation with phase preparation 17

1.4 Fault-tolerance 20

1.4.1 Simulation approach 22

1.4.2 Intrinsic fault-tolerance 23

1.5 Summary 29

2 Teleportation to and from a quantum bus **31**

2.1 Introduction 31

2.2 Quantum communication bus 33

2.3 One-bit teleportations between a qubit and a bus 35

2.3.1 Average fidelities 37

2.3.2 Post-selected teleportation . . . 39
2.4 Universal quantum computation . . . 42
2.4.1 Single qubit gates . . . 42
2.4.2 Entangling gates . . . 43
2.5 Preparation of entangled states . . . 46
2.5.1 Post-selected preparation of entangled states . . . 48
2.6 Error correction . . . 48
2.6.1 Fault-tolerance . . . 51
2.6.2 Noisy ancillas . . . 52
2.7 Summary . . . 53

3 Entanglement mediated by a ballistic particle **57**
3.1 Introduction . . . 57
3.2 Time evolution of a free particle . . . 59
3.3 Particle scattering by a qubit-dependent potential . . . 60
3.3.1 Coherent superpositions and interference . . . 63
3.3.2 Particle-mediated entanglement of qubits . . . 65
3.3.3 Protocol for entanglement verification . . . 71
3.4 Coherence length for free particles with dissipation . . . 72
3.5 Physical realization with superconducting circuits . . . 74
3.5.1 Solitons as quantum particles . . . 75
3.5.2 Interaction between particle and qubit . . . 79
3.5.3 Constraints on maximal qubit separation due to dispersion . . . 81
3.5.4 Coherence length as constrained by the qubit . . . 82
3.5.5 Coherence length of perturbed solitons . . . 83
3.6 Summary . . . 84

II Characterization of noise **87**

4 Efficient partial characterization of noise **89**

4.1 Introduction . . . 89

4.2 Background . . . 90

4.2.1 Average gate fidelity . . . 94

4.2.2 Clifford twirl . . . 98

4.3 Weight distribution of errors . . . 100

4.3.1 Weight monitoring protocol for estimating $\Pr(w)$ . . . 102

4.3.2 Parity monitoring protocol for estimating $\Pr(w)$ . . . 103

4.4 Propagation of uncertainties . . . 106

4.4.1 Use of ancillary channels . . . 109

4.5 Test for noise correlations . . . 110

4.5.1 Collective versus independent relaxation of identical qubits . . . 111

4.6 Summary . . . 114

5 Finding correctable encodings from experimental data **117**

5.1 Introduction . . . 117

5.2 Pauli Twirl . . . 118

5.3 Unitarily Correctable Codes . . . 121

5.4 PIP channel parameter space . . . 123

5.4.1 The map between probabilities and eigenvalues . . . 124

5.5 Finding Correctable Codes . . . 124

5.6 Verification and Robustness of UCC . . . 127

5.7 General unitary twirls . . . 130

5.8 Concluding remarks . . . 132

Appendix **137**

A Experimental status of superconducting circuit implementations **137**

A.1 Decoherence 137

A.2 Measurement 138

A.3 Single qubit operations 138

A.4 Interactions 138

A.5 Outlook 139

B Quantification of entanglement **141**

B.1 Entanglement Witnesses 141

B.2 Entanglement monotones 142

C Damped Harmonic Oscillator **145**

C.1 Solution at zero temperature 145

D Number of parameters to describe twirled channels **149**

D.1 A direct approach 149

D.2 A combinatorial approach 150

E Efficient computation of Ω by counting **153**

E.1 Pauli twirl 153

E.2 Clifford twirl 155

References **172**

List of Tables

3.1 Typical experimental parameters for a persistent current qubit [YHN+06] 76

3.2 Typical experimental parameters for a Josephson transmission line [Wal00, KU04, FSSKS07] 80

List of Figures

1 Circuit diagrams depicting (a) projective measurement of a qubit onto the eigenbasis of X with the outcome controlling the application of a unitary U, and (b) the interaction of two qubits via the unitary $\wedge Z$. . . . 6

1.1 Circuit diagram for the teleportation protocol. 14

1.2 Circuit diagrams for one-bit teleportation protocols (a) Z teleportation and (b) X teleportation. 15

1.3 One-bit teleportation of the unitary H. 16

1.4 Implementation of an arbitrary rotation about X in 1WQC. 16

1.5 Implementation of a the unitary $(\wedge Z)(H \otimes H)$ in 1WQC. 16

1.6 Measurement pattern operations, indexed by which qubit they operate on, and their corresponding quantum circuits. 18

1.7 Entanglement graph corresponding to the encoding of a single qubit into the 7 qubit CSS code. The boxed node corresponds to an arbitrary input qubit. All but the white qubits (corresponding to the encoding output) are measured in the X basis (up to feed-forward-based corrections). . . 24

1.8 Entanglement graphs for the fault-tolerant implementation of $\mathfrak{J}_0$. The boxed nodes correspond to input qubits, and all but the white nodes (corresponding to output qubits) are measured in the X eigenbasis (up to feed-forward-based corrections). 28

2.1 Circuits representing phase-space rotations of the qubus (red line) controlled by the state of the qubit (grey line). 34

2.2 Parity gate implemented using controlled phase space rotations. 35

2.3 Creation of entanglement through the use of a balanced beam-splitter. . 36

2.4 Approximate one-bit teleportation protocols between a qubit (grey) and a qubus (red) using controlled rotations. 36

2.5 Fidelity F_p of one-bit teleportation from the qubus to a qubit, as a function of x_d. 39

2.6 Contour lines for post-selected fidelity $F_{p,y}$ of one-bit teleportation from the qubus to a qubit (blue), and success probability for post-selection (red), as a functions of x_d and y. 41

2.7 A local gate U applied to the qubus via teleportations. 43

2.8 The entangling gate CSIGN performed via teleportation of qubus states. 44

2.9 Fidelity F_{CSIGN} due to CSIGN teleportation, as a function of x_d. 45

2.10 Contour lines for post-selected fidelity $F_{\text{CSIGN},y}$ of CSIGN teleportation (green), and success probability for post-selection (gold), as a functions of x_d and y. 46

2.11 Process fidelity F_{REP} of repetition encoding as a function of x_d. 47

2.12 Contour lines for post-selected process fidelity $F_{\text{REP},y}$ of 3-fold repetition encoding (blue), and success probability for post-selection (red), as a functions of x_d and y. 49

2.13 Contour lines for post-selected process fidelity $F_{\text{REP},y}$ of 9-fold repetition encoding (green), and success probability for post-selection (gold), as a functions of x_d and y. 50

2.14 Two parity gates combined to measure the Pauli operators ZZI and IZZ. 50

2.15 (a) Circuit for the measurement of the parity of four qubits [Sho96]. (b) Same circuit modified to use coherent states and controlled rotations. . 52

2.16 Process fidelity as a function of x_d for (a) the qubus logic single qubit gate (F_p); (b) the CSIGN teleportation (F_{CSIGN}); (c) repetition encoding with $N = 3$ shown in blue (F_{REP}); (d) repetition encoding with $N = 9$ (F_{REP}). 54

2.17 Curves of constant conditional process fidelity (solid) and the probability of post-selection success (dashed) as functions of x_d and y. In all cases, the fidelity is set to 0.9 and the probability of success to 0.5. 55

3.1 The probability distribution for the position of a particle (a) before and (b) after it has been scattered by (c) a potential which depends on the state of the qubits. 59

3.2 Circuit depicting the spatial displacement of a free particle (red line) controlled by the state of a qubit (grey line). 63

3.3 Protocol for the preparation of coherence superpositions of displaced wavefunctions of a particle (red line) by interacting with a qubit (grey line). 64

3.4 Protocol for the entanglement of two qubits (grey lines) via interaction with a particle (red line). 66

3.5 Distribution of position measurement outcomes for the state $|s(t)\rangle$, with regions of the distribution labeled by the qubit states they are correlated with. 66

3.6 Contour plot for (a) the fidelity between the post-selected state $\rho_{-w,w}$ and the maximally entangled state $|\Psi^+\rangle$ and for (b) the corresponding probability of obtaining the desired range of x measurement outcomes. 69

3.7 Cross sections of the fidelity F (a) as a function of w/σ for various $\Delta x/\sigma$ and (b) as a function of $\Delta x/\sigma$ for various w/σ. 69

3.8 Cross sections of the probability of success $\Pr([-w, w])$ (a) as a function of w/σ for various $\Delta x/\sigma$ and (b) as a function of $\Delta x/\sigma$ for various w/σ. 69

3.9 The logarithmic negativity E_N of $\rho_{-w,w}$ (a) as a function of $\Delta x/\sigma$ and w/σ, (b) as a function of w/σ for various $\Delta x/\sigma$ and (c) as a function of $\Delta x/\sigma$ for various w/σ. 71

3.10 Lumped element model of an infinitesimal section of a long Josephson junction. 76

3.11 Distribution of the phase difference ϕ, current density $\sin\phi$ and magnetic flux density ϕ_x for a fluxon. The blue line corresponds to a fluxon with $v = 0$, and the purple line to a fluxon with $v = 0.8$ 79

4.1 Circuit diagram representing the action of the ideal unitary $\mathcal{U}$, and the imperfect implementation $\tilde{\mathcal{U}}$. 94

4.2 Circuit diagram for twirling the quantum operation Λ. 97

4.3 Circuit diagram for the characterization of a $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ twirled channel. . . . 102

4.4 Bounds and numerical values for the scaling factor $\sigma_{\mathrm{Pr}(w)}/\sigma_\lambda$ as a function of the number n of qubits and the weight w of the errors. 109

4.5 Twirled channel parameters for collective and independent relaxation. . 114

4.6 Time dependence of the twirled channel parameters for independent relaxation. 115

4.7 Time dependence of the twirled channel parameters for collective relaxation. 115

5.1 Circuit diagram for the characterization of a PIP channel, where $\mathcal{C}_i \in \mathcal{C}_1$. 121

5.2 Circuit diagram corresponding to the composition of quantum operations $\mathcal{U}_E^\dagger \circ \overline{\Lambda}^2_{\mathcal{P}_n\Pi} \circ \mathcal{U}_E$. 129

D.1 Computing the number $K_n^{(M)}$ is equivalent to counting the number of ways $M-1$ separators can be placed amongst n items. These are the possible configurations for 1 item and 3 separators (corresponding to 4 categories) 151

Preface

Overview

All physical realizations of quantum information processing devices are faced with the problem of noise and decoherence. While it is clear that improvements in the controllability and observability of such devices are necessary before a large scale quantum computer can be built, technological advancements alone are not sufficient to address this problem. In order to implement longer and longer sequences of quantum operations reliably, the probability of error for each quantum operation must be lower and lower. Therefore the rate at which errors occur places a fundamental bound on the size of the computation that can be performed reliably. For this reason, scalable quantum computation is *only* possible if the error rate can be adjusted according to the size of the computation to be carried out. The general aim of this dissertation is to investigate techniques for suppressing noise and decoherence, and to propose methods to characterize noise in an efficient manner in order to evaluate and improve these techniques.

The first part of the dissertation is focused on noise suppression. The first major theoretical breakthrough on the path towards scalability was the construction of protective encodings for quantum information [Sho95, Ste96a, CS96]. Operations which act directly on the encoded data can be designed carefully enough so that the data is protected from small errors that occur before as well as during these operation [Sho96, ZL96, Got98a, GC99, ZLC00] – this is what is generally known as *fault-tolerant quantum computation*. Error correction performed after each operation then guarantees that the effective error rate on the encoded data is lower. If these encodings are nested, the effective error rate can be lowered to ensure that computation of any size can be carried out reliably with an efficient use of resources, given enough nesting levels. However, improved error rates are only possible if the physical error rate is low enough – this is what is known as the *threshold theorem* [KLZ98, Pre98, ABO99, AGP06]. The exact value of this threshold

is dependent on details of how the data is encoded, as well as how error correction is performed [AGP06, Kni05a, CDT07]. While early estimates for the threshold error rate where on the order of 10^{-5} per operation, extensive optimizations have demonstrated that this value can be significantly larger, closer to 10^{-2}. This higher noise tolerance is achieved by combining the encoded operations with the error correction operations in a single step, via teleportation of quantum states [Kni05a, Kni05b]. Teleportation also allows quantum operations to be reduced to the preparation of resource states, which can be verified to be sufficiently noiseless and stored until needed in the computation, which further improves the reliability of fault-tolerant computation [GC99, ZLC00].

The reduction of quantum operations to state preparation and measurements has been used to demonstrate that quantum computation can be performed via measurements of single qubits prepared in a large entangled state, in what is known as *the one-way model of quantum computation* [RB01]. It is natural to ask whether error correction via teleportation can be combined with the one-way model to yield a direct path to fault-tolerance. This is the first question addressed by this dissertation. In Chapter 1 we demonstrate that the one-way model can be tailored to the limitations of encoded operations, so that it can be implemented directly using encoded states and measurements. Information about the errors in the data is obtained as a by-product of teleportation, following earlier proposals [Kni05a, Kni05b]. This allows for both post-selection in the preparation of the encoded resource states needed for computation, as well as for tracking errors without the need for explicit corrections to be applied.

Teleportation has applications that go beyond enabling different models of computation and optimizing error correction. It can be used to create effective interactions between systems, such as photons, which are otherwise difficult to interact [KLM01]. More generally, it can enable universal computation and fault-tolerance in systems which are difficult to manipulate otherwise. In Chapter 2 we consider the particular case of encoding qubits in superpositions of coherent states of a quantum communication bus, or *qubus*. Such states are easily generated and measured – for example, they can be taken to be the states of a laser pulse – and thus can be highly useful as ancillas during error correction and other fault-tolerant error suppressions tasks. While these states have been considered as mediators for interactions between qubits [NM04, MNS05, SNB$^+$06], here we illustrate how to use weak interactions between the qubus and qubits in order to perform teleportation. This, in turn, enables universal quantum computation on qubus states. The teleportation protocols we consider also herald information about the fidelity of the

output states to the desired states. This information can be exploited for enhancing the fidelity of prepared states by post-selection. This is relevant not only in the case of one-way quantum computation, as described earlier, but also for fault-tolerance in general, as it is crucial that ancillas be largely error-free before they can be used in the computation. We illustrate the application to fault-tolerance by demonstrating how error correction can be performed on qubits by using qubus states as ancillas.

The ideas of weak interactions and post-selection can be applied to other quantum systems as well. In Chapter 3, we consider the weak interaction between a qubit and a free quantum particle. In particular we demonstrate how two qubits can be entangled by post-selecting on position measurements of a particle that has been scattered by the qubits. As entanglement is an essential resource for teleportation, the preparation of such states enables a host of potential applications, ranging from communication to fault-tolerant quantum computation, as discussed earlier. With these applications in mind, we investigate the feasibility of using superconducting qubits and solitons in a non-linear transmission line to implement this protocol. The solitons are non-dispersive localized excitations in the transmission line which correspond to a trapped quantum of magnetic flux, and naturally interact with the flux-based superconducting qubits [ARS06, FSSKS07]. While quantum tunneling of these solitons has been demonstrated [Wal00, WLL$^+$03], the coherent superposition of different soliton states has yet to be observed. The entanglement creation protocol proposed here acts as a method for indirect observation of these superpositions, provided dissipation in the non-linear transmission lines can be reduced significantly.

The second part of this dissertation focuses on proposals for the characterization of noise in quantum devices. Experimental progress in the implementation of quantum information processors challenges us with a major theoretical question: how do we evaluate the precision and accuracy with which operations are implemented? The complexity of recent experiments demonstrating control over systems of approximately ten qubits was considerable [WHE$^+$04, LKS$^+$05, HHR$^+$05, NMR$^+$06, RKS$^+$06] – in each instance, the number of experiments and the amount of classical post-processing required to analyze the data were formidable. This is because the number of parameters needed to describe general quantum operations grows exponentially with the number of qubits involved [CN97, Leu03, ML06]. It is thus clear that the full characterization of quantum operations on even moderately large systems is simply untenable. This has direct relevance in evaluating the progress and feasibility of proposals for the implementation

of quantum computers. The threshold theorem provides targets for the error rate in a quantum computer, but experimental techniques must be devised to estimate error rates efficiently. Moreover, the standard techniques for error correction are developed under various assumptions about the properties of noise – such as, for example, the independence of error locations – which also need to be verified experimentally.

As complete characterization is infeasible, it becomes clear that a coarse-grained description of the evolution of quantum systems is necessary. The challenge is to identify efficient methods of coarse-grained characterization that yield information about features of practical interest. In Chapter 4 we propose a general method for coarse-graining based on the symmetrization of noise. The noise symmetrization protocol is based on random application of unitaries – a process commonly referred to as *twirling* [EAZ05, DHCB05, DCEL06, LLEC07]. We focus on a particular symmetry group which naturally leads to an intuitive description of the symmetrized noise in terms of probabilities of different types of errors. We can efficiently estimate the probability of no errors occurring, as well as the probability of only a few errors occurring. The symmetry group we consider has the advantage that it consists of only local unitaries on individual qubits, avoiding the difficulty of applying interactions between qubits. The main limitations of this protocol are due to uncertainties in the experimental estimates of certain parameters. However, even within these limitations, we are able to demonstrate how a number of important assumptions about the noise can be tested. In particular, the parameters which can be efficiently estimated naturally lead to sufficient conditions for the presence of correlations in the error locations. As common approaches to fault-tolerance routinely assume that error locations are independent, these protocols are of direct practical relevance.

We conclude by discussing in Chapter 5 how protective encodings for quantum information can be constructed based on the coarse-grained description of noise. Various approaches have been proposed to find protective encodings based on complete information about noise affecting a quantum computer [Kri03, HKL04, RW05, FSW07, KSL07]. All these techniques require the manipulation of exponentially large matrices describing both the noise as well as the encoding procedures. Even if complete information about the noise can be obtained efficiently, it becomes infeasible to consider systems with more than a handful of qubits. This can be avoided by considering noise symmetrization. We demonstrate that encodings which protect information from the action of symmetrized noise also protect information from the action of the "raw" noise, without the symmetrization operations applied. This is discussed in detail for a particular

symmetry group, which allows both efficient experimental characterization, as well as simple data post-processing without the need for manipulating exponentially large matrices. The performance of the protective encoding can also be shown to depend weakly on the uncertainty of the experimental estimation of noise parameters, demonstrating that the construction proposed here is robust.

Notation

We briefly review some basic notation used throughout this dissertation. Other notation is introduced in the body of the text as needed.

The group $\mathcal{P}_1$ of Pauli operators acting on a single qubit is generated by the operators

$$\mathbb{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$Y = \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

All matrix representations discussed here are given in the eigenbasis of σ_Z, which is also known as *the computational basis*, consisting of the states $|0\rangle = \sigma_Z|0\rangle$ and $|1\rangle = -\sigma_Z|1\rangle$. Another basis which is commonly used is the eigenbasis of σ_X, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, with the sign corresponding to the eigenvalue. In the chapters focusing on fault-tolerance and error correction, the symbols X, Y and Z will be used, while in the other chapters the symbols σ_X, σ_Y and σ_Z will be used instead.

The n qubit Pauli group $\mathcal{P}_n$ is given by all n-fold tensor products of the matrices in $\mathcal{P}_1$. For example, an element of $\mathcal{P}_2$ is the operator $X \otimes Y$. For brevity, the symbol "$\otimes$" will be omitted whenever the context makes its presence clear, so that $X \otimes Y$ will be written XY.

Other common unitaries used are

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\wedge X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \wedge Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

which are known as the Hadamard gate, controlled-NOT or CNOT, and controlled-sign or CSIGN.

The n qubit Clifford group $\mathcal{C}_n$ is the group of unitaries that map $\mathcal{P}_n$ to itself under conjugation. In other words,

$$\mathcal{C}_n = \{C | CPC^\dagger \in \mathcal{P}_n \text{ given } P \in \mathcal{P}_n, C \in U(2^n)\}. \quad (1)$$

This group is generated by tensor products of the Hadamard gate, CNOT and the unitary $\exp(-i\frac{\pi}{4}\sigma_Z)$.

In quantum circuit diagrams, we use the standard notation, with thick grey lines corresponding to the qubits. Hollow grey lines correspond to classical information about the outcome of a projective measurement, which can be fed-forward to decide whether other unitaries are applied or not. Vertical dark lines connecting different qubits represent the CSIGN unitary. The depiction of these two elements, which may be unfamiliar to the reader, is given in Figure 1.

Figure 1: *Circuit diagrams depicting (a) projective measurement of a qubit onto the eigenbasis of X with the outcome controlling the application of a unitary U, and (b) the interaction of two qubits via the unitary $\wedge Z$.*

Additional information for the examiners of this thesis

Each chapter in this dissertation essentially corresponds to a different research project.

Chapter 1 is based on the paper "A direct approach to fault-tolerance in measurement-based quantum computation via teleportation" [SDKO07] written in collaboration with V. Danos, E. Kashefi, and H. Ollivier, available as a preprint at arXiv:quant-ph/0611273 and published in *New J. of Phys.* **9**, 192 (2007). The Pauli measurement model of computation was developed by V. Danos and E. Kashefi as an extension to earlier work by the

same authors along with other collaborators [DKP05]. The fault-tolerance application of these ideas in connection with teleportation were developed jointly by the present author and H. Ollivier after discussions with E. Kashefi and V. Danos.

Chapter 2 is based on parts of "Stabilizer quantum error correction with quantum bus computations" [MSNM07] written in collaboration with C. R. Myers, K. Nemoto and W. J. Munro, available as a preprint at arXiv:quant-ph/0612097 and published in *Phys. Rev. A* **76**, 012303 (2007), and the paper "Computation with Coherent States via Teleportations to and from a Quantum Bus" [SM08] written in collaboration with C. R. Myers, available as a preprint at arXiv:0804.4344 and submitted for publication. The initial objective of [MSNM07] was to generalize earlier work which was restricted to a particular stabilizer code [YNM06]. C. R. Myers and the present author developed different approaches independently and then collaborated to publish the work jointly under the guidance of K. Nemoto and W. J. Munro. The present author's approach was focused on fault-tolerant techniques, and this corresponds to the material presented at the end of the chapter, in Section 2.6. Upon realizing the connection with teleportation, techniques for general computation and state preparation were further developed and presented in Sections 2.3 through 2.5. All the mathematical work in these sections was carried out jointly by the present author and C. R. Myers.

Chapter 3 is based on unpublished work done under the supervision of F. Wilhem. The main initial motivation of this work was to demonstrate the quantum superpositions of solitons in long Josephson junctions in a manner that was experimentally accessible. This work is presented here from the perspective of developing entanglement creation protocols for the purposes of quantum communication between well separated qubits. All the calculations and feasibility studies were carried out by the present author.

Chapter 4 is based on the present author's contributions to "Symmetrized characterization of noisy quantum processes" [ESM+07], written in collaboration with J. Emerson, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. Cory and R. Laflamme, available as a preprint at arXiv:0707.0685 and published in *Science* **317**, pp. 1893-1896 (2007). The idea of characterizing noise via symmetrization was proposed by J. Emerson building on his earlier work. The largest portion of the mathematical work presented in the section starting with Sections 4.3 was carried out by the present author after discussion principally with J. Emerson, but also with O. Moussa and M. Laforest. The work describing how twirling can be used to distinguish collective and independent relaxation, in Section 4.5.1, was carried out by the present author during an extended visit with M.

Rötteler at NEC Laboratories American Inc. as a concrete example of an application listed in [ESM+07], and is based on unpublished work.

Finally, Chapter 5 is based on "Experimentally scalable protocol for identification of correctable codes" [SMKE07], written in collaboration with E. Magesan, D. W. Kribs and J. Emerson, available as a preprint at arXiv:0710.1900 and accepted for publication in *Phys. Rev. A*. This work was initiated by the present author as a natural extension to his contribution in [ESM+07]. All mathematical work was carried out by the present author, with the notable exception of the Theorem in Section 5.7, which was proven by E. Magesan. Some additional material, in particular Section 5.6, the examples in Section 5.7 and Appendix D, are not present in the published version due to space constraints but are presented here from completeness and clarity. The calculations in Appendix E were also performed by the present author, with Section E.2 being joint work with O. Moussa.

Part I

Fault-tolerance and quantum error correction

Chapter 1

Fault-tolerant computation via measurements

1.1 Introduction

The construction of a scalable quantum computer hinges on the ability to actively suppress noise [Sho96, KLZ98, AGP06]. One approach to achieve this is to encode quantum states, so that it is possible to perform error correction from time to time. However, it is also important to be able to perform operations in these quantum states in a manner that does not disturb the encoding – this is what is known as *fault-tolerant quantum computation*. While early proposals demonstrated how to construct fault-tolerant encoded operations for a wide class of quantum error correcting codes [Sho96, Got98b], the concept of teleportation [BBC$^+$93] leads to a significant conceptual simplification of the problem. Instead of applying unitaries directly to a state, unitaries can be applied indirectly in a procedure known as *gate teleportation* [GC99, ZLC00]. This presents a significant advantage for encoded operations, since it reduces the problem of applying an encoded unitary, which may be very complex, to the problem of preparing a particular quantum state, which can be stored and used as a resource.

Building on the idea of gate teleportation, the *one-way quantum computation* (1WQC) model was developed, demonstrating that universal quantum computation is possible simply by performing single-qubit measurements on a large entangled state [RB01]. One particular issue that has attracted attention is how to perform fault-tolerant quantum computation in such a model [Rau03, ND05, AL05, RHG06, RH07]. While fault-tolerant

quantum computation can be performed through such a model by simulation of circuits via 1WQC [ND05, AL05], fault-tolerance can also be achieved directly through the use of topological error correction techniques [RHG06, RH07]. The focus of this chapter is to illustrate another direct approach, building on insights into the measurement calculus [DKP05, DKP07] and generalizations of 1WQC, as well as teleportation-based approaches to error correction [Kni05a, Kni05b].

We consider a model where measurements along all directions in the XY-plane of the Bloch sphere are traded off for more complex preparations of the entangled resource state. This model, which we call the *Pauli measurement model* (PMM), uses only measurements along the X and the Y directions of the Bloch sphere, while the entangled resource state is obtained via initialization of individual qubits into the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $|+_{\frac{\pi}{4}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle)$, followed by application of the unitary interaction $\wedge Z = \mathrm{diag}(1, 1, 1, -1)$ between certain pairs of qubits. We show that the PMM model is fault-tolerant in the usual simulation sense [ND05, AL05]. Moreover, through the use of encoded or nested graph states [Dan05a], and the careful selection of quantum codes, all necessary operations for computation can be performed transversally on encoded information, so that the graph state computation itself is made fault-tolerant if the error rate is low enough.

The reason why we believe this new model to be of practical interest is that physical implementations of the two measurements this new model requires should be simpler in comparison to implementations of the 1WQC model, which allows for measurement of any observable of the form $X\cos\theta + Y\sin\theta$ for the continuous parameter $\theta \in [0, \pi]$. These simpler measurements are also significantly easier to implement as encoded measurements, which allows us to take the approach of directly encoding the PMM.

This chapter is organized as follows. First, in Section 1.2 we review the protocols for teleportation of quantum states, and their connection to 1WQC and fault-tolerance in quantum systems. Then in Section 1.3 we investigate how to extend the main properties of the 1WQC model using these modified resource states, while still maintaining the properties one needs for convenient error correction. We finally demonstrate in Section 1.4 that this modified model naturally provides the resources necessary for fault-tolerant extraction of information about the errors, and illustrate how any PMM computation can be transformed into a larger one that has a lower effective error rate if the error rate per operation is below some threshold, achieving fault-tolerance.

1.2 Teleportation and one-way quantum computation

Since the early days of quantum mechanics it has been known that entangled quantum states have properties which have no natural counterparts in classical theories [EPR35, Sch35, Boh35, Bel64]. One of the most surprising applications of entanglement is the *teleportation* of a quantum state from one subsystem to another [BBC+93]. Teleportation consists of a protocol where one party, Alice, would like to send an undisturbed quantum state $|\psi\rangle$ to another party, Bob. Alice and Bob also share a maximally entangled state of the form $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, where the first qubit is Alice's, and the second is Bob's. Alice can teleport the state $|\psi\rangle$ to Bob by simply jointly measuring $|\psi\rangle$ and her half of the entangle state in a particular basis, and informing Bob of the outcome of her measurement. The basis which Alice must measure on is determined by which maximally entangled state she shares with Bob, and in the particular case described here, the basis is known as the *Bell basis* consisting of the states

$$|\Phi^+\rangle = |B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{1.1}$$

$$|\Phi^-\rangle = |B_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{1.2}$$

$$|\Psi^+\rangle = |B_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{1.3}$$

$$|\Psi^-\rangle = |B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{1.4}$$

Depending on which outcomes Alice has obtained, Bob will perform a correction on his qubit. In particular, by direct computation we find that the relationship between the measurement outcomes and the necessary corrections to Bob's state is

$$|B_{00}\rangle \to \mathbb{1}_2 \tag{1.5}$$

$$|B_{01}\rangle \to Z \tag{1.6}$$

$$|B_{10}\rangle \to X \tag{1.7}$$

$$|B_{11}\rangle \to ZX. \tag{1.8}$$

If Alice send the bits ab corresponding to the subscripts of her measurement outcome, then Bob applies the correction $Z^b X^a$. After these corrections, Bob's qubit is in the state $|\psi\rangle$. The quantum circuit implementing this protocol is depicted in Figure 1.1. As the qubits that Alice and Bob own never interact, they can be, in principle, separated by arbitrarily large distances. Notice also that no information about the state $|\psi\rangle$ is learned by either Alice or Bob during this protocol – the state is left completely undisturbed.

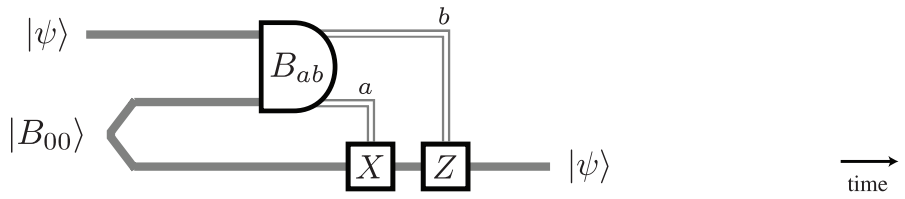

Figure 1.1: *Circuit diagram for the teleportation protocol.*

The teleportation protocol demonstrates that, in some sense, the ability of communicating a quantum state is equivalent to sharing a resource state and being able to communicate measurement outcomes, which are just classical bits. This equivalence can be taken one step further: by modifying his half of the resource state and his correction operations, Bob can obtain the result of applying some unitary U to the state $|\psi\rangle$. This is what is known as *gate teleportation* [GC99].

In order to obtain the the protocol for gate teleportation, consider teleporting a state, and then performing a unitary U immediately after the teleportation corrections have been applied. If we insert the $UU^\dagger = \mathbb{1}_2$ before the corrections are applied, it becomes clear that teleportation with the state $\mathbb{1}_2 \otimes U|\Psi^+\rangle$ and corrections $UZ^bX^aU^\dagger$ is equivalent to teleportation followed by the application of U. The main practical application of gate teleportation is that in some cases it may be difficult to apply the unitary U directly to an arbitrary state, but it may be possible to prepare the state $\mathbb{1}_2 \otimes U|\Psi^+\rangle$ in a reliable manner, either by verification of the state and post-selection, or by state purification procedures.

If teleportation is used simply for the purposes of decomposing complex operations into simpler operations and resource states, the requirement that Alice's and Bob's quantum states may not interact is unnecessary. In particular, the teleportation protocol can be simplified to obtain what are known as *one bit teleportations* [ZLC00], where "one-bit" refers to the amount of information Alice must send to Bob in order for him to know which correction to apply to his state. These one-bit teleportation protocols are depicted in Figure 1.2. They are named after the corrections which must be applied at the end of the protocol.

Building on one-bit teleportations, it is possible to demonstrate that universal quantum computation can be performed by starting with a large entangled resource state and then measuring individual qubits in bases which may depend on previous measurement outcomes [RB01]. This is what is known as *one-way quantum computation* (1WQC), as the state of qubits is repeatedly transferred from one qubit to another, before the qubit is

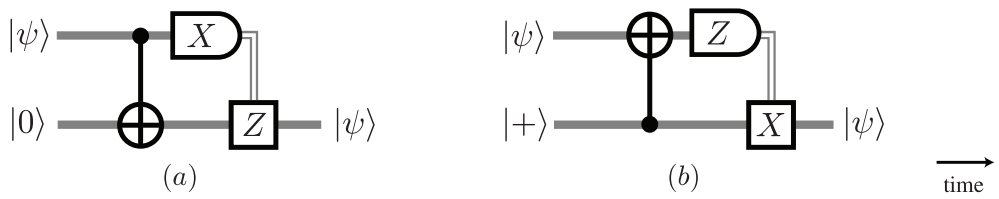

Figure 1.2: *Circuit diagrams for one-bit teleportation protocols (a) Z teleportation and (b) X teleportation.*

measured and taken to be destroyed.

The simplest way to demonstrate the 1WQC model is to consider the Z teleportation of the Hadamard unitary H, as depicted in Figure 1.3. The result of conjugating the CNOT by a H on the target qubit is the CSIGN unitary $\wedge Z = \mathrm{diag}(1, 1, 1, -1)$, depicted by a dark line connecting the two qubits. Conjugating a rotation of angle α about Z by Hadarmards results in a rotation about X, as $H \exp(-i\frac{\alpha}{2}Z)H = \exp(-i\frac{\alpha}{2}X)$. By employing the conjugation relations of Pauli operators with the interaction $\wedge Z$, it is possible to demonstrate that this can be implemented by a sequence of H teleportations and a Z rotation which simplified to the circuit depicted in Figure 1.4, where M^β is an observable which depends both on α as well as the outcome of the measurement of the first qubit (the exact form of this observable will be given in the next section). Similarly, applying H to two qubits, followed by interaction via $\wedge Z$ can be rearranged to the circuit depicted in Figure 1.5. From these circuits it is clear that 1WQC is universal, as both single qubit unitaries and two qubit interactions can be performed.

Note that all these circuits consist of preparing qubits in the state $|+\rangle$, entangling them, and then performing a sequence of measurements (the corrections correspond to measurements in bases that depend on previous measurement outcomes, so they are not taken to be additional operations). This requires some rearrangement of the operations in the teleportation protocol, which can get quite cumbersome for larger circuits. However, as we will see in the next section, this rearrangement can be done in a systematic manner which guarantees that state preparation, entanglement and measurement can alway be performed in this order.

In order to implement arbitrary unitaries using 1WQC, one must be able to measure along arbitrary directions of the XY plane of the Bloch sphere. If the basic operations are replaced by encoded operations, in order to increase tolerance to errors and noise, such measurements are in general hard to perform, and only measurements along the

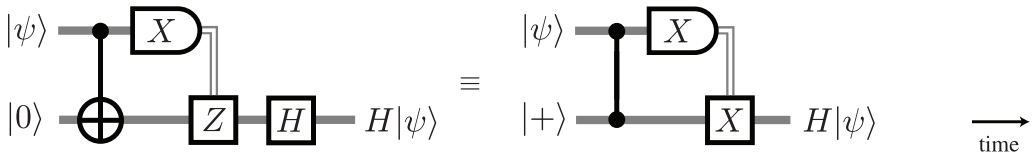

Figure 1.3: *One-bit teleportation of the unitary H.*

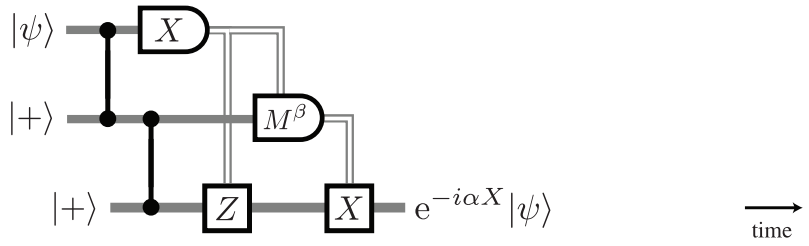

Figure 1.4: *Implementation of an arbitrary rotation about X in 1WQC.*

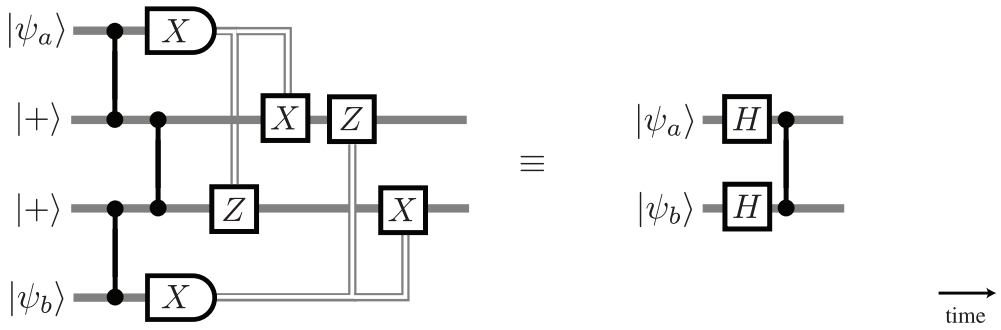

Figure 1.5: *Implementation of a the unitary $(\wedge Z)(H \otimes H)$ in 1WQC.*

encoded Pauli eigenbases are easily implemented. For this reason, we consider a slight modification of this model.

1.3 One-way quantum computation with phase preparation

The modifications of the circuit diagrams as described in the previous section can be abbreviated by using the *measurement calculus* [DKP07]. In this calculus, a sequence of operations, such as state preparation, interactions, measurements and measurement-dependent state corrections are each symbolized by a command. Such a sequence, along with the qubits they operate on, is what we call a *measurement pattern*. In essence, there is a one-to-one correspondence between a quantum circuit and a measurement pattern.

Formally, a measurement pattern, or simply a pattern, is defined by a sequence of quantum operations over a finite set of qubits V, along with two subsets $I \subseteq V$ and $O \subseteq V$ representing the pattern inputs and outputs respectively (I and O may intersect). The allowed operations are: (a) N_i^α, preparation of qubit i in the state $|+_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i\alpha}|1\rangle)$; (b) E_{ij}, unitary interaction between qubits i, j of the form $\wedge Z$; (c) M_i^α, measurement of qubit $i \notin O$ in the $|\pm_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm \mathrm{e}^{i\alpha}|1\rangle)$ eigenbasis, with outcome $s_i \in \{0, 1\}$ corresponding to collapse into the state $|+_\alpha\rangle$ or $|-_\alpha\rangle$, respectively; (d) X_j and $Z_j(\alpha) = \mathrm{e}^{-i\frac{\alpha}{2}Z_j}$, local unitaries on qubit j. In addition, local unitaries and measurement basis may depend on the outcome of measurements of other qubits, which is denoted in the natural way, e.g. $X_j^{s_k}$ indicating a unitary which acts if $s_k = 1$, or $M_j^{\alpha - s_k\beta}$ indicating a measurement in a basis which depends on the measurement outcome s_k. Temporal ordering is right to left – that is, rightmost operations are performed first. The circuits corresponding to each of these operations are depicted in Figure 1.6.

Measurements are considered to be destructive, and we require that no operations be performed on measured qubits. We also only consider patterns where no operations depend on the outcome of measurements that have not yet been performed. Both 1WQC and PMM are particular cases of this more general model: to obtain the 1WQC model set $\alpha = 0$ in clause (a) and (d); to obtain the PMM, set $\alpha = 0, \pi/4$ in clause (a), and $\alpha = n\pi/2$ in clauses (c) and (d).

Patterns, denoted by gothic letters, e.g. $\mathfrak{A}$ and $\mathfrak{B}$, can be combined to create a new pattern via parallel concatenation $\mathfrak{A}\|\mathfrak{B}$, or serial concatenation $\mathfrak{B} \circ \mathfrak{A}$. Parallel concate-

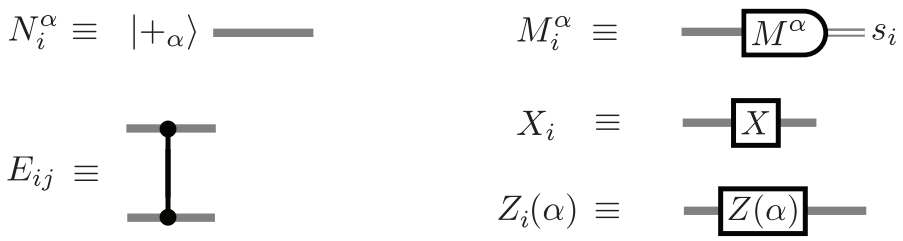

Figure 1.6: *Measurement pattern operations, indexed by which qubit they operate on, and their corresponding quantum circuits.*

nation means the qubits are relabeled in such a way that all operations in $\mathfrak{A}$ commute with all the operations in $\mathfrak{B}$ – if $\mathfrak{A}$ implements the unitary U_A, and $\mathfrak{B}$ implements U_B, then $\mathfrak{A}\|\mathfrak{B}$ implements $U_A \otimes U_B$. Serial concatenation means the output of $\mathfrak{A}$ is fed into the input of $\mathfrak{B}$ – that is, $\mathfrak{B} \circ \mathfrak{A}$ implements the unitary $U_B U_A$.

As an example, consider the pattern

$$\mathfrak{J}_\alpha = X_2^{s_1} M_1^{-\alpha} E_{12} N_2^0, \tag{1.9}$$

with $(V, I, O) = (\{1,2\}, \{1\}, \{2\})$. Given an arbitrary state ρ on qubit 1, this sequence of operations implements $J_\alpha = HZ(\alpha)$ on the input state and places the resulting state $J_\alpha \rho J_\alpha^\dagger$ on qubit 2. This is one of the fundamental building blocks for 1WQC [DKP07], since it allows for arbitrary one qubit rotations. Any of the local unitaries considered can be merged with a (destructive) measurement as follows:

$$M_i^\alpha Z_i(\beta) = M_i^{\alpha-\beta} \tag{1.10}$$

$$M_i^\alpha X_i = M_i^{-\alpha} \tag{1.11}$$

and it is readily seen that the $\mathfrak{J}_\alpha$ pattern above is the serial concatenation of a $Z(\alpha)$ rotation with a modified one-bit teleportation (implementing H) – a well known result for 1WQC [RB01, ZLC00, Nie05]. Patterns which lie outside 1WQC model can also be expressed in this extended model, such as

$$\mathfrak{X}_\alpha = X_3^{s_2} Z_3^{s_1} M_2^{-(-1)^{s_1}\alpha + \frac{\pi}{4}} M_1^0 E_{23} E_{12} N_2^{\frac{\pi}{4}} N_3^0 \tag{1.12}$$

with $(V, I, O) = (\{1,2,3\}, \{1\}, \{3\})$, which implements the unitary $HZ(\alpha)H = \mathrm{e}^{-i\frac{\alpha}{2}X} = J_\alpha J_0$. It follows from the equations above, that this pattern is equivalent to a $Z(\alpha)$ conjugated by a one-qubit teleportation. The importance of writing the pattern in this form, using the $N_2^{\frac{\pi}{4}}$ preparation, becomes clear when measurements are restricted to the X or Y eigenbasis, as will be discussed later.

Other patterns which play an important role are $\wedge\mathfrak{Z}$, $\mathfrak{N}$ and $\mathfrak{M}$, defined as follows: $\wedge\mathfrak{Z} = E_{12}$, with $(V, I, O) = (\{1,2\},\{1,2\},\{1,2\})$, implements the unitary $\wedge Z$; $\mathfrak{N} = N_i^0$ implements initialization of qubit i into the state $|+\rangle$; and, $\mathfrak{M} = M_i^0$ implements the measurement of qubit i in the $|\pm\rangle$ X eigenbasis.

The usual protocol for 1WQC requires computation to be performed in three steps: (i) individual qubit state preparation, (ii) entangling operations between qubits, and (iii) measurement of individual qubits with feed-forward of outcomes. Patterns in which operations are performed in this order are said to be in *standard form*. Any given pattern in the 1WQC model can be put in this form [RB02, DKP07]. Patterns in the generalized model just described can also be placed in the standard form, as will be discussed later. Note that the steps of the protocol do not include the application of single qubit unitaries, but adaptive measurements can be used to address this absence, since all quantum computations must end with the measurement of the qubits in order for information to be extracted. Once a pattern is in standard form, it is convenient to consider the entangled state that is prepared for the computation. Such a state can be described by an *entanglement graph*, with vertices V and edges (i, j) for every command E_{ij} in the pattern, where the vertices are labeled with the initial state in which the qubit is prepared. The states which can be described in this manner are also known as *graph states*.

The process of turning a given pattern into a pattern in standard form is called *standardization*. The rewrite rules needed for this procedure are simply (1.10) and (1.11), along with conjugation relation between unitaries, $E_{12}X_1 = X_1Z_2E_{12}$, and $E_{12}Z_1(\alpha) = Z_1(\alpha)E_{12}$, as well as all the free commutation relations between operations on different qubits. Simple rewriting theory arguments show that by applying the conjugation relations to move all the local unitaries towards the left in the pattern, and then by applying (1.10) and (1.11), any pattern can be put in standard form [DKP07].

As mentioned previously, PMM is obtained by setting (A) state preparation angles to 0 or $\frac{\pi}{4}$, (B) measurement angles to $\frac{n\pi}{2}$, and (C) local unitaries to X and $Z(\frac{n\pi}{2})$. Two simple facts follow from this: first, PMM is closed under standardization and concatenation, as can be readily seen from the merging and conjugation relations above; second, PMM contains the patterns $\wedge\mathfrak{Z}$, $\mathfrak{J}_\alpha$, $\mathfrak{X}_\beta$, $\mathfrak{N}$ and $\mathfrak{M}$, where $\alpha = \frac{n\pi}{2}$ and $\beta = \frac{n\pi}{2} + \frac{\pi}{4}$, as well as their concatenations. In particular, $\mathfrak{X}_{\frac{\pi}{4}}$ allows for an operation outside the Clifford group while requiring only Pauli measurements.

Given that $\mathfrak{X}_{\frac{\pi}{4}}$ implements the unitary $\mathrm{e}^{-i\frac{\alpha}{8}X}$, and $\mathfrak{J}_0$ implements H, concatenations of these patterns allow for efficient approximation of arbitrary single qubit rotations due

to the Solovay-Kitaev theorem [Kit97]. Thus, given interactions can be implemented with the $\wedge 3$ pattern, it follows that the PMM can perform universal quantum computation. The other single qubit patterns in the PMM are not needed for universality, but allow for a reduction of the number of commands needed to implement some unitaries.

This construction of a universal gate set is equivalent to the construction of fault-tolerant universal gate sets via teleportation [GC99, ZLC00], as described earlier.

