Ancillas in Quantum Computation: Beyond Two-Level Systems

Timothy James Proctor

School of Physics and Astronomy
University of Leeds

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

March 2016

I confirm that the work submitted in this thesis is my own, except where work which has formed part of jointly authored publications has been included. The contribution of myself and the other authors to this work has been explicitly indicated below. I confirm that appropriate credit has been given within the thesis where reference has been made to the work of others.

Publications

Chapters 3 and 4 of this thesis are based on results from the preprint:

1. T. J. Proctor, *Low depth measurement-based quantum computation beyond two-level systems*, Preprint: arXiv:1510.06472 (2015).

I carried out all of the work included in these chapters and this preprint, which has been submitted to a peer-reviewed journal.

Chapter 5 is partially based on results from the publication:

2. T. J. Proctor, S. Dooley and V. Kendon, *Quantum computation mediated by ancillary qudits and spin coherent states*, Phys. Rev. A **91**, 012308 (2015).

I carried out all of the work included in this publication. S. Dooley contributed advice and guidance on the mathematics of spin ensembles and V. Kendon contributed general advice and supervision.

Chapters 6 and 7 of this thesis contain work that is included in the three publications listed below:

3. T. J. Proctor, E. Andersson and V. Kendon, *Universal quantum computation by the unitary control of ancilla qubits and using a fixed ancilla-register interaction*, Phys. Rev. A **88** (2013).

4. T. J. Proctor and V. Kendon, *Minimal ancilla mediated quantum computation*, EPJ Quantum Technology, **1**:13 (2014).

I carried out all of the work included in these two publications. In both cases, V. Kendon contributed general advice and supervision, and in the latter case, E. Andersson contributed to the initial idea the work is based upon.

5. T. J. Proctor, M. Giulian, T. Nakano, N. Korolkova, E. Andersson and V. Kendon, *Higher-dimensional ancilla-driven quantum computation* (in preparation). A preliminary version can be found in the preprint: arXiv:1510.06462 (2015).

The work from this publication that is included in this thesis encompasses novel material for qudits and quantum continuous variables (QCVs). I carried out all of the qudit-based work. M. Giulian and T. Nakano developed the basic model for QCVs, under the supervision of N. Korolkova and E. Andersson. The further analysis included herein of this QCV-based model was performed by myself. V. Kendon contributed general advice and supervision.

Parts of the introductory material of Chapters 1 and 2, and some of the results presented in Chapters 5, 6 and 7 have been published in the review paper

6. T. J. Proctor, V. Kendon, *Hybrid quantum computing using ancillas*, Contemporary Physics 1-18 (2016).

This thesis is dedicated to my wife.

Acknowledgements

I would like to begin by thanking my supervisor Viv Kendon. She has always been extremely helpful, encouraging and enthusiastic, and I am very gratefully to all of the opportunities she has afforded me throughout my PhD. I would also like to thank the other academics from the Leeds QI group, and in particular Almut Beige, who has been lumbered with the official duties of my supervision for the second half of my PhD. I am also very grateful to Birgitta Whaley for allowing me to spend an extended period of time in her research group at UC Berkeley, and I would like to thank the members of her group, and in particular Norm Tubman, for making me feel very welcome during my visit.

I would like to thank everyone I have collaborated with during my PhD, with particular thanks to Paul Knott and Jacob Dunningham as I have immensely enjoyed working with them. Furthermore, I would also like to thank all of the Postdocs and PhD students in the Leeds QI group during my time there, with special thanks going to Paul Knott, Adam Stokes, Shane Dooley, Suva De, Rob Bennett and Tom Barlow for enthusiastically participating in our highly enjoyable 'board-sessions'. Thanks are also due to all the wonderful friends I made during my time in Leeds, with James, Sami, Fred, Jess, Robin, Claire, Tom and Jo deserving a particular mention.

I am very gratefully to my family, and in particularly to my parents, for supporting and encouraging me throughout my life. I would like to thank everyone who has dedicated time and effort to teaching me, but special thanks are due to Nigel Butterworth, who all too briefly taught me physics at high school, and whose enthusiasm inspired me to study physics at university.

Finally, I would like to thank my wonderful wife Rebecca. I will look back with fondness on the brilliant times we spent together in Leeds, and I am particularly thankful for the support she has shown me during the final stages of my PhD. She has always shown the utmost love and kindness towards me and I am infinitely grateful that we will get to spend the rest of our lives together.

Abstract

Quantum computers have the potential to solve problems that are believed to be classically intractable. However, building such a device is proving to be very challenging. In this thesis, two physically promising settings for quantum computation are investigated: the one-way quantum computer and ancilla-based quantum gates. The majority of both the theoretical and experimental focus in the field of quantum computation has been on computation using 2-level quantum systems, known as *qubits*. In contrast to this, in this thesis I consider the relatively less well-understood setting of quantum computation using continuous variables or d-level quantum systems, called *qudits*. I develop a simple notation that encompasses each different encoding, and is applicable to a 'general quantum variable'. These ideas are then used to investigate computational depth (a proxy for time) in quantum circuits and one-way quantum computations in this general quantum variable setting. In doing so, the parallelism inherent in the one-way quantum computer is made precise.

In the second half of this thesis, a range of techniques are proposed for implementing entangling gates on a well-isolated computational register via interactions with 'ancillary' systems. In particular, ancilla-based quantum gates for general quantum variables are investigated - including the interesting case of *hybrid* quantum computation, whereby more than one encoding is used in tandem. The methods proposed herein each have their own unique advantages, such as: reducing gate-counts in certain circuits, allowing for inherently parallel computation, or minimising the physical requirements for universal quantum computation. In particular, the final gate techniques that are proposed in this thesis may implement any quantum computation using *only* a single fixed ancilla-register interaction gate and ancillas prepared in simple states. This then allows the computational register to consist of well-isolated 'memory' quantum variables and the ancillas need only be optimised for a single high-quality fixed interaction gate. Hence, this provides a simple and highly promising setting for physically implementing a quantum computer.

Contents

List of Figures

Abbreviations

1WQC	One-way quantum computer / computation
ADQC	Ancilla-driven quantum computer / computation
CLV	Classical variable
CTCT	Complexity-theoretic Church-Turing
GHZ	Greenberger-Horne-Zeilinger
GPG	Geometric phase gate
GJC	Generalised Jaynes Cummings
GKP	Gottesman-Kitaev-Preskill
LHS	Left hand side
MBQC	Measurement-based quantum computer / computation
MCM	Minimal control model
QCM	Quantum circuit model
QCV	Quantum continuous variable
QFT	Quantum Fourier transform
QHO	Quantum harmonic oscillator
QPU	Quantum processing unit
QV	Quantum variable
RHS	Right hand side
RUS	Repeat-until-success

Thesis overview

This thesis consists of three relatively distinct sections, outlined below.

Introduction

The introduction