1.4 Fault-tolerance

In reality, physical implementations of any computational model are susceptible to noise. The noise model that is usually considered, and which we restrict ourselves to in this work, is the model of independent random failure of each of the operations during computation. We would like to perform useful computation on a quantum computer regardless of how long the computation is, or how many qubits are involved, simply because we would like to solve many different types of problems, of different complexities, with different input sizes. If one expects the error rate of a quantum computer to be naturally low enough so that errors are unlikely to occur during computation, one find that the acceptable error rates are dependent on the size of the computation. Thus we would like a means to perform any useful quantum computation even in the presence of a fixed probability of error for each gate. This is what is generally meant by *fault-tolerant quantum computation*.

Encoding the data to resist errors is not enough to reach this objective; it is also important to perform operation directly of the encoded data, without decoding it. These encoded operations must be constructed carefully, so that error do not propagate in a catastrophic way. Consider, for example, a controlled operation such as a CNOT. If there is an error on the control qubit, the wrong operation is applied to the target qubit. Thus, an error on a single qubit is translated to errors on two qubits. If the encoding being used can only protect against a single error in a block of qubits, performing such an operation between qubits within a single block can lead to an unrecoverable error. The general rule that can be extracted from this is that we should not allow for qubits within the same code block to interact. This, essentially, translates to the requirement that encoded gate operations be *transversal* – that they operate qubit-wise on a code block [Sho96, ZL96].

Once the data is protected by an error correcting code, the effective error rate on the

encoded data may still be unacceptably high. One way to get around this problem is to perform *concatenated or nested coding* – that is, encode the encoded data. If we have a code $C^{(1)}$ with parameters $[[n, 1, d]]$, this means that the code uses n qubits to encode 1, and that it can tolerate $\lfloor \frac{d-1}{2} \rfloor$ qubits to be corrupted without destroying the encoded information. From simplicity, we consider $d = 3$, so that only one error per block of n can be tolerated. Assuming that errors occur independently on each qubit, the probability $\epsilon^{(1)}$ of obtaining an uncorrectable error for $C^{(1)}$ is

$$\epsilon^{(1)} = \sum_{i=2}^{n} \binom{n}{i} \epsilon^i (1-\epsilon)^{n-i} < c\epsilon^2, \tag{1.13}$$

where ϵ is the probability that an error will occur at a given qubit, and the c is a combinatorial coefficient which depends only on the error correction code. Clearly, if $\epsilon < 1/c$, we have that $\epsilon^{(1)} < \epsilon$. Nesting the encoding L times leads to the the code $C^{(L)}$ with parameters $[[n^L, 1, d^L]]$ and effective error rate

$$\epsilon^{(L)} < \frac{(c\epsilon)^{2^L}}{c}, \tag{1.14}$$

which is doubly exponentially small in L, as long as $c\epsilon < 1$. The error probability $1/c$ is known as the *error threshold*, below which encoding and error correction leads to improved effective error rates. This, in essence, is what is known as the *threshold theorem* [Kit97, KLZ98, Pre98, ABO99, AGP06].

An underlying assumption of this theorem is that any state introduced into computation at concatenation level L will have errors at an effective rate $O(\epsilon^{(L)})$. For example, if we consider a single level of encoding, only encoded states with an effective error rate of $O(\epsilon^2)$ can be introduced into the computation in order to ensure that the threshold theorem holds. If one were to prepare some unencoded state, which has an error rate $O(\epsilon)$, encoded it and introduce it into the computation, the error rate for this state would be $O(\epsilon)$, which would violate this requirement. Therefore it is important that the state be verified to be sufficiently noiseless before it is used. This verification must be designed to fail due to independent errors during the verification procedure with probability $O(\epsilon)$, so that the probability of having an output with an error which the verifier claims is error-free is $O(\epsilon^2)$ – the product of the probabilities that the input has an error and that a failure during verification leads to the conclusion that the input is error free. The effect of a verifier which satisfies this condition is to modify the threshold due to additional failure modes, but the overall scaling is unchanged since the effective error rate is of the same order.

Transversal operations between different block of encoded qubits guarantee that encoded failures will only be introduced at a rate $O(\epsilon^{(L)})$, so no additional care is required. As in the case of state verification, the value of the threshold will be affected, but the scaling due to concatenation remains the same.

1.4.1 Simulation approach

One approach to achieve fault-tolerance in 1WQC is to use fault-tolerance in the circuit model as a stepping stone. The construction of fault-tolerant circuits is well understood [GC99, ZLC00], and it is now well known that the implementation of such circuits via 1WQC can lead to fault-tolerant quantum computation [AL05, ND05] – that is, each operation in the fault-tolerant circuit is implemented as a sequence of teleportations in 1WQC. This can be most simply understood and demonstrated through *composable simulations* [CLN05, AL05], which revolve around the idea that the teleportation of a unitary can be though of as a simulation of that unitary. Each one of these simulations consists of classical information (corresponding to the measurement outcomes) as well as quantum information (the states of the system). Both the classical and the quantum information are passed from one gate simulation to the next. In principle noise leads to errors on both the classical data as well as in the quantum data. However, as classical data is only used to perform Pauli corrections on the quantum data, one can simply take the classical data to be error free, at the cost of having a higher effective error rate in the quantum data. Thus these noisy simulations via teleportation just correspond to noisy quantum computers, and the usual results for fault-tolerance of quantum computers apply.

The same idea carries through to the PMM with minor modifications. The main distinction is that in the PMM, the change of measurement bases dependent on measurement outcomes corresponds to a local Clifford correction, as opposed to a local Pauli correction. Thus the noisy simulations through the PMM will have an error model which consists of random application of local Clifford operators. However, because of the linearity of quantum mechanics and the fact that the Pauli group forms a basis for all single qubit operators, the errors are still correctable as in simulations through the 1WQC model. Thus, simulating fault-tolerant quantum circuits through the PMM model is also fault-tolerant.

1.4.2 Intrinsic fault-tolerance

We now turn our attention to the possibility of making any PMM computation directly fault-tolerant, instead of simulating fault-tolerant quantum circuits within 1WQC.

1WQC relies on frequent measurement to implement a desired state evolution, but none of this information is used towards fault-tolerance in simulation-based approaches. The opportunity for improved performance becomes evident once one considers the well known link between teleportation and 1WQC [CLN05, Nie05], and the fact that fault-tolerant quantum computation in the circuit model can achieve very high thresholds via extensive use of teleportation for simultaneous error syndrome extraction and state evolution [Kni05a].

Encoded Computation

Before we consider how error syndrome information is to be extracted, we must consider encoded computation in the PMM. The basic elements of the PMM are: preparation of qubits in either $|+\rangle$ or $|+_{\frac{\pi}{4}}\rangle$, pair-wise entanglement via $\wedge Z$, and measurement in the X or Y eigenbases depending on the outcomes of previous measurements. Given some quantum code, we can consider these same elements, but in the subspace corresponding to the code chosen – that is, preparation of a block of qubits in the encoded states above, encoded entangling operations, and collective measurements in the encoded eigenbases X and Y. The use of the 7 qubit self-orthogonal doubly-even CSS codes [Ste96b] simplifies the problem considerably if the generators of the encoded Pauli operators are chosen to be $\overline{Z} = Z^{\otimes 7}$ and $\overline{X} = X^{\otimes 7}$. In that case, the encoded entangling operation $\overline{\wedge Z}$ is given by the transversal application of $\wedge Z$ gates between respective qubits in two blocks – in the PMM, it is the parallel concatenation of the pattern $\wedge\mathfrak{Z}$. Moreover, measurement in the encoded X and encoded Y eigenbases are performed by measuring each of the qubits within the code block in the same basis individually, followed by classical decoding of the outcomes to determine the encoded outcome. If we consider concatenated encoding using this 7 qubit code, i.e. $\overline{X}^{(j)} = \left(\overline{X}^{(j-1)}\right)^{\otimes 7}$ for the jth level of encoding with $\overline{X}^{(0)} \equiv X$ and similar relations for $\overline{Z}^{(j)}$, these transversality properties are preserved.

The encoding procedure of any given stabilizer code over qubits is known to correspond to a pattern in 1WQC which allows for arbitrary input and requires only measurements along the eigenbases of the Pauli operators X and Y [SW02, GKR02]. In

essence, this is just the translation of the encoding circuit into a measurement pattern and the associated graph state. If we restrict the inputs to be either $|+\rangle$ or $|+_{\frac{\pi}{4}}\rangle$, we can obtain the encoded states $|\overline{+}\rangle$ or $|\overline{+}_{\frac{\pi}{4}}\rangle$ strictly within the PMM. The entanglement graph corresponding to the encoding circuit for the 7 qubit code is depicted in Figure 1.7. Concatenated encoding proceeds in the obvious way, by serial concatenation of the measurement pattern corresponding to the encoding procedure.

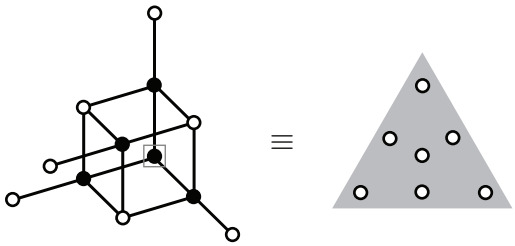

Figure 1.7: *Entanglement graph corresponding to the encoding of a single qubit into the 7 qubit CSS code. The boxed node corresponds to an arbitrary input qubit. All but the white qubits (corresponding to the encoding output) are measured in the X basis (up to feed-forward-based corrections).*

However, for the purpose of fault-tolerant quantum computation, encoding requires verification of the encoded states in order to ensure that these state do not contain errors that are too correlated [Sho96, AGP06]. This can be performed naturally in the PMM via state encoding at some given level of concatenation, followed by syndrome extracting teleportation of the lower levels of encoding [Kni05a], which we will describe shortly. If errors are detected at any concatenation level, the state is discarded and the procedure starts again. There are purification protocols for the entangled state corresponding to the encoding procedure of any CSS code [DAB03, MR06] – such as the 7 qubit code, as depicted in Figure 1.7 – which may also be employed to reduce errors and error correlations. We consider only the encoded states that have been successfully verified after preparation as part of the computation. In this manner, encoded computation in the PMM is akin to computation with nested graph states [Dan05a], where the entanglement graph for encoding is nested within the computation entanglement graph.

It is important to note that the entire concatenated graph state must not be purified directly, since the maximum vertex degree of the resulting graph grows linearly with the level of concatenation, and the purification protocol performance degrades with higher

vertex degrees [DAB03]. This is a general feature of purification protocols, including more recent protocols with improved efficiency [MR06]. In order to avoid this problem, one may perform purification of each encoded qubit (or encoded entangled pair) per level of concatenation separately, followed by syndrome extraction teleportation with post-selection of the states which have a clean syndrome, as described in [Kni05a].

Previous proposals for fault-tolerance in the 1WQC model make use of what is called the *one-buffered implementation* of cluster states [ND05]. In such implementations, which are based on the simulation of quantum circuits, the entanglement subgraph corresponding to the first two time steps in the circuit model is prepared. The measurements corresponding to the first time step are performed, followed by the state preparation and entangling operations corresponding to the third time step of the circuit model. After that, the measurements for the second time step are performed, and computation proceeds keeping a one time step "buffer" of qubits, so that the entire entanglement graph need not be prepared in one shot. However, it has been demonstrated that the 1WQC model, as well as the PMM, allow for greater parallelism in the computation [DKP05, DKP07]. In particular, some sequences of operations which lie in multiple time steps in the circuit model can be performed in a single time step in these measurement models (a large class of such operations are unitaries in the Clifford group). Thus, one may prepare states corresponding to larger subgraphs of the entanglement graph where all non-output qubits will be measured simultaneously [DKP05, DKP07]. To see how these subgraphs are defined, consider the following. First, group all qubits with measurements that do not depend on previous measurements, as well as any qubits which interact with them directly (or which are directly connected to them in the entanglement graph). The subgraph made up of these qubits, along with any edges between them in the original entanglement graph, is the subgraph corresponding to the first round of measurements. Then, consider all qubits which depend only on the outcomes of measuring these qubits, along with any qubits connected to them. This is the subgraph corresponding to the second round of measurements. Continuing in this fashion, by looking for dependence only on previous measurement outcomes, one can partition the entire entanglement graph. There is a clear temporal order in which each measurement round must be performed, as well as a temporal order in which each subgraph must be prepared and entangled with the output of previous rounds.

In the case of the PMM, as mentioned before, Pauli measurements and final corrections may depend on outcomes of previously measured qubits. This is because measure-

ment of a vertex prepared in the $|+_{\frac{\pi}{4}}\rangle$ introduces a local Clifford correction to qubits connected to it in the entanglement graph, and thus such vertices will always be on the boundary of the subgraphs. However, patterns implementing Clifford operations have measurements which are independent of each other's outcome, and thus the insertion of Clifford operations in a pattern does not increase the number of such subgraphs, or equivalently, the minimal number of time steps in which measurements can be performed in parallel. This is particularly relevant for fault-tolerance, as encoding and syndrome extraction operations for stabilizer codes are Clifford operations. In principle such operations can be performed in the same time step, if the entire corresponding subgraph is available for measurement. The preparation of the subgraph itself will require multiple time steps, due to verification, error correction and purification at different levels of encoding, but since these operations are independent of the rest of the computation, they may be performed offline.

Clearly, it is not required that maximal parallelism – corresponding to the largest subgraph – be implemented. There is a trade-off between the overhead introduced by more complex offline preparation and verification of such larger subgraphs, and the lower effective error rate which may be achieved. Implementations may range from the one-buffered approach, to the fully parallel approach, which ensures that all measurements without dependencies can be performed simultaneously.

Syndrome extraction

In order to perform fault-tolerant quantum computation, one must be able to extract information about the errors in the data in order to ensure that only sufficiently noiseless states are introduced into the computation, as described in the previous section, but also to obtain information about which errors are likely to have occurred in order to correct them. This error syndrome extraction can be performed via teleportation, as recently described in [Kni05a, Kni05b]. In essence, the idea is to start with a maximally entangled pair of encoded qubits $|\overline{\Omega}\rangle_{1,2} = \overline{\wedge Z}_{12}|\overline{+}\rangle_1|\overline{+}\rangle_2$ which is prepared offline. Given some encoded state $\overline{\rho}$, the error syndrome can be extracted in the following manner. Measure each transversal pair of physical qubits from $\overline{\rho}$ and the first half of $|\overline{\Omega}\rangle_{1,2}$ in a basis of maximally entangled states. The state $\overline{\rho}$ is then teleported into the second half of the entangled pair, up to a tensor product P of local Pauli operators which is inferred from the outcomes of the pair measurements. The error syndrome can in turn be inferred from

these corrections by considering the commutator of P with each of the generators of the stabilizer group of the code. This protocol can be seen as the transversal teleportation of all the physical qubits where the n maximally entangled pairs have been projected into the codespace being used. Note that this is different from an encoded teleportation – an encoded maximally entangled state is used, but the measurements are performed on physical qubits, not encoded qubits. The information about the errors in $\overline{\rho}$ are extracted because the target states of teleportation (the second half of $|\overline{\Omega}\rangle_{1,2}$) is taken to be, to first order, an error free encoded state. In order to teleport $\overline{\rho}$ faithfully, the errors must be teleported as well. These errors can be inferred from P, since which local Pauli operations correspond to encoded operations are well known properties of the code. If P is not one of these operations, then it is taken to be a product of a valid encoded operation and some Pauli error. Whichever Pauli error is most likely, given that the errors on each qubit are taken to be independent, is taken to be the error on $\overline{\rho}$.

This teleportation-based technique for fault-tolerant quantum computation has been rigorously proven to have an error threshold [AGP08], and extensive numerical evidence supports the claim that the error threshold for this technique is significantly higher than for other techniques [Kni05a].

Although the usual teleportation protocol [BBC+93] is performed with Bell pairs and measurement in the Bell basis, teleportation can be performed with any measurement in a basis of maximally entangled states, and this choice of basis fixes which maximally entangled states can be used as a resource. In fact, teleportation can be performed by the standard form of the serial concatenation $\mathfrak{J}_0 \circ \mathfrak{J}_0$ – that is, the pattern $X_3^{s_2} Z_3^{s_1} M_2^0 M_1^0 E_{23} E_{12} N_3^0 N_2^0$, which may be understood as a teleportation using the basis obtained by applying a Hadamard gate to one of the qubits of a Bell basis. If we allow for modified preparation of the entangled resource state, the pattern, stripped of the entanglement preparation, simply becomes $\mathfrak{T} = X_3^{s_2} Z_3^{s_1} M_2^0 M_1^0 E_{12}$, which, for completeness, must be concatenated with the pattern for the modified entangled state preparation (i.e. the pattern that prepares the encoded entangled state).

Thus, in the PMM, syndrome extraction of some encoded state $\overline{\rho}$ is performed by: (I) preparing and verifying the encoded state $|\overline{\Omega}\rangle_{12}$, (II) teleporting all qubits in $\overline{\rho}$ individually using the resource state $|\overline{\Omega}\rangle_{12}$, and (III) performing classical post-processing to infer the syndrome information from the teleportation measurement outcomes. As discussed, step (I) can be performed by hierarchical teleportation and post-selection [Kni05a, Kni05b], while step (II) can be performed by parallel concatenation of the pattern $\mathfrak{T}$ above, and

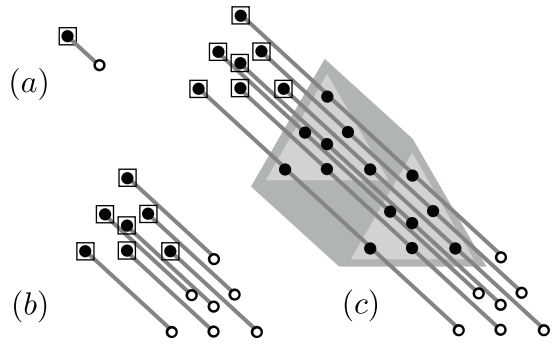

Figure 1.8: *Entanglement graphs for the fault-tolerant implementation of $\mathfrak{J}_0$. The boxed nodes correspond to input qubits, and all but the white nodes (corresponding to output qubits) are measured in the X eigenbasis (up to feed-forward-based corrections).*

step (III) is merely classical post-processing which affects the bases of subsequent measurements. Partial syndrome information can be extracted in a similar fashion, as in the case of the $\mathfrak{J}_\alpha$ pattern with $\alpha = \frac{n\pi}{2}$, where, depending on α, one can obtain information about Pauli errors which anti-commute with X or Y.

Performing the computation

Given any measurement pattern in the PMM, one may make it fault-tolerant by first translating each of the commands to a larger pattern representing its encoded form, then inserting instances of the syndrome extracting teleportation between each operation, and standardizing the resulting pattern.

As a simple example, consider the pattern fragment $X_2^{s_1} M_1^0 E_{12}$ that implements the unitary $J_0 = H$, with entanglement graph depicted by Figure 1.8(a). Using a single level of encoding under the 7 qubit CSS code, the resulting pattern is already long and omitted for brevity, but its entanglement graph in Figure 1.8(b) demonstrates the simplicity of the transformation. With the data protected by an error correction code and offline preparation of encoded qubits, one inserts the syndrome extracting teleportation to obtain the final fault-tolerant pattern with corresponding entanglement graph depicted in Figure 1.8(c). The subgraph enclosed in the shaded triangle corresponds to the encoded state that must be prepared and verified before the remaining operations can be performed, in what can be seen as an extension of the one-buffered implementation of the unencoded case [ND05]. The subgraph inside the irregular pentagon (corresponding

to the preparation of the encoded maximally entangled pair) is to be prepared and verified before the qubits within it interact with the remainder of the graph. This demonstrates the fact that only three subgraphs need to be prepared and verified offline: the smaller subgraphs corresponding to the encoded states $|\overline{+}\rangle$ and $|\overline{+}_{\frac{\pi}{4}}\rangle$, and the larger subgraph corresponding to the encoded state $|\overline{\Omega}\rangle$. This procedure for implementing fault-tolerance works for any linear graph. Other graphs, such as the one corresponding to a $\wedge\mathfrak{Z}$ pattern interacting between two linear chains, can be handled in a similar fashion, by simply inserting syndrome extracting teleportations before and after the $\wedge\mathfrak{Z}$ pattern.

It is important to note that the qubits, interactions and measurements added to the computation in order to extract syndrome information correspond to Clifford operations on the quantum states. As pointed out earlier in the chapter, the measurements associated with a sequence of Clifford operations can be performed in any order, even simultaneously and immediately after the qubits are made available for measurement, and thus they do not increase the depth complexity of the computation [Rau03, DKP07]. Moreover, this also allows for the offline preparation of subgraphs corresponding to Clifford operations, along with measurement of parts of the subgraph, which allows for the elimination of some types of error via post-selection – as pointed out in [DHN06], for the case of repeated syndrome extraction, one can post-select on subgraphs which will yield agreeing syndromes.

1.5 Summary

We have described a measurement-based model of computation called the Pauli Measurement Model (PMM) with the notable feature that measurements are restricted to the eigenbases of the Pauli operators X and Y, and qubit state preparation is extended to both $|+\rangle$ and $|+_{\frac{\pi}{4}}\rangle$. With the appropriate choice of quantum codes, any measurement pattern in this model can be directly modified into another pattern within the same model, which will have a lower effective error rate as long as the failure rate per operation is below a threshold. The approach described here opens the door for further optimizations based on the inherent parallelism of the operations in the PMM [DKP05, DKP07], generalizing ideas about buffered computation in [ND05].

Chapter 2

Teleportation to and from a quantum bus

2.1 Introduction

The question of which physical system is best suited for quantum information processing is still open, each implementation proposal having strengths and weaknesses. Due to the technical challenges of building qubit systems, it may be practical to use other quantum systems that do not fit naturally into the qubit paradigm to accomplish some limited tasks. A concrete example of this is the use of laser pulses in the implementation of quantum key distribution systems instead of single photons [BHK+98], as single photons are difficult to produce reliably on demand. Various other proposals have also taken a mixed approach to the implementation of more general quantum information processors, using a physical realization of a qubit for operations, and transferring to another physical realization for storage, exploiting the fact that some of these systems interact easily. One example of this is the use of electron spins for fast operations, and nuclear spins for long coherence times [Kan98, DCJ+07]. This is not limited to naturally occurring quantum systems, as in some implementations of superconducting qubits a harmonic mode in a transmission line is used to store the state of the qubit more reliably when operations are not being performed [KKM+06, BDKS08]. The flexibility that such mixed implementation provides is a great practical advantage because it allows different properties of the different physical systems to be exploited to maximal potential.

More abstractly, coherent states of a quantum oscillator with large amplitude, such

as a laser pulse or a voltage pulse, have been proposed as replacements for ancillary qubits in quantum computers [MNS05, SNB+06]. In these systems, the oscillator can be used as a *quantum communication bus* (also referred to as a *qubus*), which can act as a mediator for interactions between distant qubits. The essential building block for these proposals is weak interaction between qubits and the qubus. The effective interaction between the qubits is then achieved by rounds of communication via the qubus, and for this reason these proposals are described as *quantum computation by communication*.

In this work, we consider the possibility of encoding a qubit directly into superpositions of coherent states of the quantum bus. Such a possibility has been considered previously, but the main difficulty of earlier proposals was the need for strong interactions between qubits and the qubus, which is hard to achieve in practice [RGM+03, GNM+04]. Our approach is to exploit the strong points of the qubus, such as simple entanglement generation, along with the strong points of qubits, such as simple individual system manipulation, and to join them together via teleportation. This can be achieved by using only weak interactions between qubits and the qubus, in a manner similar to the proposals of computation via communication, thereby avoiding the main technical challenge of the earlier proposals of quantum computation with coherent states.

The techniques we present here also have features that go beyond universal quantum computations. In particular, the teleportation protocols we propose herald the fidelity of the resulting state to the desired outcome. In a setting where this fidelity is on average lower than some desirable threshold due to technological limitations, the protocols can still be used to prepare useful resource states with high fidelity, albeit in a probabilistic manner. In principle this fidelity can be brought arbitrarily close to one, at the cost super-exponentially small probability of success. In a more realistic setting, significant gains in fidelity are still achievable with only moderate losses in the probability of success.

As concrete demonstration of the power and flexibility of this teleportation based approach, we describe how to perform error correction fault-tolerantly for a large class of quantum codes. This extends earlier work which demonstrated how to perform error correction for repetition codes [YNM06].

The chapter is organised as follows. First, in Section 2.2 we briefly describe the qubus and its properties, along with how we encode information in the qubus states. In Section 2.3 we describe the fundamental building block of our proposal: one bit teleportations between a qubus and a qubit. This allows us to perform universal quantum computation, as described in Section 2.4. In Section 2.5 we also describe how the same

teleportation protocols, along with beam-splitters, can be exploited to prepare large entangled states, or to encode states into the quantum repetition code. Finally, in Section 2.6 we describe how all these proposals for gates and state preparations can be used to perform fault-tolerant error correction on qubits using qubus states as ancillas.

2.2 Quantum communication bus

Although quantum information proposals usually focus on finite dimensional systems represented by qubits, there are many continuous variable systems available with interesting quantum properties. A prime example of such a continuous variable system is the quantum harmonic oscillator, and a common physical realization is a mode of the electromagnetic field [WM94]. Recent proposals have demonstrated how such systems can be used for quantum communication or as well as mediators for interactions between the qubits [MNS05, SNB$^+$06], so that this continuous variable mode is referred to as a *quantum communication bus*, or simply a *qubus*. The basic element used in these proposals is a weak interaction between a qubit and qubus. The interaction we consider has the form

$$\mathcal{H} = \hbar\chi|1\rangle\langle 1| \otimes \hat{n}, \tag{2.1}$$

where χ is the interaction strength, $|1\rangle\langle 1|$ acts on the qubit state, $\hat{n}$ is the number operator acting on the qubus. This type of interaction can be implemented by a large number of physical systems [SNB$^+$06], ranging from a superconducting qubit interacting with the electromagnetic field in a cavity resonator [BHW$^+$04], to photon-photon interactions mediated by non-linear media [NM04, MNS05, MNBS05, FEF$^+$08], or even interactions between vibrational modes of ions in an ion trap [RMK$^+$08].

While previous investigations have focused on building qubit interactions by using geometric phases accumulated during communication [SNB$^+$06], here we will take a more direct approach, by encoding a qubit on states of the qubus. If we allow the interaction to act for a time t resulting in a unitary evolution $U(t)$, the action of $U(t)$ on basis states of the qubit and the qubus is

$$U(t)|0\rangle|\alpha\rangle = |0\rangle|\alpha\rangle \tag{2.2}$$

$$U(t)|1\rangle|\alpha\rangle = |1\rangle|\alpha e^{i\theta}\rangle \tag{2.3}$$

where $\theta = \chi t$, and $|\alpha\rangle/|\alpha e^{i\theta}\rangle$ are coherent states [WM94]. It is clear than that the interaction can be taken as a controlled rotation by θ of the state of the qubus in phase

space [Sch00]. Rotations by a negative angle can also be implemented, simply by acting with the Pauli operation Z on the qubit before and after the interaction. The symbols we will be using to denote this *controlled phase space rotation* are depicted in Figure 2.1.

The weakness of the interaction manifests itself on the magnitude of θ. Recent optical experiments have θ on the order of 0.1 rad, but such large values can be hard to achieve, and tend to be much lower. For this reason, we take θ to be fixed by the implementation, but we allow for the possibility of varying α.

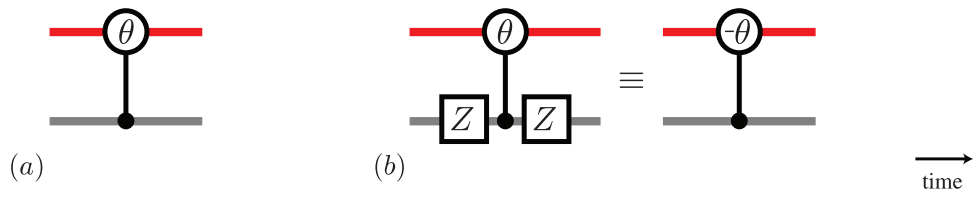

Figure 2.1: *Circuits representing phase-space rotations of the qubus (red line) controlled by the state of the qubit (grey line).*

There is a close analogy between these controlled rotations and the CNOT operation common in quantum information. If we make the identification $|0\rangle \rightarrow |\alpha\rangle$ and $|1\rangle \rightarrow |\alpha \mathrm{e}^{\pm i\theta}\rangle$ – what we will call *qubus logic* from here on – we see that the action of the controlled rotation resembles the action of the CNOT, with the qubit controlling the operation on the qubus. Moreover, a quadrature measurement along x is able to distinguish between $|\alpha\rangle$ and $|\alpha \mathrm{e}^{\pm i\theta}\rangle$ (if $\alpha\theta^2$ is large enough). If we have a superposition of the states $|\alpha\rangle$ and $|\alpha \mathrm{e}^{-i\theta}\rangle$ and we apply the interaction, then we obtain a superposition of the states $|\alpha\rangle$ and $|\alpha \mathrm{e}^{+i\theta}\rangle$. This analogy breaks down when we consider multiple applications of the controlled rotations to qubit states which are in superpositions, as this will lead to potentially applying a rotation by θ to the state $|\alpha \mathrm{e}^{i\theta}\rangle$, resulting in a state outside the qubus logic space (namely, the superpositions of $|\alpha\rangle$ and $|\alpha \mathrm{e}^{\pm i\theta}\rangle$).

In order to avoid this problem, we can restrict the application of controlled rotations to superpositions of $|\alpha\rangle$ and only one of $|\alpha \mathrm{e}^{\pm i\theta}\rangle$. This can be enforced by allowing controlled rotations to be applied only twice between starting with the state $|\alpha\rangle$ and measuring the qubus state. Although this may appear overly restrictive at first, a number of useful quantum information processing tasks can be performed in this manner. The first example of this is the *parity gate*, depicted in Figure 2.2 [YNM06]. It can be seen that this circuit is a parity gate when we consider its effect on the input state $|\psi_{\text{in}}\rangle = \big(c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle\big)|\alpha\rangle$. After the interactions, the state of the system is

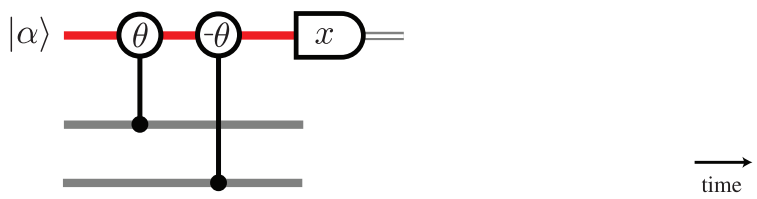

Figure 2.2: *Parity gate implemented using controlled phase space rotations.*

$\big(c_0|00\rangle + c_3|11\rangle\big)|\alpha\rangle + c_1|01\rangle|\alpha e^{-i\theta}\rangle + c_2|10\rangle|\alpha e^{i\theta}\rangle$. Due to the entanglement between the qubits and the qubus, it is possible to distinguish between $c_0|00\rangle + c_3|11\rangle$ and $c_1|01\rangle + c_2|10\rangle$ by measuring the x-quadrature of the qubus, since the projection $\langle x|\alpha\rangle$ is peaked around 2α for $|\alpha\rangle$, and $2\alpha\cos\theta$ for $|\alpha e^{\pm i\theta}\rangle$. For small θ, in order to distinguish the two states with high fidelity, we require that $\alpha\theta^2 \gg 1$.

This parity gate is capable of preparing entangled pairs of qubits via post-selection. Preparing the qubits in the states $|++\rangle$, projection onto the even parity subspace yields $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, while projection onto the odd parity subspace yields $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ – regardless of the parity measurement outcome, the result is a maximally entangled state. It also possible to demonstrate how these two-qubit parity measurements can be used directly to perform error correction in some very specific types of quantum codes [YNM06], which we will discuss in more detail in Section 2.6, along with generalizations we have developed to more general codes. In order to perform more general quantum operations, we must consider teleportation.

2.3 One-bit teleportations between a qubit and a bus

For states encoded in qubus logic, most unitary operations are difficult to implement, precisely because the coherent states have a finite overlap. Given a superposition of qubus states, however, entanglement can be created relatively easily. Sending the state $|\sqrt{2}\alpha\rangle$ through balanced two port beam-splitter, with the vacuum as the other input, results in the state $|\alpha\rangle|\alpha\rangle$. If we send the state $|\sqrt{2}\alpha\rangle + |\sqrt{2}\alpha e^{\pm i\theta}\rangle$ instead, known as a *Schrödinger cat state* (or simply a *cat state*) one obtains [RGM+03, GNM+04]

$$|\alpha\rangle|\alpha\rangle + |\alpha e^{\pm i\theta}\rangle|\alpha e^{\pm i\theta}\rangle, \tag{2.4}$$

which is clearly entangled. This is depicted in Figure 2.3.

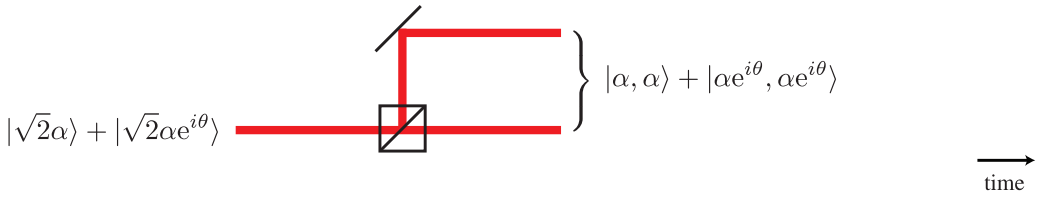

Figure 2.3: *Creation of entanglement through the use of a balanced beam-splitter.*

Single qubits, on the other hand, are usually relatively easy to manipulate, while interactions between them can be challenging. As we have discussed in the previous chapter, the teleportation of quantum states is powerful tool which can be used not only for communication, but also to implement unitary operations on quantum states. For this reason, we consider one-bit teleportation between states of a qubit and states of the qubus. The two types of one-bit teleportations for qubus computation are shown in Figure 2.4, based on similar constructions proposed for qubits [ZLC00].

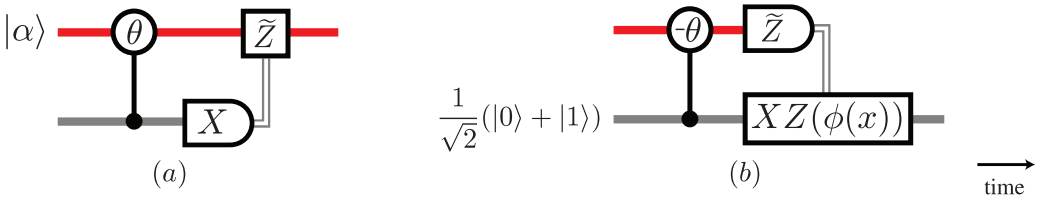

Figure 2.4: *Approximate one-bit teleportation protocols between a qubit (grey) and a qubus (red) using controlled rotations.*

The one-bit teleportation of the qubit state $c_0|0\rangle + c_1|1\rangle$ into a state of qubus logic is depicted in Figure 2.4(a). The initial state, before any operation, is $\big(c_0|0\rangle + c_1|1\rangle\big)|\alpha\rangle$. After the controlled rotation by θ the state becomes $c_0|0\rangle|\alpha\rangle + c_1|1\rangle|\alpha e^{i\theta}\rangle$. Representing the qubit state in the X eigenbasis, this is $|+\rangle\big(c_0|\alpha\rangle + c_1|\alpha e^{i\theta}\rangle\big)/\sqrt{2} + |-\rangle\big(c_0|\alpha\rangle - c_1|\alpha e^{i\theta}\rangle\big)/\sqrt{2}$. When we detect $|+\rangle$ we have successfully teleported the qubit state into the qubus. When we detect $|-\rangle$ we have the state $c_0|\alpha\rangle - c_1|\alpha e^{i\theta}\rangle$ (up normalization, due to the finite overlap between the coherent states). The relative phase discrepancy can be corrected by the operation $\widetilde{Z}$, which approximates the Pauli Z operation in qubus logic. This correction can be delayed until the state is teleported back to a qubit, where it is more easily implemented.

The one-bit teleportation of the qubus state $c_0|\alpha\rangle + c_1|\alpha e^{i\theta}\rangle$ to a state of the qubit can be performed by the circuit depicted in Figure 2.4(b). Starting with $\big(c_0|\alpha\rangle + c_1|\alpha e^{i\theta}\rangle\big)(|0\rangle + |1\rangle)/\sqrt{2}$, after the controlled rotation by $-\theta$, the state becomes $|\alpha\rangle\big(c_0|0\rangle + c_1|1\rangle\big)/\sqrt{2} +$

$\big(c_1|\alpha e^{i\theta}\rangle|0\rangle + c_0|\alpha e^{-i\theta}\rangle|1\rangle\big)/\sqrt{2}$. Projecting the qubus state into the x-quadrature eigenstate $|x\rangle$ via homodyne detection, which is the measurement we depict as $\widetilde{Z}$ (to evoke the idea of measuring the the Z eigenbasis), results in the conditional unnormalized state $|\psi(x)\rangle$

$$|\psi(x)\rangle = \frac{f(x,\alpha)}{\sqrt{2}}(c_0|0\rangle + c_1|1\rangle) + \frac{f(x,\alpha\cos\theta)}{\sqrt{2}}(e^{i\phi(x)}c_1|0\rangle + e^{-i\phi(x)}c_0|1\rangle) \tag{2.5}$$

where

$$f(x,\beta) = \frac{1}{(2\pi)^4}\exp\left(\frac{-(x-2\beta)^2}{4}\right) \tag{2.6}$$

$$\phi(x) = \alpha x\sin(\theta) - \alpha^2\sin(2\theta), \tag{2.7}$$

since $\langle x|\alpha e^{\pm i\theta}\rangle = e^{\pm i\phi(x)}f(x,\alpha\cos\theta)$ and $\langle x|\alpha\rangle = f(x,\alpha)$ for real α [WM94, NM04].

The weights $f(x,\alpha)$ and $f(x,\alpha\cos\theta)$ are Gaussian functions with the same variance but different means, given by 2α and $2\alpha\cos\theta$, respectively. Given $x_0 = \alpha(1+\cos\theta)$, the midpoint between $f(x,\alpha)$ and $f(x,\alpha\cos\theta)$, one can maximize the fidelity of obtaining the desired state $c_0|0\rangle + c_1|1\rangle$ (averaged over all possible values of x) by simply doing nothing when $x > x_0$ (where $f(x,\alpha) > f(x,\alpha\cos\theta)$), or applying $Z(\phi(x)) = \exp(-i\phi(x)Z)$, a Z rotation by $\phi(x)$, followed by a Pauli X operator, when $x \leq x_0$. For simplicity, these teleportation corrections are not depicted in the circuit diagrams in the sections to follow, and it is left implicit that they must be performed when the state is transferred to a qubit.

2.3.1 Average fidelities

In order to quantify the performance of the protocols just described, we use the *process fidelity* [HHH99, GLN05]. The process fidelity between two quantum operations is obtained by computing the fidelity between states isomorphic to the processes under the Choi-Jamiołkowski isomorphism [Jam72, Cho75]. For example, in order to compare a quantum process $\mathcal{E}$ acting on a D dimensional system to another quantum process $\mathcal{F}$ acting on the same system, we compute the fidelity between the states

$$\rho_{\mathcal{E}} = \mathbb{1}_D \otimes \mathcal{E}\left(\frac{1}{\sqrt{D}}\sum_{i=1}^{D}|ii\rangle\right) \tag{2.8}$$

$$\rho_{\mathcal{F}} = \mathbb{1}_D \otimes \mathcal{F}\left(\frac{1}{\sqrt{D}}\sum_{i=1}^{D}|ii\rangle\right). \tag{2.9}$$

In the case of single qubit processes, we just need to consider the action of the process on one of the qubits of the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The operational meaning of the process fidelity is given by considering the projection of the first qubit into a particular state $a|0\rangle + b|1\rangle$. In this case the second qubit collapses into the state corresponding to the output of the process acting on the state $a|0\rangle + b|1\rangle$. Thus a high fidelity between $\rho_{\mathcal{E}}$ and $\rho_{\mathcal{F}}$ implies a high fidelity between the outputs of the $\mathcal{E}$ and $\mathcal{F}$.

Consider the state resulting from the teleportation of half of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ using the circuit in Figure 2.4(a). This state is

$$|\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|0, \alpha\rangle \pm |1, \alpha e^{i\theta}\rangle), \tag{2.10}$$

where the sign depends on the qubit measurement outcome. As the relative phase is known, and the correction can be performed after the state is teleported back to a qubit, for each of the outcomes we can compare this state with the ideal state expected from the definition of the basis states for the qubus. This results in the process fidelity of 1 for one-bit teleportation into the qubus.

For the case where we teleport the state from the qubus back into the qubit, using the circuit in Figure 2.4(b), we consider the action of the process on the second half of the state $|\psi_+\rangle$ from (2.10). This is not, strictly speaking, the Choi-Jamiołkowski isomorphism, but it gives the same operational meaning for the process fidelity as a precursor to the fidelity between the outputs of the different processes being compared, as any qubus logic state can be prepared from $|\psi_+\rangle$ by projecting the qubit into some desired state. We expect the output state to be $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ from the definition of the basis states, but we instead obtain the unnormalized states

$$|\psi_E(x > x_0)\rangle = \frac{f(x,\alpha)}{\sqrt{2}}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) + \frac{f(x,\alpha\cos\theta)}{\sqrt{2}}\left(\frac{e^{-i\phi(x)}|01\rangle + e^{i\phi(x)}|10\rangle}{\sqrt{2}}\right), \tag{2.11}$$

$$|\psi_E(x < x_0)\rangle = \frac{f(x,\alpha)}{\sqrt{2}}\left(\frac{e^{-i\phi(x)}|01\rangle + e^{i\phi(x)}|10\rangle}{\sqrt{2}}\right) + \frac{f(x,\alpha\cos\theta)}{\sqrt{2}}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right). \tag{2.12}$$

The normalized output state, averaged over all x outcomes, is

$$\rho = \int_{x_0}^{\infty} |\psi_E(x > x_0)\rangle\langle\psi_E(x > x_0)|\, dx + \int_{-\infty}^{x_0} |\psi_E(x < x_0)\rangle\langle\psi_E(x < x_0)|\, dx, \tag{2.13}$$

so that the average process fidelity for one-bit teleportation into a qubit is

$$F_p = \frac{1}{2} + \frac{1}{2}\,\mathrm{erf}\left(\frac{x_d}{2\sqrt{2}}\right), \tag{2.14}$$

where $x_d = 2\alpha(1-\cos\theta) \approx \alpha\theta^2$ for small θ. Teleportation from the qubus into the qubit is not perfect, even in the ideal setting we consider, because the states $|\alpha\rangle$ and $|\alpha e^{\pm i\theta}\rangle$ cannot be distinguished perfectly. However, F_p can be made arbitrarily close to one by letting $x_d \to \infty$, or $\alpha\theta^2 \to \infty$ if $\theta \ll 1$, as seen in Figure 2.5. This corresponds to increasing the distinguishability of the coherent states $|\alpha\rangle$ and $|\alpha e^{i\theta}\rangle$. For fixed θ both these limits correspond to making α large. If θ is exceedingly small, this can be problematic in an experimental setting – in the optical case, a large α corresponds to using high power lasers, which may have detrimental effects on the material used to implement the interaction. Thus the strength of the interaction will impose limits on how well these teleportations can be performed deterministically.

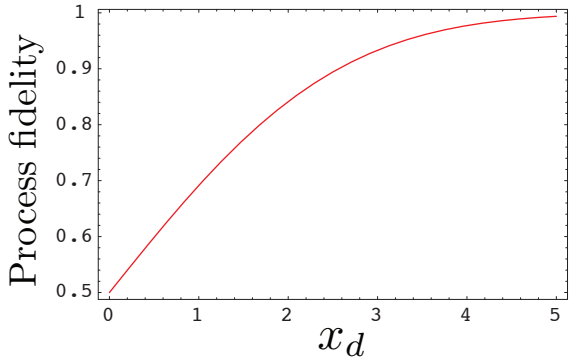

Figure 2.5: *Fidelity F_p of one-bit teleportation from the qubus to a qubit, as a function of x_d.*

2.3.2 Post-selected teleportation

In order to improve the average fidelity of the teleportations without changing the physical parameters α and θ of the basis states, one can post-select the outcomes of the x-quadrature measurements when teleporting states from the qubus to a qubit, as these outcomes essentially herald the fidelity of the output state with the desired state. Discarding the states with fidelity below a certain threshold allows for the average fidelity to be boosted, even in the case where $\alpha\theta^2 \not\gg 1$, at the cost of a certain probability of failure. This is particularly useful for the preparation of special quantum states which are used

as resources for some quantum information processing tasks, as we have discussed in Chapter 1.

Instead of accepting all states corresponding to all x outcomes of the homodyne measurement which implements $\widetilde{Z}$, we only accept states corresponding to outcomes which are far enough away from the midpoint x_0, since the state at x_0 has the lowest fidelity with the desired state. More explicitly, we only accept states corresponding to measurement outcomes which are smaller than $x_0 - y$ or larger than $x_0 + y$. This post-selection can only be performed for one-bit teleportation from the qubus to the qubit, yielding a probability of success given by

$$\Pr(|x - x_0| > y) = \frac{1}{2}\left[\operatorname{erfc}\left(\frac{2y - x_d}{2\sqrt{2}}\right) + \operatorname{erfc}\left(\frac{2y + x_d}{2\sqrt{2}}\right)\right], \tag{2.15}$$

and process fidelity conditioned on the successful outcome given by

$$F_{p,y} = \frac{\operatorname{erfc}\left(\frac{2y - x_d}{2\sqrt{2}}\right)}{\operatorname{erfc}\left(\frac{2y - x_d}{2\sqrt{2}}\right) + \operatorname{erfc}\left(\frac{2y + x_d}{2\sqrt{2}}\right)}. \tag{2.16}$$

The effect of discarding some of the states depending on the measurement outcome for the teleportation in Figure 2.4(b) is depicted in Figure 2.6. In particular, we see that the process fidelity can be made arbitrarily close to 1 at the cost of lower probability of success, while α and θ are unchanged, since

$$\lim_{y \to \infty} F_{p,y} = 1. \tag{2.17}$$

As the probability mass is highly concentrated due to the Gaussian shape of the distribution of quadrature measurement outcomes, the probability of success drops super-exponentially fast as a function of y. This is because for $z > 0$ we have [Wei08]

$$\frac{2}{\sqrt{\pi}} \frac{\mathrm{e}^{-z^2}}{z + \sqrt{z^2 + 2}} < \operatorname{erfc}(z) < \frac{2}{\sqrt{\pi}} \frac{\mathrm{e}^{-z^2}}{z + \sqrt{z^2 + \frac{4}{\pi}}}. \tag{2.18}$$

This fast decay corresponds to the contour lines for decreasing probability of success getting closer and closer in Figure 2.6. Thus, while the fidelity can be increased arbitrarily via post-selection (by increasing y), this leads to a drop in the probability of obtaining the successful post-selection outcome. Note that, despite this scaling, significant gains in fidelity can be obtained by post-selection while maintaining the physical resources such as α and θ fixed, and while maintaining a reasonable probability of success. In particular, if $x_d = 2.5$, increasing y from 0 to 1.25 takes the fidelity from 0.9 to 0.99 while the probability of success only drops from 1 to 0.5.

If the probability of success is to be maintained constant, a linear increase in x_d can bring the fidelity exponentially closer to unity, as is evident in Figure 2.6. As x_d is proportional to the amplitude α of the coherence state, this can be achieved while maintaining θ constant. Since θ is usually the parameter which is hard to increase in an experimental setting, this ability to improve the fidelity without changing θ is highly advantageous.

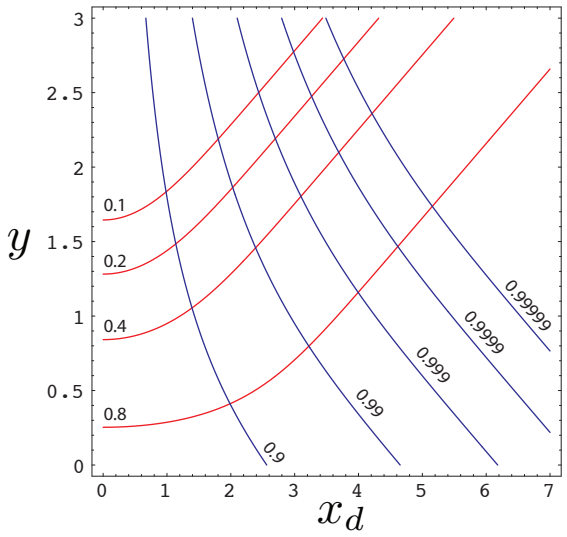

Figure 2.6: *Contour lines for post-selected fidelity $F_{p,y}$ of one-bit teleportation from the qubus to a qubit (blue), and success probability for post-selection (red), as a functions of x_d and y.*

Instead of discarding the outputs with unacceptable fidelity, one can also use the information that the failure is heralded to recover and continue the computation. In the case of the one-bit teleportations described here, such an approach would require active quantum error correction or quantum erasure codes – the type of codes necessary for heralded errors – which have much higher thresholds than general quantum error correcting codes [Kni05a, Kni05b]. We will not discuss such a possibility further in this paper, and will focus instead on post-selection for quantum gate construction and state preparation.

2.4 Universal quantum computation

As we have demonstrated, a quantum state can be transferred between a qubit and a qubus relatively easily. In order to demonstrate universal quantum computation, it is necessary to demonstrate both arbitrary single qubit unitaries, as well as entangling operations between two quantum systems. For illustration purposes, we will focus on implementing universal quantum operations on states of the qubus, as at first glance it is not clear how unitary operations can be performed in such systems.

It is important to note that there is little flexibility regarding the measurement of the qubus. The measurement of the x-quadrature is tailored to distinguish between $|\alpha\rangle$ and its rotated versions. It is not clear whether it would be possible to make measurements which can distinguish between particular superpositions of these states while at the same time not distinguishing between $|\alpha e^{i\theta}\rangle$ and $|\alpha e^{-i\theta}\rangle$. While in principle such a measurement can be implemented by applying a unitary in qubus logic using technique we will describe later, for simplicity we will not consider this possibility. This precludes, for example, a direct implementation of 1WQC or the Pauli measurement model, as these computational models require the ability to perform projective measurements of the qubus state into superposition of the qubus logic basis states. However, it is still possible to use teleportation to implement universal quantum computation, as we now describe.

2.4.1 Single qubit gates

In the special case of applying the Pauli operator X on the state $c_0|\alpha\rangle + c_1|\alpha e^{i\theta}\rangle$, we can simply apply the phase shifter $e^{-i\theta\hat{n}}$ to obtain $c_0|\alpha e^{-i\theta}\rangle + c_1|\alpha\rangle$, similarly to the bit flip gate in [RGM+03].

An arbitrary single qubit unitary gate U can be applied to the state $c_0|\alpha\rangle + c_1|\alpha e^{i\theta}\rangle$ by the circuit shown in Figure 2.7. We first teleport this state to the qubit using the circuit in Figure 2.4(b) and then perform the desired unitary U on the qubit, giving $U\big(c_0|0\rangle + c_1|1\rangle\big)$. We can teleport this state back to the qubus with Figure 2.4(a), while the $\widetilde{Z}$ correction can be delayed until the next single qubit gate, where it can be implemented by applying a Z in addition to the desired unitary. If it happens that this single qubit rotation is the last step of an algorithm, we know that this $\widetilde{Z}$ error will not effect the

outcome of a homodyne measurement (which is equivalent to a measurement in the Pauli Z eigenbasis), so that this correction may be ignored.

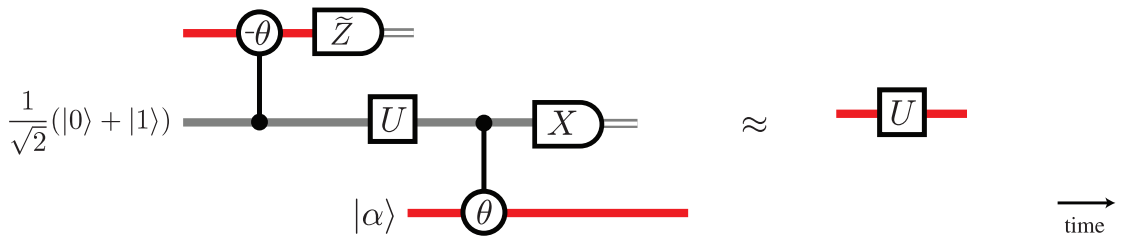

Figure 2.7: *A local gate U applied to the qubus via teleportations.*

Since arbitrary single qubit gates are implemented directly in the two level system, the only degradation in the performance comes from the teleportation of the state from the qubus to the qubit, resulting in the fidelity given in (2.14).

Post-selected implementation of single qubit gates

The fidelity of single qubit gates in qubus logic can be improved simply by using post-selected teleportations. For simplicity, if we disregard the second one-bit teleportation which transfers the state back to qubus logic, we obtain the probability of success given in (2.15) and the conditional process fidelity given in (2.16).

2.4.2 Entangling gates

The entangling gate we consider is $\wedge Z$, which, as discussed in Chapter 1, can be implemented by one-bit teleportations. The resource state necessary is

$$\frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\big) = (\mathbb{1} \otimes H)(|00\rangle + |11\rangle)/\sqrt{2}, \tag{2.19}$$

which can be produced offline by any method that generates a maximally entangled pair of qubits. One possible approach for preparing maximally entangled pairs of qubits is the parity measurement we have already discussed [YNM06]. However, this maximally entangled pair of qubits can also be generated by teleporting the qubit state $(|0\rangle + |1\rangle)/\sqrt{2}$ onto a qubus using Figure 2.4(a), as this results in the cat state $|\sqrt{2}\alpha\rangle + |\sqrt{2}\alpha e^{i\theta}\rangle$. Sending the cat state through a symmetric beam splitter yields $|\alpha, \alpha\rangle + |\alpha e^{i\theta}, \alpha e^{i\theta}\rangle$ [RGM+03, GNM+04]. If we now teleport this state to a qubit with Figure 2.4(b) we have, to a good

approximation, the Bell state $\big(|00\rangle + |11\rangle\big)/\sqrt{2}$, and with a local Hadamard gate we finally obtain $\frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\big)$. Since we are only concerned with preparing a resource state which in principle can be stored, we can perform post-selection at the teleportations to ensure the state preparation is of high fidelity, as described in Section 2.3.2. After the necessary corrections the state is teleported back to the qubus. The overall circuit is shown in Figure 2.8. As with the single qubit gates, $\widetilde{Z}$ corrections may be necessary after the final teleportations, but these corrections can also be delayed until the next single qubit gate.

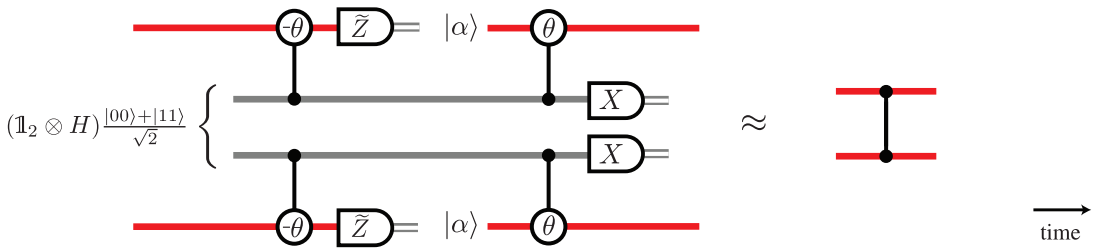

Figure 2.8: *The entangling gate CSIGN performed via teleportation of qubus states.*

We can see what affect the condition $\alpha\theta^2 \not\gg 1$ has on the function of the gate in Figure 2.8 by looking at the process fidelity. As this gate operates on two qubits, the input state to the process we want to compare is

$$\frac{1}{2}\left(|0,0\rangle|\alpha,\alpha\rangle + |0,1\rangle|\alpha,\alpha e^{i\theta}\rangle + |1,0\rangle|\alpha e^{i\theta},\alpha\rangle + |1,1\rangle|\alpha e^{i\theta},\alpha e^{i\theta}\rangle\right). \tag{2.20}$$

From the basis states we have defined, we expect the output

$$|\psi_2\rangle = \frac{1}{2}\left(|0,0\rangle|\alpha,\alpha\rangle + |0,1\rangle|\alpha,\alpha e^{i\theta}\rangle + |1,0\rangle|\alpha e^{i\theta},\alpha\rangle - |1,1\rangle|\alpha e^{i\theta},\alpha e^{i\theta}\rangle\right). \tag{2.21}$$

The unnormalized state output from Figure 2.8 is

$$\begin{aligned}
|\psi_{2,o}\rangle = \frac{1}{4}\Big\{ & f(x,\alpha)f(x',\alpha)\left[|00\rangle|00\rangle + |01\rangle|01\rangle + |10\rangle|10\rangle - |11\rangle|11\rangle\right] \\
& + f(x,\alpha)f(x',\alpha\cos\theta)\left[e^{-i\phi(x')}(|00\rangle|01\rangle + |10\rangle|11\rangle) + e^{i\phi(x')}(|01\rangle|00\rangle - |11\rangle|10\rangle)\right] \\
& + f(x,\alpha\cos\theta)f(x',\alpha)\left[e^{-i\phi(x)}(|00\rangle|10\rangle + |01\rangle|11\rangle) + e^{i\phi(x)}(|10\rangle|00\rangle - |11\rangle|01\rangle)\right] \\
& + f(x,\alpha\cos\theta)f(x',\alpha\cos\theta)\Big[e^{-i(\phi(x)+\phi(x'))}|00\rangle|11\rangle + e^{i(\phi(x')-\phi(x))}|01\rangle|10\rangle + \\
& \qquad e^{i(\phi(x)-\phi(x'))}|10\rangle|01\rangle - e^{i(\phi(x)+\phi(x'))}|11\rangle|00\rangle\Big]\Big\},
\end{aligned} \tag{2.22}$$

where x and x' are the outcomes of the $\widetilde{Z}$ measurements (top and bottom in Figure 2.8, respectively). For simplicity, we disregard the final teleportations back to qubus modes,

as we have already discussed how they affect the average fidelity of the state in Section 2.3. Since we have two homodyne measurements to consider, we need to look at the four cases: (i) x greater than x_0 and x' greater than x_0; (ii) x greater than x_0 and x' less than x_0; (iii) x greater than x_0 and x' less than x_0; (iv) x less than x_0 and x' less than x_0. The necessary corrections for each of these cases are (i) $\mathbb{1} \otimes \mathbb{1}$ (ii) $\mathbb{1} \otimes XZ_{\phi(x')}$ (iii) $XZ_{\phi(x)} \otimes \mathbb{1}$ (iv) $XZ_{\phi(x)} \otimes XZ_{\phi(x')}$. Integrating over x and x' for these four different regions, one finds the process fidelity to be

$$F_{\text{CSIGN}} = \frac{1}{4}\left(1 + \text{erf}\left(\frac{x_d}{2\sqrt{2}}\right)\right)^2, \tag{2.23}$$

which just corresponds to the square of the process fidelity for a one-bit teleportation into qubits, as the only source of failure is the indistinguishability of the basis states for qubus logic. A plot showing how this fidelity scales as a function of x_d is shown in Figure 2.9.

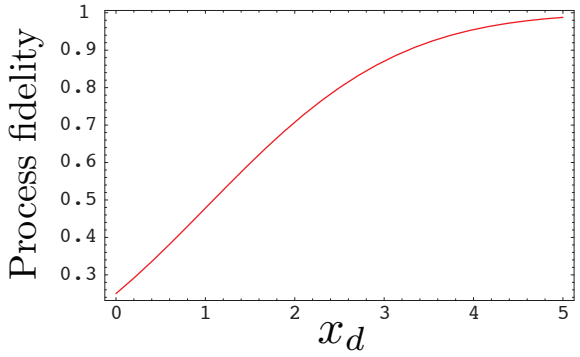

Figure 2.9: *Fidelity F_{CSIGN} due to CSIGN teleportation, as a function of x_d.*

Post-selected implementation of the entangling gate

We can counteract the reduction in fidelity shown in Figure 2.9 in a similar way to the single qubit gate case, by only accepting measurement outcomes less than $x_0 - y$ and greater than $x_0 + y$. We find the success probability and conditional fidelity to be

$$P_{\text{CSIGN}} = \frac{1}{4}\left(\text{erfc}\left(\frac{2y - x_d}{2\sqrt{2}}\right) + \text{erfc}\left(\frac{2y + x_d}{2\sqrt{2}}\right)\right)^2 \tag{2.24}$$

$$F_{\text{CSIGN},y} = \left(\frac{\text{erfc}\left(\frac{2y-x_d}{2\sqrt{2}}\right)}{\text{erfc}\left(\frac{2y-x_d}{2\sqrt{2}}\right) + \text{erfc}\left(\frac{2y+x_d}{2\sqrt{2}}\right)}\right)^2, \tag{2.25}$$

respectively. As before, we see that the process fidelity can be made arbitrarily close to 1 at the cost of lower probability of success. It should also be immediately clear that as $y \to 0$, we have $P_{\text{CSIGN}} \to 1$ and $F_{\text{CSIGN},y} \to F_{\text{CSIGN}}$.

We see how discarding some of the teleportation outcomes improves the the performance in Figure 2.10. Even though there is some degradation due to the use of two approximate teleportations instead of one, the general scalings of the fidelity and probability of success with respect to y and x_d are similar to the one-bit teleportation. In particular, we see that the fidelity can be increased by increasing x_d (or equivalently, α) or by increasing y.

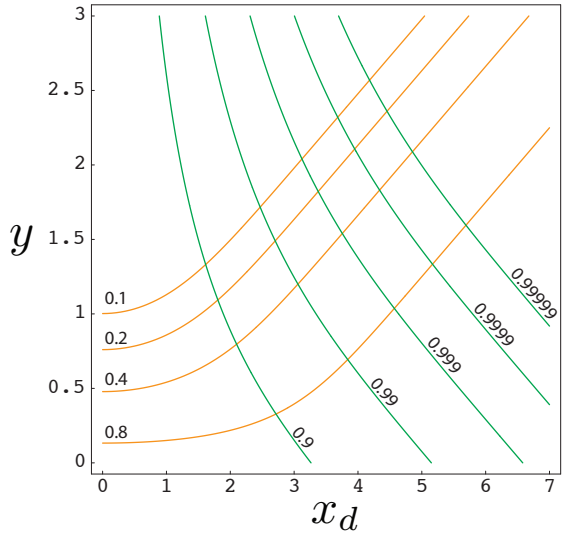

Figure 2.10: *Contour lines for post-selected fidelity $F_{\text{CSIGN},y}$ of CSIGN teleportation (green), and success probability for post-selection (gold), as a functions of x_d and y.*

2.5 Preparation of entangled states

The technique we have describe for the preparation of the maximally entangled qubit pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ can be generalized to prepare entangled states known as *GHZ states* [GHZ89], which have the general form

$$\frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \tag{2.26}$$

Such states are locally equivalent to a star-shaped graph states [HDE+06], which in turn can be used in the preparation of the large entangled states used in the one-way model of computation [RB01, BR05].

We first start with the state $(|0\rangle + |1\rangle)/\sqrt{2}$ and teleport it to a qubus initially in the larger amplitude $|\sqrt{N}\alpha\rangle$, resulting in $|\sqrt{N}\alpha\rangle + |\sqrt{N}\alpha e^{i\theta}\rangle$. Sending this state through an N port beam splitter with $N-1$ vacuum states in the other ports yields $|\alpha\rangle^{\otimes N} + |\alpha e^{i\theta}\rangle^{\otimes N}$, by the same linearity arguments as before. Each of these modes can then be teleported back to qubits, yielding $(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$.

Beyond preparing GHZ states, this same circuits can be used to encode quantum states into a quantum *repetition code* [Sho96]. An n qubit repetition code makes the correspondence

$$c_0|0\rangle + c_1|1\rangle \rightarrow c_0|0\rangle^{\otimes N} + c_1|1\rangle^{\otimes N}, \tag{2.27}$$

so that it is possible to correct X errors on up to $\lfloor \frac{n}{2} \rfloor$ qubits. Such an encoding can be performed by simply preparing the input of the teleportation in the state $c_0|0\rangle + c_1|1\rangle$ and obtain an approximation to $c_0|0\rangle^{\otimes N} + c_1|1\rangle^{\otimes N}$. In order to evaluate the performance of this process, we once again calculate the process fidelity by using the input state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and acting on the second subsystem. Using a generalization of (2.22) we calculate the effect of $\alpha\theta^2 \not\gg 1$ on the production of a GHZ state of size N to be

$$F_{\text{REP}} = \frac{1}{2^N}\left(1 + \text{erf}\left(\frac{x_d}{2\sqrt{2}}\right)\right)^N. \tag{2.28}$$

Again, this corresponds to the Nth power of the process fidelity of a single one-bit teleportation. The fidelity of preparing repetition encoded states drops exponentially with N. In Figure 2.11 we show the fidelity as a function of x_d for $N = 3$ and for $N = 9$.

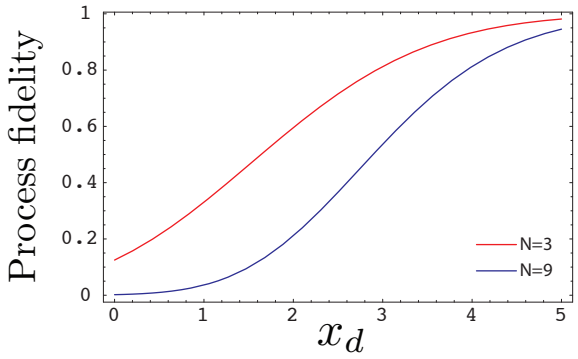

Figure 2.11: *Process fidelity F_{REP} of repetition encoding as a function of x_d.*

2.5.1 Post-selected preparation of entangled states

The reduction in fidelity due to $\alpha\theta^2 \not\gg 1$ in (2.28) can be counteracted, as before, by simply performing post-selection during the one-bit teleportations into the qubits.

As each teleportation has independent quadrature measurement outcomes, we find the success probability and conditional fidelity to be

$$P_{\text{REP}} = \frac{1}{2^N}\left(\text{erfc}\left(\frac{2y - x_d}{2\sqrt{2}}\right) + \text{erfc}\left(\frac{2y + x_d}{2\sqrt{2}}\right)\right)^N \tag{2.29}$$

$$F_{\text{REP},y} = \left(\frac{\text{erfc}\left(\frac{2y-x_d}{2\sqrt{2}}\right)}{\text{erfc}\left(\frac{2y-x_d}{2\sqrt{2}}\right) + \text{erfc}\left(\frac{2y+x_d}{2\sqrt{2}}\right)}\right)^N \tag{2.30}$$

As $y \to 0$ we see that $P_{\text{REP}} \to 1$ and $F_{\text{REP},y} \to F_{\text{REP}}$.

The effect of discarding some of states corresponding to undesired homodyne measurement outcomes can be seen in Figures 2.12 and 2.13. One can prepare a state encoded in the repetition code with an arbitrarily high process fidelity, regardless of what θ and α are. The expected degradation in performance due to the additional teleportations is also evident in the faster decay of the probability of success with larger y. In reality, due to the exponential dependence in N, this approach is only practical for a small number of qubits.

2.6 Error correction

In order to perform quantum error correction, it is necessary not only to prepare encoded states, but to also detect errors without collapsing quantum superpositions. In the case of the repetition code, this is done by measuring the parity of multiple pairs of qubits in the encoded state [Sho96]. Intuitively, this is because any two qubits in the encoded basis states will be in the state state, and thus measuring the parity will not be able to distinguish between the basis encoded basis state – any two qubits of an encoded state will always have even parity (either $|00\rangle$ or $|11\rangle$). If an X error acts on a particular qubit, it will cause some subset of parities become odd, and the location of the error can then be inferred.

As we have discussed previously in Section 2.2, the parity of two qubits can be obtained by rotating the qubus state twice depending on the state of each qubit, each time in

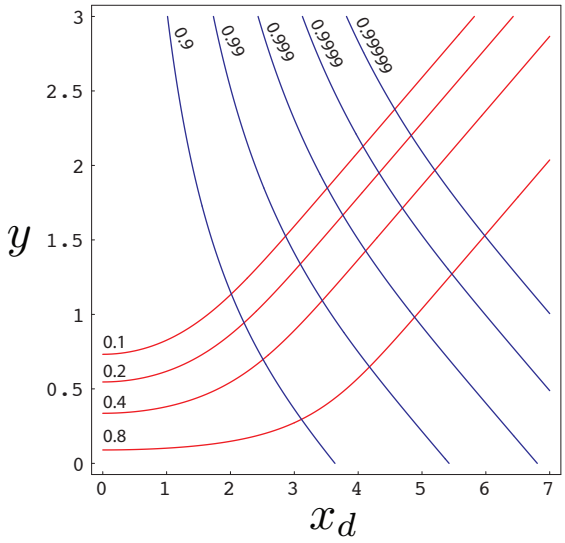

Figure 2.12: *Contour lines for post-selected process fidelity $F_{REP,y}$ of 3-fold repetition encoding (blue), and success probability for post-selection (red), as a functions of x_d and y.*

a different direction, as first demonstrated in [YNM06]. Quantum mechanically, the measurement of the parity of two qubits corresponds to the measurement of the Pauli operator ZZ. With two parity gates we can measure the Pauli operators ZZI and IZZ. That is, one parity gate is applied to qubits 1 and 2 to measure ZZI while the second parity gate is applied to qubits 2 and 3 to measure IZZ. There are four subspaces to consider: no error, spanned by $|000\rangle$ and $|111\rangle$; an error on qubit 1, spanned by $|100\rangle$ and $|011\rangle$; an error on qubit 2, spanned by $|010\rangle$ and $|101\rangle$; or an error on qubit 3, spanned by $|001\rangle$ and $|110\rangle$. We can see what the effect of a bit flip error on each of the modes is by considering the state $|b_1b_2b_3\rangle|\alpha\rangle|\alpha\rangle$, where $b_i \in \{0, 1\}$. Directly before the measurement of the qubus state in Figure 2.14 the joint state of the system is $|b_1b_2b_3\rangle|\alpha e^{i(b_1-b_2)\theta}\rangle|\alpha e^{i(b_3-b_2)\theta}\rangle$. When we measure the probe states to be $|\alpha e^{\pm im\theta}\rangle|\alpha e^{\pm in\theta}\rangle$, where $m, n \in \{0, \pm 1\}$, we know whether there was no error ($m, n = 0$) or a one bit flip error, the location of the bit flip also being identified by the values of m and n.

There are many different codes that are more powerful and more efficient than the repetition code. The class usually considered for the purposes of fault-tolerant quantum computation is the class of *stabilizer codes* [Got97]. In order to perform error correction with stabilizer codes, it is sufficient to be able to measure the parity of m different qubits, for some number m which depends on the code. These observables that must be

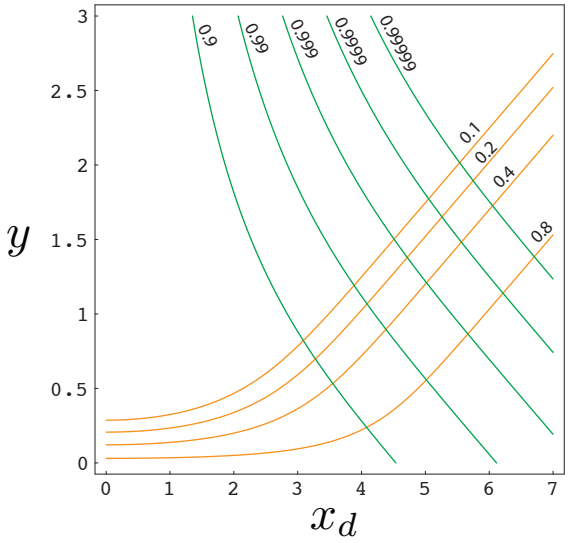

Figure 2.13: *Contour lines for post-selected process fidelity $F_{REP,y}$ of 9-fold repetition encoding (green), and success probability for post-selection (gold), as a functions of x_d and y.*

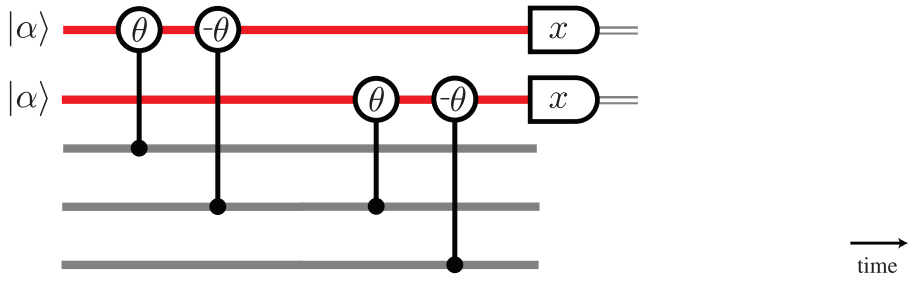

Figure 2.14: *Two parity gates combined to measure the Pauli operators ZZI and IZZ.*

measured are the generators of a group, called the stabilizer group, which is the origin of the name for this class of codes. In general, however, $m > 2$, and the techniques we have described above cannot be applied without modification. As we have discussed earlier, if we simply apply a longer sequence of controlled rotations, the resulting qubus states will lie outside the logical space we have defined, and will also disturb the quantum superpositions of encoded states. As a concrete example, consider the $[[7, 1, 3]]$ stabilizer code [Ste96b], which we have discussed in Chapter 1. This code can correct a single arbitrary quantum error in any of the 7 qubits, and it has been used extensively in studies of fault-tolerance in quantum computers due to the fact that it allows for simple constructions of fault-tolerant encoded gates [Got98a]. In order to detect which error

has corrupted the data, one must measure six multi-qubit Pauli operators which, up to qubit permutations and local unitaries, are equivalent to the Pauli operator $ZZZZ$, or the measurement of *only* the parity of 4 qubits. For an arbitrary stabilizer code, various multi-qubit Pauli operator must be measured, each of which is always equivalent to a measurement of only the parity of a subset of qubits, thus it is sufficient to consider only multi-qubit parity measurements in order to perform quantum error correction with stabilizer codes.

2.6.1 Fault-tolerance

The measurement of the parity of two qubits using a single probe mode also has the problem that it is not fault-tolerant. If there is an error on the coherent probe mode during one of the controlled rotations, say photon loss, it would be transferred to a phase error in each of the physical qubits it interacts with afterwards – that is, a single fault can cause a number of errors which is greater than the number of errors the code can correct. For this reason we now look at measuring the syndromes of stabilizers fault-tolerantly.

Shor [Sho96] first described how to fault-tolerantly measure the generators of the stabilizer group of a quantum error correcting code using ancilla GHZ states $\left(|0\rangle^{\otimes m} + |1\rangle^{\otimes m}\right)/\sqrt{2}$, CNOTs and Hadamards. For example, in order to measure the Pauli operator $ZZZZ$, we would use the circuit shown in Figure 2.15(a). The main feature of this circuit that enables fault-tolerance is the fact that all operations are transversal – each qubit in the computation (the bottom four lines) interacts with only once ancilla.

In order to see how this circuit measures the parity of m qubits, consider the following. Applying $H^{\otimes m}$ to the ancilla in the GHZ state results in an equal superposition of all binary string of even weight. The CNOTs will cause the ancilla bits to flip depending on the input state. For states of even parity, an even number of bit flips occur, and odd parity will cause an odd number of bits to flip. By inspecting the parity of the measurement outcomes, it is possible to infer the parity of the input state. The fact that the ancillas are prepared in a superposition of all possible even states parity ensures that we learn nothing but the parity of the input state, guaranteeing that we do not disturb superpositions of states with the same parity. This circuit generalizes in the obvious way in the case of m qubits.

Using qubus logic and the correspondence between controlled rotations and CNOTs, as introduced in Section 2.2, the interactions can be directly translated to interactions be-

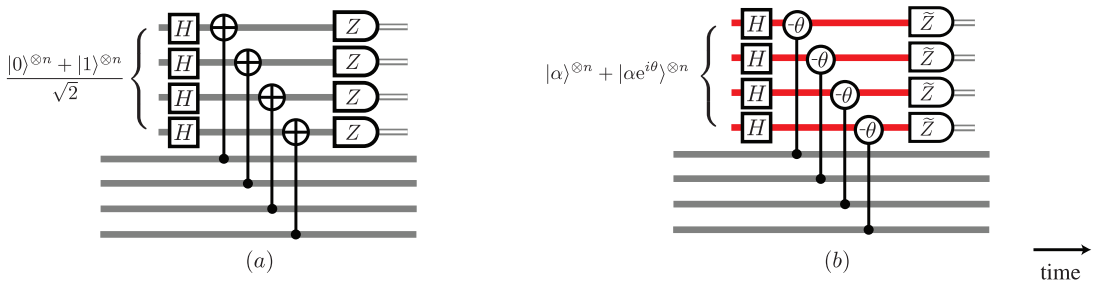

Figure 2.15: *(a) Circuit for the measurement of the parity of four qubits [Sho96]. (b) Same circuit modified to use coherent states and controlled rotations.*

tween qubits and qubuses, while the measurements are simply quadrature measurements of the qubits. The GHZ state can be prepared by the use of teleportations and beamsplitters, as outlined in Section 2.5. The Hadamard unitaries can be implemented by teleportation, along with unitaries acting on qubits, as described in Section 2.3. Therefore Shor's fault-tolerant parity measurement circuit can be translated with little modification. The resulting abbreviated circuit is depicted in Figure 2.15(b).

2.6.2 Noisy ancillas

If the probability of error at each gate is bounded by ϵ, transversal operations and encoding can ensure that the probability of an uncorrectable error is $O(\epsilon^2)$ instead of $O(\epsilon)$. We consider two possible errors in qubus logic: X-like errors, where the probabilities of the states $|\alpha\rangle$ and $|\alpha e^{\pm i\theta}\rangle$ are randomized, and Z-like errors, where the relative phase between superpositions is randomized.

Z-like errors in the cat state (including dephasing of coherent superpositions, one of the consequences of photon loss in the controlled rotations) do not lead to errors in the encoded data, just errors in the outcome of the Pauli operator measurement. This is because the Hadamard gate will map Z-like errors to X-like errors. If error correction is to be performed on the data, instead of just error detection, the parity measurement must be repeated three times, and a majority vote of the outcomes taken, in order to ensure that the measurement outcome is reliable [Pre97].

An error during cat state preparation may lead to correlated X-like errors in the cat state with probability $O(\epsilon)$, which can lead to uncorrectable errors in the encoded data during the measurement of the Pauli operator, thus defeating the purpose of encoding the data for fault-tolerant quantum computation. In order to avoid this, one can verify the

integrity of the cat state via non-destructive state measurement [Pre97, AGP06]. When using controlled rotations and coherent beam probes, this translates to preparing an extra copy of the cat state, which remains in coherent state logic, interacting with the qubit GHZ state transversally with controlled $-\theta$ rotations, and $\widetilde{Z}$ measuring each mode of the redundant cat state. As the basis states in an error free GHZ state correspond to strings encoded in a repetition code, by performing classical error correction on the measurement outcomes one can deduce the locations of X-like errors in either the GHZ state or the redundant cat state just measured. Repeating this procedure with yet another redundant cat state allows for the inference of which locations in the qubit GHZ state have X errors with high enough probability to ensure uncorrectable errors are only introduced into the data with probability $O(\epsilon^2)$ [Pre97], so that parity measurements with a verified ancilla can be used for fault-tolerant quantum computation.

Some of the systematic errors in the probe beams, such as phase rotation or attenuation, can be partially compensated for by additional phase space rotations and by adjusting the threshold x_0 of the $\widetilde{Z}$ measurements individually to minimize additional X-like errors. Moreover, errors in the transversal operations during the preparation of the cat state are independent, and thus do not need special consideration during this verification stage – they do contribute to ϵ, however, and are thus crucial for fault-tolerance threshold calculations.

2.7 Summary

We have described in detail various applications for one-bit teleportations between a qubit and a qubus. Using these teleportations, we proposed a scheme for universal quantum computation, called qubus logic, which is a significant improvement over other proposals for quantum computation using coherent states, as it requires only weak interactions. This scheme also allows for the use of post-selection to arbitrarily increase the fidelity of the gates given any interaction strength at the cost of lowering the probability of obtaining the desired outcome. We also demonstrate how fault-tolerant error correction in qubits can be performed by using qubus states as ancillas, allowing for greater flexibility in the construction of quantum information processing devices.

The one-bit teleportations also allow for the preparation of highly entangled N party states known as GHZ states, which can be used as building blocks in the preparation

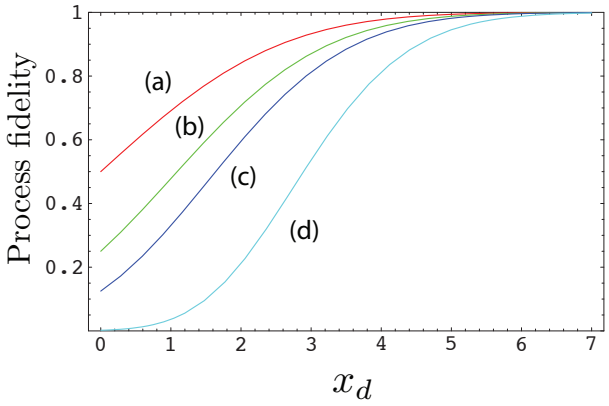

Figure 2.16: *Process fidelity as a function of x_d for (a) the qubus logic single qubit gate (F_p); (b) the CSIGN teleportation (F_{CSIGN}); (c) repetition encoding with $N = 3$ shown in blue (F_{REP}); (d) repetition encoding with $N = 9$ (F_{REP}).*

of the entangled states discussed in Chapter 1. Moreover, the same circuitry can be used to encode states in the repetition code. In these cases, where we are interested in preparing resource states, the power and flexibility of post-selected teleportations can be fully exploited, as the achievable fidelity of the state preparation is independent of the interaction strength available, as long as it is finite. The fact that the coherent state measurements essentially herald the fidelity of the operations opens the possibility for the use of post-selection in conjunction with error heralding to optimize resource usage.

The main property of the qubus which is exploited in the schemes described here is the fact that entanglement can be easily created in the qubus through the use of a beam splitter. Local operations, on the other hand, are easier to perform on a qubit. The controlled rotations allow for information to be transferred from one system to the other, allowing for each physical system to be exploited to maximal advantage.

Given the strength of interaction and coherent state amplitude, both the fidelity and the probability of success suffer as the operations become more complex, as can be seen in Figures 2.16 and 2.17. This is because multiple instances of the imperfect one-bit teleportation from qubus to qubit are used. This only imposes serious restrictions on the size of GHZ states prepared, as all other operations use a fixed number of one-bit teleportations.

We also demonstrated how all these different applications of one-bit teleportations can be combined to allow for fault-tolerant quantum error correction, which is essential for the implementation of scalable quantum computers. The use of qubus states as an-

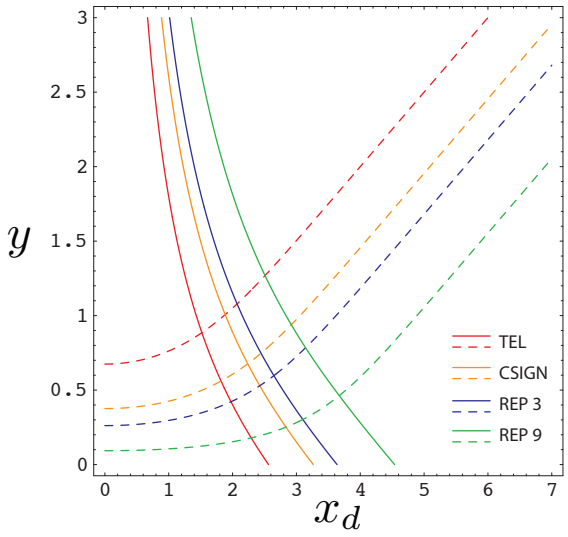

Figure 2.17: *Curves of constant conditional process fidelity (solid) and the probability of post-selection success (dashed) as functions of x_d and y. In all cases, the fidelity is set to 0.9 and the probability of success to 0.5.*

cillas, instead of qubits, can be used to allow for greater flexibility in the construction of quantum information processing devices.

While the scheme presented has been abstracted from particular physical implementations, any physical realizations of a qubit and a harmonic oscillator would suffice. The only requirements are controlled rotations, along with fast single qubit gates and x-quadrature measurements, which are necessary to enable feed-forward of results for the implementation of the relevant corrections.

Chapter 3

Entanglement mediated by a ballistic particle

3.1 Introduction

We have discussed how interactions between a qubit and a harmonic oscillator can aid the implementation of quantum information processing tasks. This idea can be adapted, to a large extent, to work with different interactions, such as controlled phase-space displacements instead of controlled phase-space rotations [SNB+06]. In this chapter we consider not only modifying the interaction, but also the the ancillary system. We replace the harmonic oscillator with the position and momentum state of a free quantum particle, and the replace the controlled phase space rotation with the scattering of the quantum particle by a potential which depends on the qubit state.

Similar ideas have been proposed to perform high-fidelity measurement of flux-type qubits by scattering solitons in a non-linear transmission line [ARS06, FSSKS07]. The vortices trapped in the transmission line behave as localized particles, and thus are referred to as *fluxons*. These fluxons have a magnetic moment which interacts with the magnetic moment of the flux qubit. If the interaction is weak with respect to the strength of the qubit Hamiltonian, and if the particles have a well defined momentum, then the effect of this interaction is to either slow down or speed up the fluxons, depending on the state of the qubit. The state of the qubit can then be inferred by monitoring the time of arrivals of the fluxons after interaction with the qubit.

Fluxons are predicted to behave as quantum particles at sufficiently low tempera-

tures [KI96, SBJM97]. This behavior has been demonstrated by investigating the escape rate of fluxons from a well [Wal00]. At low temperatures, where thermal activation is exponentially suppressed, macroscopic quantum tunneling of these particles has been observed [WLL+03]. Energy level quantization in the well was demonstrated by inducing excitations with microwave radiation and observing enhancement of the tunneling rate. However, the coherent superposition of different state of fluxons has not been demonstrated. This is because the approach of populating the ground state of a double well and distorting the well so that interference fringes between the wave functions can be observed leads to a breakdown of the interpretation of fluxons as particles [MS78].

Here we propose a protocol for entangling two qubits via the scattering of a quantum particle, as depicted in Figure 3.1. Just as in Chapter 2, this can also be exploited for quantum information processing tasks. In particular, this enables the preparation of entanglement between distant qubits mediated by the fluxon. This entanglement can then be used for tasks such as teleportation [BBC+93] and distributed computation [CEHM99]. The protocol can also be used as an indirect demonstration of superpositions of fluxon states by using the fluxon as the quantum particle interacting with superconducting flux qubits. Each qubit is initially prepared in a superposition of the pointer states of the interaction. After scattering of the fluxon wave packet, data is collected only when no delay is observed in the time of arrival of the fluxon. This corresponds to the fluxon having being delayed by one qubit, but advanced by the other. As the qubits are in a superposition of states that cause delay and advancement, which-path information is lost, and the corresponding state of the qubit is an entangled state. This requires the presence of coherent superpositions of different path alternatives for the fluxon. If decoherence precludes this, then the corresponding state of the qubits will be a highly mixed state with no entanglement. Thus, through the use of post-selection and entanglement verification, it is possible to infer that the fluxons were in a coherent superposition. We find, however, that such an experiment would be difficult with present day technology, as it requires energy dissipation rates significantly lower than what has been observed to date.

This chapter is organized as follows. First, in Section 3.2 we review properties of a free particle in the quantum setting, and in Section 3.3 we illustrate how the scattering of quantum particles by qubits can be used to create entanglement between the qubits in a probabilistic manner. In Section 3.4 we consider the effects of dissipation in the free-particle by estimating the distance it can travel before decohering significantly. We describe a possible physical implementation of the protocol in Section 3.5, and investi-

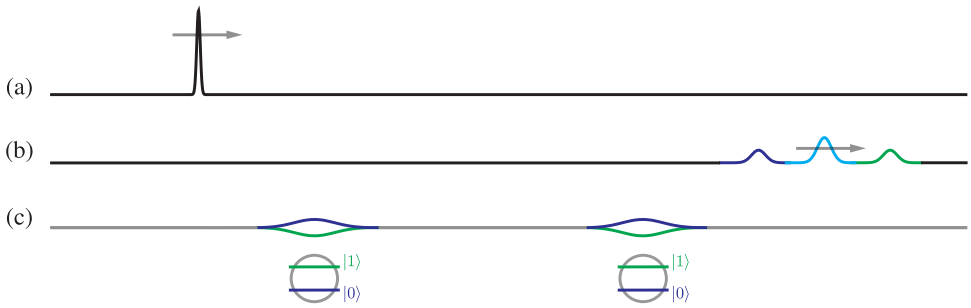

Figure 3.1: *The probability distribution for the position of a particle (a) before and (b) after it has been scattered by (c) a potential which depends on the state of the qubits.*

gate the feasibility of an experiment using present-day technology.

3.2 Time evolution of a free particle

Consider a point-like quantum particle in one spatial dimension and in the absence of any potentials. We take the particle to have mass m, and ignore any internal degrees of freedom. In this case, the Hamiltonian governing the evolution of such a particle only has a contribution due to the kinetic energy of the particle, or

$$\mathcal{H}_F = \frac{p^2}{2m}, \tag{3.1}$$

where p is the momentum operator. It is immediatelly clear then that the momentum eigenbasis $|p\rangle$ diagonalizes this Hamiltonian, and the time evolution operator from time t_0 to time t_1 is

$$U(t_1, t_0) = \exp\left[-\frac{i}{\hbar} H_F (t_1 - t_0)\right] \tag{3.2}$$

$$= \int_{-\infty}^{+\infty} dp\, |p\rangle\langle p|\ \exp\left[-\frac{i}{\hbar}\frac{p^2}{2m}(t_1 - t_0)\right]. \tag{3.3}$$

If one is interested in position measurements, it is convenient to consider the representation of this operator in the position eigenbasis $|x\rangle$, or

$$\langle x|U(t_1, t_0)|x'\rangle = \int_{-\infty}^{+\infty} dp\, \langle x|p\rangle\langle p|x'\rangle\ \exp\left[-\frac{i}{\hbar}\frac{p^2}{2m}(t_1 - t_0)\right], \tag{3.4}$$

$$= \frac{1}{2\pi\hbar}\int_{-\infty}^{+\infty} dp\ \exp\left[i\frac{p(x - x')}{\hbar}\right]\ \exp\left[-\frac{i}{\hbar}\frac{p^2}{2m}(t_1 - t_0)\right], \tag{3.5}$$

$$= \sqrt{\frac{m}{2\pi\hbar i(t_1 - t_0)}}\exp\left[i\frac{m(x - x')^2}{2\hbar(t_1 - t_0)}\right]. \tag{3.6}$$

Given any initial pure state $|\psi(t=0)\rangle$ with position representation

$$|\psi(t=0)\rangle = \int_{-\infty}^{+\infty} dx\ \psi(x;t=0)|x\rangle, \tag{3.7}$$

it is possible to compute the state at time t from the time evolution operator by using

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \tag{3.8}$$

$$= \int_{-\infty}^{+\infty} dx \int_{-\infty}^{+\infty} dx'\ \langle x|U(t,0)|x'\rangle\ \psi(x';t=0)|x\rangle, \tag{3.9}$$

so that it becomes clear that the wavefunction at time t is given by

$$\psi(x;t) = \int_{-\infty}^{+\infty} dx'\ \langle x|U(t,0)|x'\rangle\ \psi(x';t=0). \tag{3.10}$$

In the extreme case where the initial state has a wavefunction $\psi(x;0) = \delta(x-a)$, the integral is easily evaluated and we find that $\psi(x;t) = \langle x|U(t,0)|a\rangle$. Initially the wave packet has no spread and is perfectly localized, but as it evolves under the action of the free Hamiltonian it spreads to a Gaussian of finite width, as given by (3.6). Similarly, any initial Gaussian wavefunction of the form

$$\psi(x,t=0) = \frac{1}{(2\pi\sigma^2)^{1/4}} \exp\left(i\frac{p_0 x}{\hbar}\right) \exp\left(-\frac{x^2}{4\sigma^2}\right) \tag{3.11}$$

will lead to

$$\psi(x,t) = \frac{1}{(2\pi)^{1/4}\sqrt{\sigma + i\frac{\hbar t}{2m\sigma}}} \exp\left[i\frac{p_0\left(x-\frac{p_0 t}{2m}\right)}{\hbar}\right] \exp\left[-\frac{\left(x-\frac{p_0 t}{m}\right)^2}{4\sigma^2\left(1+i\frac{\hbar t}{2m\sigma^2}\right)}\right], \tag{3.12}$$

which is a Gaussian wave packet with mean $x - \frac{p_0 t}{m}$, and the corresponding probability distribution has variance

$$\sigma(t)^2 = \sigma^2\left(1 + \frac{\hbar^2 t^2}{4m^2\sigma^4}\right). \tag{3.13}$$

The time dependence of the mean leads to the interpretation of p_0 as the average momentum of the wavefunction. The fact that the variance increases with time is what is known as *dispersion*, and is a consequence of the free particle Hamiltonian being quadratic in p, so that different momentum eigenstates propagate at different speeds.

3.3 Particle scattering by a qubit-dependent potential

Consider a particle which is only free to move along one spatial dimension, as before, but that now interacts with a qubit via the Hamiltonian

$$\mathcal{H}_I = g\ \sigma_Z \otimes U(x), \tag{3.14}$$

where the first tensor factor corresponds to the qubit, and the second tensor factor corresponds to the particle degrees of freedom, and g is the strength of the interaction. We restrict ourselves to the case where the potential $U(x)$ is a smooth positive function peaked around a, where the qubit is located, with $\max_x |U(x)| = 1$, and which vanishes with growing $|x-a|$. The particle Hamiltonian is just the free-particle Hamiltonian, while the qubit is assumed to have a Hamiltonian which commutes with $\mathcal{H}_I$, for simplicity, so that in the rotating frame of the qubit the interaction and the free-particle Hamiltonian are unchanged. For the remainder of this section the implied frame of interest is the rotating frame of the qubit. The total Hamiltonian for this system is then

$$\mathcal{H} = \mathcal{H}_F + \mathcal{H}_I. \tag{3.15}$$

Physically, what are are describing is a localized potential with a sign which depends on the projection of state of the qubit on to the eigenbasis of σ_Z. If the particle and the qubit are prepared in some initial state $|\psi(0)\rangle$, then the joint state of the after interaction is $|\psi(t)\rangle = \mathrm{e}^{-\frac{i}{\hbar}\mathcal{H}t}|\psi(0)\rangle$. Even if $|\psi(0)\rangle$ is initially a product state between the particle and qubit subsystem, the state after the particle and the qubit interact will, in general, be entangled. The simplest way to see how entanglement comes about is by considering the evolution of the quantum particle in the WKB or semi-classical approximation [LL03].

For the regions far from the center of the potential $U(x)$, the fluxon evolves under the action of the free-particle Hamiltonian. The plane-wave solutions for the time-independent Schrödinger equation under the free-particle Hamiltonian are

$$\psi(k) = \mathrm{e}^{ikx}, \tag{3.16}$$

with momentum $p_k = \hbar k$. For any given potential $U(x)$, the scattering matrix can be computed to determine what is the ratio between the incoming amplitude and outgoing amplitude of the plane wave $\psi(k)$ that impinges on the potential. For plane waves with kinetic energy $E_k = -\frac{\hbar^2 k}{2m}$ which is significantly higher than the g, the magnitude of this ratio is close to one. Close to the center of the potential, however, kinetic energy is converted to potential energy, and thus the momentum of the particle will change. This induces a phase shift $\chi(k)$ between the plane wave before and after interaction with the potential so that the scattered plane wave has the form

$$\psi(k) = \mathrm{e}^{ikx+i\chi(k)}. \tag{3.17}$$

In the case where $U(x)$ varies slowly compared to the wavelength $\lambda = \frac{2\pi}{k}$, and under the assumption that $g \ll E_k$, this phase shift is given by [ARS06]

$$\chi(k) \approx k(x_1 - x_0) - \int_{x_0}^{x_1} dx \, \frac{\sqrt{2m[E_k - gU(x)]}}{\hbar} \tag{3.18}$$

$$= k(x_1 - x_0) - \int_{x_0}^{x_1} dx \, \frac{\sqrt{2mE_k}}{\hbar} \sqrt{1 - \frac{g}{E_k} U(x)} \tag{3.19}$$

$$= k(x_1 - x_0) - \frac{\sqrt{2mE_k}}{\hbar} \int_{x_0}^{x_1} dx \, \sqrt{1 - \frac{g}{E_k} U(x)} \tag{3.20}$$

$$\approx k(x_1 - x_0) - \frac{\sqrt{2mE_k}}{\hbar} \int_{x_0}^{x_1} dx \, \left[1 - \frac{g}{2E_k} U(x)\right] \tag{3.21}$$

$$= -\frac{\sqrt{2mE_k}}{\hbar} \int_{x_0}^{x_1} dx \, \frac{g}{2E_k} U(x) \tag{3.22}$$

$$= -\frac{1}{\hbar u_k} \int_{x_0}^{x_1} dx \, U(x) \tag{3.23}$$

where have defined $u_k = p_k/m$ to be the velocity of the plane wave, and where $x_{0,1}$ are on opposite sides of the potential and far from the center. This can be approximated by

$$\chi(k) \approx -\frac{1}{\hbar u_k} \int_{-\infty}^{+\infty} dx \, U(x). \tag{3.24}$$

For a wave packet which is well localized in momentum, one may linearize χ around the average wave number $\langle k \rangle$ so that we may write

$$\chi(k) \approx \chi(\langle k \rangle) + (k - \langle k \rangle) \left. \frac{d\chi}{dk} \right|_{\langle k \rangle}, \tag{3.25}$$

and the phase shift experienced by the wave packet is proportional to the wave number of each of the components. Due to the fact that momentum and position representations of the wave packet are related by Fourier transforms, this k-proportional phase shift in momentum representation corresponds to a spatial shift in the position representation [AW95]. In other words, after interacting with the potential, the wave packet discussed above will be shifted in space by some amount

$$\left. \frac{d\chi}{dk} \right|_{\langle k \rangle} = -\frac{1}{2E_{\langle k \rangle}} \int_{-\infty}^{+\infty} dx \, U(x). \tag{3.26}$$

with respect to an identical wave packet that has not interacted with the potential, where $\langle u \rangle = \hbar \langle k \rangle / m$ is the mean velocity of the packet. Similar argument apply to the case where the potential has its sign flipped. Thus, we may say that, far from the qubit, the

spatial difference between a wave packet that has interacted with the qubit in state $|0\rangle$ and a wave packet that has not is

$$\frac{\Delta x}{2} = \int_{-\infty}^{+\infty} dx \, \frac{g}{2E_{\langle k \rangle}} U(x), \tag{3.27}$$

where $E_{\langle k \rangle}$ is the average kinetic energy of the packet.

Abstractly, the effect of the wave packet being scattered by the qubit can be described by the unitary corresponding to a controlled spatial displacement, or

$$|0\rangle\langle 0| \otimes D(-\Delta x/2) + |1\rangle\langle 1| \otimes D(\Delta x/2), \tag{3.28}$$

which is depicted in Figure 3.2. As spatial displacements are generated by the momentum operators, this unitary commutes with the free particle unitary.

Figure 3.2: *Circuit depicting the spatial displacement of a free particle (red line) controlled by the state of a qubit (grey line).*

If we take the state of the particle, in the absence of interactions, to be $|\psi(t)\rangle$, then after interacting with a qubit in the state

$$\frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{i\theta}|1\rangle), \tag{3.29}$$

the joint state of the system will be well approximated by

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes D(-\Delta x/2)|\psi(t)\rangle + \mathrm{e}^{i\theta}|1\rangle \otimes D(\Delta x/2)|\psi(t)\rangle), \tag{3.30}$$

which is clearly entangled.

3.3.1 Coherent superpositions and interference

A superposition of different displaced states of the particle wave packet can be prepared by measuring the qubit in the σ_X eigenbasis, as depicted in Figure 3.3, resulting in the unnormalized particle state

$$D(-\Delta x/2)|\psi(t)\rangle \pm \mathrm{e}^{i\theta} D(\Delta x/2)|\psi(t)\rangle, \tag{3.31}$$

where the sign depends on the outcome of the σ_X measurement. This is analogous to the one-bit teleportation described in Section 2.3. If we now project into the position eigenbasis, we obtain the amplitude

$$\psi(x - \Delta x/2; t) \pm \mathrm{e}^{i\theta}\psi(x + \Delta x/2; t), \tag{3.32}$$

where

$$\psi(x \pm \Delta x/2; t) = \langle x|D(\pm\Delta x/2)|\psi(t)\rangle. \tag{3.33}$$

This yields the probability density

$$\begin{aligned}\rho(x; t) = |\psi(x - \Delta x/2; t)|^2 + |\psi(x + \Delta x/2; t)|^2 \\ \pm 2\,\mathrm{Re}\,\mathrm{e}^{i\theta}\psi^*(x - \Delta x/2; t)\psi(x + \Delta x/2; t),\end{aligned} \tag{3.34}$$

where the last term corresponds to the interference between the two displaced wave packets. If we had instead a probabilistic mixture of different displaced states, this term would be absent, therefore it can be taken as a signature of quantum behavior.

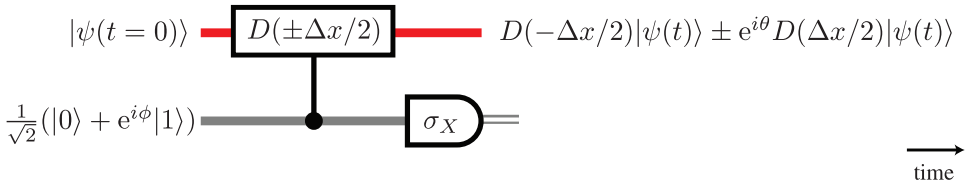

Figure 3.3: *Protocol for the preparation of coherence superpositions of displaced wavefunctions of a particle (red line) by interacting with a qubit (grey line).*

In order to see how interference manifests itself, consider once again a Gaussian wave packet, as described in Section 3.2. For simplicity, we let $t = 0$ correspond to the time at which the the particle is measures. This leads to the probability density

$$\begin{aligned}\rho(x) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left[-\frac{(x - \Delta x/2)^2}{2\sigma^2}\right] + \frac{1}{\sqrt{2\pi}\sigma}\exp\left[-\frac{(x + \Delta x/2)^2}{2\sigma^2}\right] + \\ \pm 2\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{x^2}{4\sigma^2}\right)\exp\left(-\frac{\Delta x^2}{16\sigma^2}\right)\cos\left(\frac{p_0\Delta x}{2\hbar} + \theta\right).\end{aligned} \tag{3.35}$$

By adjusting θ, it is possible to enhance or diminish the effect of the interference term, so that the probability density $\rho(x = 0)$ at the center can be made smaller or greater than what it would be if the state was simply an incoherent mixture of two wave packets centered at $x - \Delta x/2$ and $x + \Delta x/2$.

It is important to note that $\frac{p_0 \Delta x}{\hbar}$ occurs in the argument of the cosine in the interference term. This can be re-written as $\frac{2\pi\Delta x}{\lambda}$ where $\lambda = \frac{2\pi\hbar}{p_0}$ is the deBroglie wavelength of the particle. Therefore this protocol requires the error in Δx to be significantly smaller than λ so as to ensure the reliable observation of the interference term. This can pose a significant experimental challenge for experiments employing sufficiently massive particles.

3.3.2 Particle-mediated entanglement of qubits

It is possible to demonstrate quantum behavior by a different approach, which is more directly related to properties which are associated with non-classical behavior in quantum systems. Imagine two well-separated qubits prepared in the unentangled state

$$|+\rangle|+\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \tag{3.36}$$

If a particle wave packet is scattered by the two qubits, the result at some time t after scattering will be the entangled state

$$|s(t)\rangle = \frac{1}{2}[|00\rangle \otimes D(-\Delta x)|\psi(t)\rangle + (|01\rangle + |10\rangle) \otimes |\psi(t)\rangle + |11\rangle \otimes D(\Delta x)|\psi(t)\rangle]. \tag{3.37}$$

This sequence of steps in depicted in Figure 3.4. We can interpret this as four different alternative interactions: the particle being slowed down twice, the particle being slowed then advanced, the particle being advanced then slowed, and finally the particle being advanced twice. If we measure the position of the particle at time t, we expect to find a distribution that is multi-modal, as depicted in Figure 3.5. It should be immediatelly clear, however, that x outcomes around the peak of $\psi(x;t)$ should yield corresponding qubit state that is close to the maximally entangled state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. This state can be used to demonstrate the violation of Bell's inequalities, ruling out the possibilities of local hidden variable theories that match the predictions of quantum mechanics. In this sense, the state $|\Psi^+\rangle$ has no classical probability theory counterpart, and thus its observation can be seen a signature of quantum behavior. Moreover, the preparation of such a state is only possible if the states of the qubit as well as the state of the quantum particle are coherent. Thus, the preparation of entanglement between qubits using this protocol corresponds to the indirect observation of coherent superpositions of quantum particle states.

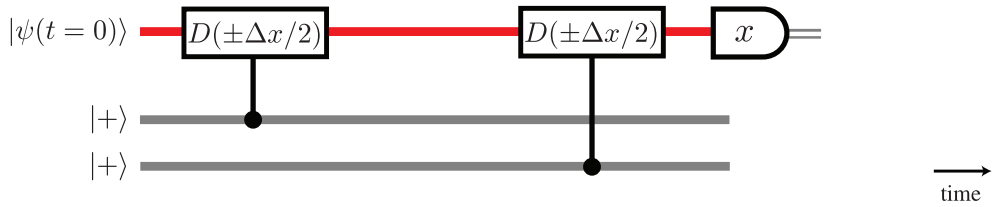

Figure 3.4: *Protocol for the entanglement of two qubits (grey lines) via interaction with a particle (red line).*

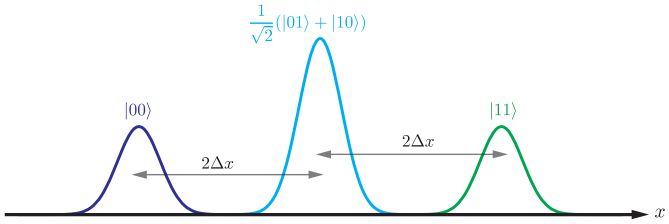

Figure 3.5: *Distribution of position measurement outcomes for the state $|s(t)\rangle$, with regions of the distribution labeled by the qubit states they are correlated with.*

In order to quantify how close we get to the state $|\Psi^+\rangle$ by post-selecting on the x measurement outcome, we compute the exact expressions for the fidelity. The conditional state of the qubits, depending of the outcome x of the position measurement, is given by

$$|q(x)\rangle = \frac{1}{2}[\psi(x+\Delta x;t)\,|00\rangle + \psi(x;t)\,(|01\rangle + |10\rangle) + \psi(x-\Delta x;t)\,|11\rangle], \quad (3.38)$$

This unnormalized state has norm $\sqrt{\langle q(x)|q(x)\rangle}$ which in turn leads to

$$\rho(x) = \langle q(x)|q(x)\rangle = \frac{1}{4}[|\psi(x+\Delta x;t)|^2 + 2|\psi(x;t)|^2 + |\psi(x-\Delta x;t)|^2], \quad (3.39)$$

which is the probability density for the outcome x in the position measurement. The normalized conditional state, for some range of outcomes between $x \in [a,b]$ is

$$\rho_{a,b} = \frac{1}{\Pr(x \in [a,b])} \int_a^b dx\, |q(x)\rangle\langle q(x)|. \quad (3.40)$$

where

$$\Pr(x \in [a,b]) = \int_a^b dx\, \rho(x), \quad (3.41)$$

is the *probability of success*, or the probability of obtaining the desired post-selected outcome.

All these quantities can be readily computed for Gaussian wave packets. Taking $t = 0$ to be the time of measurement, the free particle wavefunction (3.12) yields

$$\psi(x;t) = \frac{1}{(2\pi\sigma^2)^{1/4}} \exp\left(i\frac{p_0 x}{\hbar}\right) \exp\left(-\frac{x^2}{4\sigma^2}\right), \tag{3.42}$$

and the probability density $\rho(x)$ for the wavefunction after it has interacted with the qubits is

$$\rho(x) = \frac{1}{4\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x+\Delta x)^2}{2\sigma^2}} + \frac{1}{2\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{x^2}{2\sigma^2}} + \frac{1}{4\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x-\Delta x)^2}{2\sigma^2}}. \tag{3.43}$$

As this probability density is the weighted sum of normalized Gaussian distributions, it is immediatelly clear that $\rho(x)$ is normalized. Considering only symmetric intervals $[a, b] = [-w, w]$ because of the symmetry of the wavefunction, this leads to

$$\Pr(x \in [-w, w]) = \frac{1}{4}\left[\mathrm{erf}\left(\frac{\Delta x + w}{\sqrt{2}\sigma}\right) + 2\,\mathrm{erf}\left(\frac{w}{\sqrt{2}\sigma}\right) + \mathrm{erf}\left(\frac{w - \Delta x}{\sqrt{2}\sigma}\right)\right], \tag{3.44}$$

where erf is the usual error function $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x dx\ \exp\left(-\frac{x^2}{2\sigma^2}\right)$. It becomes clear then that σ sets the length scale for the problem. Due to dispersion in the free particle Hamiltonian, σ depends both on the initial width of the packet as well as the time of propagation.

The fidelity F between $\rho_{-w,w}$ and $|\Psi^+\rangle$ is given by

$$F = \langle\Psi^+|\rho_{-w,w}|\Psi^+\rangle, \tag{3.45}$$

$$= \frac{1}{2\Pr(x \in [-w, w])} \int_{-w}^{w} dx\ |\psi(x;t)|^2, \tag{3.46}$$

$$= \frac{1}{2\Pr(x \in [-w, w])} \mathrm{erf}\left(\frac{w}{\sqrt{2}\sigma}\right). \tag{3.47}$$

Contour plots for the fidelity and probability of success as a function of w/σ and $\Delta x/\sigma$ is given in Figure 3.6. Cross-sections of the fidelities are given in Figure 3.7, and of the probability of success are given in Figure 3.8.

Intuitively, if we want to maximize the fidelity with $|\Psi^+\rangle$, we need to single out regions which maximize the contribution of the wave function $\psi(x, t)$ while minimizing the contribution of the displaced wave functions. This leads to the region around $x = 0$. Taking the limit of F as $w \to 0$, we have

$$F_{\max}(\Delta x, \sigma) = \lim_{w\to 0} F = \left(1 + e^{-\frac{\Delta x^2}{2\sigma^2}}\right)^{-1}. \tag{3.48}$$

This corresponds to the maximal fidelity which may be obtained for a given separation of the wave packets, assuming that the position measurements can be made to arbitrary precision. Note that unlike the wave function in Chapter 2, the contribution from the unwanted wave functions cannot be made arbitrarily small. For any given desired fidelity, initial wave packet width $\sigma(0)$, and separation of the packets $2\Delta x$, this effectively sets an upper bound to the separation between the two qubits. Rearranging (3.48) leads to

$$\sigma_{\max} = \frac{\Delta x}{\sqrt{2 \ln \frac{F_{\max}}{1-F_{\max}}}}. \tag{3.49}$$

For example, if the desired fidelity to be achieved is $F_{\max} = .9$, this translates to $\Delta x/\sigma_{\max} \approx 2.09$ – that is, the separation between the centers of wave packets must be roughly 4.18 times their width at the time of measurement.

The time required for $\sigma(0)$ to increase to $\sigma_{\max}$ can be solved from (3.13) to yield

$$t_{\max} = \frac{2m\sigma(0)}{\hbar}\sqrt{\sigma_{\max}^2 - \sigma(0)^2}, \tag{3.50}$$

which can be related to distance by the average momentum p_0 of the wave packets, finally yielding

$$d_{\max} = \frac{2p_0\sigma(0)}{\hbar}\sqrt{\sigma_{\max}^2 - \sigma(0)^2}. \tag{3.51}$$

All these expressions can be adjusted to take into account finite w simply by using (3.45) instead of $F_{\max}$. However, this cannot be done analytically and requires numerical computation.

The integrals of the matrix elements $\langle i|q(x)\rangle\langle q(x)|j\rangle$ can be computed by evaluating Gaussian integrals of the form

$$f_{\mu_1,\mu_2} = \int_{-w}^{w} dx\ \psi(x-\mu_1;t)\psi^*(x-\mu_2;t) \tag{3.52}$$

$$= \frac{1}{\sqrt{2\pi}\sigma}\int_{-w}^{w} \exp\left[-\frac{(x-\mu_1)^2}{4\sigma^2} - \frac{(x-\mu_2)^2}{4\sigma^2}\right] \tag{3.53}$$

$$= \frac{1}{2}\mathrm{e}^{i\frac{p(\mu_2-\mu_1)}{\hbar}}\mathrm{e}^{\frac{-(\mu_1-\mu_2)^2}{8\sigma^2}}\left[\mathrm{erf}\left(\frac{\mu_1+\mu_2+2w}{2\sqrt{2}\sigma}\right) - \mathrm{erf}\left(\frac{\mu_1+\mu_2-2w}{2\sqrt{2}\sigma}\right)\right] \tag{3.54}$$

This leads to

$$\rho_{-w,w} = \frac{1}{4\Pr(x\in[-w,w])}\begin{pmatrix} f_{-\Delta x,-\Delta x} & f_{0,-\Delta x} & f_{0,-\Delta x} & f_{\Delta x,-\Delta x} \\ f_{-\Delta x,0} & f_{0,0} & f_{0,0} & f_{\Delta x,0} \\ f_{-\Delta x,0} & f_{0,0} & f_{0,0} & f_{\Delta x,0} \\ f_{-\Delta x,\Delta x} & f_{0,\Delta x} & f_{0,\Delta x} & f_{\Delta x,\Delta x} \end{pmatrix}. \tag{3.55}$$

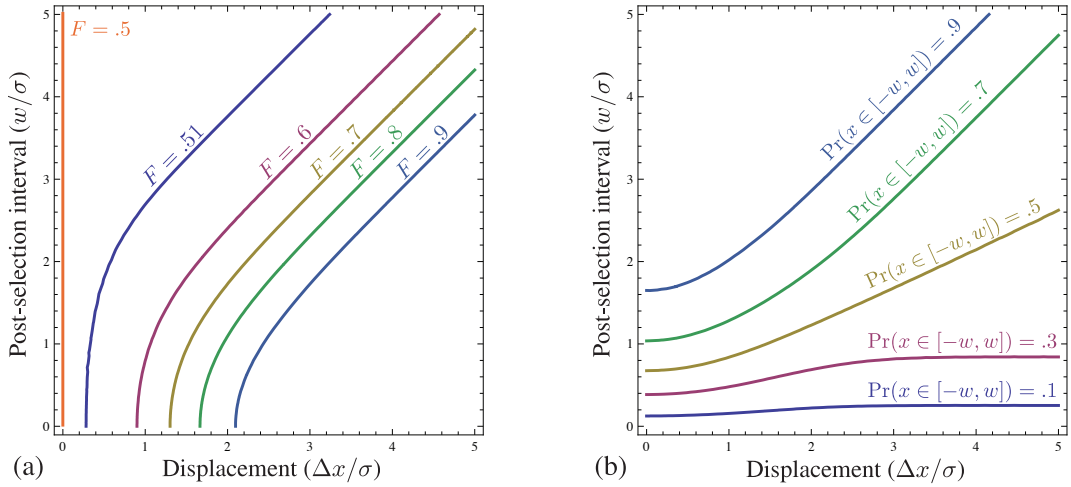

Figure 3.6: *Contour plot for (a) the fidelity between the post-selected state $\rho_{-w,w}$ and the maximally entangled state $|\Psi^+\rangle$ and for (b) the corresponding probability of obtaining the desired range of x measurement outcomes.*

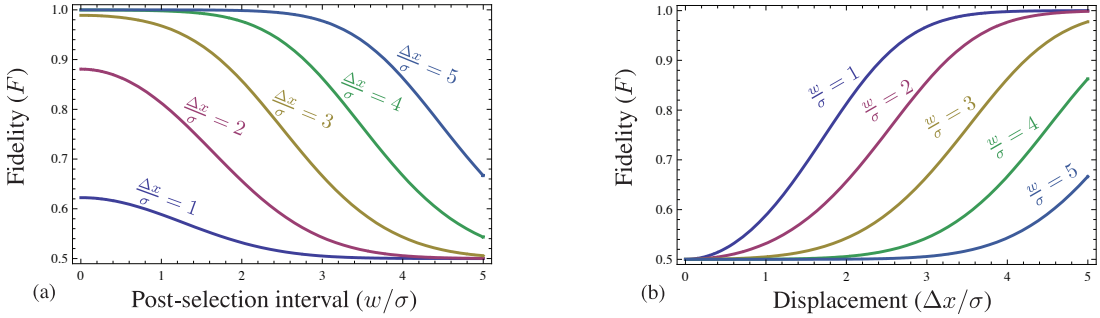

Figure 3.7: *Cross sections of the fidelity F (a) as a function of w/σ for various $\Delta x/\sigma$ and (b) as a function of $\Delta x/\sigma$ for various w/σ.*

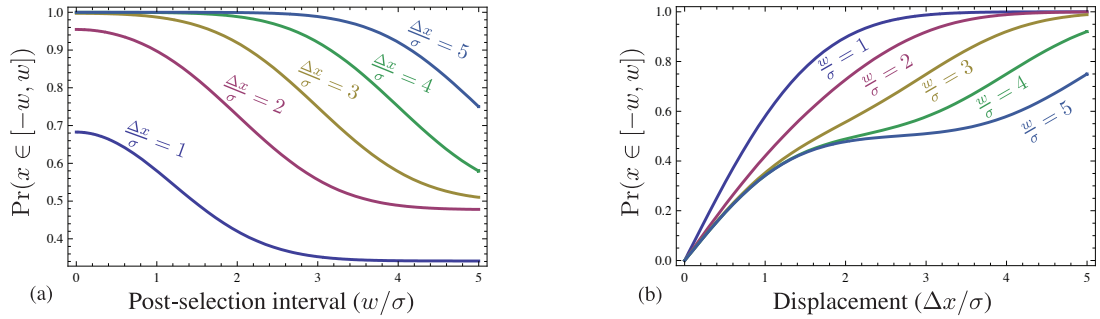

Figure 3.8: *Cross sections of the probability of success $\Pr([-w, w])$ (a) as a function of w/σ for various $\Delta x/\sigma$ and (b) as a function of $\Delta x/\sigma$ for various w/σ.*

As $|\Psi^+\rangle$ is a maximally entangled state, the performance of the protocol can also be quantified by considering measures of entanglement of the post-selected state $\rho_{-w,w}$ (More details about these measures can be found in Appendix B).

Entanglement witnesses are observables which have negative expectation value only for states which are entangled. We consider the entanglement witness W tailored to the state $|\Psi^+\rangle$. This observable is

$$W = \frac{1}{2}\mathbb{1}_4 - |\Psi^+\rangle\langle\Psi^+| \tag{3.56}$$

$$= \frac{1}{4}(\mathbb{1}_4 - \sigma_X \otimes \sigma_X + \sigma_Z \otimes \sigma_Z - \sigma_Y \otimes \sigma_Y). \tag{3.57}$$

The expectation value $\langle W\rangle = \operatorname{tr} W\rho_{-w,w}$ can be simplified to

$$\langle W\rangle = \frac{1}{2} - \langle\Psi^+|\rho_{-w,w}|\Psi^+\rangle = \frac{1}{2} - F, \tag{3.58}$$

where F is the fidelity between $\rho_{-w,w}$ and $|\Psi^+\rangle$. If $\langle W\rangle < 0$, then $\rho_{-w,w}$ is an entangled state. As $F = \frac{1}{2}$ only when $\Delta x = 0$, we have that $\rho_{-w,w}$ is entangled *for all* w *and for all non-zero* Δx, so that the proposed protocol can produce entanglement for all experimental parameters, in the ideal case.

A lower bound for the *generalized robustness of entanglement* E_R can be computed directly from the expectation value of the entanglement witness, which in turn can be computed from the fidelity to the state $|\Psi^+\rangle$ [EBA07]. This implies that, for $\langle W\rangle < 0$,

$$E_R(\rho_{-w,w}) \geq 2|\langle W\rangle| = 2F - 1, \tag{3.59}$$

which matches the intuition that the greater the fidelity to the state $|\Psi^+\rangle$, the more entangled the state is. We find that $E_R > 0$ as long as $\Delta x > 0$, which is consistent with the finding that all states in that region are entangled.

The *logarithmic negativity* $E_N(\rho_{-w,w})$ can also be computed numerically. The logarithmic negativity of a state gives an upper bound to the efficiency with which maximally entangled Bell pairs which can be distilled from many copies of that state, as well as an upper bound on the teleportation capacity of the state [VW02, PV07]. As the negativity is based on properties of the spectrum of $\rho_{-w,w}$, it is difficult to give succinct analytical results of its dependence on w or Δx. However, numerical calculations of this measure are consistent with the conclusion drawn form the entanglement witness in the sense that they appear to be non-zero for all w and for all non-zero Δx. The logarithmic negativity for $\rho_{-w,w}$ is plotted for various values of w/σ and $\Delta x/\sigma$ in Figure 3.9.

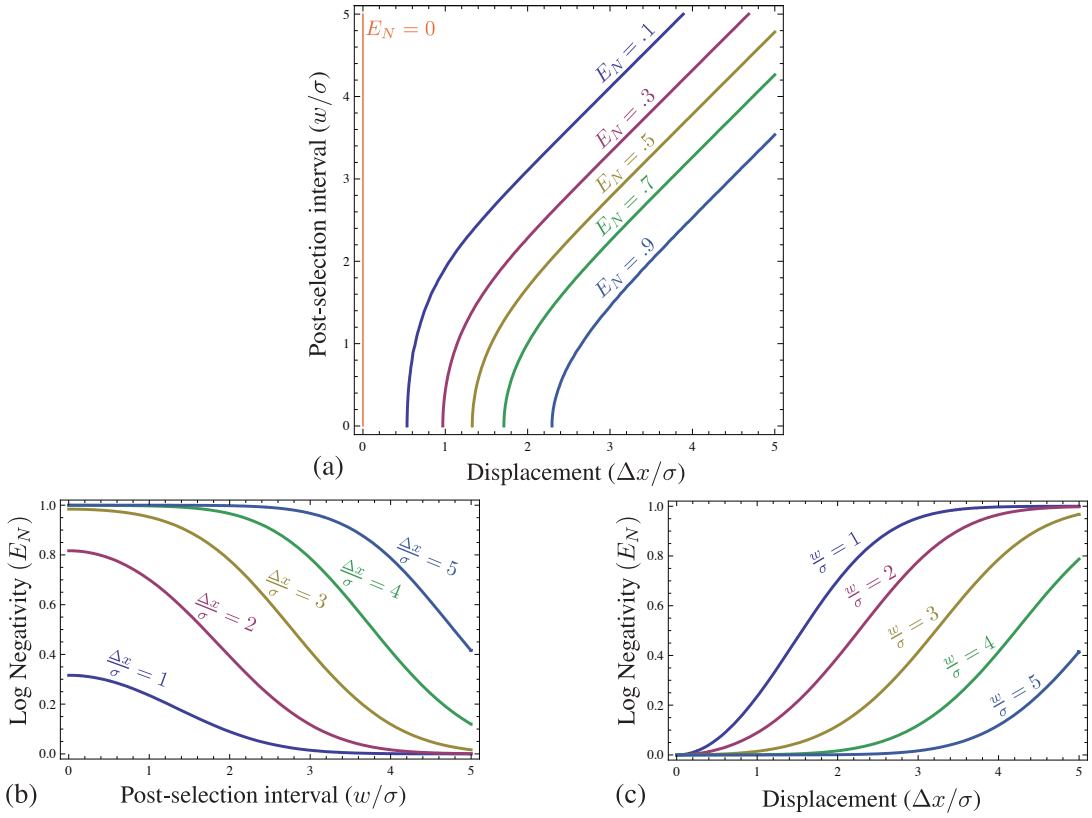

Figure 3.9: *The logarithmic negativity E_N of $\rho_{-w,w}$ (a) as a function of $\Delta x/\sigma$ and w/σ, (b) as a function of w/σ for various $\Delta x/\sigma$ and (c) as a function of $\Delta x/\sigma$ for various w/σ.*

3.3.3 Protocol for entanglement verification

We have described a protocol for creation of entanglement between two qubits. In order to verify that the qubits are indeed entangled, an experimenter can simply measure the appropriate entanglement witness. This is an approach that has been used to verify entanglement in ion trap systems [LKS+05, HHR+05] as well as in photonic systems [KSW+05, LZG+07].

The entanglement witness can be estimated by repeating the experiment a number of times, and measuring each qubit individually but on the same eigenbasis. The eigenbasis that must be measured are σ_X, σ_Y and σ_Z. From the measurement record it is then possible to estimate the expectations $\langle \sigma_X \otimes \sigma_X \rangle$, $\langle \sigma_Y \otimes \sigma_Y \rangle$ and $\langle \sigma_Z \otimes \sigma_Z \rangle$, so that the expectation of the witness is

$$\langle W \rangle = \frac{1}{4}(1 - \langle \sigma_X \otimes \sigma_X \rangle + \langle \sigma_Z \otimes \sigma_Z \rangle - \langle \sigma_Y \otimes \sigma_Y \rangle). \tag{3.60}$$

If $\langle W \rangle < 0$ with high confidence, then the state of the qubits can be said to be entangled

with high confidence.

While we have demonstrated that $\rho_{-w,w}$ is essentially always entangled, in order to increase tolerance to noise and statistical uncertainty in the measurements it is important to design an experiment where $\Delta x/\sigma$ and w/σ yield a state $\rho_{-w,w}$ with fidelity reasonably larger than $1/2$. How much larger than $1/2$ it must be depends on the amount of noise in the system and on the number of experiments to be performed.

3.4 Coherence length for free particles with dissipation

A fundamental assumption of the protocol just described is that there is a high level of coherence in the evolution of the quantum particle between the interaction with the first particle and the measurement of the position of the particle. More explicitly, if one were to perform the previous calculation with a classical probability distribution for the position of the particle, one would find that the state of qubits would approximate $\frac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|)$ instead of the desired

$$|\Psi^+\rangle\langle\Psi^+| = \frac{1}{2}\left(|01\rangle\langle 01| + |10\rangle\langle 10| + |01\rangle\langle 10| + |10\rangle\langle 01|\right) \tag{3.61}$$

Similarly, if the qubits dephase to $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ in the time necessary to scatter the particle and perform the measurement, then one would obtain a similar unentangled state.

In order to evaluate the feasibility of the protocol as a practical approach to entangling distant qubits, it is important to estimate how far the particle can travel before either the state of the qubit or the state of the particle dephases significantly.

The dephasing time T_2 for the qubit is defined as the characteristic time it takes for the off-diagonal elements of a single qubit density matrix to decay [Blu96]. Taking the velocity of the particle to be v, the distance traveled by the particle in the time it takes for the qubit to dephase significantly is

$$d_{\max,Q} = v\, T_2. \tag{3.62}$$

This can be taken as a constraint on the maximal separation between the qubits, as for distances comparable with $d_{\max,Q}$ the qubits will decohere significantly before the position of the particle is measured.

In analogy to the definition of dephasing time for the state of the qubit, we will define the dephasing time of the state of the particle to be the time it takes for the off-diagonal terms in the density matrix to decay significantly. However, the calculation

of the evolution of a free particle under the action of dissipation at low temperatures poses a number of different challenges. At low temperatures it is not possible to derive a Markovian master equation for a damped free particle – in other words, it is not possible to derive a differential equation which is local in time and independent of the initial state preparation. While it is possible to solve this model of dissipation exactly [vK04, Amb06], the objective here is to obtain a rough estimate of the coherence length in order to check the feasibility of the proposed experiment.

A simple approach to estimate the coherence length is to consider the effect of dissipation in the simple harmonic oscillator. The free particle Hamiltonian can be seen as a limit of the simple harmonic oscillator Hamiltonian,

$$\mathcal{H}_{\text{HO}} = \frac{p^2}{2m} + \frac{1}{2}m\omega_0^2 x^2 \tag{3.63}$$

where $\omega_0 \to 0$. If a force F is applied to compensate dissipation, then the H_{HO} can still be used, but with coordinates shifted so that we have

$$\mathcal{H}_{\text{HO}} = \frac{p^2}{2m} + \frac{1}{2}m\omega_0^2 (x+\delta)^2. \tag{3.64}$$

Taking the limit of large δ and small ω_0, so that $\delta = -\frac{F}{m\omega_0^2}$ remains constant, yields the Hamiltonian

$$\mathcal{H}_F = \frac{p^2}{2m} - Fx, \tag{3.65}$$

where the constant term has been neglected as it is not observable. Thus, both Hamiltonians of interest can be seen as limiting cases of the simple harmonic oscillator.

Energy dissipation in the motion of a particle can be modeled by taking the particle to interact with a bath of harmonic oscillators [CL83]. In the case of a harmonic oscillator undergoing dissipation at zero temperature, the corresponding Markovian master equation can be solved exactly, as described in Appendix C. We define the decoherence time t_D to be the time scale of exponential decay for the off-diagonal terms in the density matrix. The energy relaxation time t_R is given by the time scale at which the total energy decays. In the case of the damped harmonic oscillator, we find that the ratio of these quantities depends only on the initial overlap of the wave functions that make up the superposition. By analogy, starting with a superposition of the form (3.31) as the initial state of the free particle, the ratio of the decoherence time to the relaxation time is estimated to be

$$\frac{t_D}{t_R} = \left(\ln \frac{1}{|\langle \psi(0)|D(\Delta x)|\psi(0)\rangle|} \right)^{-1}, \tag{3.66}$$

where $\langle\psi(0)|D(\Delta x)|\psi(0)\rangle$ is the overlap between the displaced wave functions that make the up superposition. The smaller the overlap between the states is, the shorter the decoherence time relative to the relaxation time.

The physical picture behind this is that, in essence, the bath randomly perturbs the position of the particle in the oscillator. Equivalently, information about the particle's position is imprinted into the bath. If the overlap is small, it is easier for the environment to distinguish the two possible states that make up the superposition, and thus the state decoheres faster. From this physical picture, we expect that t_D depends more strongly on the overlap between the states than on details of the wave function. This is important for our estimates because in the free particle limit, the wave function we are interested in have finite position variances, and thus correspond to squeezed states. The overlap between the different states that make up the superposition is still finite, however. For our purposes, we will take the decoherence time for superpositions of coherent states as an upper bound to the decoherence time of squeezed superposition.

We therefore estimate the characteristic length for decoherence in a damped free-particle system to be

$$d_{\max,\mathrm{sol}} = v\, t_D = \frac{v\, t_R}{\ln \frac{1}{|\langle\psi(0)|D(\Delta x)|\psi(0)\rangle|}}. \tag{3.67}$$

It is important to note that this definition of the decoherence time scale is only applicable for time much shorter than the energy relaxation time scale, as discussed in Appendix C. For time comparable to t_R, the system will have decohered to its steady state value.

These estimates for decoherence and relaxation times are based on the assumption of weak damping with respect to the frequency of the harmonic oscillator. While such an assumption does not hold in the free-particle limit, we expect the results for the harmonic oscillator to be representative of the results for the free-particle, or, at worst, to be somewhat optimistic. A more involved analysis of the problem can be carried out to avoid these assumptions [vK04, Amb06], but we leave such considerations for future work.

3.5 Physical realization with superconducting circuits

Superconducting circuits are natural candidates for the implementation of the protocol above. There are many well established qubit implementations using superconducting circuits [MSS01, DWM04, YN05], and one of the most successful is known as a

persistent-current or *flux qubit* [MOL+99, OMT+99]. Such qubits consist of a $\sim 5\mu\text{m}$ loop of superconducting material interrupted by a small Josephson junction. One possible basis for the states of the qubit consists of a persistent current flowing clockwise, which we denote $|\tilde{0}\rangle$, or anti-clockwise, which we denote $|\tilde{1}\rangle$.

The finite inductance of the loop leads to a Hamiltonian term proportional to $\tilde{\sigma}_Z$ (the tilde emphasizes we are in the persistent current basis). The Josephson junction allows for the qubit to tunnel between these two current states, so in this persistent current basis it leads to a Hamiltonian term proportional to $\tilde{\sigma}_X$. The full Hamiltonian is then written as

$$\mathcal{H}_q = -\frac{\epsilon}{2}\tilde{\sigma}_Z - \frac{\delta}{2}\tilde{\sigma}_X, \tag{3.68}$$

where ϵ is the energy bias between the qubit states, controlled by the a magnetic flux applied externally, and δ is the tunnel splitting, which is set the circuit fabrication. The energy eigenvalues are separated by $\sqrt{\epsilon^2 + \delta^2}$.

Low frequency noise is one of the dominant sources of noise in superconducting qubit, and in flux qubits this low frequency noise manifests itself as flux noise, randomly varying the parameters ϵ over time [YHN+06]. This can lead to rapid dephasing of the qubits, on time scales much shorter than the time scale for energy relaxation. However, an important property of flux qubits is that they can operate in what is known as the *optimal (biasing) point*, which minimizes this additional sources of dephasing noise. This optimal point is a flux biasing point at which the separation of the energy eigenvalues are insensitive to flux variations (to first order). This corresponds to $\epsilon = 0$, so that the energy eigenstates $|0\rangle = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle + |\tilde{1}\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle - |\tilde{1}\rangle)$ have the same current expectation values. In this energy eigenbasis, the Hamiltonian is given by

$$\mathcal{H}_q = -\frac{\delta}{2}\sigma_Z. \tag{3.69}$$

Typical experimental parameters for these qubits are listed in Table 3.1. These are the values which will be used in the following section to estimate the feasibility of implementing the protocol just described using superconducting circuits.

3.5.1 Solitons as quantum particles

Although small Josephson junctions have been widely used for the implementation of qubits, long and narrow Josephson junctions have many interesting properties that have

Quantity	Approximate value	Meaning
δ/h	5.5 GHz	Qubit energy level splitting
T_2	4 μs	Time scale for dephasing

Table 3.1: *Typical experimental parameters for a persistent current qubit [YHN+06]*

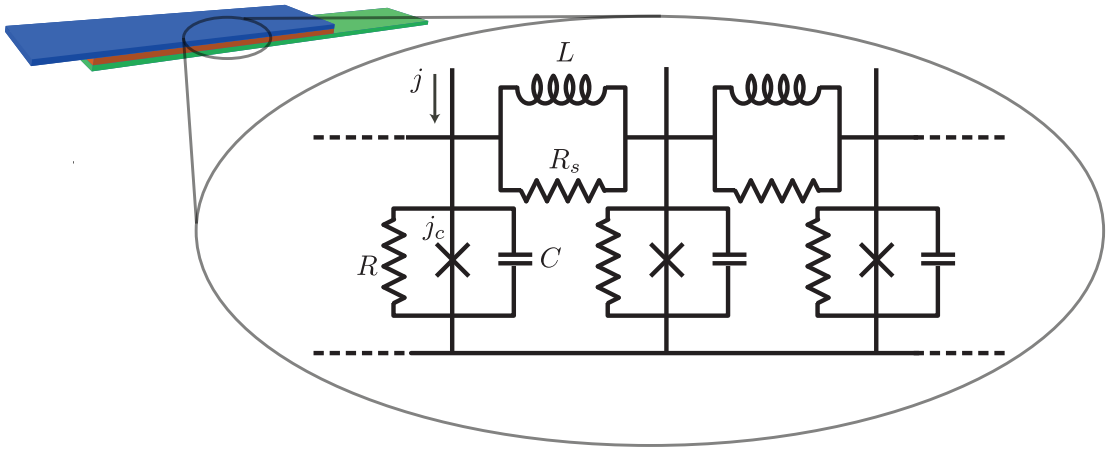

Figure 3.10: *Lumped element model of an infinitesimal section of a long Josephson junction.*

been investigated as potential building blocks for qubits [Wal00, WLL+03, KU04]. In particular, there are stable non-linear excitations along these *Josephson transmission lines*, as they are often called, which are particle-like. These non-linear excitations are called solitons, and comprise of current vortices tunneling across the junction to trap flux quanta, and therefore these solitons are also known as *fluxons*.

Consider a standard lumped element model of an infinitesimal section of the junction, as depicted in Figure 3.10. It becomes then clear that these long junctions can be simulated by a ladder network of superconducting tunnel junctions arranged precisely in the manner of this lumped element model. This will be the model we will focus on here in order to leverage previous research into the interaction between fluxons and flux qubits [ARS06, FSSKS07].

Taking the continuous limit of the equations describing current conservation in this lumped element model allows for a compact description of the system which is more amenable to analytical treatment. The evolution of the phase difference $\phi(x,t)$ of the superconducting condensate at position x along the transmission line is governed by the

equation [OD91]

$$\phi_{xx} - \phi_{tt} - \sin\phi = -\frac{j}{j_c} + \alpha\phi_t - \beta\phi_{xxt} \tag{3.70}$$

where each subscript of ϕ denotes partial derivative with respect to the corresponding variable, j_c is the critical current density, j is the bias current density, and α and β are positive valued scalars corresponding to the strength of different sources of dissipation. Position x is given in units of the *Josephson length* λ_j and time is given in units inverse to the *plasma frequency* ω_P, which are set by fabrication parameters of the junction, such as the critical current density j_c, the inductance per unit length L, and the capacitance per unit length C. The parameters α and β are similarly given by these fabrication parameters along with the quasi-particle resistance R and surface impedance of the superconductor R_s – in essence, they are the ratios of the appropriate RC and RL frequencies to the plasma frequency. Typical values for these parameters are given in Table 3.2.

Each of the terms in this equation can be given a more familiar physical interpretation: from the Josephson relations [Tin04], the density of current tunneling across the junction at position x is given by $j_c \sin\phi(x,t)$ and the voltage is given by $\frac{\Phi_0}{2\pi}\phi_t$, while flux quantization implies the magnetic field density is given by $\frac{\Phi_0}{4\pi\lambda_J}\phi_x$ – where Φ_0 is the flux quantum $\Phi_0 = \frac{h}{2e}$.

Neglecting the current bias and the dissipative terms, we obtain

$$\phi_{xx} - \phi_{tt} = \sin\phi \tag{3.71}$$

which is known as *the sine-Gordon equation*. If we assume the the junction extends to infinity, for simplicity, the Hamiltonian corresponding to (3.71) is proportional to

$$\mathcal{H} = \int_{-\infty}^{+\infty} dx\, \frac{1}{2}{\phi_t}^2 + \frac{1}{2}{\phi_x}^2 + 1 - \cos\phi, \tag{3.72}$$

which can be interpreted as a dimensionless integral over the electric field energy, the magnetic field energy and the Josephson coupling energy.

The sine-Gordon equation is clearly Lorentz covariant if we take the "speed of light" to be

$$c_0 = \lambda_J \omega_P, \tag{3.73}$$

known as the *Swihart velocity*, which is typically a few percent of the speed of light in vacuum. Although highly non-linear, this equation can be solved exactly, and all its solutions are known [Raj82, DP06]. In particular, it can be shown that a topologically

stable solution is

$$\phi(x,t) = 4\arctan\left[\exp\left(-\frac{x-vt-x_0}{\sqrt{1-v^2}}\right)\right]. \tag{3.74}$$

Here, and for the remainder of the discussion about Josephson transmission lines, the speed v is given in units of c_0 (and therefore it is at most 1). This solution is depicted in Figure 3.11. Inserting $\phi(x,t)$ in the Hamiltonian (3.72) leads to the energy $E(v)$ of a soliton as a function of its velocity

$$E(v) = \frac{8}{\sqrt{1-v^2}}, \tag{3.75}$$

which is analogous to the energy of a relativistic particle with normalized mass 8. In the non-relativistic limit $v \ll 1$, all standard results which can be obtained by Taylor expanding $\sqrt{1-v^2}$ follow, further strengthening the interpretation of a fluxon as a particle. Formally, sophisticated mathematical methods can be used to show that the highly non-linear equation (3.71) is equivalent to a linear equation describing the motion of relativistic particles [Raj82].

A remarkable feature of the fluxon solution is that its shape does not change in time – only its center will move with uniform velocity v. Because of this and other properties[1], these solutions are known as *solitons*. Another general features of these fluxons is that the current and magnetic flux are exponentially concentrated around λ_J from the center, as $\frac{d}{dz}\arctan z = \frac{1}{\sqrt{1+z^2}}$ and $\sin\arctan z = \frac{z}{\sqrt{1+z^2}}$. Note, however, that regardless of the velocity, the total flux trapped in the junction is Φ_0, and that is why these solutions are known as *fluxons*.

When j/j_c, α and β are much smaller than 1, the effect of the bias and dissipation terms on the fluxon can be taken into account by perturbation theory [MS78]. To first order, the effect of these perturbation terms is to change the dynamics of the center of mass of the soliton, without disturbing its shape – in particular, the velocity v becomes a function of time. Perturbation theory also allows the translation of small local perturbations to potential barriers for the equivalent relativistic particles. Thus, it is natural to think of fluxons are particle-like excitations in these transmission lines.

Fluxons can be reliably injected into the transmission line by applying a strong localized current density $j > j_c$ into the junction [KU04, Kem06]. This causes superconducivity to break down locally, and for a flux quantum to slip into the junction with high

[1] These other properties relate to the collision of solitons. As we will not be dealing with multiple solitons, they are not relevant to our discussion.

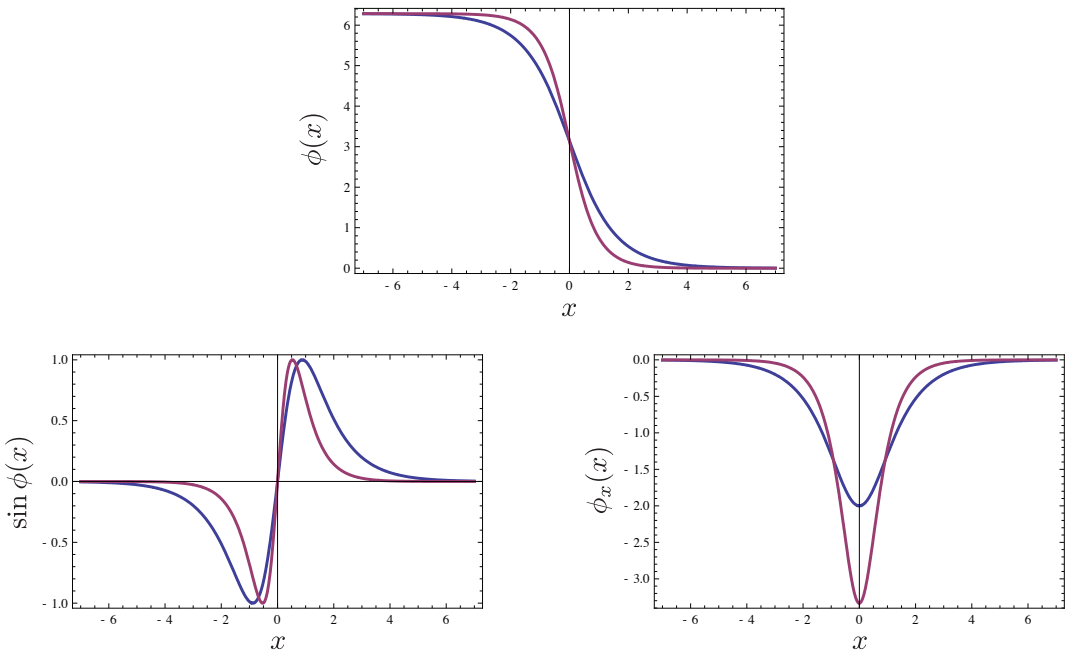

Figure 3.11: *Distribution of the phase difference ϕ, current density $\sin\phi$ and magnetic flux density ϕ_x for a fluxon. The blue line corresponds to a fluxon with $v = 0$, and the purple line to a fluxon with $v = 0.8$*

probability. The detection of the fluxon can be carried out by measuring the magnetic flux at some localized portion of the junction. One approach that has been implemented is the use of fast digital flux-based electronics for the detectors [KU04], which can achieve a timing resolution on the order of 3 ps [FSSKS07].

3.5.2 Interaction between particle and qubit

The interaction between a flux qubit and a fluxon has been investigated as a possible approach to fast and reliable measurement of the qubit state [ARS06, FSSKS07]. The inductive coupling between the qubit and the transmission line will perturb the overall Hamiltonian, especially when the fluxon is nearby the qubit. In the limit of weak coupling between the fluxon and the qubit, the qubit remains in the optimal point at all times, which is important as the protocol described in Section 3.3.2 relies on the coherence of the qubit.

If the fluxon velocity is low enough, the adiabatic approximation can be invoked to show that the interaction commutes with the qubit Hamiltonian at the optimal point, to a good approximation, and just perturbs its eigenvalues. For the fabrication parameters of

Quantity	Approximate value	Meaning
$\omega_p/2\pi$	50 GHz	plasma frequency
λ_J	12 μm	Josephson length
c_0	3.77×10^6m/s	Swihart velocity
α	10^{-2}	tunneling dissipation strength
β	10^{-2}	surface dissipation strength
m	$\frac{m_e}{500}$	effective rest mass of a fluxon
t_{res}	3ps $\approx \frac{1}{\omega_P}$	timing resolution for detection

Table 3.2: *Typical experimental parameters for a Josephson transmission line [Wal00, KU04, FSSKS07]*

the qubit and transmission line we have considered, this translates to the requirement that $v < 0.05$ for a probability of transition between the states which is negligible [FSSKS07].

The effect of the qubit on the transmission line, on the other hand, is that it will locally modulate the effective inductance of the transmission line, and it will lead to an additional perturbation to the right-hand side of (3.70). In the limit where the size of the qubit is smaller than one cell of the discrete transmission line, this term can be shown to be of the form [MS78, ARS06, FSSKS07]

$$\pm\xi \frac{\partial}{\partial x} \left(\delta(x)\phi_x\right), \tag{3.76}$$

where the sign is given by the eigenstate of the qubit (the positive sign for the excited states, and the negative sign for the ground state), and ξ is the dimensionless perturbation strength. Typical values of this interaction strength are on the order of 10^{-4}, and to estimate the performance of the protocol we will take $\xi \approx 3 \times 10^{-4}$ [FSSKS07]. From perturbation theory the variation of the fluxon velocity around the qubit can be computed, leading to a delay between fluxon arrival time depending on the eigenstate of the qubit. In the non-relativistic limit of $v \ll 1$, this time delay can be shown to be [FSSKS07]

$$t_{\text{delay}} \gtrsim \frac{\xi}{v^3}, \tag{3.77}$$

as long as $v > \sqrt{\frac{\xi}{2}} \approx 0.0123$, which is a minimal speed requirement to avoid pinning or reflection of the fluxon by the interaction.

3.5.3 Constraints on maximal qubit separation due to dispersion

In order to investigate the feasibility of implementing the proposed protocol with superconducting circuits, we must investigate what is the maximal qubit separation that can be achieved while still allowing for the observation of entanglement between the qubits. The measure of entanglement we use is the entanglement robustness E_R, which was shown to be simply related to the fidelity of the final states with the state $|\Phi^+\rangle$. The displacement Δx that can be applied to the wave packets after an interactions is given by the time delay caused by each interaction and the speed at which they are traveling

$$\Delta x = t_{\text{delay}} v c_0 \tag{3.78}$$

$$= \frac{\xi}{v^2}\lambda_J. \tag{3.79}$$

Assuming that the wave packet can be prepared with a spread that is no smaller than λ_J, the approximate size of the fluxon, combining (3.51) with (3.79) leads to

$$d_{\max} = \frac{2mc_0\lambda_J^2}{v\hbar}\sqrt{\left(\frac{\sigma_{\max}}{\Delta x}\right)^2 4\xi^2 - v^4} \tag{3.80}$$

$$= d_0\sqrt{\left(\frac{\sigma_{\max}}{\Delta x}\right)^2 4\xi^2 - v^4}. \tag{3.81}$$

It is clear then that, in order to obtain a positive distance between the qubits, the speed of the soliton is bounded by

$$v \leq \sqrt{2\xi\frac{\sigma_{\max}}{\Delta x}}. \tag{3.82}$$

In the previous section, we have a lower bound on the velocity, given by $\sqrt{\xi/2}$, which implies that $\frac{\Delta x}{\sigma_{\max}} < 4$ in order to have any velocity which can satisfy both equation simultaneously. Choosing $\frac{\Delta x}{\sigma_{\max}} \approx 1.53$ for a fidelity of $F \approx 0.76$ and entanglement robustness $E_R > 0.53$, we have that

$$0.0122474 < v < 0.019803. \tag{3.83}$$

Given the fluxon experimental parameters in Table 3.2, if we choose $v = 0.0145$ to accommodate fabrication variations in the experimental parameters, we have that the maximal separation between the qubits is $d_{\max} \approx 425\mu\text{m}$. The corresponding time it takes the soliton to travel this distance is $t_{\max} \approx 7.8\text{ns}$.

In order to resolve the different peaks in the position distribution of the fluxons, we require that the separation between the peaks be greater than the spatial resolution of the

detector. As the detector is fixed in space, this translates to a constraint on the timing resolution of the detector and time delay corresponding to the displacement Δx for a soliton traveling at v. We find that, for the experimental parameters given

$$\frac{2t_{\text{delay}}}{t_{\text{res}}} \approx 2\frac{\xi}{v^3} \approx 196, \tag{3.84}$$

confirming that the detector is able to distinguish the displaced wave functions with very high accuracy.

The above calculations rely on $F_{\max}$, which in turn assumes that the detector resolution is much smaller than the spread of the wave function – in other words $w/\sigma \ll 1$. The ratio of the spatial resolution of the detector to the spread of the wave function at the time of detection is given by

$$\frac{t_{\text{res}} v c_0}{\sigma_{\max}} \approx \frac{t_{\text{res}} v c_0}{0.65\Delta x} \tag{3.85}$$

$$\approx 1.56 \times 10^{-2}. \tag{3.86}$$

Taking this minimal spatial resolution to be the window size for the measurement clearly guarantees that we are in the assumed limit which allows for $F_{\max}$ to be met. Given that this resolution is so high compared to the width of the packet at the time of measurement, the probability of success can be boosted by taking the window to larger than the minimal resolution. From Figures 3.6 it is clear that the probability of success can be made as large as 0.1 by making $w/\sigma = 0.2$ without significant impact on the fidelity.

In summary, neglecting decoherence, the experimental parameters indicate that the achievable separation between the qubits for a target fidelity of 0.76 is on the order of 0.425mm, which is significantly larger than the size of the qubits. With a normalized velocity of $v = 0.0145$, the time it takes the soliton to travel this distance is approximately 7.8ns. Thus, dispersion of the wave function does not pose significant constraints on the implementation of this protocol.

3.5.4 Coherence length as constrained by the qubit

Recent experiments have demonstrated flux qubit with relaxation time $T_1 = 2\mu\text{s}$ [YHN+06]. The measurement was performed at the optimal point, where the dephasing time T_2 is saturated at $T_2 = 2T_1$. The distance $d_{\max,Q}$ that the soliton can travel in this characteristic time is

$$d_{\max,Q} = vT_2 \approx 0.21\text{m}, \tag{3.87}$$

so clearly the dephasing of the qubit does not impose serious constraints to the separation of the qubits.

3.5.5 Coherence length of perturbed solitons

In order to estimate the relaxation length for sine-Gordon solitons, we must consider the effects of dissipation and current bias in (3.70). In the case where all of α, β and j/j_c are small, perturbation theory allows for a simple description of the time evolution of the soliton [MS78]. In this limit, corrections to the shape of the soliton are neglected, and only changes in the center of mass coordinates of the soliton are considered. The time dependence of the velocity can then be describe by taking a power balance approach. First, we have the velocity dependence of the energy of a soliton from (3.75), so that the change in energy as a function of time can be described as a function of the change in velocity as

$$\frac{d\mathcal{H}}{dt} = 8\frac{v}{(1-v^2)^{3/2}}\frac{dv}{dt}. \tag{3.88}$$

Taking the time derivative of the Hamiltonian as a function of ϕ leads to

$$\frac{d\mathcal{H}}{dt} = -\int_{-\infty}^{+\infty} dx\ \phi_t(\phi_{xx} - \phi_{tt} - \sin\phi), \tag{3.89}$$

and from (3.70) we conclude that

$$\frac{d\mathcal{H}}{dt} = \int_{-\infty}^{+\infty} dx\ (-\alpha\phi_t^2 - \beta\phi_{xt}^2 + \frac{j}{j_c}\phi_t), \tag{3.90}$$

by integration by parts of the middle term. Inserting the fluxon solutions with a variable velocity into (3.90) and equating it to (3.88) leads to

$$\frac{dv}{dt} = -\alpha v(1-v^2) - \frac{1}{3}\beta v - \frac{1}{4}\pi\frac{j}{j_c}(1-v^2)^{3/2}. \tag{3.91}$$

In the limit of $v \ll 1$, this gives

$$\frac{dv}{dt} \approx -(\alpha + \frac{1}{3}\beta)v - \frac{1}{4}\pi\frac{j}{j_c}, \tag{3.92}$$

which can be immediatelly solved to yield

$$v(t) = \left[v(0) + \frac{\pi\frac{j}{j_c}}{4\left(\alpha + \frac{1}{3}\beta\right)}\right] \mathrm{e}^{-\left(\alpha+\frac{1}{3}\beta\right)t} - \frac{\pi\frac{j}{j_c}}{4\left(\alpha + \frac{1}{3}\beta\right)}, \tag{3.93}$$

and therefore the can define the energy relaxation time for the soliton to be

$$t_R = \frac{1}{\alpha + \frac{1}{3}\beta}. \tag{3.94}$$

Taking into consideration the time and length scales of the sine-Gordon problem, we arrive at the soliton relaxation length scale

$$d_{\max,R} = v\, t_R. \tag{3.95}$$

Given the typical fabrication parameters, the fluxon relaxation time is $t_R \approx 0.24\text{ns}$, and the fluxon relaxation length scale is $d_{\max,R} \approx 13\mu\text{m}$.

Following the discussion in Section 3.4, the corresponding decoherence scales are by definition much shorter than the relaxation lengths. We estimate that fluxon superpositions decohere over a length scale much shorter than the size of the qubit, which is approximately $5\mu\text{m}$, or the size of the fluxon itself, which is approximately $12\mu\text{m}$. It is then evident that the length constraints imposed by decoherence are severe, making experimental implementations of the protocol using present day technology quite challenging, as they would require significant reduction of the dissipation parameters α and β.

3.6 Summary

In this chapter we have described a probabilistic protocol for entangling two distant qubits via the scattering of a quantum particle. The notable feature of this protocol is that, in the absence of decoherence, it is possible to entangle the qubits for any non-negligible interaction strength between the particle and the qubit.

We also evaluated the feasibility of implementing this protocol using superconducting circuits, with a fluxon in a Josephson transmission line as the particle interacting with a flux qubit. The figure of merit used was the maximal separation of the qubits which can be achieved with present day circuit fabrication parameters. If decoherence is neglected, the maximal separation between the qubits is bounded by the desired fidelity between the final qubit state and the maximally entangled states $|\Phi^+\rangle$. This fidelity decreases with separation because the fluxon wave-packets disperse and become harder to distinguish. We find that the strength of interaction between the qubits and the fluxon places an upper bound on the fidelity which can be achieved. In particular, we find that in this ideal case,

a fidelity of 0.76 can be achieved with the qubits separated by almost half a millimeter. Thus, we find that dispersion does not impose stringent limits in the separation of the qubits.

In order to estimate how decoherence affects the performance of the protocol, we estimated the distance the fluxons can travel before either the qubits or the superpositions of fluxon wave packets decohere significantly. It was found that the decoherence of the qubits do not impose significant constraints on the separation of qubits, as in principle the fluxon can travel a distance on the order of centimeters before the qubit decoheres significantly. The effect of decoherence on the fluxon, on the other hand, was found to be significant. In particular, given current experimental values for dissipation, superposition of fluxon wave packets would decohere on length scales smaller than the qubit size. It would thus appear that an experimental implementation of such a protocol using superconducting circuits would be very challenging with present day technology.

Part II

Characterization of noise

Chapter 4

Efficient partial characterization of noise

4.1 Introduction

Experimental implementation of quantum information processing devices, even of modest size, is a challenge in and of itself. Quantum systems are inherently fragile due to unwanted interactions with surrounding degrees of freedom, leading to what is known as *decoherence*. As we have described in previous chapters, it is necessary to actively pursue methods to suppress noise by adding redundancy and removing entropy through fault-tolerant quantum computation and related approaches [Sho96, KLZ98, ABO99, AGP06]. In order to apply these techniques effectively, a detailed understanding of how the noise acts on the system is necessary. Thus, aside from the technical barriers to the implementation of quantum devices, the question of how noise can be characterized is another significant challenge. While it is possible to fully characterize these quantum operations through a procedure known as *quantum process tomography*, the number of parameters necessary for this complete characterization grows exponentially with the number of subsystems [CN97, Leu03, ML06]. Tasks that cost a number of resources, such as time or energy, that grow exponentially with the size of the system, usually given in number of qubits, are considered infeasible even for moderately large systems. Therefore it is clear that such a fine grained description is not realistic as an experimental protocol for noise characterization.

A significant effort has been made in recent years to find alternative methods to quan-

tify noise in a quantum system without complete characterization [EAZ05, DHCB05, DCEL06, ML06, LLEC07, LSB+07, KLR+08]. In this chapter we propose a method of systematically coarse-graining the description of noise. This is done by operationally symmetrizing the noise to yield an effective map with a reduced number of independent parameters reflecting properties of interest. This symmetrization is achieved by conjugating the noise with a unitary operator drawn randomly from the relevant symmetry group and then averaging over these random trials [EAZ05, DHCB05, DCEL06, LLEC07]. This averaging is known as a *twirl*. Different choices of symmetry group can give access to different properties of the noise. We give rigorous statistical bounds which guarantee that the number of experimental trials required is independent of the dimensions of the symmetry group.

The main advantage of this protocol is that it provides a natural path towards systematically obtaining partial information for other uses, as will be explored in Chapter 5. Our randomization method leads to efficient partial characterization of the noise map whenever the group elements admit efficient circuit decompositions, and as long as an appropriate parameterization of the map is used. We demonstrate how the natural parameterization used in the proposed experiments can be used to test important assumptions about noise which are routinely used in the estimation of error threshold for efficient quantum computation [KLZ98, AGP06].

This chapter is organized as follows. First, in Section 4.2 we give some background about the mathematical description of quantum operations, as well as some background about how to quantify noise in these operations. Then in Section 4.3 we describe experimental protocols which allow for partial information about noise to be extracted. The scaling of the uncertainties in estimates of these parameters from the experimental data is detailed in Section 4.4. Beyond the quantification of noise, the partial information obtained via these twirling protocols can also be used to test for the independence of noise in different subsystems, which we describe in Section 4.5.

4.2 Background

According to the postulates of quantum mechanics, the state of a quantum system is described by a vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$. This state evolves in time as described by the Schrödinger equation, which implies that this evolution is unitary. In other words,

there is an unitary operator $U(t)$ such that $|\psi(t)\rangle = U(t)|\psi(t=0)\rangle$.

As alluded to previously, not all degrees of freedom can be controlled or observed easily. These unobserved degrees of freedom are usually called *the environment*, so that the total Hilbert space is naturally divided into system and environment, or $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_E$. In general there will be interactions between system and environment, so that they will be entangled, and the state of the system cannot be describe by a vector in $\mathcal{H}_S$. Instead, the state is described by a density operator $\rho_S \in \mathcal{B}(H_S)$, where $\mathcal{B}(H_S)$ denotes the set of bounded operators acting on $\mathcal{H}_S$ (*i.e.* operators with bounded eigenvalues). For the remainder of this work, we will only consider density operators such that $\operatorname{tr}\rho = 1$. Given the state $|\psi\rangle \in \mathcal{H}$, one has that $\rho_S = \operatorname{tr}_E |\psi\rangle\langle\psi|$, where tr_E is the partial trace with respect to the environment. If one attempts to describe the evolution of the system alone, without describing the evolution of the environment, one has

$$\begin{aligned}
\rho_S(t) &= \operatorname{tr}_E U(t)\rho(t=0)U^\dagger(t) && (4.1)\\
&= \sum_k \langle e_k|U(t)\rho_S(t=0)\otimes|\psi_E\rangle\langle\psi_E|U^\dagger(t)|e_k\rangle && (4.2)\\
&= \sum_k \langle e_k|U(t)|\psi_E\rangle\ \rho_S(t=0)\ \langle\psi_E|U^\dagger(t)|e_k\rangle && (4.3)\\
&= \sum_k E_k(t)\rho_S(t=0)E_k(t)^\dagger, && (4.4)\\
&= \mathcal{E}(t)\rho_S(t=0) && (4.5)
\end{aligned}$$

where we have assumed that the environment is in the state $|\psi_E\rangle$ which is initially unentangled with the system, and that the $\{|e_k\rangle\}$ form an orthonormal basis for $\mathcal{H}_E$. The operators $E_k(t) = \langle e_k|U(t)|\psi_E\rangle$ are known as the Kraus operators, and (4.4) is known as the Kraus sum representation of the superoperator $\mathcal{E}(t)$ [Kra83]. These superoperators are also referred to as *completely positive (CP) maps*, because they preserved the positivity of density operators even when they act only on subsystems [Cho75, Kra83]. In the discussion to follow, we will denote CP maps by capital Greek letters such as Λ, or capital calligraphic letters such as $\mathcal{A}$, $\mathcal{B}$, *etc.* For many of the physical settings usually considered, CP maps are general enough to describe all observed forms of noise, especially in systems such as NMR and ion traps [AL87, ALZ06]. For this reason we will restrict ourselves consider noise described by CP maps. Superoperators are also referred to as *quantum channels*, and we will use the terms superoperator, channel and CP map interchangeably.

In the case that there is no interaction with the environment, the evolution of the

system is given by a unitary $U(t)$ acting on the system alone. The corresponding superoperator will be denoted $\mathcal{U}$ such that $\mathcal{U}\rho_S = U\rho_s U^\dagger$. In an ideal setting the state of a system is taken to be a pure state, and the operations performed by a quantum information processor on the system are taken to be unitaries. Realistically, it is unavoidable that the system interact with the environment, so that these noisy operations implemented by an experiment will be CP maps.

While in principle the environment can be arbitrarily large, it is possible to describe a CP map without describing all degrees of freedom in the environment. The simplest way to see how this comes about is by considering the representation of ρ_S in a particular orthonormal basis, such as

$$\rho = \sum_{ij} [\rho]_{ij} |i\rangle\langle j|, \tag{4.6}$$

where $[\rho]_{ij}$ denotes the entry in the ith row of the jth column of the matrix representation of ρ in this particular basis (we will omit the subscript S from here on for brevity). Since the density operator ρ can be represented in this manner by a matrix, we use the terms 'density operator' and 'density matrix' interchangeably. It is clear from the Kraus representation that CP maps are linear operations, so that if we represent the Kraus operators in the same basis as above we obtain

$$[\rho(t)]_{ij} = \sum_{klm} [E_k]_{il} [E_k]^*_{jm} [\rho]_{lm}. \tag{4.7}$$

Rearranging the entries of the density matrix ρ into a column vector $|\rho\rangle\rangle$ by stacking the columns, such that a two dimensional density matrix can be written as

$$|\rho\rangle\rangle = \begin{pmatrix} \rho_{00} \\ \rho_{10} \\ \rho_{01} \\ \rho_{11} \end{pmatrix}, \tag{4.8}$$

allows us to rewrite (4.7) in the more compact form

$$|\rho(t)\rangle\rangle = \sum_k E_k^*(t) \otimes E_k(t) |\rho\rangle\rangle, \tag{4.9}$$

$$= \widehat{\mathcal{E}} |\rho\rangle\rangle. \tag{4.10}$$

$\widehat{\mathcal{E}}$ is what we call *the natural or Liouville representation of* $\mathcal{E}$ [Blu96]. This representation can also be derived directly from *Roth's lemma* [HJ91], which states

$$|ABC\rangle\rangle = C^T \otimes A |B\rangle\rangle, \tag{4.11}$$

where A, B and C are matrices of the appropriate dimensions. Since the natural representation describes a CP in full generality, it is clear that for a d dimensional Hilbert space, one requires at most d^4 different complex parameters to describe $\widehat{\mathcal{E}}$, regardless of how many degrees of freedom are in the environment. It can be shown that in fact at most d^4 *real* parameters are necessary, as the elements of $\widehat{\mathcal{A}}$ can be rearranged to form a positive $d^2 \times d^2$ known as the *Choi matrix* [Cho75]. Imposing the additional requirement that $\mathcal{E}$ preserve the trace of ρ translates to

$$\sum_i E_i^\dagger E_i = \mathbb{1}_d, \tag{4.12}$$

which leads to d^2 constraints on the parameters of $\widehat{\mathcal{E}}$, and therefore in reality we need $d^4 - d^2$ real parameters.

While the Kraus sum representation is not unique (it depends on which basis is used to trace over the environment), $\widehat{\mathcal{E}}$ is a unique representation for $\mathcal{E}$. Another way to describe $\mathcal{E}$ in a unique manner is to decompose the Kraus operators in a particular operator basis. This is possible by defining the *Hilbert-Schmidt inner product* between two operators Q and R acting on a d dimensional space as $\mathrm{tr}\, Q^\dagger R$. Note that

$$\mathrm{tr}\, Q^\dagger R = \langle\langle Q|R\rangle\rangle, \tag{4.13}$$

so that we may write the Hilbert-Schmidt inner product as $\langle\langle Q|R\rangle\rangle$.

If we are dealing with a system consisting of qubits, one such basis is the n qubit Pauli group $\mathcal{P}_n$, consisting of all n fold tensor products of the Pauli operators $\mathbb{1}_2$, σ_X, σ_Y and σ_Z. After normalizing the Pauli group, we can decompose each of the E_i as

$$E_i = \sum_{P_j \in \mathcal{P}_n} \frac{1}{d} \langle\langle P_j|E_i\rangle\rangle P_j, \tag{4.14}$$

$$= \sum_{P_j \in \mathcal{P}_n} e_{ij} P_j, \tag{4.15}$$

to arrive at

$$\mathcal{E}\rho = \sum_{P_i, P_j \in \mathcal{P}_n} [\chi]_{ij} P_i \rho P_j \tag{4.16}$$

where $[\chi]_{ij} = \sum_k e_{ki} e_{kj}^*$. This is what we call *the χ representation of $\mathcal{E}$*. This representation has many attractive features. In particular trace-preservation implies that $\mathrm{tr}\, \chi = 1$, while Hermiticity-preservation implies $[\chi]_{ij} = [\chi]_{ji}^*$. The fact that $\mathcal{E}$ is CP also implies $\chi \geq 0$, which follows from the fact that Choi matrix is positive for CP

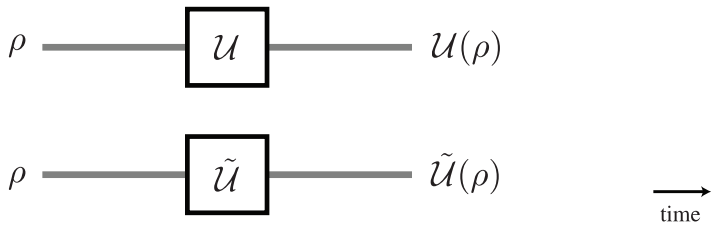

Figure 4.1: *Circuit diagram representing the action of the ideal unitary $\mathcal{U}$, and the imperfect implementation $\tilde{\mathcal{U}}$.*

maps [Cho75, Kra83]. Thus it can be concluded that all entries in the diagonal of χ are positive, and since trace preservation requires $\mathrm{tr}\,\chi = 1$, the diagonal elements $[\chi]_{ii}$ can be interpreted as probabilities. As we will see later in this chapter, this allows us to use these diagonal entries as a measure of probability of different errors occurring.

In order to describe any given CP map, it is sufficient to describe the parameters of any of the representations above. Due to the linearity of the maps we have described, this can be reduced to solving a linear set of equations for $\widehat{\mathcal{E}}$ by considering its action on d^2 linearly independent density operators. This procedure is known as *process tomography* [CN97, Leu03, ML06]. Because these density operator have unit trace, there are $d^4 - d^2$ free parameters, so that there is a unique solution to this linear problem.

It is important to note that the number of parameters needed to completely describe such maps grows exponentially with the number of subsystems. In particular case of a system consisting of n qubits, which will be our focus for the remainder of the thesis, one has $d = 2^n$, and a CP map acting on such a system requires $2^{4n} - 2^{2n}$ real parameters to be described [CN97]. This in turn implies an exponential number of experiments need to be performed [ML06], which is infeasible even for modestly large collections of qubits. In order to characterize noise in quantum operations via scalable experiments, a different strategy must be taken.

4.2.1 Average gate fidelity

A measure of how closely $\tilde{\mathcal{U}}$ approximates $\mathcal{U}$ is how close the results of applying $\mathcal{U}$ and $\tilde{\mathcal{U}}$ to the same pure state are. As we have mentioned in the previous chapters, a good measure of how alike two states are is the fidelity. When comparing a pure state $|\psi\rangle$ with

a mixed state ρ, the fidelity is defined as

$$F(|\psi\rangle, \rho) = \langle\psi|\rho|\psi\rangle. \tag{4.17}$$

In particular, $F(|\psi\rangle, \rho) \in [0, 1]$ for all states $|\psi\rangle \in \mathcal{H}$ and all density matrices $\rho \in \mathcal{B}(\mathcal{H})$. We then define the fidelity between two superoperators $\mathcal{U}$ and $\tilde{\mathcal{U}}$ with respect to the state $|\psi\rangle$ to be

$$F_{|\psi\rangle}(\mathcal{U}, \tilde{\mathcal{U}}) = \langle\psi|U^\dagger \tilde{\mathcal{U}}(|\psi\rangle\langle\psi|)U|\psi\rangle, \tag{4.18}$$

$$= \langle\psi|\mathcal{U}^\dagger \circ \tilde{\mathcal{U}}(|\psi\rangle\langle\psi|)|\psi\rangle. \tag{4.19}$$

This is what we call the *gate fidelity* between $\tilde{\mathcal{U}}$ and $\mathcal{U}$ with respect to $|\psi\rangle$. Here we have used $\circ$ to symbolized the composition of superoperators, and $\mathcal{U}^\dagger$ to represent the Heisenberg dual of the superoperator $\mathcal{U}$. This dual is defined by

$$\mathrm{tr}[B\ \mathcal{E}(\rho)] = \mathrm{tr}[\mathcal{E}^\dagger(B)\ \rho] \tag{4.20}$$

for all quantum observables B. In terms of the Kraus operator decomposition of $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$, we have that $\mathcal{E}^\dagger(\rho) = \sum_k E_k^\dagger \rho E_k$. In the case of unitaries, the superoperator dual corresponds to the inverse superoperator, so that in essence (4.19) measures how close $\mathcal{U}$ and $\tilde{\mathcal{U}}$ are by measuring how close $\mathcal{U}^\dagger \circ \tilde{\mathcal{U}}$ is to the identity map.

In order to make this measure independent of the particular choice of input state, one can compute the average fidelity for a uniform or unitarily invariant distribution of pure states, to obtain *the average fidelity between* $\mathcal{U}$ *and* $\tilde{\mathcal{U}}$

$$\overline{F}(\mathcal{U}, \tilde{\mathcal{U}}) = \int d\mu(\psi)\ \langle\psi|\mathcal{U}^\dagger \circ \tilde{\mathcal{U}}(|\psi\rangle\langle\psi|)|\psi\rangle, \tag{4.21}$$

where $d\mu(\psi)$ is the unitarily invariant distribution of states known as the *Fubini-Study measure* [EAZ05, BZ06]. The most attractive feature of this measure of distance between quantum processes is that it can be interpreted as an lower bound to the *probability of successfully applying* $\mathcal{U}$ [GLN05].

As we are only interested in characterizing the noisy part of $\tilde{\mathcal{U}}$, it is convenient to define

$$\tilde{\mathcal{U}} = \Lambda \circ \mathcal{U}, \tag{4.22}$$

where Λ is the undesired part of the evolution. Equivalently, one defines $\Lambda = \tilde{\mathcal{U}} \circ \mathcal{U}^\dagger$. The average fidelity then reduces to

$$\overline{F}(\mathcal{U}, \tilde{\mathcal{U}}) = \int d\mu(\psi)\ \langle\psi|U^\dagger\ \Lambda(\ U|\psi\rangle\langle\psi|U^\dagger\ )\ U|\psi\rangle, \tag{4.23}$$

$$= \int d\mu(\psi)\ \langle\psi|\ \Lambda(|\psi\rangle\langle\psi|)\ |\psi\rangle, \tag{4.24}$$

due to the fact that the distribution is unitarily invariant. This demonstrates that the average fidelity depends only on the noisy part of $\tilde{\mathcal{U}}$ [EAZ05].

In an experimental setting, one does not have access to a perfect implementation of a unitary $\mathcal{U}$ to be composed with the imperfect implementation $\tilde{\mathcal{U}}$. As an alternative, one can consider the implementation of some sequence of unitaries which, when composed, is intended to implement the identity gate over the qubits involved, in essence setting $U = \mathbb{1}_{2^n}$. In that case $\tilde{\mathcal{U}} = \Lambda$, and (4.24) makes no requirement for ideal resources, so that it may be used to estimate strength of Λ. In order to simplify the expressions to follow, we take the average gate fidelity to be

$$\overline{F} = \int d\mu(\psi)\ \langle\psi|\ \Lambda(|\psi\rangle\langle\psi|)\ |\psi\rangle, \tag{4.25}$$

so that it is implicit that $U = \mathbb{1}_{2^n}$ [Nie02, EAZ05].

A random state can be generated from a fixed state by applying a random unitary operator. In order to obtain a unitarily invariant distribution of states, one must chose the distribution for random unitaries to also be unitarily invariant under conjugation. This leads to the *Haar measure* over unitaries [EAZ05], so that $\overline{F}$ can be rewritten as

$$\overline{F} = \int d\mu(V)\ \langle\psi|\ \mathcal{V}^\dagger \circ \Lambda \circ \mathcal{V}(|\psi\rangle\langle\psi|)\ |\psi\rangle, \tag{4.26}$$

where $\mathcal{V}(\rho) = V\rho V^\dagger$, $V \in U(2^n)$ and $d\mu(V)$ is the Haar measure over $U(2^n)$. Thus, in order to evaluate the average gate fidelity, one can consider the averaged channel

$$\overline{\Lambda} = \int d\mu(V)\ \mathcal{V}^\dagger \circ \Lambda \circ \mathcal{V}, \tag{4.27}$$

and the fidelity between the output state of $\overline{\Lambda}$ and the corresponding pure input state. This averaging of a channel composed with a unitary and its inverse is known as a *twirl*, and is depicted in Figure 4.2. In this case, it is known as a *Haar twirl* as the average is taken over the Haar measure. Because of the unitary invariance of the Haar measure, $\overline{\Lambda}$ is a symmetrized version of Λ, such that the fidelity $\langle\psi|\overline{\Lambda}(|\psi\rangle\langle\psi|)|\psi\rangle$ is independent of $|\psi\rangle$. In essence, twirling over the Haar measure makes the noise isotropic across the Hilbert space of possible states.

Due to this isotropy, the twirled channel can be shown to have the form [HHH99, Nie02, EAZ05]

$$\mathcal{D}_n[p](\rho) \equiv p\ \rho + (1-p)\frac{\mathbb{1}_{2^n}}{2^n}, \tag{4.28}$$

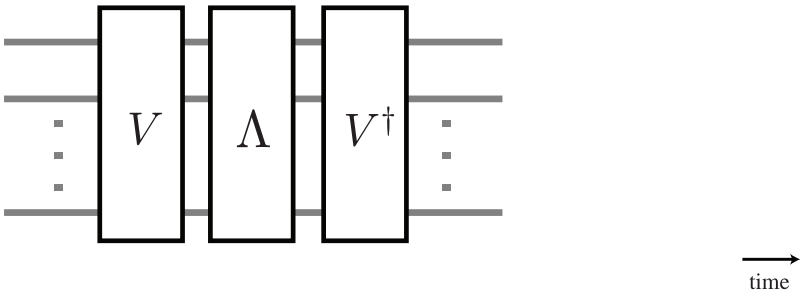

Figure 4.2: *Circuit diagram for twirling the quantum operation* Λ.

known as a *depolarizing channel*. In the case where $\Lambda(\rho) = \sum_k A_k \rho A_k^\dagger$ for some set of Kraus operators $\{A_k\}_k$, the parameter p can be shown to reduce to

$$p = \frac{\sum_k |\operatorname{tr} A_k|^2 - 1}{4^n - 1} = \frac{\operatorname{tr} \widehat{\Lambda} - 1}{4^n - 1}, \tag{4.29}$$

where $\widehat{\Lambda}$ is the Liouville representation of Λ. The average gate fidelity is then

$$\overline{F} = p\langle\psi|\psi\rangle\langle\psi|\psi\rangle + \frac{1-p}{2^n}\langle\psi|\mathbb{1}_{2^n}|\psi\rangle \tag{4.30}$$

$$= p + \frac{1-p}{2^n} \tag{4.31}$$

$$= \frac{\operatorname{tr} \widehat{\Lambda} + 2^n}{4^n + 2^n}. \tag{4.32}$$

At first glance, this requires a complete description of Λ in terms of its Kraus operators, and as we have discussed, estimating the parameters of a full description of Λ, in any representation, requires an number of experiments which is exponential in n [CN97, Leu03, ML06].

However, as the Haar measure for $U(2^n)$ is exponentially concentrated, only a few random unitary samples are necessary to estimate $\overline{F}$ to some desired accuracy [EAZ05]. In order to estimate the average fidelity, one simply takes the following steps:

1. prepare a state $|\psi\rangle$ which is both easy to prepare and easy to project into.
2. chooses a unitary V according to the Haar measure, and apply it to $|\psi\rangle$.
3. let Λ act on the state.
4. apply $V^\dagger$ to the state.

5. detect whether the result is $|\psi\rangle$ ($F = 1$) or its complement subspace $|\psi^{\perp}\rangle$ ($F = 0$).

While the number of experiments is greatly reduced, the main drawback of this proposal is that the implementation of a unitary picked at random from the Haar distribution requires, in general, a number of elementary gates that is exponential in n.

4.2.2 Clifford twirl

A solution to the problem of sampling from the Haar measure is to sample from a distribution of more easily implementable operations which still lead to the same average fidelity [DCEL06]. A set of unitaries $\{V_i\}_i$, coupled with a probability distribution $\Pr(V_i)$ with the property

$$\overline{F} = \int d\mu(V)\ \langle\psi|\ \mathcal{V}^{\dagger} \circ \Lambda \circ \mathcal{V}(|\psi\rangle\langle\psi|)\ |\psi\rangle, \tag{4.33}$$

$$= \sum_i \Pr(V_i) \langle\psi|\ \mathcal{V}_i^{\dagger} \circ \Lambda \circ \mathcal{V}_i(|\psi\rangle\langle\psi|)\ |\psi\rangle, \tag{4.34}$$

is sufficient. Such mathematical objects are known as *unitary 2-designs*, because the quantity being computed is a second-order polynomial in the matrix elements of V as well as in the matrix elements of $V^{\dagger}$.

One example of a unitary 2-design is the Clifford group [BDSW96, DLT02, Cha05, DCEL06]. In order to see how the Clifford twirl greatly simplifies the description of the twirled channel $\overline{\Lambda}$, first recall the χ representation of Λ

$$\Lambda(\rho) = \sum_{ij} [\chi]_{ij} P_i \rho P_j, \tag{4.35}$$

for all $P_{i,j} \in \mathcal{P}_n$. By convention, we let $P_0 = \mathbb{1}^{\otimes n}$. From the definition of the Clifford group, it is clear that $\mathcal{P}_n \subset \mathcal{C}_n$, so that if we twirl uniformly over the Pauli group, and then twirl uniformly over the full Clifford group, the effect is the same as only twirling over the Clifford group[1]. Twirling Λ over $\mathcal{P}_n$ yields [Dan05b, DCEL06]

$$\overline{\Lambda}_{\mathcal{P}_n}(\rho) = \sum_{P_i \in \mathcal{P}_n} [\chi]_{ii} P_i \rho P_i, \tag{4.36}$$

[1]The usual approach is to decompose a $\mathcal{C}_n$ twirl into a $\mathcal{P}_n$ twirl composed with what is called a symplectic twirl [DCEL06]. However, for our purposes it suffices to consider the composition of $\mathcal{P}_n$ and $\mathcal{C}_n$ twirl, thus avoiding the introduction of another group.

that is, the off-diagonal entries of χ are set to zero. Due to properties of the χ representation of a CP map discussed earlier, we can interpret $\overline{\Lambda}_{\mathcal{P}_n}$ as a map where $P_i \in \mathcal{P}_n$ is applied with probability $[\chi]_{ii}$. From the definition of the Clifford group, twirling $\overline{\Lambda}_{\mathcal{P}_n}$ over the $\mathcal{C}_n$ distributes the probability mass evenly over the non-identity Pauli operators, yielding

$$\overline{\Lambda}_{\mathcal{C}_n}(\rho) = [\chi]_{00}\rho + \frac{1-[\chi]_{00}}{4^n-1} \sum_{P_i \in \mathcal{P}_n \setminus \{\mathbb{1}_{2^n}\}} P_i \rho P_i. \tag{4.37}$$

Given that for any density matrix ρ

$$\frac{1}{4^n} \sum_{P_i \in \mathcal{P}_n} P_i \rho P_i = \frac{\mathbb{1}_{2^n}}{2^n} \tag{4.38}$$

it follows that

$$\overline{\Lambda}_{\mathcal{C}_n}(\rho) = p\rho + (1-p)\frac{\mathbb{1}_{2^n}}{2^n}, \tag{4.39}$$

where $p = \frac{4^n[\chi]_{00}-1}{4^n-1}$. Note that because Pauli operators are traceless, we have that $\operatorname{tr}\widehat{\Lambda} = 4^n[\chi]_{00}$ and so (4.32) implies

$$\overline{\Lambda}_{\mathcal{C}_n} = \overline{\Lambda}. \tag{4.40}$$

Therefore the average fidelity estimated by averaging over $\mathcal{C}_n$ is identical to the average fidelity estimated by averaging over unitaries distributed according to the Haar measure [Dan05b, DCEL06], as claimed.

The main advantage of this approach is that it is possible to sample $\mathcal{C}_n$ to estimate the average fidelity in an efficient manner, as each unitary in $\mathcal{C}_n$ can be implemented using $O(n^2/\log n)$ instances of the generator unitaries [AG04]. The protocol for estimating the fidelity then becomes

1. prepare a state $|\psi\rangle$ which is both easy to prepare and easy to project into.
2. chooses a unitary $V \in \mathcal{C}_n$ uniformly, and apply it to $|\psi\rangle$.
3. let Λ act on the state.
4. apply $V^\dagger$ to the state.
5. detect whether the result is $|\psi\rangle$ ($F = 1$) or its complement subspace $|\psi^\perp\rangle$ ($F = 0$).

For simplicity, we can let $|\psi\rangle = |0\rangle^{\otimes n}$, and then the final measurement can simply be the measurement of each qubit into the σ_Z eigenbasis. After repeating the experiment K times, the Chernoff bound states that

$$\Pr(|\overline{F} - \tilde{F}| > \delta) \leq 2\exp(-\delta^2 K), \tag{4.41}$$

where the $\tilde{F}$ is the mean of the K samples taken from the experiments. In other words, the probability of the average fidelity estimate being farther than δ away from the true average $\overline{F}$ decreases exponentially with the K. Inverting this relationship leads to

$$K \leq \frac{1}{\delta^2} \ln \frac{2}{\Pr(|\overline{F} - \tilde{F}| > \delta)}, \tag{4.42}$$

which implies that, given a fixed probability of being within δ of the true mean, the number of experiments is independent of the number of qubits in the system being characterized.

Other methods can be used to approximate $\mathcal{C}_n$ twirling with $O(n \log \frac{1}{\epsilon})$ gates arranged in $O(\log n \log \frac{1}{\epsilon})$ time steps, where ϵ is how accurately one would like to approximate an exact $\mathcal{C}_n$ twirl [Dan05b, DCEL06]. However, it is clear from the previous arguments that, even without optimizations, the average fidelity can be estimated through experiments that scale well with the number of qubits.

4.3 Weight distribution of errors

The decomposition of a $\mathcal{C}_n$ twirl into a $\mathcal{P}_n$ twirl composed with a $\mathcal{C}_n$ twirl highlights the fact that characterization of the twirled channel can be interpreted as partial characterization of the original channel. Twirling over $\mathcal{P}_n$ discards information about the off-diagonal entries of χ, and twirling over $\mathcal{C}_n$ places errors in different equivalence classes – *i.e.* trivial or non-trivial – and we only learn about the probability that an error belongs to each equivalence class. From this perspective, we can consider twirling over different sets of operations that will not leads to 2-designs, but that will still provide different kinds of partial information about the noise, such as classifying errors into different equivalence classes.

Instead of twirling over $\mathcal{C}_n$, consider twirling over the *local Clifford group* ${\mathcal{C}_1}^{\otimes n}$, which consists of tensor products of single qubit Clifford group operations. From an experimental perspective, the main attraction of considering ${\mathcal{C}_1}^{\otimes n}$ is that it lacks interactions between the qubits, and interactions are often more difficult to implement than single qubit operations. Once again we find that $\mathcal{P}_n \subset {\mathcal{C}_1}^{\otimes n}$, so we may take twirling over ${\mathcal{C}_1}^{\otimes n}$ to be a $\mathcal{P}_n$ twirl composed with a ${\mathcal{C}_1}^{\otimes n}$ twirl. Under conjugation, any operation $C \in \mathcal{C}_1$ will map the set $\{\sigma_X, \sigma_Y, \sigma_z\}$ onto itself, given the definition of the Clifford group and the fact that any unitary will map $\mathbb{1}_2$ to itself under conjugation. This

implies that conjugating any $P \in \mathcal{P}_n$ by an operation in ${\mathcal{C}_1}^{\otimes n}$ will preserve the number of non-identity elements in the tensor factor decomposition, and it will also preserve the locations of the Pauli errors. In other words, the *weight* $\mathrm{wt}(P)$ *of a Pauli operator* P *is preserved under conjugation by local Clifford operations.* However, because the error locations are also preserved, this would imply that a super-polynomial number of parameters is needed to describe a channel twirled over this group. In order to discard information about the error locations, one can twirl over Π_n, the group of permutations of n qubits. The group $\mathcal{C}_1\Pi$ generated by composition of Π_n and ${\mathcal{C}_1}^{\otimes n}$ is also a subgroup of $\mathcal{C}_n$. Interestingly, it is not necessary to apply the unitaries in Π_n to implement the Π_n twirl – one can simply discard error location information when performing the parameter estimation, as we will show later. We still call an $\mathcal{C}_1\Pi$ twirl a local Clifford twirl, in order to emphasize that only the ${\mathcal{C}_1}^{\otimes n}$ operations are explicitly applied, and that the Π_n operations are implicitly applied by marginalization of data.

Composing a $\mathcal{C}_1\Pi$ twirl with a $\mathcal{P}_n$ twirl will uniformly distributes the probability mass over n-qubit Pauli operators of the same weight. Thus we may write

$$\overline{\Lambda}_{\mathcal{C}_1\Pi}(\rho) = \sum_{w=0}^{n} \Pr(w)\mathcal{M}_w^p(\rho), \tag{4.43}$$

$$\mathcal{M}_w^p(\rho) = \frac{1}{3^w \binom{n}{w}} \sum_{\mathrm{wt}(P_i \in \mathcal{P}_n)=w} P_i \rho P_i, \tag{4.44}$$

where $\Pr(w)$ is the probability that a Pauli error of weight w will occur. The CP maps $\mathcal{M}_w^p$ correspond to random application of one of the $3^w \binom{n}{w}$ Pauli errors of weight w with uniform probability, so that we can make the identification

$$\Pr(w) = \sum_{\mathrm{wt}(P_i \in \mathcal{P}_n)=w} [\chi]_{ii}. \tag{4.45}$$

On the other hand, $\mathcal{C}_n$ twirled channels have the form

$$\overline{\Lambda}(\rho)_{\mathcal{C}_n} = \Pr(0)\rho + (1 - \Pr(0))\frac{1}{4^n - 1} \sum_{\mathrm{wt}(P_i \in \mathcal{P}_n)\neq 0} P_i \rho P_i. \tag{4.46}$$

While $\mathcal{C}_n$ twirling leads to a channel with a single parameters $\Pr(0)$, $\mathcal{C}_1\Pi$ twirling leads to a channel with $n+1$ parameters $\{\Pr(w)\}_{w=0}^n$. In either case, estimating the parameter $\Pr(0) = [\chi]_{00}$ is sufficient to estimate the average fidelity of the channel Λ. The same experimental protocol used for estimating $\overline{F}$ using a $\mathcal{C}_n$ twirl can be be used to estimate $\overline{F}$ using a $\mathcal{C}_1\Pi$ twirl. However, in order to estimate the $\Pr(w)$ the collected data must be post-processed in a different way.

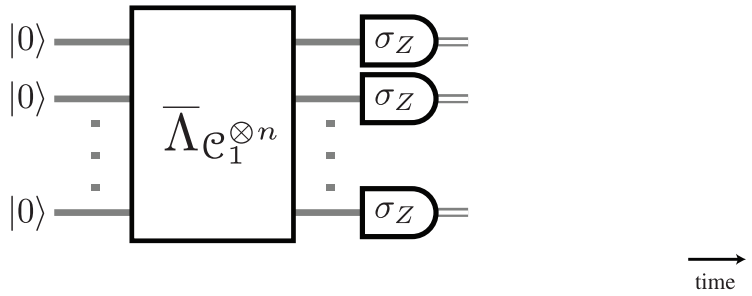

Figure 4.3: *Circuit diagram for the characterization of a $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ twirled channel.*

4.3.1 Weight monitoring protocol for estimating $\Pr(w)$

Instead of simply checking whether the state after $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ acted is $|0\rangle^{\otimes n}$ or not, one approach to estimate the $\Pr(w)$ is to estimate the probability distribution q_w of the weights of the binary strings observed in the experiment – in other words, w is the number of qubit measurement outcomes with eigenvalues -1. The circuit diagram for the protocol is depicted in Figure 4.3. Since the initial state as well as the measurements are qubit permutation invariant, there is no need for the explicit application of the qubit permutations. Gathering only information about the weight of the measurement outcomes ensures that all information about the error locations is discarded. This is why the circuit diagram in Figure 4.3 depicts a $\overline{\Lambda}_{\mathcal{C}_1{}^{\otimes n}}$ twirled channel when we are in fact estimating the parameters of $\overline{\Lambda}_{\mathcal{C}_1\Pi}$.

Given that the input state $|0\rangle^{\otimes n}$ is an eigenstate of σ_Z acting on any of the qubits, errors of this type will not lead to observable change is the string weight distribution. However the structure of the $\mathcal{C}_1\Pi$ twirled channel implies that the probability of a Pauli error depends only on its weight, and σ_X and σ_Y errors leads to observable changes in the weight distribution. Given the error weight distribution $\Pr(w)$, it is possible to infer what is the distribution of the strings weights through by a simple argument. The probability q_w that a binary string of weight w is observed is given by sum of the probability that an error of weight $w' \geq w$ has occurred times the probability that this error has w errors which are either σ_X or σ_Y (as these are independent events). Formally we write

$$q_w = \sum_{w' \geq w}^{n} R_{w,w'} \Pr(w'), \tag{4.47}$$

$$R_{w,w'} = \frac{2^w \binom{w'}{w}}{3^{w'}}, \tag{4.48}$$

where $R_{w,w'}$ is the conditional probability that a string of weight w is observed given that an error of weight w' has occurred.

If we arrange the $\{q_w\}$ and the $\{\Pr(w)\}$ as vectors, $R_{w,w'}$ can be seen as an upper triangular matrix. Since its diagonal entries are all non-zero, its determinant is also non-zero, and therefore $R_{w,w'}$ is invertible [HJ85]. The estimates of the $\{\Pr(w)\}$ can be obtained from the estimates of the $\{q_w\}$ by back-substitution, given the upper-triangular form of $R_{w,w'}$.

4.3.2 Parity monitoring protocol for estimating $\Pr(w)$

Instead of describing $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ in terms of how it transforms states, it is possible to describe this twirled channel in terms of how it transforms observables by considering the dual channel in the Heisenberg picture. $\mathcal{C}_1\Pi$ twirled channels have Kraus operators which are Hermitian, and therefore their are self-dual, or

$$\overline{\Lambda}_{\mathcal{C}_1\Pi} = \overline{\Lambda}^{\dagger}_{\mathcal{C}_1\Pi}. \tag{4.49}$$

As pointed out earlier, the Pauli group $\mathcal{P}_n$ forms an operator basis. Since these operators are Hermitian, we can get a complete description of $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ by considering its action on the observables that make up $\mathcal{P}_n$.

Elements of $\mathcal{P}_n$ have the important property that they either commute or anti-commute with each other. In other words, we have that for $P_i, P_j \in \mathcal{P}_n$ either $P_iP_j = P_jP_i$ or $P_iP_j = -P_jP_i$. This is easily verified for single qubits, and extended to n qubits due to properties of the tensor product. If we consider the action of $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ on an element $P \in \mathcal{P}_n$ we find that

$$\begin{aligned}
\overline{\Lambda}_{\mathcal{C}_1\Pi}(P) &= \sum_{P_i \in \mathcal{P}_n} \Pr(P_i)\ P_iPP_i && (4.50)\\
&= \sum_{P_iP = PP_i} \Pr(P_i)\ P_iP_iP - \sum_{P_iP = -PP_i} \Pr(P_i)\ P_iP_iP && (4.51)\\
&= \sum_{P_iP = PP_i} \Pr(P_i)\ P - \sum_{P_iP = -PP_i} \Pr(P_i)\ P && (4.52)\\
&= \lambda(P)P, && (4.53)
\end{aligned}$$

or, in other words, the action of $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ is to scale a Pauli observable P by $\lambda(P) \in [-1, 1]$. Due to the group structure of $\mathcal{C}_1\Pi$, we find that $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ is invariant under the action of any

unitary in $\mathcal{C}_1\Pi$, thus the scaling factors $\lambda(P)$ can only depend on $\mathrm{wt}(P)$. We can label these scaling factors by the weight of the Pauli operators instead, *i.e.* $\lambda_w = \lambda(P)$ for $\mathrm{wt}(P) = w$. This translates to the fact that there are only $n+1$ different scaling factors to be estimated, just as there are only $n+1$ different $\Pr(w)$ to be estimated.

As the scaling factors depend only on the weight, it is possible to estimate λ_w by focusing on how the observables $\sigma_Z^{\otimes w} \otimes \mathbb{1}_2^{n-w}$ are scaled. These observables can be measured by first measuring each qubit in the σ_Z eigenbasis, and then computing the parity of the outcomes on w different qubits – recall that in order to discard error location information, these qubits must be chosen randomly. It then becomes clear that the the same circuit depicted in Figure 4.3 can be used to estimate these scaling factors.

An important feature of this protocol is that it is robust against certain types of imperfections during input state preparation and measurement. If these imperfections are well described by channels which have a diagonal χ representation, then this just corresponds to additional scaling factors for any Pauli observable sent through the channel, as it is clear from (4.53). These scaling factors due to the imperfections can be estimated separately by running the protocol without letting Λ act on the system – which can be done if the error being characterized corresponds to a sequence of unitaries intended to approximated $\mathbb{1}_{2^n}$, for example. The ratio of the scaling factors for the full protocol with Λ and this calibration step correspond to the scaling factors of $\overline{\Lambda}_{\mathcal{C}_1\Pi}$. As long as the expectation values of the observables can be estimated to high enough precision, the parameters of the twirled channel can be estimated despite these imperfections. This is particularly relevant in the case of solid-state and liquid-state nuclear magnetic resonance based quantum information processing devices [BCC+07, ESM+07], where the initial state is a highly mixed state with only a small bias towards the state $|00\ldots0\rangle$, but where the detectors are highly sensitive.

In order to prove that there is a one-to-one relationship between λ_w and $\Pr(w)$, we must consider different parameterizations of the Liouville representation of the twirled channel $\overline{\Lambda}_{\mathcal{C}_1\Pi}$. Given the Kraus presentation of $\overline{\Lambda}_{\mathcal{C}_1\Pi}$ as depicted in (4.43), it follows that

$$\overline{\Lambda}_{\mathcal{C}_1\Pi} = \sum_{w=0}^{n} \Pr(w)\mathcal{M}_w^p, \tag{4.54}$$

$$\widehat{\mathcal{M}}_w^p = \frac{1}{3^w \binom{n}{w}} \sum_{\mathrm{wt}(P_i \in \mathcal{P}_n)=w} P_i^* \otimes P_i, \tag{4.55}$$

is a parameterization in terms of the $\Pr(w)$. The description in terms of the scaling factors λ_w also leads to a parameterization precisely because $\mathcal{P}_n$ is an orthogonal basis

of operators. This leads to the parameterization

$$\overline{\Lambda}_{\mathfrak{C}_1\Pi} = \sum_{w=0}^{n} \lambda_w \mathcal{M}_w^{\lambda}, \tag{4.56}$$

$$\widehat{\mathcal{M}}_w^c = \sum_{\mathrm{wt}(P_i \in \mathcal{P}_n)=w} \frac{1}{2^n} |P_i\rangle\!\rangle \langle\!\langle P_i|, \tag{4.57}$$

which can be interpreted as a projection into each of the subspaces of the same weight w followed by scaling according λ_w.

Orthogonality between the $\widehat{\mathcal{M}}_w^p$ and the $\widehat{\mathcal{M}}_w^{\lambda}$ can be established by computing the Hilbert-Schmidt inner product in the Liouville representation, so that

$$\begin{aligned}
\langle \widehat{\mathcal{M}}_i^p, \widehat{\mathcal{M}}_j^p \rangle &= \mathrm{tr}(\widehat{\mathcal{M}}_i^p)^\dagger \widehat{\mathcal{M}}_j^p && (4.58)\\
&= \frac{1}{3^{i+j}\binom{n}{i}\binom{n}{j}} \sum_{\mathrm{wt}(P_k)=i} \sum_{\mathrm{wt}(P_l)=j} \mathrm{tr}(P_k^T \otimes P_k)(P_l^* \otimes P_l) && (4.59)\\
&= \frac{1}{3^{i+j}\binom{n}{i}\binom{n}{j}} \sum_{\mathrm{wt}(P_k)=i} \sum_{\mathrm{wt}(P_l)=j} (\mathrm{tr}\, P_k^T P_l^*)(\mathrm{tr}\, P_k P_l) && (4.60)\\
&= 4^n \frac{1}{3^i \binom{n}{i}} \delta_{ij}, && (4.61)
\end{aligned}$$

and

$$\begin{aligned}
\langle \widehat{\mathcal{M}}_i^{\lambda}, \widehat{\mathcal{M}}_j^{\lambda} \rangle &= \mathrm{tr}(\widehat{\mathcal{M}}_i^{\lambda})^\dagger \widehat{\mathcal{M}}_j^{\lambda} && (4.62)\\
&= \frac{1}{4^n} \sum_{\mathrm{wt}(P_k)=i} \sum_{\mathrm{wt}(P_l)=j} \mathrm{tr}\, |P_k\rangle\!\rangle \langle\!\langle P_k|^\dagger |P_l\rangle\!\rangle \langle\!\langle P_l| && (4.63)\\
&= \frac{1}{4^n} \sum_{\mathrm{wt}(P_k)=i} \sum_{\mathrm{wt}(P_l)=j} |\langle\!\langle P_k | P_l \rangle\!\rangle|^2 && (4.64)\\
&= \frac{1}{4^n} \sum_{\mathrm{wt}(P_k)=i} \sum_{\mathrm{wt}(P_l)=j} |\,\mathrm{tr}\, P_k P_l|^2 && (4.65)\\
&= 3^i \binom{n}{i} \delta_{ij}. && (4.66)
\end{aligned}$$

Equating the Liouville representations of (4.54) and (4.56), and computing the Hilbert-Schmidt inner product with each of the operators $\widehat{\mathcal{M}}_w^{\lambda}$ and $\widehat{\mathcal{M}}_w^p$, we reach the relationships

$$\lambda_w = \sum_{w'} [\Omega]_{w,w'} \Pr(w'), \tag{4.67}$$

$$\Pr(w) = \sum_{w'} [\Omega^{-1}]_{w,w'} \lambda_{w'} \tag{4.68}$$

where

$$[\Omega]_{w,w'} = \frac{\langle \widehat{\mathcal{M}}^{\lambda}_{w}, \widehat{\mathcal{M}}^{p}_{w'} \rangle}{\langle \widehat{\mathcal{M}}^{\lambda}_{w}, \widehat{\mathcal{M}}^{\lambda}_{w} \rangle} \tag{4.69}$$

$$[\Omega^{-1}]_{w,w'} = \frac{\langle \widehat{\mathcal{M}}^{p}_{w}, \widehat{\mathcal{M}}^{\lambda}_{w'} \rangle}{\langle \widehat{\mathcal{M}}^{p}_{w}, \widehat{\mathcal{M}}^{p}_{w} \rangle}. \tag{4.70}$$

Thus the relationship between λ_w and $\Pr(w)$ is invertible, and it is explicitly given by the matrices Ω and Ω^{-1}.

The problem of computing the matrix elements of Ω and Ω explicitly appears daunting at first, as they are defined by inner products of the exponentially large matrices $\widehat{\mathcal{M}}^{\lambda}_{w}$ and $\widehat{\mathcal{M}}^{p}_{w}$. However, as this relationship is linear, one can choose convenient channels to infer the entries on the rows of Ω, and use (4.70) to compute the entries of Ω^{-1}. More explicitly, consider an $\mathcal{C}_1\Pi$ twirled channel with $\Pr(w') = 1$. For this channel $\lambda_w = [\Omega]_{w,w'}$, and λ_w can be computed by straightforwardly counting commutation and anti-commutations, as described in detail in Appendix E. One then finds the compact expressions

$$[\Omega]_{w,w'} = \left[\sum_{L=0}^{n} \frac{\binom{n-w}{w'-L}\binom{w}{L}}{\binom{n}{w'}} \frac{3^L + (-1)^L}{3^L} \right] - 1 \tag{4.71}$$

$$[\Omega^{-1}]_{w,w'} = \frac{3^{w+w'}\binom{n}{w}\binom{n}{w'}}{4^n} [\Omega]_{w,w'}. \tag{4.72}$$

This demonstrates that given the λ_w for any channel, it is possible to compute the $\Pr(w)$ efficiently.

4.4 Propagation of uncertainties

Using the same arguments from Section 4.2.2, the Chernoff bound can be applied to demonstrate that, for any given w, q_w and λ_w can be estimated with a number of samples which grows quadratically with the desired accuracy. Taking each experiment to be independent, the number of experimental trials necessary to estimate all $n+1$ different parameters is in the worse case linear in the number of qubits and quadratic in the error δ. This can be improved by considering *the union bound*. This bound states that the probability that any of the $n+1$ estimates are more than δ away from the true value is bounded above by the sum of the probabilities of each of the estimates being more than δ away from the true value. Using the union bound and the Chernoff bound together

allows us to finally conclude that the number of trials K necessary to estimate all the $n+1$ parameters to some desired accuracy is $K = O(\delta^{-2}\log(2n+1))$.

It is natural to ask with what confidence the $\Pr(w)$ can be estimated. For any given confidence interval for the parameters q_w or λ_w, the confidence interval for $\Pr(w)$ can be computed from the corresponding linear transformations. The scaling of the volume of this confidence interval under the action of the linear transformation can be used as a measure of how the uncertainties propagate. This scaling can be computed by the corresponding Jacobian of the transformation, which are just the determinant of the matrices R^{-1} and Ω^{-1}. The dependence of these determinants on the number of qubits n can then be used as a measure of the efficiency with which the $\Pr(w)$ can be estimated. Recall that confidence intervals are given as functions of the standard deviation of the estimates – so that the length of the confidence interval along one parameter scales as $O(1/\sqrt{K})$.

As R is upper triangular, its determinant is just the product of its diagonal elements [HJ85]. From the definition of R, we know that

$$[R]_{w,w} = \left(\frac{2}{3}\right)^{w}, \tag{4.73}$$

and therefore

$$|R^{-1}| = |R|^{-1} = \left(\frac{3}{2}\right)^{n(n+1)/2}. \tag{4.74}$$

Thus it is clear that any confidence region for $\{q_w\}$ with finite volume will lead to a confidence region of volume which is super-exponentially larger. In order to better understand the consequences of this scaling, take the uncertainty region to be hyper-cubic. In that case the ratio of the length of the sides of the corresponding hyper-cubes would be $\left(\frac{3}{2}\right)^{n/2}$, which scales exponentially with n. This is an indication that not all of the $\Pr(w)$ can be estimated from the q_w without requiring an exponential number of experiments. It is not clear if a closed form for $|\Omega^{-1}|$ can be obtained, but numerical calculations show that it also scales as $O(2^{n^2})$, and therefore the λ_w do not lead to fundamentally better estimates of the $\Pr(w)$.

However, it is important to note that R^{-1} and Ω^{-1} do not preserve the shape of hyper-cubic regions. These linear transformation distort the parameter space differently along different directions. In order to estimate how the uncertainty propagates along each each coordinate, we consider the scaling of the variance $\sigma^2_{\Pr(w)}$ of the estimates of $\Pr(w)$ as a function of n. Taking the estimates for the λ_w to have covariance $\mathrm{Cov}(\lambda_i, \lambda_j)$ we have

that

$$\sigma^2_{\Pr(w)} = \sum_{i,j} [\Omega^{-1}]_{w,i} [\Omega^{-1}]_{w,j} \mathrm{Cov}(\lambda_i, \lambda_j). \tag{4.75}$$

Note that the magnitude of the covariance between different estimates is bounded by the product of their standard deviations. If we then take the sign of the covariance to be the same as the sign of the product of the matrix elements, we arrive at the upper bound

$$\sigma^2_{\Pr(w)} \leq \sigma^2_\lambda \sum_{i,j} |[\Omega^{-1}]_{w,i} [\Omega^{-1}]_{w,j}|, \tag{4.76}$$

where we have taken all the λ_w estimates to have the same variance σ^2_λ. From the definition of the matrix elements, we have that $|[\Omega]_{w,i}| \leq 1$, so that

$$\sigma_{\Pr(w)} \leq \sigma_\lambda \, \frac{3^w}{4^n} \binom{n}{w} \sqrt{\sum_{i,j} \binom{n}{i} \binom{n}{j} 3^{i+j}}, \tag{4.77}$$

$$= \sigma_\lambda \, 3^w \binom{n}{w}, \tag{4.78}$$

$$\leq \sigma_\lambda \left(\frac{3}{w}\right)^w n^w \mathrm{e}^w \tag{4.79}$$

For fixed w, the scaling between the lengths of the confidence intervals is just a polynomial in n, of order w. However, for any given n, the scaling grows at most exponentially with w. While we have not been able to evaluate useful lower bounds for this quantity, numerical calculation indicate that the true scaling also grows as $O(n^w)$, as depicted in Figure 4.4. Similar results for the scaling of confidence intervals when the q_w are used to estimate the $\Pr(w)$.

While it is possible to estimate all the q_w and the λ_w of an n qubit channel efficiently, the precision necessary to infer the $\Pr(w)$ from these estimates would be exponential in w. This is not a barrier for the estimate of $\Pr(0)$, which can be used to estimate the average fidelity of the channel with the identity, as described in Section 4.2.2. In fact, it follows from the previous arguments that the variance of the estimate of $\Pr(0)$ is exactly the same as the variance of the λ_w, which is consistent with previous findings about the scalability of estimating the average fidelity.

The probability of other low weight error can also be estimated efficiently, for any maximal error weight which is independent of n. For quantum error correction codes that only correct a small number of errors, these probabilities can be used directly to estimate the probability of an uncorrectable error under the action of the twirled channel.

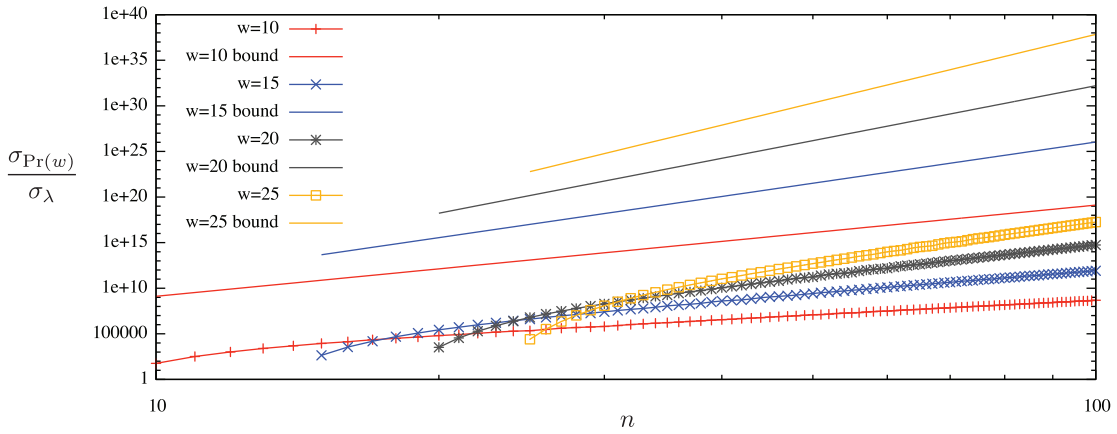

Figure 4.4: *Bounds and numerical values for the scaling factor $\sigma_{\Pr(w)}/\sigma_\lambda$ as a function of the number n of qubits and the weight w of the errors.*

4.4.1 Use of ancillary channels

In principle, it is possible to estimate the probabilities of different Pauli error directly, instead of attempting to infer them from different observables as we have done here. Given the Bell state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{4.80}$$

it is well known that the other Bell states can be obtained by local transformation

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \mathbb{1}_2 \otimes \sigma_z |\Psi^+\rangle \tag{4.81}$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \mathbb{1}_2 \otimes \sigma_X |\Psi^+\rangle \tag{4.82}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \mathbb{1}_2 \otimes \sigma_Y |\Psi^+\rangle, \tag{4.83}$$

where we have neglected unobservable global phases. Thus, if we let a twirled channel act on half of $|\Psi^+\rangle$, and then measure the two qubits in the Bell basis, we can obtain a direct estimate of the different Pauli errors. If the channel acts on multiple qubits, one can simply send half a Bell pair for each qubit input, and measure each pair separately. In fact, it can be shown that twirling is unnecessary in this scheme, and the diagonal elements of the χ matrix can be obtained by sending halves of the state $|\Psi^+\rangle$ across the channel, and measuring the pairs in the Bell basis [ML06]. The diagonal entries in the χ matrix may also be measured by using a single coherent ancilla which can interact with the system in a controlled fashion [BPP08]. Both these approaches allow for the $\Pr(w)$ to be estimated efficiently by sampling, but only under strong assumptions about

the noise in the ancillas. This is because in these approaches the protocol is not able to distinguish between errors in the ancilla or errors in the channel being characterized. When certain errors occur on both the ancillas and the system being characterized, the protocol can incorrectly infer that no error occurred. One would have to assume that the ancillary system is perfectly noiseless, and ascribe all observed errors to the system being characterized. The twirling protocol, on the other hand, requires no such assumptions.

4.5 Test for noise correlations

While there are limitations to which of the $\Pr(w)$ can be estimated efficiently, the other parameters such as λ_m can still provide valuable information. Although the familiar interpretation of probabilities is attractive, the λ_m can also provide information about correlations in the noise, without the explicit estimation of the $\Pr(w)$. In particular, the λ_w can be applied directly to test some of the assumptions that affect estimates of the fault-tolerance threshold [KLZ98, AGP06].

A noise model which is often assumed in these estimates is one in which the error locations are uncorrelated, but otherwise arbitrary – in other words, the environment is allowed to "choose" the types of errors which maximize the damage in the system, but not which qubits are affected by these errors. Under an $\mathcal{C}_1\Pi$ twirl, such a noise model is mapped to a n qubit depolarizing channel $\mathcal{D}_n$, which consists of identical single qubit depolarizing $\mathcal{D}_1$ channels acting on each qubit independently. Given the scaling λ_1 of a single qubit observable, the scaling of an observable of weight w is

$$\lambda_w = \lambda_1^w. \tag{4.84}$$

Hence, observed deviations from this scaling imply a violation of the above assumptions. Namely, violations of (4.84) can be taken as a sufficient condition for the presence of noise correlations. However, there are correlated distributions which also give rise to this scaling, so the converse implication does not hold.

In the case where the noise models acts with different intensity on each qubit, but still independently, a similar result holds. The main difference then would be that each qubit scales the Pauli observable differently, so that the overall scaling would be the product of the scaling of each qubit. The individual scaling for each qubit can then be measured and compared against the scaling for observables of weight two, and then weight three, and

so forth. This leads to an exponential number of conditions similar to (4.84), and while it would be inefficient to check all of them, they can still be individually used to test the assumptions of fault-tolerant quantum computation.

4.5.1 Collective versus independent relaxation of identical qubits

As a concrete example of noise correlations and how they can be distinguished by looking at the $\mathcal{C}_1\Pi$ twirled channel parameters, consider the problem of *energy relaxation*. This type of noise corresponds the energy of the system leaking out into the environment, which is usually modeled as a bath or harmonic oscillators weakly coupled to the qubit. Phenomenologically, it is known that the dominant source of noise in many physical implementations of quantum computers. In the eigenbasis of the qubit Hamiltonian $H_0 = -\frac{\delta}{2}\sigma_Z$, relaxation is characterized by a coupling of the form $\sigma_X\ x_i$, where σ_X acting on the qubit and x_i acts on the ith bath degree of freedom. This leads to bit-flip errors on the qubit in a manner such that the population of the excited state is depleted and the state converges to the ground state (assuming that the bath is at a zero temperature). In the interaction picture the state $\rho_I(t)$ of a single qubit undergoing relaxation can be described by the master equation [Blu96, BP02]

$$\frac{\partial}{\partial t}\rho_I(t) = \Gamma\left(\sigma^-\rho_I(t)\sigma^+ - \frac{1}{2}\sigma^+\sigma^-\rho_I(t) - \frac{1}{2}\rho(t)_I\sigma^+\sigma^-\right) \tag{4.85}$$

where $\sigma^\pm$ are the usual spin raising and lowering operators, and Γ is the rate at which energy is depleted. This master equation can be integrated to yield the time dependent superoperator $\mathcal{E}(t)$ with Kraus representation

$$\mathcal{E}(t)[\rho_I] = E_0(t)\rho_I E_0(t)^\dagger + E_1(t)\rho_I E_1(t)^\dagger \tag{4.86}$$

where, in the energy eigenbasis,

$$E_0(t) = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{e^{-\Gamma t}} \end{pmatrix} \tag{4.87}$$

$$E_1(t) = \begin{pmatrix} 1 & \sqrt{1-e^{-\Gamma t}} \\ 0 & 0 \end{pmatrix}. \tag{4.88}$$

Given this error model, one can estimate Γ by simply preparing the state in the excited states, allowing the system to relax for some time t, and then measuring the state of the

system to determine what is the probability of being in either the ground state or the excited state. We have that

$$\Pr(\text{excited state}) = e^{-\Gamma t} \tag{4.89}$$

$$\Pr(\text{ground state}) = 1 - e^{-\Gamma t}. \tag{4.90}$$

Similarly, one can twirl this relaxation superoperator and obtain the probabilities of error

$$\Pr(w=0) = \frac{1}{4}\left(1 + 2e^{-\frac{\Gamma t}{2}} + e^{-\Gamma t}\right) \tag{4.91}$$

$$\Pr(w=1) = \frac{1}{4}\left(3 - 2e^{-\frac{\Gamma t}{2}} - e^{-\Gamma t}\right). \tag{4.92}$$

If we consider now two qubits undergoing relaxation independently, this implies that if one were to twirl the relaxation superoperator over the $\mathcal{C}_1\Pi$ group, one would obtain the scaling parameters

$$\lambda_0 = 1 \tag{4.93}$$

$$\lambda_1 = \frac{1}{3}\left(2e^{-\frac{\Gamma_1 t}{2}} + e^{-\Gamma_1 t}\right) \tag{4.94}$$

$$\lambda_2 = \frac{1}{9}\left(2e^{-\frac{\Gamma_1 t}{2}} + e^{-\Gamma_1 t}\right)^2. \tag{4.95}$$

Clearly, there parameters satisfy the condition given by (4.84).

In the case of multiple qubits, relaxation can be significantly different. This is due to the possibility of correlations, which may be caused by multiple qubits being coupled the same mode of the environment through which energy leaks out. This is the case if identical qubits (with the same energy splitting) are coupled to the same bath. One of the consequences of collective relaxation is the presence of sub-radiance [Dic53], meaning that some states have an extended lifetime due to quantum interference. To see how this comes about, consider the master equation for collective relaxation of two qubits [DG98]

$$\begin{aligned}\frac{\partial}{\partial t}\rho_I(t) = \Gamma\Big[&\left(\sigma_1^- + \sigma_2^-\right)\rho_I(t)\left(\sigma_1^+ + \sigma_2^+\right) + \\ &-\frac{1}{2}\left(\sigma_1^+ + \sigma_2^+\right)\left(\sigma_1^- + \sigma_2^-\right)\rho_I(t) - \frac{1}{2}\rho_I(t)\left(\sigma_1^+ + \sigma_2^+\right)\left(\sigma_1^- + \sigma_2^-\right)\Big]\end{aligned} \tag{4.96}$$

where $\sigma_i^{\pm}$ are the pseudo-spin raising and lowering operators for qubit i (for simplicity we have assumed that both qubits relax at the same rate). In other words, we have that

$$\frac{\partial}{\partial t}\rho_I(t) = \mathcal{L}\rho_I(t), \tag{4.97}$$

with linear operator $\mathcal{L}$ defined implicitly by (4.96). Integrating this differential equation by considering the Liouville representation, we obtain

$$\rho_I(t) = e^{\mathcal{L}t}\rho_I(0). \tag{4.98}$$

Note however, that the singlet state $|01\rangle - |10\rangle$ is such that

$$\left(\sigma_1^- + \sigma_2^-\right)\left(|01\rangle - |10\rangle\right) = 0. \tag{4.99}$$

In other words this states is unaffected collective relaxation even though it is an excited state. This is an example of a sub-radiant state.

The parameters of the corresponding $\mathcal{C}_1\Pi$ twirled channel can be extracted from $e^{\mathcal{L}t}$ is the usual manner, and one obtains the scaling parameters

$$\lambda_0 = 1 \tag{4.100}$$

$$\lambda_1 = \frac{1}{6}\left(1 + 5e^{-\Gamma t} + \Gamma t e^{-2\Gamma t}\right) \tag{4.101}$$

$$\lambda_2 = \frac{1}{9}\left(2 + 3e^{-\Gamma t} + 4e^{-2\Gamma t} - \Gamma t e^{-\Gamma t}\right) \tag{4.102}$$

It is immediately clear that these eigenvalues violate the condition for independence since $\lambda_2 \neq \lambda_1^2$. Another notable feature is the fact that the eigenvalues do not vanish in the limit of infinite time. In particular, we have that

$$\lim_{t\to\infty} \lambda_1 = \frac{1}{6} \tag{4.103}$$

$$\lim_{t\to\infty} \lambda_2 = \frac{2}{9}. \tag{4.104}$$

This corresponds to the fact that not all states decay under collective relaxation. In particular, the populations of the singlet state does not decay at all, even though it is an excited state.

In order to visualize how the independence condition (4.84) is violated, consider all the possible values of λ_w for the independent and collective relaxation as depicted in Figure 4.5. In the case of collective relaxation, λ_2 is consistently higher than λ_1^2. The qualitative distinction between the two cases is best visualized by considering the time dependence of this parameters, as depicted in Figures 4.6 and 4.7. In the independent case, $\lambda_2 < \lambda_1$ at all times, while for the collective case, λ_2 crosses over λ_1 for long enough times, indicating that at least some two qubit Pauli observables are better preserved due to the correlations of the noise.

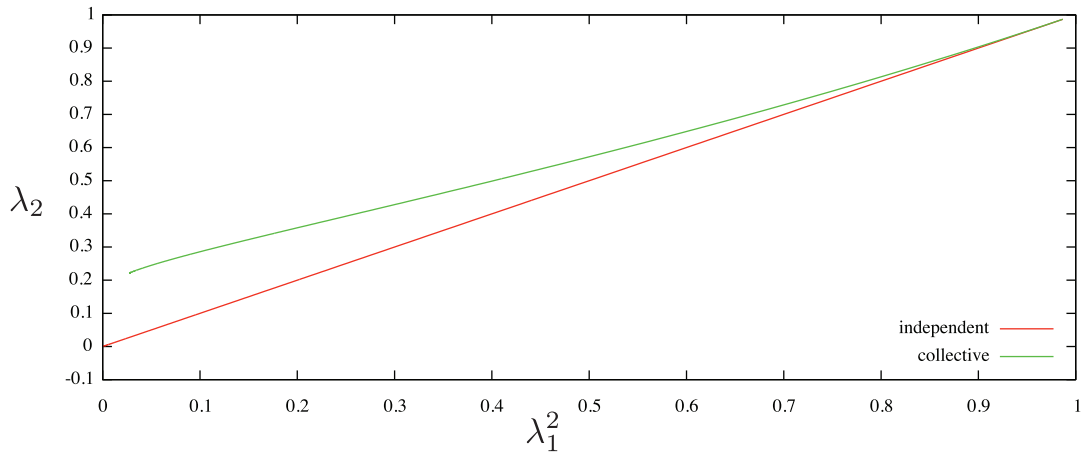

Figure 4.5: *Twirled channel parameters for collective and independent relaxation.*

4.6 Summary

In this chapter we have discussed the problem of characterization of noise in quantum devices, and presented an efficient protocol for the partial characterization of noise. In particular, we gave a detailed mathematical description of two experimental protocols that can be used to estimate the distribution of weights of Pauli errors affecting a quantum system.

While it was found that uncertainties in the estimates greatly limits how well this probability distribution can be estimated, we have demonstrated that the probabilities of error with low weight can always be estimated with a number of experiments which is only polynomial in the number of qubits. In particular, this allows for the estimation of the average fidelity of quantum states under the action of noise, but also for the estimate of the performance of certain error correcting codes.

Describing the noise by a different set of parameters, we also demonstrated that it is possible to test for a sufficient condition for the presence of correlations in the distribution of error locations. As the independence of error locations is a standard assumption in the construction of fault-tolerant quantum devices, this test is of direct practical relevance. Using these same ideas, we demonstrated how independent and collective relaxation can be distinguished by looking only at the parameters of the twirled channel.

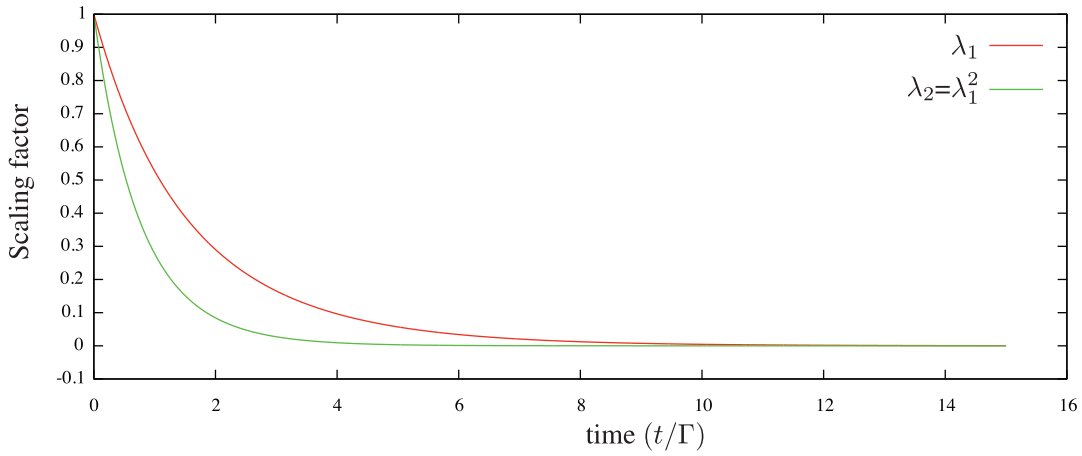

Figure 4.6: *Time dependence of the twirled channel parameters for independent relaxation.*

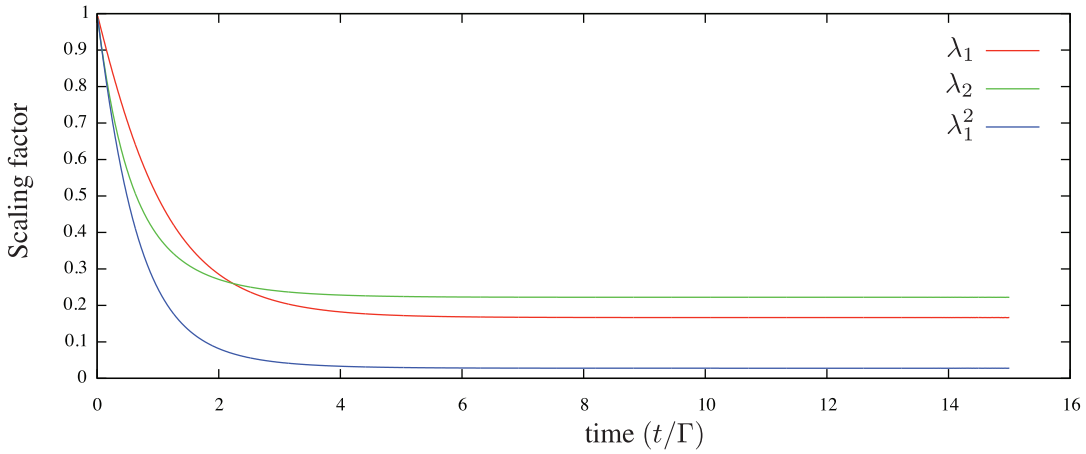

Figure 4.7: *Time dependence of the twirled channel parameters for collective relaxation.*

Chapter 5

Finding correctable encodings from experimental data

5.1 Introduction

The coherent experimental manipulation of quantum systems, and their application to various quantum information tasks, confronts significant limitations in the presence of noise, and in particular, decoherence. The discovery of quantum error correction codes enables methods for overcoming these limitations whenever the decoherence satisfies various well-defined sets of conditions. Specifically, the applicability of particular codes depends crucially on the details of the physical noise model affecting a particular system. The standard approach for experimentally characterizing the full noise model and then assessing the usefulness of a given code are costly procedures. Indeed, full quantum process tomography requires a number of experiments [CN97, Leu03, ML06] that grows exponentially with the number of subsystems, and the dimension growth of matrices involved in classical post-processing [Kri03, HKL04, RW05, FSW07, KSL07] is also exponential. These limitations make the standard approach infeasible for the kinds of quantum information systems required in practical applications. In this chapter we describe a general method that can be used to overcome these issues, and we apply the approach to an experimentally relevant class of noise models.

We focus on a particular type of twirl, the *Pauli twirl*, which has a number of special features that make finding noiseless and unitarily correctable encodings more tractable than the general case. First, in Section 5.2 we demonstrate how the partial information

obtained via a Pauli twirl can be accessed with only a polynomial number of experiments, making such experimental characterization strictly scalable. In Sections 5.3 and 5.4 we describe the types of encodings we are considering, as well as how they relate to the parameters of Pauli twirled channels. Then, in Section 5.5 we discuss how this partial information lends itself to an algebraic algorithm for finding correctable encodings. This new approach does not require the manipulation of exponentially large matrices. We also discuss in Section 5.6 how these encodings are robust against experimental uncertainties, and how their performance can be can be verified experimentally in an efficient manner by using the techniques described in the previous chapter. We conclude in Section 5.7 by showing how, in general, *partial information about the noise, obtained via unitary twirls, can be sufficient to construct correctable encodings*. This result is independent of the details of the unitary twirl, and is motivated by the fact that valuable partial information about the noise can efficiently be extracted by twirling a quantum channel [BDSW96, DLT02, Cha05, DCEL06, ESM+07], as discussed in the previous chapter.

5.2 Pauli Twirl

Quantum operations require $O(2^{4n})$ parameters to be fully described, and thus require an exponential number of experiments to be fully characterized [CN97, Leu03, ML06]. Due to this exponential cost, it is impractical to obtain a complete description about noise and decoherence acting on even a moderately large system of qubits. In the previous chapter, we demonstrated how useful partial information about the noise can be obtained by averaging the action of the quantum operation under the composition $\mathcal{U} \circ \Lambda \circ \mathcal{U}^\dagger$ for unitary operations $\mathcal{U}(\rho) = U\rho U^\dagger$ randomly chosen according to some distribution [DCEL06, ESM+07]. This averaging is known as a "twirl", and the averaged channel $\overline{\Lambda}(\rho) = \int d\mu(\mathcal{U})\mathcal{U} \circ \Lambda \circ \mathcal{U}^\dagger(\rho)$ is known as the "twirled channel". The case where the distribution over unitaries is discrete is of particular interest. In that case, the twirled channel is given by $\overline{\Lambda}(\rho) = \sum \Pr(\mathcal{U}_i)\mathcal{U}_i \circ \Lambda \circ \mathcal{U}_i^\dagger(\rho)$, where $\Pr(\mathcal{U}_i)$ is a probability distribution over the $\mathcal{U}_i$.

We also have seen that twirling a channel Λ by the Pauli group $\mathcal{P}_n$ yields the effective channel $\overline{\Lambda}$ of the form

$$\overline{\Lambda}_{\mathcal{P}_n}(\rho) = \frac{1}{4^n} \sum_{P_i \in \mathcal{P}_n} P_i \Lambda(P_i \rho P_i) P_i = \sum_i [\chi]_{ii} P_i \rho P_i. \tag{5.1}$$

In other words, the off-diagonal elements of χ are eliminated. Channels of this form are known as *Pauli channels*. Pauli channels have a number of useful properties which facilitate the search for some types of correctable codes. However, the description of a general Pauli channel still requires an exponential number of parameters, as there are 4^n different Pauli operators acting on n qubits. Such parameters are not realistically accessible due to this exponential overhead. Instead, one can consider an additional twirl by the group Π_n consisting of all qubit permutations. This uniformly distributed probability mass across all Pauli operators which are equivalent up to permutation. The channel $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ resulting from a combination of a $\mathcal{P}_n$ twirl and a Π_n twirl is what we call a *permutation invariant Pauli* (PIP) channel. Such channels can be written in terms of Choi-Kraus operators

$$\overline{\Lambda}_{\mathcal{P}_n\Pi}(\rho) = \sum_{\mathbf{w}} p_{\mathbf{w}} \frac{1}{K_{\mathbf{w}}^{\nu}} \sum_{\nu_{\mathbf{w}}} \frac{1}{K_{\nu_{\mathbf{w}}}^{\mathbf{i}}} \sum_{\mathbf{i}_{\mathbf{w}}} P_{w,\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}} \rho P_{w,\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}, \tag{5.2}$$

where $\mathbf{w} = (w_x, w_y, w_z)$ labels the number of the σ_X, σ_Y and σ_Z Pauli operators in the tensor decomposition of $P_{w,\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$, $\nu_{\mathbf{w}}$ labels the $w_x + w_y + w_z$ qubits over which $P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$ acts non-trivially, and $\mathbf{i}_{\mathbf{w}}$ labels which single qubit Pauli operator act on each of the qubits.

The number K_n of different labels $\mathbf{w}$ is computed in Appendix D to be

$$K_n = \frac{1}{6}n^3 + n^2 + \frac{11}{6}n + 1 \tag{5.3}$$

demonstrating that the number of parameters needed to describe an n qubit PIP channel scales well with n.

For a fixed $\mathbf{w}$ there are $K_{\mathbf{w}}^{\nu} = \binom{n}{w_x+w_y+w_z}$ different $\nu_{\mathbf{w}}$, and for fixed $\mathbf{w}$ and $\nu_{\mathbf{w}}$, there are $K_{\nu_{\mathbf{w}}}^{\mathbf{i}} = \binom{w_x+w_y+w_z}{w_x}\binom{w_y+w_z}{w_z}$ different $\mathbf{i}_{\mathbf{w}}$. These parameters need not be estimated in the experiment, as they are fixed for all PIP channels, and thus their abundance has no bearing on the efficiency of experimental characterization of such channels.

Two equivalent descriptions of the channel (with the same number of parameters) are the Choi-Kraus decomposition and the diagonal representation. The Choi-Kraus decomposition (5.2) can be rewritten as

$$\overline{\Lambda}_{\mathcal{P}_n\Pi}(\rho) = \sum_{\mathbf{w}} p_{\mathbf{w}} \mathcal{M}_{\mathbf{w}}^{p}(\rho), \tag{5.4}$$

where $\mathcal{M}_{\mathbf{w}}^{p}$ are the superoperators

$$\mathcal{M}_{\mathbf{w}}^{p}(\rho) = \frac{1}{K_{\mathbf{w}}^{\nu}} \sum_{\nu_{\mathbf{w}}} \frac{1}{K_{\nu_{\mathbf{w}}}^{\mathbf{i}}} \sum_{\mathbf{i}_{\mathbf{w}}} P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}} \rho P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}. \tag{5.5}$$

The $\mathcal{M}^p_{\mathbf{w}}$ are trace-preserving channels which apply each of the $P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$ for a given $\mathbf{w}$ with the same probability. The $\mathcal{M}^p_{\mathbf{w}}$ form a basis for PIP channels.

Recall that, given some n-fold tensor product of Pauli operators $P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$, we have $\overline{\Lambda}_{\mathcal{P}_n\Pi}(P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}) = \lambda_{\mathbf{w}} P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}$ for some real constant $\lambda_{\mathbf{w}} \in [-1,1]$, since Pauli operators either commute or anti-commute. Moreover $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ is self-dual; i.e. $\overline{\Lambda}_{\mathcal{P}_n\Pi} = \overline{\Lambda}^{\dagger}_{\mathcal{P}_n\Pi}$, a fact that follows directly from the fact that Pauli operators are Hermitian. Since the $\{P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\}$ form an operator basis, it follows that the scaling factors $\lambda_{\mathbf{w}}$ are in fact the the eigenvalues of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$, with high degeneracy, as they depend only on $\mathbf{w}$. Thus, Pauli channels are diagonalizable and Hermitian.

Just as we did with $\mathcal{C}_1\Pi$ twirled channels, we can describe a PIP channel in terms of its eigenoperators as

$$\overline{\Lambda}_{\mathcal{P}_n\Pi}(\rho) = \sum_{\mathbf{w}=0}^{n} \lambda_{\mathbf{w}} \mathcal{M}^{\lambda}_{\mathbf{w}}(\rho), \tag{5.6}$$

where $M^{\lambda}_{\mathbf{w}}$ are the superoperators with Liouville representation

$$\widehat{\mathcal{M}}^{\lambda}_{\mathbf{w}}(\rho) = \frac{1}{2^n} \sum_{\nu_{\mathbf{w}}} \sum_{\mathbf{i}_{\mathbf{w}}} |P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\rangle\rangle\langle\langle P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}|\rho. \tag{5.7}$$

This diagonal description of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ allows for straightforward description of the composition of channels. For example, suppose two PIP channels $\overline{\Lambda}_{\mathcal{P}_n\Pi}{}^{(1)}$ and $\overline{\Lambda}_{\mathcal{P}_n\Pi}{}^{(2)}$ are composed to yield $\overline{\Lambda}_{\mathcal{P}_n\Pi}{}^{(1)} \circ \overline{\Lambda}_{\mathcal{P}_n\Pi}{}^{(2)}$. This simply translates to the multiplication of the corresponding eigenvalues for each of the two channels because all Pauli channels commute.

It is crucial to note that, because there is at most a polynomial number of different eigenvalues, they can be estimated efficiently by determining how a Pauli observable in a $\mathbf{w}$ class is scaled under the action of the twirled channel. This is done in a manner closely related to the characterization of $\mathcal{C}_1\Pi$ twirled channels using the parity monitoring protocol described in Section 4.3.2. Due to the degeneracy of $\mathcal{C}_1\Pi$ twirled channels, the equivalence classes of Pauli observables are distinguished only by the weight of the operators they contain. For this reason, when characterizing $\mathcal{C}_1\Pi$ twirled channels it is sufficient to measure only tensor products of σ_Z operators acting on n different qubits, which corresponds to measuring the parity of n different qubits. It is also sufficient to prepare the state $|0\rangle^{\otimes n}$, which has maximal expectation for any tensor product of σ_Z. In the case of PIP channels, it is necessary to measure observables which act with σ_X on w_x different qubits, σ_Y on w_y different qubits and σ_Z on w_z different qubits. Moreover, it is

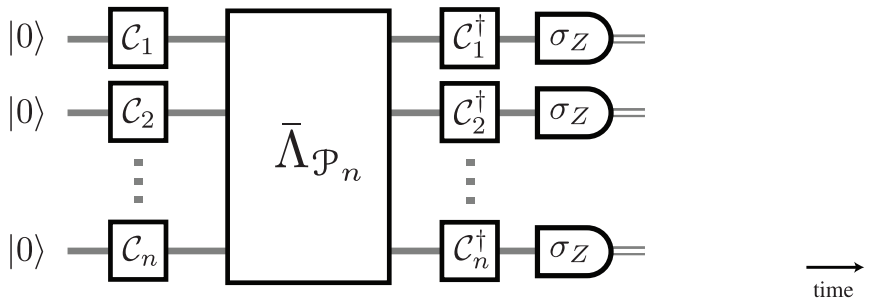

Figure 5.1: *Circuit diagram for the characterization of a PIP channel, where* $\mathcal{C}_i \in \mathcal{C}_1$.

also necessary to prepare a state which is guaranteed to have non-zero expectation value for these observables. These observables are equivalent to a tensor product of σ_Z under conjugation by unitaries in ${\mathcal{C}_1}^{\otimes n}$, and thus the necessary state which maximizes the expectation value is equivalent to $|0\rangle^{\otimes n}$ up to the action of the same unitary. By choosing a random subset of qubits, the local Clifford operations determine which Pauli observable are measured, and the parity of the binary measurement outcomes determines whether the result is a $+$ or $-$ eigenvalue of the observable. The circuit necessary to perform this characterization is depicted in Figure 5.1. Once again, it is not necessary to apply random qubit permutations as long as information about the qubit positions is discarded.

Notice that, in effect, we end up applying exactly the same operations as if we were characterizing an $\mathcal{C}_1\Pi$ twirled channel. The only difference is how the data is post-processed: for $\mathcal{C}_1\Pi$ twirled channels we average the data over $\mathcal{C}_1\Pi$ operations, while for PIP channels we distinguish outcomes based on what ${\mathcal{C}_1}^{\otimes n}$ operation is applied.

5.3 Unitarily Correctable Codes

We use the general definition for a quantum error correcting subsystem code [KLP05]: If A and B are subsystems of a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \oplus \mathcal{H}_K$, and we have some channel $\Lambda : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, then $\mathcal{H}_A$ is *correctable* for Λ if there is a recovery operation $\mathcal{R}$ acting on $\mathcal{B}(\mathcal{H})$ such that $\forall \rho_A \in \mathcal{B}(\mathcal{H}_A)$ and $\forall \rho_B \in \mathcal{B}(\mathcal{H}_B)$ there exists a $\tau_B \in \mathcal{B}(\mathcal{H}_B)$ for which $(\mathcal{R} \circ \Lambda)(\rho_A \otimes \rho_B) = \rho_A \otimes \tau_B$. Using these definitions, we can state a general fact about error correction codes.

Fact — If $\mathcal{R}$ is a operation recovering $\mathcal{H}_A$ from the action of $\Lambda(\rho) = \sum_k A_k \rho A_k^\dagger$, then $\mathcal{R}$ also recovers $\mathcal{H}_A$ from the action of any channel with Kraus operators in the

linear span of $\{A_k\}$ [NC00, KLP05, NP07].

Corollary 1 — A correctable subsystem $\mathcal{H}_A$ for the PIP channel $\overline{\Lambda}_\Pi$ with recovery $\mathcal{R}$ is also a correctable subsystem for the original channel Λ with the same recovery operation.

This follows immediately from the fact that the Pauli operators $\mathcal{P}_n$ form an operator basis, and so the Kraus operators $\{A_k\}$ of Λ are in the linear span of the Kraus operators of $\overline{\Lambda}_\Pi$. This result will be generalized in Section 5.7.

A special type of code we consider is one for which a unitary recovery operation $\mathcal{R} = \mathcal{U}$ can be found. That is, $\mathcal{H}_A$ defines a correctable encoding for Λ that can be returned to its initial location within the system Hilbert space with a single unitary operation. The problem of finding such *unitarily correctable codes* (UCC) for a unital channel is equivalent to finding the structure of the commutant of the noise algebra of $\Lambda^\dagger \circ \Lambda$ [KS06]. In terms of the Choi-Kraus operators $\{A_k\}$ for Λ, this "noise commutant" is defined as the set of operators that commute with the operators $\{A_k^\dagger A_j\}$. If Λ is unital and trace preserving, this commutant coincides with the *fixed point set* of $\Lambda^\dagger \circ \Lambda$ (the set of operators which are invariant under the action of this composed channel) [HKL04] – in essence, $\Lambda^\dagger$ can act as the recovery operation. This result can be refined somewhat for diagonalizable channels.

Proposition 1 — Let Λ be a unital, diagonalizable and trace preserving channel with eigenvalues λ_i and eigenoperators L_i. Then, the noise commutant of $\Lambda^\dagger \circ \Lambda$ is the space spanned by eigenoperators L_i with eigenvalues $|\lambda_i| = 1$.

Proof: Λ is unital and trace preserving, thus so is $\Lambda^\dagger \circ \Lambda$. Moreover, Λ is diagonalizable, so $\Lambda^\dagger \circ \Lambda$ has eigenoperators L_i with eigenvalues $\lambda_i^* \lambda_i = |\lambda_i|^2$, where the λ_i are the eigenvalues of Λ. Since $\Lambda^\dagger \circ \Lambda$ is unital, its fixed point set and its noise commutant coincide, and both are given by the space spanned by the eigenoperators L_i with $|\lambda_i|^2 = 1$. □

This result allows us to relate the parameters of a channel Λ that can be characterized by experiments, to the parameters of the formal construct $\Lambda^\dagger \circ \Lambda$ which can be used to find correctable encodings.

Pauli channels are unital channels, and since they are diagonalizable and Hermitian, these channels have a particularly simple fixed-point set structure. In particular, we immediately obtain the following result.

Corollary 2 — Let Λ be a Pauli channel. Then the noise commutant of $\Lambda^\dagger \circ \Lambda$ is the space spanned by the eigenoperators of Λ with eigenvalues ± 1.

We say that a UCC code is *unitarily noiseless* (UNC) for Λ if it is a UCC of Λ^n for all $n \geq 1$, where Λ^n is the channel Λ composed with itself n times [BKNPV07]. This includes, for instance, codes for which the recovery operation has the special form $\mathcal{U} = \mathcal{U}_A \otimes \mathcal{R}_B$; that is, a unitary acting only on the subsystem in which information is preserved, and an arbitrary quantum channel on subsystem B. Interestingly, the sets of UCC and UNC codes coincide for Pauli channels.

Corollary 3 — A UCC of a Pauli channel Λ is also a UNC.

Proof: As Λ is a Pauli channel, it commutes with its dual $\Lambda^\dagger = \Lambda$ which is also a Pauli channel, and thus we have that $(\Lambda^n)^\dagger \circ \Lambda^n = (\Lambda^\dagger \circ \Lambda)^n$. Since the eigenvalues of Λ are real, this implies that the fixed point set of $\Lambda^\dagger \circ \Lambda$ is identical to the fixed point set of $(\Lambda^n)^\dagger \circ \Lambda^n$. □

5.4 PIP channel parameter space

Considering the Liouville representation of the superoperators $\{\mathcal{M}^p_{\mathbf{w}}\}$ and $\{\mathcal{M}^\lambda_{\mathbf{w}}\}$

$$\widehat{\mathcal{M}}^p_{\mathbf{w}} = \frac{1}{K^\nu_{\mathbf{w}}} \sum_{\nu_{\mathbf{w}}} \frac{1}{K^{\mathbf{i}}_{\nu_{\mathbf{w}}}} \sum_{\mathbf{i}_{\mathbf{w}}} P^*_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}} \otimes P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}, \tag{5.8}$$

$$\widehat{\mathcal{M}}^\lambda_{\mathbf{w}} = \sum_{\nu_{\mathbf{w}}} \sum_{\mathbf{i}_{\mathbf{w}}} |P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}\rangle\!\rangle \langle\!\langle P_{\mathbf{w},\nu_{\mathbf{w}},\mathbf{i}_{\mathbf{w}}}|. \tag{5.9}$$

Following the techniques described in the previous chapter, it is clear that there is a linear invertible map Ω taking the $p_{\mathbf{w}}$ to the $\lambda_{\mathbf{w}}$. More explicitly, we have that

$$\lambda_{\mathbf{w}} = \sum_{\mathbf{v}} [\Omega]_{\mathbf{w},\mathbf{v}} p_{\mathbf{v}} \qquad [\Omega]_{\mathbf{w},\mathbf{v}} = \frac{\langle \widehat{\mathcal{M}}^\lambda_{\mathbf{w}}, \widehat{\mathcal{M}}^p_{\mathbf{v}} \rangle}{\langle \widehat{\mathcal{M}}^\lambda_{\mathbf{w}}, \widehat{\mathcal{M}}^\lambda_{\mathbf{w}} \rangle}, \tag{5.10}$$

where $\langle \cdot, \cdot \rangle$ is the Hilbert-Schmidt inner product in the Liouville representation. This follows directly from the fact that each Pauli belongs to a single weight class $\mathbf{w}$, and the set $\mathcal{P}_n$ is orthonormal under the Hilbert-Schmidt inner product. Therefore, $\langle \widehat{\mathcal{M}}^\lambda_{\mathbf{w}}, \widehat{\mathcal{M}}^\lambda_{\mathbf{v}} \rangle = \delta_{\mathbf{w},\mathbf{v}} \langle \widehat{\mathcal{M}}^\lambda_{\mathbf{w}}, \widehat{\mathcal{M}}^\lambda_{\mathbf{w}} \rangle$. Similarly, because $\langle \widehat{\mathcal{M}}^p_{\mathbf{w}}, \widehat{\mathcal{M}}^p_{\mathbf{v}} \rangle = \delta_{\mathbf{w},\mathbf{v}} \langle \widehat{\mathcal{M}}^p_{\mathbf{w}}, \widehat{\mathcal{M}}^p_{\mathbf{w}} \rangle$, we have

$$p_{\mathbf{w}} = \sum_{\mathbf{v}} [\Omega^{-1}]_{\mathbf{w},\mathbf{v}} \lambda_{\mathbf{v}} \qquad [\Omega^{-1}]_{\mathbf{w},\mathbf{v}} = \frac{\langle \widehat{\mathcal{M}}^p_{\mathbf{w}}, \widehat{\mathcal{M}}^\lambda_{\mathbf{v}} \rangle}{\langle \widehat{\mathcal{M}}^p_{\mathbf{w}}, \widehat{\mathcal{M}}^p_{\mathbf{w}} \rangle}. \tag{5.11}$$

As the set of all probability distributions is convex, with vertices at $p_{\mathbf{w}} = 1$ for each of the $\mathbf{w}$, the set of valid $\{p_{\mathbf{w}}\}$ forms a $K_n - 1$ standard simplex called *the probability simplex*. As the eigenvalues $\{\lambda_{\mathbf{w}}\}$ are related to the probabilities $\{p_{\mathbf{w}}\}$ by a simple linear transformation, the set of valid eigenvalues also forms a $K_n - 1$ simplex, which we call *the eigenvalue simplex*. The set of all possible different fixed-point sets for a PIP channel can be computed directly from this fact, by investigating the points in the eigenvalue simplex which have coordinates of magnitude 1.

5.4.1 The map between probabilities and eigenvalues

As in the case of $\mathcal{C}_1\Pi$ twirled channels, direct computation of the entries of Ω from the matrix elements of a Liouville representation for a superoperator is inefficient, as these representations have dimensions exponentially large in n. However, as before, one can consider a set of extremal channels corresponding to the distribution $p_{\mathbf{v}} = 1$ for each of the weight classes $\mathbf{v}$, and compute how a particular operator for each of the weight classes $\mathbf{w}$ gets scales. This leads to

$$[\Omega]_{\mathbf{v},\mathbf{w}} = \frac{N_c(\mathbf{v},\mathbf{w}) - N_a(\mathbf{v},\mathbf{w})}{N_c(\mathbf{v},\mathbf{w}) + N_a(\mathbf{v},\mathbf{w})} = 2\frac{N_c(\mathbf{v},\mathbf{w})}{4^n} - 1, \tag{5.12}$$

where $N_c(\mathbf{v},\mathbf{w})$ is the number of operators of weight class $\mathbf{v}$ which commute with any given operator of weight class $\mathbf{w}$ (and $N_a(\mathbf{v},\mathbf{w})$ is similarly defined, but counting operators which anti-commute). The complete expression is given in Appendix E.

5.5 Finding Correctable Codes

The fixed points of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ can be thought of as the observables that are conserved under the action of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ in the Heisenberg picture, as $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ is self-dual. Once the fixed points of these channels are determined, in order to determine possible encodings one needs to compute the possible operator algebras generated by these fixed points. Note that, because of the degeneracy of the eigenvalues of a PIP channel, the existence of a single weight class with eigenvalue 1 corresponds to a large number of Pauli operators which are fixed points of the channel. More explicitly, for a weight class $\mathbf{w} = (w_x, w_y, w_z)$ over n qubits, there are

$$\binom{n}{w_x + w_y + w_z}\binom{w_x + w_y + w_z}{w_x}\binom{w_y + w_z}{w_y} \tag{5.13}$$

different Pauli operators.

The identification of the fixed point set of a unital channel can be used to find a UCC using the general algorithms described in Refs. [HKL04, Kri03, KS06]. However, these algorithms requires the manipulation of exponentially large matrices, a problem shared with numerical algorithms used to search for more general codes in a broader class of channels [RW05, FSW07, KSL07]. Since the Pauli operators form an eigenbasis for PIP channels, the task of computing the algebra of conserved observables is relatively simpler than in the general case. One simply has to group the conserved Pauli observables into triplets of observables which satisfy the commutation relations

$$[\sigma_j, \sigma_k] = 2i\epsilon_{jkl}\sigma_l, \tag{5.14}$$

for the Lie algebra $su(2)$, as these can be taken as the generators of the Pauli group.

These commutation relations can be computed without writing the observables explicitly in a particular representation. Instead, one observes that any two of $\{\mathbb{1}, \sigma_X, \sigma_Y, \sigma_Z\}$ either commute or anti-commute. Tensor products of these operators will commute if they anti-commute at an even number of different locations, thus it is sufficient to investigate the tensor product decomposition of the Pauli operators in order to determine their commutation relations. A set S of mutually exclusive triplets which commute with each other implicitly describes how to encode a noiseless Hilbert space of dimension $2^{|S|}$.

Another way to think about about this problem is to consider the fact that Pauli operators form a basis for operators. The description of what the basis elements get mapped to under a unitary is nothing but the description of a concrete representation of this unitary. As we are only concerned with constraining how a few of the elements gets mapped – *i.e.* how the Pauli operators acting on $|S|$ qubits get mapped to Pauli operators in the fixed-point set of the channel – we have some freedom in choosing how the remaining operators are transformed. The search can be restricted to the generators of the Pauli group because the group structure is preserved under unitary transformation. That is, $P_iP_j = P_k$ if and only if $UP_iU^\dagger UP_jU^\dagger = UP_kU^\dagger$ for any unitary U.

The search for triplets can be simplified by noting the following result, which can be obtained by direct computation.

Proposition 2 — Given Pauli operators $\{P_j, P_k, P_l\}$ satisfying the commutation relations $[P_j, P_k] = 2i\sum_l \tilde{\epsilon}_{jkl}P_l$, where $\tilde{\epsilon}_{jkl} = \epsilon_{jkl}\frac{s_l}{s_js_k}$, ϵ_{jkl} is the Levi-Civita symbol and $s_j, s_k, s_l \in \{\pm 1, \pm i\}$, then $\{s_jP_j, s_kP_k, s_lP_l\}$ obey the $su(2)$ commutation relations.

It is clear that $\{s_j P_j, s_k P_k, s_l P_l\}$ are unitarily related to $\{\sigma_X, \sigma_Y, \sigma_Z\}$, as all Pauli operators have the same spectrum and Proposition 2 guarantees they have the same commutation relations. The unitary which performs the encoding is guaranteed to be in the Clifford group, since it maps a set of Pauli operators to another set of Pauli operators with the same commutation relations. Using the techniques in [Got98a, AG04], this mapping of the generator set of the Pauli group can be used to obtain an explicit gate decomposition of the encoding unitary in terms the generators of the Clifford group. The length of this gate sequence, as well as the number of time steps necessary to obtain it, is polynomial in the number of qubits.

This leads to the following algorithm for finding a correctable encoding given the eigenvalues of the PIP channel $\overline{\Lambda}_{\mathcal{P}_n\Pi}$: (i) Enumerate the Pauli operators with eigenvalues 1 under the action of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$, and call this set F. (ii) Choose a triplet of Pauli operators in F satisfying the commutation relations in Proposition 2 – if none can be found, the search is over. (iii) Remove this triplet from F, and add them to S. Also remove from F all operators that do not commute with the operators in this triplet, and go back to step (ii). The number of mutually exclusive triplets found in this manner corresponds to an allowable number of encoded qubits which can be protected from the action of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$.

Finding unitarily correctable codes is similarly simple. One can easily compute the observables preserved by the action of the channel $\overline{\Lambda}^{\dagger}_{\mathcal{P}_n\Pi} \circ \overline{\Lambda}_{\mathcal{P}_n\Pi}$ [KS06]. In the case of PIP channels, this corresponds to finding observables with eigenvalue ± 1 for the channels $\overline{\Lambda}_{\mathcal{P}_n\Pi}$, so that these observables have eigenvalue 1 for $\overline{\Lambda}^{\dagger}_{\mathcal{P}_n\Pi} \circ \overline{\Lambda}_{\mathcal{P}_n\Pi} = \overline{\Lambda}^{2}_{\mathcal{P}_n\Pi}$. The same procedure described above can be applied to the ± 1 eigenspace to find a correctable encoding.

Example 1 — Consider the 2 qubit PIP channel with Kraus operators proportional to $\{\mathbb{1}_2\mathbb{1}_2, \sigma_Z\sigma_Z\}$. The Pauli operators with eigenvalue 1 are $\{\mathbb{1}_2\mathbb{1}_2, \sigma_X\sigma_X, \sigma_Y\sigma_Y, \sigma_Z\sigma_Z, \sigma_X\sigma_Y, \sigma_Y\sigma_X, \mathbb{1}_2\sigma_Z, \sigma_Z\mathbb{1}_2\}$. Out of this set, $\{\sigma_X\sigma_X, \sigma_X\sigma_Y, \mathbb{1}_2\sigma_Z\}$ satisfy the commutation relations, and no other triplets which commute with these can be found, so a single qubit can be encoded noiselessly through this channel. □

Example 2 — Consider the 2 qubit PIP channel with Kraus operators proportional to $\{\mathbb{1}_2\mathbb{1}_2, \sigma_Y\sigma_X, \sigma_X\sigma_Y\}$. The eigenoperators with eigenvalue 1 are $\{\mathbb{1}_2\mathbb{1}_2, \sigma_X\sigma_Y, \sigma_Y\sigma_X, \sigma_Z\sigma_Z\}$. There are no triplets with the right commutation relations. The eigenoperators with eigenvalues -1 are $\{\mathbb{1}\sigma_Z, \sigma_Z\mathbb{1}_2, \sigma_X\sigma_X, \sigma_Y\sigma_Y\}$. If we consider the ± 1 eigenspace, we obtain the same eigenoperators with eigenvalue 1 as the previous example, and thus there exists a UCC consisting of a single qubit. □

In the case of the previous examples, we want to map the generating set of Pauli operators $\{\mathbb{1}_2\sigma_X, \mathbb{1}_2\sigma_Z\}$ to the generating set $\{\sigma_X\sigma_X, \mathbb{1}_2\sigma_Z\}$, which can be done by a CNOT gate, where the second qubit is the control, and the first qubit is the target.

While it is possible to consider all the possible fixed-point sets for PIP channels by investigating the structure of the eigenvalues simplex, the question as to whether this algorithm can find all unitarily correctable encodings for an arbitrary PIP channel remains open.

5.6 Verification and Robustness of UCC

All experimental data contains some degree of uncertainty, due to either a finite number of sample or the finite precision of instruments – one can never conclude with certainty that a true fixed point has been observed, as the estimated eigenvalue will always have some associated uncertainty. The conditions for error correction are known to be robust against perturbations [SW01, Kle07], and a similar result applies to the scheme presented here. Formally, we can say that the eigenvalues $\lambda^2_{\mathbf{w}}$ for the channel $\overline{\Lambda}^2_{\mathcal{P}_n\Pi} = \overline{\Lambda}^\dagger_{\mathcal{P}_n\Pi} \circ \overline{\Lambda}_{\mathcal{P}_n\Pi}$ are such that

$$\lambda^2_{\mathbf{w}} \in [\tilde{\lambda}^2_{\mathbf{w}} - \delta_{\mathbf{w}}, \tilde{\lambda}^2_{\mathbf{w}} + \delta_{\mathbf{w}}] \tag{5.15}$$

where $\tilde{\lambda}_w$ are the experimental estimates, and δ_w corresponds to the uncertainty for some desired confidence level. We focus on the eigenvalues of $\overline{\Lambda}^2_{\mathcal{P}_n\Pi}$ because these are the quantities used to find a larger class of codes, as discussed in the previous section. Under the constraints of the parameters space discussed in Section 5.4, we can then find a valid PIP channel $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ with eigenvalues $\lambda_{\mathbf{w}}$ inside the interval given by (5.15).

Say that the generator for the encoded Pauli group over m qubits can then be found from the fixed-point sets for $\overline{\Lambda}^2_{\mathcal{P}_n\Pi}$ – in other words, we have m triplets of Pauli operators which are taken to be Pauli operators for m different encoded qubits. As the $\lambda^2_{\mathbf{w}}$ are only estimates, we have that the eigenvalues for these generators have a lower bound

$$\lambda^2_{\mathbf{w}} \geq 1 - \epsilon, \tag{5.16}$$

which is given by the confidence intervals. Consider now a product of any two of these generators, which we label Q and R. The eigenvalue corresponding to the product of these two operators can be computed from the probability that a Pauli error in $\overline{\Lambda}^2_{\mathcal{P}_n\Pi}$ commutes with either Q or R. More formally, if we write the probability that an error in

$\overline{\Lambda}^2_{\mathcal{P}_n\Pi}$ commutes with Q as $\Pr([Q,E])$, and similarly for anti-commutation, then we have that

$$\lambda^2(QR) = \Pr([QR,E]) - \Pr(\{QR,E\}), \tag{5.17}$$

$$\Pr([QR,E]) = \Pr([R,E] \text{ and } [Q,E]) + \Pr(\{R,E\} \text{ and } \{Q,E\}), \tag{5.18}$$

$$\Pr(\{QR,E\}) = \Pr([R,E] \text{ and } \{Q,E\}) + \Pr(\{R,E\} \text{ and } [Q,E]). \tag{5.19}$$

It is then possible to compute a lower bound for $\lambda^2(QR)$ by placing a lower bound on $\Pr([QR,E])$ and an upper bound on $\Pr(\{QR,E\})$. As the eigenvalue of Q is

$$\lambda^2(Q) = \Pr([Q,E]) - \Pr(\{Q,E\}) > 1-\epsilon, \tag{5.20}$$

we have that

$$\Pr([Q,E]) > 1 - \frac{\epsilon}{2}, \tag{5.21}$$

$$\Pr(\{Q,E\}) < \frac{\epsilon}{2}, \tag{5.22}$$

and similarly for R. We then find that

$$\Pr([R,E] \text{ and } [Q,E]) > 1 - \frac{\epsilon}{2} \tag{5.23}$$

$$\Pr(\{R,E\} \text{ and } \{Q,E\}) < \frac{\epsilon}{2} \tag{5.24}$$

$$\Pr([R,E] \text{ and } \{Q,E\}) < \frac{\epsilon}{2} \tag{5.25}$$

$$\Pr(\{R,E\} \text{ and } [Q,E]) < \frac{\epsilon}{2} \tag{5.26}$$

and therefore we obtain the lower bound

$$\lambda^2(QR) > 1 - \frac{3}{2}\epsilon > 1 - 2\epsilon. \tag{5.27}$$

In order to obtain a similar bound on all elements of the Pauli group, we can apply this bound to any product of two elements in the group. As we have m encoded qubits, we need to multiply at most m different Pauli operators which act on different encoded qubits, each with eigenvalues bounded below by $1-\epsilon$. Applying the bound pair-wise to products of generators, then to products of products of generators and so forth, we arrive at

$$\lambda^2 > 1 - 2^{\lg m}\epsilon, \tag{5.28}$$

$$= 1 - m\epsilon \tag{5.29}$$

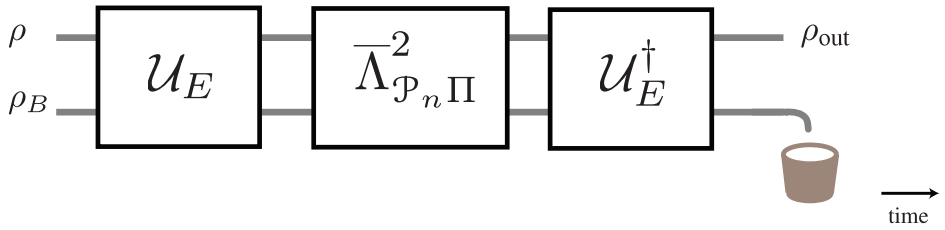

Figure 5.2: *Circuit diagram corresponding to the composition of quantum operations* $\mathcal{U}_E^\dagger \circ \overline{\Lambda}^2_{\mathcal{P}_n\Pi} \circ \mathcal{U}_E$.

where lg is the base 2 logarithm. That is, given that the generators have eigenvalues at least $1-\epsilon$, then all elements of the encoded Pauli group will have eigenvalues at least $1-m\epsilon$.

This can be translated to a bound on the fidelity of encoded states transmitted through the squared channel. Consider an m qubit pure state ρ, along with an $n-m$ qubit ancilla ρ_B. The ideal encoding operation $\mathcal{U}_E$ maps the Pauli operators over the m qubits into Pauli operators over the n qubits which are guaranteed to have eigenvalue at least $1-m\epsilon$ under the action of $\overline{\Lambda}^2_{\mathcal{P}_n\Pi}$. The output state after encoding, transmission through the squared channel, and decoding and discarding of the ancilla is

$$\rho_{\text{out}} = \text{tr}_B \mathcal{U}^\dagger_{\text{enc}} \circ \overline{\Lambda}^2_{\mathcal{P}_n\Pi} \circ \mathcal{U}_{\text{enc}}(\rho \otimes \rho_{\text{B}}). \tag{5.30}$$

The circuit diagram corresponding to this is depicted in Figure 5.2. Decomposing the pure state ρ into the Pauli basis we obtain

$$\rho_{\text{out}} = \sum_{P_i \in \mathcal{P}_m} \rho_i \lambda^2(P_i) P_i \tag{5.31}$$

where the ρ_i are real numbers. As ρ is a pure state, the fidelity between ρ and ρ_{out} is

$$\begin{aligned} \text{tr}\,\rho\rho_{\text{out}} &= \sum \rho_i^2 \lambda^2(P_i) 2^m && (5.32)\\ &> (1-m\epsilon) \sum \rho_i^2 2^m && (5.33)\\ &= (1-m\epsilon), && (5.34) \end{aligned}$$

as $\text{tr}\,\rho^2 = \sum \rho_i^2 2^m = 1$. Since the fidelity is a concave function, this demonstrates that any encoded state transmitted though the channel will have a fidelity of at least $1-m\epsilon$.

It should be noted that this is useful not only in the context where the eigenvalues are estimated with finite precision, but also in the case where no exact UCCs can be found

for a twirled channel – these bounds can then be used to find encodings for quantum data which merely improve the fidelity under the action of noise.

Bounds on the fidelity of the encoded states under the action of Λ, instead of $\overline{\Lambda}_{\mathcal{P}_n\Pi}$, can be computed given complete information about the channel. However, as argued earlier, complete information about the channel cannot be obtained in a scalable manner. For this reasons it is important to check experimentally what the fidelity of the encoding constructed for $\overline{\Lambda}_{\mathcal{P}_n\Pi}$ is under the action of Λ. This can be done by twirling the effective encoded channel $\tilde{\mathcal{U}}_E^\dagger \circ \mathcal{R} \circ \Lambda \circ \tilde{\mathcal{U}}_E$ and estimating its average gate fidelity with the identity channel. The estimate can be done efficiently, as described in the previous chapter. In the event that the average performance of the code under the action of Λ is worse, one can simply use the twirled channel instead. Thus the average performance of the code under the action of twirled channel can always be taken as a lower bound.

5.7 General unitary twirls

In the previous sections we have restricted ourselves to considering PIP channels simply because it was clear an algorithm for finding UCCs could be devised. However, we can generalize Corollary 1 in Section 5.3 to include all channels resulting from any twirl over a set of unitaries.

Theorem — Any correctable code for a unitarily twirled channel $\overline{\Lambda}$ is a correctable code for the original channel Λ up to an additional unitary correction.

Proof: Without loss of generality, consider $\Lambda(\rho) = \sum_k A_k \rho A_k^\dagger$ and a twirl with unitaries $\{U_j\}$ where $U_1 = \mathbb{1}$. Any unitary twirl is unitarily equivalent to a twirl that includes the identity, and this unitary equivalence leads to the additional unitary correction. A set of Choi-Kraus operators for $\overline{\Lambda}$ is then $\{U_j^\dagger A_k U_j\}$. As shown in [KLP05], the existence of a correctable code $\mathcal{H}_A$ under the action of $\overline{\Lambda}$, with recovery operations $\mathcal{R}(\rho) = \sum_m R_m \rho R_m^\dagger$, corresponds to the projector P onto the subspace $\mathcal{H}_A \otimes \mathcal{H}_B$ satisfying $PR_mU_j^\dagger A_k U_j P = R_m U_j^\dagger A_k U_j P$ and $R_m U_j^\dagger A_k U_j|_P \in \mathbb{1}_A \otimes \mathcal{B}(\mathcal{H}_B)$ for all j, k, m. Since $U_1 = \mathbb{1}$, this implies $PR_mA_kP = R_mA_kP$ and $R_mA_k|_P \in \mathbb{1}_A \otimes \mathcal{B}(\mathcal{H}_B)$ for all k, m. Thus it follows that $\mathcal{H}_A$ is also correctable under the action of Λ with the same recovery operation $\mathcal{R}$. □

While some correctable codes from Λ may not be correctable for the Pauli twirled channel $\overline{\Lambda}$, there may be other unitary twirls of Λ for which they are. In some sense

twirling adds noise, and the unitaries in the twirl must be chosen carefully, or they may break symmetries which can be used to store information. These other unitary twirls may preserve these symmetries while still allowing for the efficient experimental characterization of this new twirled channel, even thought the resulting channel may not be as simple as a PIP channel. This theorem shows that any correctable code found in this manner will always yield correctable codes for the original channel.

As a concrete example, consider the case of collective unitary noise over n qubits, represented by the CP map

$$\Lambda_\mu(\rho) = \int d\mu(U)\, U^{\otimes n} \rho U^{\dagger \otimes n} = \int d\mu(U)\, \mathcal{U}^{\otimes n}(\rho), \tag{5.35}$$

for some measure $d\mu(U)$ over single qubit unitaries U. Λ_μ is, by construction, invariant under permutations of the qubits, as it acts on all qubits in the same manner. The earliest known examples of decoherence-free subspaces are correctable codes for this type of noise [ZR97]. In particular, these decoherence-free subspaces allow for the ratio between the number of encoded qubits and n to approach 1 asymptotically, demonstrating that these can be extremely efficient encodings [KBLW01, BRS07].

For any given $\mathcal{U}$ in the integral above, twirling over $\mathcal{P}_n$ results in n identical Pauli channels acting independently on each qubit. If each of these Pauli channels have eigenvalues $|\lambda_{\mathbf{w}}| < 1$, then the $\mathcal{P}_n$ twirled channel will only have the trivial fixed-point $\mathbb{1}_{2^n}$. No exact correctable encodings for Λ_μ would be found, even though such a channel supports very large noiseless encodings [KBLW01, BRS07].

If one were to twirl collective unitary noise uniformly only over the group of all possible qubit permutations Π_n instead of the group generated by $\mathcal{P}_n$ and Π_n, the channel would be unchanged, and thus these decoherence-free subspaces would also be correctable codes from the Π_n twirled channel. Surprisingly, an arbitrary permutation invariant channel requires only a polynomial number of parameters to be described.

Proposition 3 — An n-qubit CP map which is invariant under qubit permutations requires $O(n^{15})$ parameters to be described.

Proof: Given $\Lambda(\rho) = \sum_{ij} [\chi]_{ij} P_i \rho P_j$ is invariant under qubit permutations, we have

that, for any qubit permutation π,

$$\Lambda(\rho) = \sum_{ij} [\chi]_{ij} P_i \rho P_j \tag{5.36}$$

$$= \sum_{ij} [\chi]_{ij} \pi P_i \pi^\dagger \rho \pi P_j \pi^\dagger \tag{5.37}$$

$$= \sum_{ij} [\chi]_{ij} P_{\pi(i)} \rho P_{\pi(j)} \tag{5.38}$$

$$= \sum_{ij} [\chi]_{\pi^{-1}(i),\pi^{-1}(j)} P_i \rho P_j, \tag{5.39}$$

where, in a slight abuse of notation, we have used $\pi(i)$ to denote the index map which corresponds to quit permutation, *i.e.* $P_{\pi(i)} = \pi P_i \pi^\dagger$. This implies that, for any permutation π, $[\chi]_{\pi(i),\pi(j)} = [\chi]_{ij}$, so we only need to count the number of equivalence classes of pairs of n-qubit Pauli operators. In Appendix D this is computed to be

$$\frac{1}{1307674368000}(n^{15} + 120n^{14} + 6580n^{13} + 218400n^{12} + 4899622n^{11} + 78558480n^{10} + 928095740n^9 + 8207628000n^8 + 54631129553n^7 + 272803210680n^6 + 1009672107080n^5 + 2706813345600n^4 + 5056995703824n^3 + 6165817614720n^2 + 4339163001600n + 1307674368000) \tag{5.40}$$

and thus the number of different real parameters needed to describe a general permutation invariant CP map is $O(n^{15})$. □

While we have emphasized the applications of twirling over the Pauli and Clifford groups, this result demonstrates that there may be much to be gained by investigating other types of twirls. In particular, it may be possible to efficiently extract much more information about the channel, potentially opening the door for the search of broader classes of noiseless encodings using experimental data.

5.8 Concluding remarks

In this chapter we have shown that correctable encodings for a quantum operation can be found by searching for correctable encodings using the twirled version of that quantum operation. We investigated in detail the case of channels twirled by Pauli operators and qubit permutations, and demonstrated a simple scheme for identifying encodings with

unitary recovery operations. Such twirled channels are important because they are described by a polynomial number of parameters which are experimentally accessible via a scalable protocol.

The scheme does not require the manipulation of exponentially large matrices, and the performance of the constructed correctable code can be estimated experimentally in an efficient manner. Further work is needed to determine whether all unitarily correctable codes for PIP channels can be found through the scheme we described.

We have also demonstrated that twirling over different sets of unitaries, such as qubit permutations alone, can yield a larger number of correctable codes. It would be interesting to investigate other unitarily twirled channels that can be efficiently characterized in an experiment, as well as a generalization of the algorithm presented here for channels which are not Pauli channels.

Appendix

Appendix A

Experimental status of superconducting circuit implementations

Some of the most promising physical systems for the implementation of scalable quantum computers are based on superconducting circuits [MSS01, DWM04, YN05, CW08]. Here we outline the major experimental milestones achieved to date.

A.1 Decoherence

The main source of noise in superconducting circuits is low-frequency noise known as $1/f$ *noise* [CW08]. The main effect that $1/f$ noise can have on superconducting circuits is to drastically reduce the characteristic dephasing time of quantum superpositions. This is because this low-frequency noise randomly disturbs the parameters of Hamiltonian of the qubit, causing the relative phases between superpositions of eigenstates to average out.

Most designs of qubits based on superconducting circuits have been adapted to reduce the effects of low-frequency noise. This is done by setting the parameters of the Hamiltonian so that they are largely insensitive to the perturbations induced by the noise. This is known as the *optimal bias point*, as it can be used to greatly increase the dephasing times of charge and flux qubits. Phase qubits are the notable exception, as these circuits do not have an optimal bias point.

To date [CW08], the highest relaxation times reported are 2μs for charge qubits,

4.5μs for flux qubits, and 0.5μs for phase qubits. The highest dephasing times are 2μs for charge qubits, 1.2μs for flux qubits and 0.3μs for phase qubits.

A.2 Measurement

The reliable measurement of quantum systems is necessary for the implementation of quantum information processing devices. While early implementations based on superconducting circuits had low fidelity measurements which were also non-repeatable, all proposed implementations have non-destructive high fidelity measurement schemes now.

Fast measurement approaching the quantum non-demolition limit have been demonstrated using Josephson bifurcation amplifiers [SVP+05], and fast dispersive readout of flux qubits has also been demonstrate [LSP+07]. In the case of flux qubits, the fidelity of the repeated measurement of the same qubit has been reported to be over 85%. Similarly, fast measurements of phase qubits have also been demonstrated, allowing the state to be measured in approximately 5ns [CSM+04] with a fidelity which was later improved to approximately 98% [LHA+08].

A.3 Single qubit operations

High fidelity single qubit operations have been demonstrated for all superconducting circuit implementations. Although the methods used for these demonstrations are not strictly compatible, the error rates per single qubit operation are on the order of $2-4\%$ [LHA+08, Gam08].

A.4 Interactions

Fixed coupling interactions have been demonstrated for all forms of superconducting qubits [PYA+03, BXR+03, MSS+05, MPtH+05], as such interactions can be implemented by capacitive or inductive coupling between circuits. Using these types of fixed coupling, the entanglement between two qubits has been demonstrated by state tomography [SAB+06].

One of the main motivations for the use superconducting circuits is the potential for *in situ* tunable couplings. Tunable couplings have been demonstrated for flux qubits [HRP+06, NHY+07], and simple gate operations have also been demonstrate [YPA+03, NHY+07, PdGHM07], although with relatively low fidelity.

A.5 Outlook

Given the range of values of the error threshold mentioned in Chapter 1, it is clear that the fidelities listed here, although high, are not sufficient and therefore these devices are not yet suitable for scalable quantum computation. However, given the steady progress in these experiments over the last decade, there is reason to be optimistic that in the near future superconducting circuits will yield qubit with much better control and much lower error rates, opening the door for physical implementations of many of the experiments proposed in this thesis.

A first step in better evaluating these different technologies would be to put them on equal footing before comparison. This is one of the motivations for the experiments proposed in Chapter 4 of this thesis, which can be used to benchmark the performance of the various operations used in a quantum information processor.

Appendix B

Quantification of entanglement

B.1 Entanglement Witnesses

An observable W is called an *entanglement witness* [HHH96, Ter00] if and only if

- for all separable state ρ_S we have that $\langle W \rangle = \mathrm{tr}\, W\rho_S \geq 0$,
- there exists a state ρ such that $\langle W \rangle = \mathrm{tr}\, W\rho < 0$.

Such a definition is possible because the set of separable states is convex and compact [LBHC01].

From this definition it is clear that there are entangled states such that $\langle W \rangle \geq 0$, and thus the observable W must be tailored to the state which is being tested for entanglement. In the case that interests us, the state which is being prepared is the Bell state

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{B.1}$$

Consider then the density matrix (represented in the computational basis)

$$\rho_{\Phi^-} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \tag{B.2}$$

corresponding to the state

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{B.3}$$

Applying the linear map T_A known as *partial transpose of subsystem A*, defined by

$$|i\rangle|j\rangle\langle k|\langle l|^{T_A} = |k\rangle|j\rangle\langle i|\langle l|, \tag{B.4}$$

we obtain the operator

$$W = \rho_{\Phi^-}^{T_A} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{B.5}$$

which does not correspond to a density matrix, as it is not positive. Note that for any product state $\rho_A \otimes \rho_B$ we have

$$\begin{aligned} \operatorname{tr} W\rho_A \otimes \rho_B &= \operatorname{tr} \rho_{\Phi^-}^{T_A}\ \rho_A \otimes \rho_B && \text{(B.6)} \\ &= \operatorname{tr} \rho_{\Phi^-}\ (\rho_A \otimes \rho_B)^{T_A} && \text{(B.7)} \\ &= \operatorname{tr} \rho_{\Phi^-}\ \rho_A^* \otimes \rho_B && \text{(B.8)} \\ &= \langle \Phi^-|\rho_A^* \otimes \rho_B|\Phi^-\rangle. && \text{(B.9)} \end{aligned}$$

As $\rho_A^* \otimes \rho_B$ is a positive operator, $\langle W\rangle \geq 0$ for all separable states, since they are convex combinations of product states. Moreover, we have that

$$W = \frac{1}{2}\mathbb{1}_4 - |\Psi^+\rangle\langle\Psi^+| \tag{B.10}$$

so that the expectation of the witness for a state ρ is

$$\langle W\rangle = \frac{1}{2} - \langle\Psi^+|\rho|\Psi^+\rangle \tag{B.11}$$

and for $\rho = |\Psi^+\rangle\langle\Psi^+|$ we have

$$\langle W\rangle = -\frac{1}{2}. \tag{B.12}$$

Therefore W is an entanglement witness for the state $|\Psi^+\rangle$.

Entanglement witnesses were originally created only to detect entanglement, and not to quantify it. However, it has been recently demonstrated that they can be used to place bounds on entanglement measures, as discussed below.

B.2 Entanglement monotones

An *entanglement monotone* is a function mapping states to positive real numbers, and which can be used to quantify the amount of entanglement in a state. These functions

satisfy a number of properties to ensure that this operational meaning is valid. However, for our purposes, we will simply describe two convenient entanglement monotones, and we refer the interested reader review papers such as [PV07] for a more detailed discussion of their properties.

The *generalized entanglement robustness* $E_R(\rho)$ of a state ρ [VT99, Ste03] is the defined as the smallest positive s such that the state

$$\frac{1}{1+s}(\rho + s\rho_{\text{noise}}) \tag{B.13}$$

is separable, where ρ_{noise} is another arbitrary state. As the notation implies, the robustness can be interpreted as the minimal amount of noise that unentangles an entangled state. Moreover, it has been show that $E_R(\rho)$ can be used to quantify how useful the state ρ is as an ancilla in teleportation protocols [Bra07].

It has been shown that E_R can be bounded by the negativity of any entanglement witness [EBA07]. In particular, it was shown that if $\operatorname{tr} W\rho = c < 0$, then

$$E_R(\rho) \geq |c|/\lambda_{\max}(W), \tag{B.14}$$

where $\lambda_{\max}(W)$ is the largest eigenvalue of W. For the entanglement witness described above, we have that $\lambda_{\max}(W) = 1/2$, so that

$$E_R(\rho) \geq 2F - 1, \tag{B.15}$$

demonstrating that the fidelity can be used to compute a bound for the entanglement monotone E_R.

Another useful entanglement monotone is the *logarithmic negativity* $E_N(\rho)$ [Ple05], which is defined as

$$E_N(\rho) = \log_2 \|\rho^{T_A}\|, \tag{B.16}$$

where $\|\rho\| = \operatorname{tr}\sqrt{\rho^\dagger\rho}$ is the trace norm. The logarithmic negativity is an upper bound on the amount of entanglement which can be distilled from the state ρ, as well as an upper bound on the teleportation capacity of ρ (i.e. how well states can be teleported by using the state ρ) [VW02].

Appendix C

Damped Harmonic Oscillator

C.1 Solution at zero temperature

Here we review the solution to the damped harmonic oscillator as presented in [BP02].

The zero temperature master equation for the damped harmonic oscillator is given by [GZ00]

$$\frac{d}{dt}\rho_{\text{HO}} = \left(-i\omega_0 - \frac{\gamma_0}{2}\right) a^\dagger a \rho_{\text{HO}} + \left(i\omega_0 - \frac{\gamma_0}{2}\right) \rho_{\text{HO}} a^\dagger a + \gamma a^\dagger \rho_{\text{HO}} a. \tag{C.1}$$

An assumption for the derivation of this equation is that $\gamma_0 \ll \omega_0$, which demonstrates why the free particle limit cannot be obtained straightforwardly from this equation for finite dissipation rate γ_0.

If we interpret the harmonic oscillator as a mode of the electromagnetic field, this master equation can be seen as the continuous limit of sending the state through a series of beam splitters which cause photons to leak at a rate γ_0. As beam splitter maps coherent states to coherent states, it is natural to take the operator

$$f(t)|\alpha(t)\rangle\langle\beta(t)| \tag{C.2}$$

where $|\alpha(t)\rangle$ and $|\beta(t)\rangle$ are coherent states with time dependent amplitudes, and $f(t)$ is a complex valued function, as an ansatz to (C.1).

Noting that, from the decomposition of coherent states into the energy eigenbasis, we

have

$$\frac{d}{dt}|\alpha(t)\rangle = \frac{d}{dt}\mathrm{e}^{-\frac{|\alpha(t)|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha(t)^n}{\sqrt{n!}}|n\rangle, \tag{C.3}$$

$$= -\frac{1}{2}\left(\frac{d}{dt}|\alpha(t)|^2\right)\mathrm{e}^{-\frac{|\alpha(t)|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha(t)^n}{\sqrt{n!}}|n\rangle + \mathrm{e}^{-\frac{|\alpha(t)|^2}{2}}\sum_{n=1}^{\infty}\dot{\alpha}(t)\frac{n\alpha(t)^{n-1}}{\sqrt{n!}}|n\rangle, \tag{C.4}$$

$$= -\frac{1}{2}\left(\frac{d}{dt}|\alpha(t)|^2\right)\mathrm{e}^{-\frac{|\alpha(t)|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha(t)^n}{\sqrt{n!}}|n\rangle + \frac{\dot{\alpha}(t)}{\alpha(t)}\mathrm{e}^{-\frac{|\alpha(t)|^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha(t)^n}{\sqrt{n!}}a^\dagger a|n\rangle, \tag{C.5}$$

$$= \left(\frac{\dot{\alpha}(t)}{\alpha(t)}a^\dagger a - \frac{1}{2}\frac{d}{dt}|\alpha(t)|^2\right)|\alpha(t)\rangle, \tag{C.6}$$

and thus the left side of (C.1) yields

$$\frac{d}{dt}f(t)|\alpha(t)\rangle\langle\beta(t)| = \dot{f}(t)|\alpha(t)\rangle\langle\beta(t)| + f(t)\left(\frac{\dot{\alpha}(t)}{\alpha(t)}a^\dagger a - \frac{1}{2}\frac{d}{dt}|\alpha(t)|^2\right)|\alpha(t)\rangle\langle\beta(t)| + f(t)|\alpha(t)\rangle\langle\beta(t)|\left(\frac{\dot{\beta}(t)^*}{\beta(t)^*}a^\dagger a - \frac{1}{2}\frac{d}{dt}|\beta(t)|^2\right). \tag{C.7}$$

As the coherent state $|\alpha(t)\rangle$ is an eigenstate of a, we find that the right side of (C.1) yields

$$f(t)\left(-i\omega_0 - \frac{\gamma_0}{2}\right)a^\dagger a|\alpha(t)\rangle\langle\beta(t)| + f(t)\left(i\omega_0 - \frac{\gamma_0}{2}\right)|\alpha(t)\rangle\langle\beta(t)|a^\dagger a + \gamma_0 f(t)\alpha(t)\beta(t)^*|\alpha(t)\rangle\langle\beta(t)|. \tag{C.8}$$

Matching the coefficients of $a^\dagger a|\alpha(t)\rangle\langle\beta(t)|$, $|\alpha(t)\rangle\langle\beta(t)|a^\dagger a$ and $|\alpha(t)\rangle\langle\beta(t)|$ on both sides yields

$$\frac{\dot{\alpha}(t)}{\alpha(t)} = -i\omega_0 - \frac{\gamma_0}{2}, \tag{C.9}$$

$$\left(\frac{\dot{\beta}(t)}{\beta(t)}\right)^* = i\omega_0 - \frac{\gamma_0}{2}, \tag{C.10}$$

$$\dot{f}(t) - f(t)\,\frac{1}{2}\frac{d}{dt}\left(|\alpha(t)|^2 + |\beta(t)|^2\right) = \gamma_0\alpha(t)\beta(t)^*\,f(t). \tag{C.11}$$

The first two equations are immediatelly solved yielding

$$\alpha(t) = \alpha(0)\mathrm{e}^{-i\omega_0 - \frac{\gamma_0}{2}t} \tag{C.12}$$

$$\beta(t) = \beta(0)\mathrm{e}^{-i\omega_0 - \frac{\gamma_0}{2}t}. \tag{C.13}$$

Back substitution into the equation for $f(t)$ yields

$$\frac{\dot{f}(t)}{f(t)} = \gamma_0 \mathrm{e}^{-\gamma_0 t}\left(-\frac{1}{2}|\alpha(0)|^2 - \frac{1}{2}|\beta(0)|^2 + \alpha(0)\beta(0)^*\right), \tag{C.14}$$

$$= \gamma_0 \mathrm{e}^{-\gamma_0 t}\langle\beta(0)|\alpha(0)\rangle, \tag{C.15}$$

which is readily integrated, resulting in

$$f(t) = \langle\beta(0)|\alpha(0)\rangle^{\left(1-\mathrm{e}^{-\gamma_0 t}\right)}. \tag{C.16}$$

Thus, we if take the initial states to be

$$|\alpha\rangle + |\beta\rangle, \tag{C.17}$$

the density matrix at time t will be

$$|\alpha(t)\rangle\langle\alpha(t)| + |\beta(t)\rangle\langle\beta(t)| + f(t)|\alpha(t)\rangle\langle\beta(t)| + f(t)^*|\beta(t)\rangle\langle\alpha(t)|. \tag{C.18}$$

The decay rate of the off-diagonal terms in the density matrix if thus given by

$$\ln|f(t)| = \left(1 - \mathrm{e}^{-\gamma_0 t}\right)\ln|\langle\beta|\alpha\rangle|. \tag{C.19}$$

For $\gamma_0 t \gg 1$ we have

$$\ln|f(t)| \approx \ln|\langle\beta|\alpha\rangle|, \tag{C.20}$$

For $\gamma_0 t \ll 1$ we have

$$\ln|f(t)| \approx -\gamma_0 t \ln|\langle\beta|\alpha\rangle|, \tag{C.21}$$

So we can define the characteristic time of decoherence to be

$$\frac{1}{\gamma_0 \ln\left(\frac{1}{|\langle\beta|\alpha\rangle|}\right)}. \tag{C.22}$$

As energy is proportional to the number of photons in a harmonic oscillator, (C.12) makes it clear that the energy relaxation rate is γ_0, and thus the characteristic energy relaxation time is $1/\gamma_0$. This leads to the ratio of decoherence time t_D to relaxation time t_R

$$\frac{t_D}{t_R} = \frac{1}{\ln\left(\frac{1}{|\langle\beta|\alpha\rangle|}\right)}, \tag{C.23}$$

as claimed.

Appendix D

Number of parameters to describe twirled channels

D.1 A direct approach

Say we have an alphabet of size M and we want to form string of length n with M different letters, allowing repetition. In the case of PIP channels the strings correspond to Kraus operators, each given by the tensor product of n Pauli operators, so $M = 4$. In the case of permutation-invariant channels, the string represent the left and right Pauli operator from the description of the CP in the Pauli operator basis, so $M = 16$, as for each qubit location there is a pair of Pauli operators – one acting from the left and one acting from the right.

As in both cases the channels are permutation-invariant, we consider two string that are related by a permutation to be in the same equivalence class, we want to simply count the number of equivalence classes in order to count the number $K_n^{(M)}$ of parameters needed to describe each channels. The equivalence classes can be labeled by the number of times w_i each of the different letters i appear in the strings in that class, under the constraint that the total number of letters be equal to n. Thus, the number of equivalence classes is simply the number of non-negative integer solutions to the equation

$$\sum_{i=1}^{M} w_i = n. \tag{D.1}$$

This can be done by fixing w_1 and counting the solutions for each remaining w_i. The number of solutions for each w_i can in turn be calculated by fixing w_i and counting the

number of solutions to the smaller equation, and so forth. This results in

$$K_n^{(M)} = \sum_{w_1=0}^{n} K_{n-w_1}^{(M-1)} \tag{D.2}$$

$$K_n^{(1)} = 1, \tag{D.3}$$

which can be computed explicitly using computer packages such as Mathematica [Mat05].

In the case of $M = 4$, for PIP channels, this leads to

$$K_n^{(4)} = \sum_{w_1=0}^{n} \sum_{w_2=0}^{n-w_1} \sum_{w_3=0}^{n-w_1-w_2} 1 = \frac{1}{6}n^3 + n^2 + \frac{11}{6}n + 1. \tag{D.4}$$

Evaluating $K_n^{(4)}$ for the first few $n \geq 1$ we obtain

$$4, 10, 20, 35, 56, \ldots \tag{D.5}$$

which is sequence A000292 in the on-line encyclopedia of integer sequences [Slo08a].

In the case of $M = 16$, for permutation-invariant channels, this leads to

$$\begin{aligned} K_n^{(16)} &= \sum_{w_1=0}^{n} \sum_{w_2=0}^{n-w_1} \cdots \sum_{w_15=0}^{n-\sum_{i=1}^{1} 4w_i} 1 \\ &= \frac{1}{1307674368000}(n^{15} + 120n^{14} + 6580n^{13} + 218400n^{12} + 4899622n^{11} + 78558480n^{10} \\ &+928095740n^9+8207628000n^8+54631129553n^7+272803210680n^6+1009672107080n^5 \\ &+ 2706813345600n^4 + 5056995703824n^3 + 6165817614720n^2 + 4339163001600n \\ &+ 1307674368000). \end{aligned} \tag{D.6}$$

Evaluating $K_n^{(16)}$ for the first few $n \geq 1$ we obtain

$$16, 136, 816, 3876, 15504, \ldots \tag{D.7}$$

which is sequence A010968 in the on-line encyclopedia of integer sequences [Slo08b].

D.2 A combinatorial approach

$K_n^{(M)}$ can be computed more directly by considering an equivalent problem which lends itself to combinatorial counting. Consider n different items, depicted as black dots in

Figure D.1: *Computing the number $K_n^{(M)}$ is equivalent to counting the number of ways $M-1$ separators can be placed amongst n items. These are the possible configurations for 1 item and 3 separators (corresponding to 4 categories)*

Figure D.1, which we want to separate into M different categories, potentially leaving some categories empty. We do not care exactly which items go into which category, as the items are indistinguishable, we only care about how many go into each category. One way to do this would be to put a separator (depicted by a vertical bar in Figure D.1) between different categories, so that all items from the left to the first separator are in the first category, all items from the first separator to the second are in the second category, and so forth, so that all items from the last separator to the right are in the last category. $K_n^{(M)}$ is the number of different ways to arrange the separators between the items.

One way to compute $K_n^{(M)}$ is to then consider $n+M-1$ different slots, and count the ways to place $M-1$ separators in the slots, leaving the remaining slots to be occupied by items. This immediatelly leads to the straightforward formula

$$K_n^{(M)} = \binom{n+M-1}{M-1}. \tag{D.8}$$

Appendix E

Efficient computation of Ω by counting

E.1 Pauli twirl

In order to efficiently describe the linear transformation Ω relating the probabilities which parameterize a PIP channel and the eigenvalues of a channel, one must compute the number $N_c(\mathbf{v}, \mathbf{w})$ of operators P_1 of weight class $\mathbf{v}$ which commute with any given operator P_2 of weight class $\mathbf{w}$.

First, we know that Pauli operators either commute or anti-commute. Most importantly, we note that, for $\sigma_{i,j} \in \mathcal{P}_n$, then $\sigma_i\sigma_j\sigma_k = -\sigma_j$ if $\{\sigma_i, \sigma_j\} = 0$, and $\sigma_i\sigma_j\sigma_k = \sigma_j$ if $[\sigma_i, \sigma_j] = 0$. Thus two operators $P_1, P_2 \in \mathcal{P}_n$ will commute if the respective Pauli operators at an even number of locations anti-commute, so that the negative signs cancel and $P_1P_2 = P_2P_1$.

Moreover, the set given by any weight class is invariant over qubit permutations, so we can choose any convenient operator from the weight class $\mathbf{w}$ in order to count the operators from $\mathbf{v}$ which commute with it. Let $\mathbf{v} = (a, b, c)$ and let $\mathbf{w} = (x, y, z)$. In order to count $N_c(\mathbf{v}, \mathbf{w})$, one simply needs to count the number of operators in $\mathbf{v}$ which commute with $\sigma_x^{\otimes x} \otimes \sigma_Y^{\otimes y} \otimes \sigma_Z^{\otimes z} \otimes \mathbb{1}^{\otimes n-x-y-z}$.

First, we count the number of operators which commute in the trivial way, *i.e.* the number of ways which we can distribute the σ_X operators of P_1 such that the corresponding position of P_2 has either σ_X or $\mathbb{1}$ and so forth. Choose i locations in the σ_X region, then j locations in the σ_Y region and then k locations in the σ_Z region. There are $a + b + c - i - j - k$ non-trivial Pauli operators in P_1 remaining to be placed and

these will be placed in the remaining $n-x-y-z$ qubits. Of these, we are constrained to choose $a-i$ locations for σ_X operators, $b-j$ locations for σ_Y operators and $c-k$ locations for σ_Z operators. Thus, the number of operators in $\mathbf{v}$ which trivially commute with any given operators in $\mathbf{w}$ is

$$F(n,x,y,z,a,b,c) = \sum_{i=0}^{\min(x,a)} \sum_{j=0}^{\min(y,b)} \sum_{k=0}^{\min(z,c)} \binom{x}{i}\binom{y}{j}\binom{z}{k} \times \binom{n-x-y-z}{a+b+c-i-j-k}\binom{a+b+c-i-j-k}{a-i}\binom{b+c-j-k}{b-j}. \quad \text{(E.1)}$$

Now we can compute the total number of commuting Pauli operators by first choosing an even number of locating for the Pauli operators to anti-commute, and then simply using F as defined above to count the number of locations where the Pauli operators trivially commute. Choose $a_{xy}+a_{xz}$ locations in the σ_X region to place a_{xy} σ_Y operators and a_{xz} σ_Z operators, and define similar parameters for the different Pauli operators. The remaining locations and Pauli operators are left to commute trivially, and thus their number can be computer by F. We finally obtain

$$\begin{aligned} N_c(n,x,y,z,a,b,c) = & \sum_{a_{xy}=0}^{x-a_{xz}} \sum_{a_{xz}=0}^{x} \sum_{a_{yx}=0}^{y-a_{yz}} \sum_{a_{yz}=0}^{y} \sum_{a_{zx}=0}^{z-a_{zx}} \sum_{a_{zy}=0}^{z} \\ & \binom{x}{a_{xy}+a_{xz}}\binom{a_{xy}+a_{xz}}{a_{xy}}\binom{y}{a_{yx}+a_{yz}}\binom{a_{yx}+a_{yz}}{a_{yx}}\binom{z}{a_{zx}+a_{zy}}\binom{a_{zx}+a_{zy}}{a_{zx}} \times \\ & F(n-a_{xy}-a_{xz}-a_{yx}-a_{yz}-a_{zx}-a_{zy}, \\ & x-a_{xy}-a_{xz}, y-a_{yx}-a_{yz}, z-a_{zx}-a_{zy}, \\ & a-a_{yx}-a_{zx}, b-a_{xy}-a_{zy}, c-a_{xz}-a_{yz}) \times \\ & \mathrm{Even}(a_{xy}+a_{xz}+a_{yx}+a_{yz}+a_{zx}+a_{zy}), \end{aligned} \quad \text{(E.2)}$$

where $\mathrm{Even}(x)$ is a function which returns 1 if x is even, and 0 if x is odd.

Using the computer algebra package *Mathematica* [Mat05], one can simplify the overall expression for N_c down to a sum over seven different variables. However, the expression is not any more elucidating then the expression above. As this function can be computed quite quickly in a computer, no attempts to further simplify it have been made.

Thus, the entries $[\Omega]_{\mathbf{w},\mathbf{v}}$ are given by

$$[\Omega]_{\mathbf{w},\mathbf{v}} = 2\frac{N_c(n,x,y,z,a,b,c)}{4^n} - 1. \tag{E.3}$$

Direct computation of Ω for $n = 1, 2$ yields

$$\Omega_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{E.4}$$

$$\Omega_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & -1 & 0 & 0 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 0 & -1 & 1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 & 1 & -1 & -1 & 0 & 0 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 0 & -1 & -1 & 1 & 0 & 0 & 1 \\ 1 & 0 & -1 & -1 & 0 & 1 & 0 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \end{pmatrix} \tag{E.5}$$

E.2 Clifford twirl

Similar arguments can be made for the case of a Clifford twirl, as Clifford twirls also yield Pauli channels. In that case the final expression is significantly simpler, yielding

$$[\Omega]_{w,v} = \sum_{l=0}^{n} \frac{3^l + (-1)^l}{3^l} \frac{\binom{n-w}{v-l}\binom{w}{l}}{\binom{n}{v}} - 1. \tag{E.6}$$

This expression was computed in collaboration with Osama Moussa.

Direct computation of Ω for $n = 2, 3, 4$ yields

$$\Omega_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \frac{1}{3} & -\frac{1}{3} \\ 1 & -\frac{1}{3} & \frac{1}{9} \end{pmatrix} \tag{E.7}$$

$$\Omega_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \frac{5}{9} & \frac{1}{9} & -\frac{1}{3} \\ 1 & \frac{1}{9} & -\frac{5}{27} & \frac{1}{9} \\ 1 & -\frac{1}{3} & \frac{1}{9} & -\frac{1}{27} \end{pmatrix} \tag{E.8}$$

$$\Omega_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \frac{2}{3} & \frac{1}{3} & 0 & -\frac{1}{3} \\ 1 & \frac{1}{3} & -\frac{1}{27} & -\frac{1}{9} & \frac{1}{9} \\ 1 & 0 & -\frac{1}{9} & \frac{2}{27} & -\frac{1}{27} \\ 1 & -\frac{1}{3} & \frac{1}{9} & -\frac{1}{27} & \frac{1}{81} \end{pmatrix} \tag{E.9}$$

References

[ABO99] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error rate. E-print arXiv:quant-ph/9906129, 1999.

[AG04] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70(05):052328, 2004.

[AGP06] P. Aliferis, D. Gottesman, and J. Preskill. Quantum accuracy threshold for concatenated distance-3 codes. *Quant. Inf. Comp.*, 6(2):97–165, 2006.

[AGP08] P. Aliferis, D. Gottesman, and J. Preskill. Accuracy threshold for postselected quantum computation. *Quant. Inf. Comp.*, 8(3–4):181–244, 2008.

[AL87] R. Alicki and K. Lendi. *Quantum Dynamical Semigroups and Applications*. Lecture Notes in Physics. Springer, 1st edition, 1987.

[AL05] P. Aliferis and D. W. Leung. Fault-tolerant quantum computation in the graph-state model. E-print arXiv:quant-ph/0503130, 2005.

[ALZ06] R. Alicki, D. A. Lidar, and P. Zanardi. Internal consistency of fault-tolerant quantum error correction in light of rigorous derivations of the quantum Markovian limit. *Phys. Rev. A*, 73:052311, 2006.

[Amb06] V. Ambegaokar. Dissipation and decoherence in a quantum oscillator. *J. Stat. Phys.*, 125(5/6):1187–1196, 2006.

[ARS06] D. V. Averin, K. Rabenstein, and V. K. Semenov. Rapid ballistic readout for flux qubits. *Phys. Rev. B*, 73:094504, 2006.

[AW95] G. B. Arfken and H.-J. Weber. *Mathematical methods for physicists*. Academic Press, 4th edition, 1995.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[BCC+07] J. Baugh, J. Chamilliard, C. M. Chandrashekar, M. Ditty, A. Hubbard, R. Laflamme, M. Laforest, D. Maslov, O. Moussa, C. Negrevergne, M. Silva, S. Simmons, C. A. Ryan, D. G. Cory, J. S. Hodges, and C. Ramanathan. Quantum information processing using nuclear and electron magnetic resonance: review and prospects. *Physics in Canada*, 63(4), 2007.

[BDKS08] F. Brito, D. P. DiVincenzo, R. H. Koch, and M. Steffen. Efficient one- and two-qubit pulsed gates for an oscillator stabilized Josephson qubit. *New J. Phys.*, 10:033027, 2008.

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, 1996.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 4(1):195–290, 1964.

[BHK+98] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283 – 3286, 1998.

[BHW+04] A. Blais, R.-S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf. Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation. *Phys. Rev. A*, 69:062320, 2004.

[BKNPV07] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola. The structure of preserved information in quantum processes. E-print arXiv:0705.4282, 2007.

[Blu96] K. Blum. *Density matrix theory and applications*. Plenum Press, New York, NY, 1996.

[Boh35] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696–702, 1935.

[BP02] H.-P. Breuer and F. Petruccione. *The theory of open quantum systems*. Oxford University Press, 2002.

[BPP08] A. Bendersky, F. Pastawski, and J.-P. Paz. Selective and efficient estimation of parameters for quantum process tomography. *Phys. Rev. Lett.*, 100:190403, 2008.

[BR05] D. E. Browne and T. Rudolph. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.*, 95:010501, 2005.

[Bra07] F. G. S. L. Brandão. Entanglement activation and the robustness of quantum correlations. *Phys. Rev. A*, 76:030301(R), 2007.

[BRS07] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79:555, 2007.

[BXR+03] A. J. Berkley, H. Xu, R. C. Ramos, M. A. Gubrud, F. W. Strauch, P. R. Johnson, J. R. Anderson, A. J. Dragt, C. J. Lobb, and F. C. Wellstood. Entangled macroscopic quantum states in two superconducting qubits. *Science*, 300(5625):1548–1550, 2003.

[BZ06] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2006.

[CDT07] A. Cross, D. P. DiVincenzo, and B. M. Terhal. A comparative code study for quantum fault-tolerance. E-print arXiv:0711.1556, 2007.

[CEHM99] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Distributed quantum computation over noisy channels. *Phys. Rev. A*, 59:4249–4254, 1999.

[Cha05] H. Chau. Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Transactions on Information Theory*, 51(4):1451, 2005.

[Cho75] M.-D. Choi. Completely positive linear maps on complex matrices. *Lin. Alg. Appl.*, 10:285–290, 1975.

[CL83] A. O. Caldeira and A. J. Leggett. Path integral approach to quantum brownian motion. *Physica A*, 121(3):587–616, 1983.

[CLN05] A. M. Childs, D. W. Leung, and M. A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. *Phys. Rev. A*, 71, 2005. quant-ph/0404132.

[CN97] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11):2455–2467, 1997.

[CS96] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996.

[CSM+04] K. B. Cooper, Matthias Steffen, R. McDermott, R. W. Simmonds, S. Oh, D. A. Hite, D. P. Pappas, and J. M. Martinis. Observation of quantum oscillations between a josephson phase qubit and a microscopic resonator using fast readout. *Phys. Rev. Lett.*, 93:180401, 2004.

[CW08] J. Clarke and F. W. Wilhelm. Superconducting quantum bits. *Nature*, 453:1031–1042, 2008.

[DAB03] W. Dür, H. Aschauer, and H.-J. Briegel. Multiparticle entanglement purification for graph state. *Phys. Rev. Lett.*, 91:107903, 2003.

[Dan05a] D. E. Danielsen. On-self dual quantum codes, graphs, and boolean functions. Master's thesis, University of Bergen, 2005.

[Dan05b] C. Dankert. Efficient simulation of random quantum states and operators. Master's thesis, University of Waterloo, 2005.

[DCEL06] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs: constructions and applications. E-print arXiv:quant-ph/0606161, 2006.

[DCJ+07] M. V. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, and M. D. Lukin. Quantum register based on individual electronic and nuclear spin qubits in diamond. *Science*, 316:1312, 2007.

[DG98] L.-M. Duan and G.-C. Guo. Optimal quantum codes for preventing collective amplitude damping. *Phys. Rev. A*, 58:3491–3495, 1998.

[DHCB05] W. Dür, M .Hein, J. Cirac, and H.-J. Briegel. Standard forms of noisy quantum operations via depolarization. *Phys. Rev. A*, 72(052326), 2005.

[DHN06] C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen. Noise thresholds for optical cluster-state quantum computations. *Phys. Rev. A*, 73:0502306, 2006.

[Dic53] R. H. Dicke. Coherence in spontaneous radiation processes. *Phys. Rev.*, 93:99–110, 1953.

[DKP05] V. Danos, E. Kashefi, and P. Panangaden. Parsimonious and robust realisations of unitary maps in the one-way model. *Phys. Rev. A*, 72(06):064301, 2005.

[DKP07] V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. *Journal of the ACM*, 54(2):8, 2007.

[DLT02] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Transactions on Information Theory*, 48(3):580, 2002.

[DP06] T. Dauxois and M. Peyrard. *Physics of solitons*. Cambridge University Press, 2006.

[DWM04] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting qubits: A short review. E-print arXiv:cond-mat/0411174, 2004.

[EAZ05] J. Emerson, R. Alicki, and K. Zyczkowski. Scalable noise estimation wth random unitary operators. *J. Opt. B: Quantum and Semiclassical Optics*, 7:S347–S352, 2005.

[EBA07] J. Eisert, F. G. S. L. Brandão, and K. M. R. Audenaert. Quantitative entanglement witnesses. *New J. Phys.*, 9:46, 2007.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanics description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[ESM+07] J. Emerson, M. Silva, O. Moussa., C. Ryan., M. Laforest, J. Baugh, D. Cory, and R. Laflamme. Symmetrised characterisation of noisy quantum processes. *Science*, 317:1893–1896, 2007.

[FEF+08] I. Fushman, D. Englund, A. Faraon, N. Stoltz, P. Petroff, and J. Vackovic. Controlled phase shifts with a single quantum dot. *Science*, 320:769–772, 2008.

[FSSKS07] A. Federov, A. Shnirman, G. Schön, and A. Kidiyarova-Shevchenko. Reading out the state of a flux qubit by Josephson transmission line solitons. *Phys. Rev. B*, 75:224504, 2007.

[FSW07] A. S. Fletcher, P. W. Shor, and M. Z. Win. Optimum quantum error recovery using semidefinite programming. *Phys. Rev. A*, 75(01):012338, 2007.

[Gam08] J. Gambetta. Personal communication, 2008.

[GC99] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390, 1999.

[GHZ89] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, pages 73–76. Kluwer Academics, 1989.

[GKR02] M. Grassl, A. Klappenecker, and M. Rötteler. Graphs, quadratic forms and quantum codes. In *Proceedings of the ISIT, Lausanne*, page 45, Lausanne, 2002. IEEE.

[GLN05] A. Gilchrist, N. K. Langford, and M. A. Nielsen. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A*, 71:062310, 2005.

[GNM+04] A. Gilchrist, K. Nemoto, W. J. Munro, T. C. Ralph, S. Glancy, S. L. Braunstein, and G. J. Milburn. Schrodinger cats and their power for quantum information processing. *J. Opt. B: Quantum and Semiclassical Optics*, 6:S828, 2004.

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997.

[Got98a] D. Gottesman. The Heisenberg representation of quantum computers. E-print arXiv:quant-ph/9805080, 1998.

[Got98b] D. Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127 – 137, 1998.

[GZ00] C. W. Gardiner and P. Zoller. *Quantum Noise*. Springer, 2000.

[HDE+06] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel. Entanglement in graph states and its applications. In *Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos"*, 2006.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1–8, 1996.

[HHH99] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60:1888, 1999.

[HHR+05] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, , and R. Blatt. Scalable multiparticle entanglement of trapped ions. *Nature*, 438:643–646, 2005.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[HJ91] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1991.

[HKL04] J. A. Holbrook, D. W. Kribs, and R. Laflamme. Noiseless subsystems and the structure of the commutant in quantum error correction. *Quant. Inf. Proc.*, 2:381–419, 2004.

[HRP+06] T. Hime, P. A. Reichardt, B. L. T. Plourde, T. L. Robertson, C.-E. Wu, A. V. Ustinov, and J. Clarke. Solid-state qubits with current-controlled coupling. *Science*, 314(5804):1427–1429, 2006.

[Jam72] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys*, 3:275, 1972.

[Kan98] B. E. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393:133, 1998.

[KBLW01] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley. Theory of decoherence-free fault-tolerant universal quantum computation. *Phys. Rev. A*, 63:042307, 2001.

[Kem06] A. Kemp. *Quantum and thermal phase escape in extended Josephson systems*. PhD thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2006.

[KI96] T. Kato and M. Imada. Macroscopic quantum tunneling of a fluxon in a long Josephson junction. *J. Phys. Soc. Jpn.*, 65(2963), 1996.

[Kit97] A. Kitaev. Quantum computation: algorithms and error correction. *Russ. Math. Surv.*, 52(6):1191–1249, 1997.

[KKM+06] R. H. Koch, G. A. Keefe, F. P. Milliken, J. R. Rozen, C. C. Tsuei, J. R. Kirtley, and D. P. DiVincenzo. Experimental demonstration of an oscillator stabilized Josephson flux qubit. *Phys. Rev. Lett.*, 96:127001, 2006.

[Kle07] R. Klesse. Approximate quantum error correction, random codes, and quantum channel capacity. *Phys. Rev. A*, 75(06):062315, 2007.

[KLM01] E. Knill, R. Laflamme, and G. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

[KLP05] D. Kribs, R. Laflamme, and D. Poulin. Unified and generalized approach to quantum error correction. *Phys. Rev. Lett.*, 94(18):180501, 2005.

[KLR+08] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. Randomized benchmarking of quantum gates. *Phys. Rev. A*, 77:012307, 2008.

[KLZ98] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. *Proc. Roy. Soc. Lond. A*, 454:365, 1998.

[Kni05a] E. Knill. Quantum computing with realistically noisy devices. *Nature*, 434:39–44, 2005.

[Kni05b] E. Knill. Scalable quantum computing in the presence of large detected-error rates. *Phys. Rev. A*, 71:042322, 2005.

[Kra83] K. Kraus. *States, effects and operations: fundamental notions of quantum theory*, volume 190 of *Lecture Notes in Physics*. Springer-Verlag, 1983.

[Kri03] D. W. Kribs. Quantum channels, wavelets, dilations and representation of O_n. *Proc. Edin. Math. Soc.*, 46:421–433, 2003.

[KS06] D. W. Kribs and R. W. Spekkens. Quantum error correcing subsystems are unitarily recoverable subsystems. *Phys. Rev. A*, 74(04):042329, 2006.

[KSL07] R. L. Kosut, A. Shabani, and D. A. Lidar. Robust quantum error correction via convex optimization. E-print arXiv:quant-ph/0703274, 2007.

[KSW+05] N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter. Experimental analysis of a four-qubit photon cluster state. *Phys. Rev. Lett.*, 95:210502, 2005.

[KU04] V. K. Kaplunenko and A. V. Ustinov. Experimental test of a superconducting digital interface for vortex qubits. *Eur. Phys. J. B*, 38(1):3–8, 2004.

[LBHC01] M. Lewenstein, Kraus B, P. Horodecki, and J. I. Cirac. Characterization of separable states and entanglement witnesses. *Phys. Rev. A*, 4:6304, 2001.

[Leu03] D. W. Leung. Choi's proof as a recipe for quantum process tomography. *J. Math. Phys*, 44(2):528–533, 2003.

[LHA+08] E. Lucero, M. Hofheinz, M. Ansmann, R. C. Bialczak, N. Katz, M. Neeley, A. D. O'Connell, H. Wang, A. N. Cleland, and J. M. Martinis. High-fidelity gates in a single josephson qubit. *Phys. Rev. Lett.*, 100:247001, 2008.

[LKS+05] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland. Creation of a six-atom 'Schrödinger cat' state. *Nature*, 438:639–642, 2005.

[LL03] L. D. Landau and L. M. Lifshitz. *Quantum Mechanics: Non-Relativistic Theory*, volume 3. Elsevier Science, 3rd edition, 2003.

[LLEC07] B. Levi, C. Lopez, J. Emerson, and D. G. Cory. Efficient error characterization in quantum information processing. *Phys. Rev. A*, 75:022314, 2007.

[LSB+07] M. Laforest, D. Simon, J.-C. Boileau, J. Baugh, M. J. Ditty, and R. Laflamme. Using error correction to determine the noise model. *Phys. Rev. A*, 75:012331, 2007.

[LSP+07] A. Lupascu, S. Saito, T. Picot, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij. Quantum non-demolition of a superconducting two-level system. *Nature Physics*, 3:119–125, 2007.

[LZG+07] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan. Experimental entanglement of six photons in graph states. *Nature Physics*, 3:91–95, 2007.

[Mat05] *Mathematica*. Wolfram Research, Inc., Champaign, Illinois, 5th edition, 2005.

[ML06] M. Mohseni and D. A. Lidar. Direct characterization of quantum dynamics. *Phys. Rev. Lett*, 97(17):170501, 2006.

[MNBS05] W. J. Munro, K. Nemoto, R. G. Beausoleil, and T. P. Spiller. High-efficiency quantum-nondemolition single-photon-number-resolving detector. *Phys. Rev. A*, 71:033819, 2005.

[MNS05] W. J. Munro, K. Nemoto, and T. P. Spiller. Weak nonlinearities: a new route to optical quantum computation. *New J. Phys.*, 7:137, 2005.

[MOL+99] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Wal, and S. Lloyd. Josephson persistent-current qubit. *Science*, 285:1036, 1999.

[MPtH+05] J. B. Majer, F. G. Paauw, A. C. J. ter Haar, C. J. P. M. Harmans, and J. E. Mooij. Spectroscopy on two coupled superconducting flux qubits. *Phys. Rev. Lett.*, 94:090501, 2005.

[MR06] K. Goyal A. McCauley and R. Raussendorf. Purification of large bicolorable graph states. *Phys. Rev. A*, 74:032318, 2006.

[MS78] D. W. McLaughlin and A. C. Scott. Perturbation analysis of fluxon dynamics. *Phys. Rev. A*, 18:1652–1680, 1978.

[MSNM07] C. R. Myers, M. Silva, K. Nemoto, and W. J. Munro. Stabilizer quantum error correction with quantum bus computations. *Phys. Rev. A*, 76:012303, 2007.

[MSS01] Y. Makhlin, G. Schön, and A. Shnirman. Quantum-state engineering with Josephson-junction devices. *Rev. Mod. Phys.*, 73:357, 2001.

[MSS+05] R. McDermott, R. W. Simmonds, M. Steffen, K. B. Cooper, K. Cicak, K. D. Osborn, S. Oh, D. P. Pappas, and J. M. Martinis. Simultaneous state measurement of coupled josephson phase qubits. *Science*, 307(5713):1299–1302, 2005.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 1st edition, 2000.

[ND05] M. A. Nielsen and C. M. Dawson. Fault-tolerant quantum computation with cluster states. *Phys. Rev. A*, 71(04):042323, 2005.

[NHY+07] A. O. Niskanen, K. Harrabi, F. Yoshihara, Y. Nakamura, S. Lloyd, and J. S. Tsai. Quantum coherent tunable coupling of superconducting qubits. *Science*, 316(5825):723–726, 2007.

[Nie02] M. A. Nielsen. A simple formula for the average gate fidelity of a quantum dynamical operation. *Phys. Lett. A*, 303:249–252, 2002.

[Nie05] M. Nielsen. Cluster-state quantum computation. E-print arXiv:quant-ph/0504097, 2005.

[NM04] K. Nemoto and W. J. Munro. Nearly deterministic linear optical controlled-not gate. *Phys. Rev. Lett.*, 93:250502, 2004.

[NMR+06] C. Negrevergne, T.S. Mahesh, C. A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D.G. Cory, and R. Laflamme. Benchmarking quantum control methods on a 12-qubit system. *Phys. Rev. Lett.*, 96:170501, 2006.

[NP07] M. A. Nielsen and D. Poulin. Algebraic and information-theoretic conditions for operator quantum error correction. *Phys. Rev. A*, 75:064304, 2007.

[OD91] T. P. Orlando and K. A. Delin. *Foundations of Applied Superconductivity*. Prentice Hall, 1991.

[OMT+99] T. P. Orlando, J. E. Mooij, L. Tian, C. H. van der Wal, L. Levitov, S. LLoyd, and J. J. Mazo. Superconducting persistent-current qubit. *Phys. Rev. B*, 60:153988, 1999.

[PdGHM07] J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij. Demonstration of controlled-not quantum gates on a pair of superconducting quantum bits. *Nature*, 447:836–839, 2007.

[Ple05] M. B. Plenio. Logarithmic negativity: A full entanglement monotone that is not convex. *Phys. Rev. Lett.*, 95:090503, 2005.

[Pre97] J. Preskill. Fault-tolerant quantum computation. E-print arXiv:quant-ph/9712048, 1997.

[Pre98] J. Preskill. Reliable quantum computers. *Proc. Roy. Soc. Lond. A*, 454:385–410, 1998.

[PV07] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *Quant. Inf. Comp.*, 7(1/2):1–51, 2007.

[PYA+03] Yu. A. Pashkin, T. Yamamoto, O. Astafiev, Y. Nakamura, D. V. Averin, and J. S. Tsai. Quantum oscillations in two coupled charge qubits. *Nature*, 421:823–826, 2003.

[Raj82] R. Rajaraman. *Solitons and Instantons: an introduction to solitons and instantons in quantum field theory*. North Holland, 1982.

[Rau03] R. Raussendorf. *Measurement-based quantum computation with cluster states*. PhD thesis, Ludwig-Maximilians-Universität München, 2003.

[RB01] R. Raussendorf and H.-J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[RB02] R. Raussendorf and H. Briegel. Computational model underlying the one-way quantum computer. *Quant. Inf. Comp.*, 2(6), 2002.

[RGM+03] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy. Quantum computation with optical coherent states. *Phys. Rev. A*, 68:042319, 2003.

[RH07] R. Raussendorf and J. Harrington. Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.*, 98:190504, 2007.

[RHG06] R. Raussendorf, J. Harrington, and K. Goyal. A fault-tolerant one-way quantum computer. *Annals of Physics*, 321:2242, 2006.

[RKS+06] M. Riebe, K. Kim, P. Schindler, T. Monz, P. O. Schmidt, T. K. Körber, W. Hänsel, H. Häffner, C. F. Roos, and R. Blatt. Process tomography of ion trap quantum gates. *Phys. Rev. Lett.*, 97:220407, 2006.

[RMK+08] C. F. Roos, T. Monz, K. Kim, M. Riebe, H. Häffner, D. F. V. James, and R. Blatt. Nonlinear coupling of continuous variables at the single quantum level. *Phys. Rev. A*, 77:040302(R), 2008.

[RW05] M. Reimpell and R. F. Werner. Iterative optimization of quantum error correcting codes. *Phys. Rev. Lett.*, 94(08):080501, 2005.

[SAB+06] M. Steffen, M. Ansmann, R. C. Bialczak, N. Katz, E. Lucero, R. McDermott, M. Neeley, E. M. Weig, A. N. Cleland, and J. M. Martinis. Measurement of the entanglement of two superconducting qubits via state tomography. *Science*, 313(5792):1423—1425, 2006.

[SBJM97] A. Shnirman, E. Ben-Jacob, and B. Malomed. Tunneling and resonant tunneling of fluxons in a long Josephson junction. *Phys. Rev. B*, 56:14677, 1997.

[Sch35] E. Schrödinger. Discussion of probability relations between separated systems. *Proc. Cambridge Philos. Soc.*, 31:553, 1935.

[Sch00] W. P. Schleich. *Quantum Optics in Phase Space*. Wiley-VCH, 2000.

[SDKO07] M. Silva, V. Danos, E. Kashefi, and H. Olivier. A direct approach to fault-tolerance in measurement-based quantum computation via teleportation. *New J. Phys.*, 9:192, 2007.

[Sho95] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493, 1995.

[Sho96] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, page 56, 1996. E-print arXiv:quant-ph/9605011.

[Slo08a] N. J. A. Sloane. Integer sequence a000292, 2008.

[Slo08b] N. J. A. Sloane. Integer sequence a010968, 2008.

[SM08] M. Silva and C. R. Myers. Computation with coherent states via teleportations to and from a quantum bus. E-print arXiv:0804.4344, 2008.

[SMKE07] M. Silva, E. Magesan, D. W. Kribs, and J. Emerson. Experimentally scalable protocol for identification of correctable codes. E-print arXiv:0710.1900, 2007.

[SNB+06] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn. Quantum computation by communication. *New J. Phys.*, 8:30, 2006.

[Ste96a] A. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793, 1996.

[Ste96b] A. Steane. Multiple particle interference and quantum error correction. *Proc. Roy. Soc. Lond. A*, 452:2551–2577, 1996.

[Ste03] M. Steiner. Generalized entanglement robustness. *Phys. Rev. A*, 67:054305, 2003.

[SVP+05] I. Siddiqi, R. Vijay, F. Pierre, C. M. Wilson, L. Frunzio, M. Metcalfe, C. Rigetti, R. J. Schoelkopf, M. H. Devoret, D. Vion, and D. Esteve. Direct observation of dynamical bifurcation between two driven oscillation states of a josephson junction. *Phys. Rev. Lett.*, 94:027005, 2005.

[SW01] B. Schumacher and M. D. Westmoreland. Approximate quantum error correction. E-print arXiv:quant-ph/0112106, 2001.

[SW02] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65(01):012308, 2002.

[Ter00] B. M. Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A*, 271:319, 2000.

[Tin04] M. Tinkham. *Introduction to Superconductivity*. Dover, 2nd edition, 2004.

[vK04] N. G. van Kampen. A new approach to noise in quantum mechanics. *J. Stat. Phys.*, 115(3–4):1057–1072, 2004.

[VT99] G. Vidal and R. Tarrach. Robustness of entanglement. *Phys. Rev. A*, 59:141–155, 1999.

[VW02] G. Vidal and R.F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:32314, 2002.

[Wal00] A. Wallraff. *Fluxon dynamics in annular Josephson junction: from relativistic strings to quantum particles*. PhD thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2000.

[Wei08] E. W. Weisstein. "Erfc" from MathWorld — A Wolfram Web Resource., 2008.

[WHE+04] Y. S. Weinstein, T. F. Havel, J. Emerson, N. Boulant, M. Saraceno, S. Lloyd, and D. G. Cory. Quantum process tomography of the quantum fourier transform. *J. Chem. Phys.*, 121(13):6117–6133, 2004.

[WLL+03] A. Wallraff, A. Lukashenko, J. Lisenfeld, A. Kemp, M. V. Fistul, Y. Koval, and A. V. Ustinov. Quantum dynamics of a single vortex. *Nature*, 425:155–158, 2003.

[WM94] D. F. Walls and G. Milburn. *Quantum Optics*. Springer-Verlag, Berlin, 1994.

[YHN+06] F. Yoshihara, K. Harrabi, A. O. Niskanen, Y. Nakamura, and J. S. Tsai. Decoherence of flux qubits due to 1/f flux noise. E-print arXiv:cond-mat/0606481, 2006.

[YN05] J. Q. You and F. Nori. Superconducting circuits and quantum information. *Physics Today*, 58(11):42, 2005.

[YNM06] F. Yamaguchi, K. Nemoto, and W. J. Munro. Quantum error correction via robust probe modes. *Phys. Rev. A*, 73:060302R, 2006.

[YPA+03] T. Yamamoto, Yu. A. Pashkin, O. Astafiev, Y. Nakamura, and J. S. Tsai. Demonstration of conditional gate operation using superconducting charge qubits. *Nature*, 425:941–944, 20003.

[ZL96] W. H. Zurek and R. Laflamme. Quantum logical operations on encoded qubits. *Phys. Rev. Lett.*, 77:4683 – 4686, 1996.

[ZLC00] X. Zhou, D. W. Leung, and I. L. Chuang. Methodology for quantum logic gate construction. *Phys. Rev. A*, 62:052316, 2000.

[ZR97] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79:3307–3309, 1997.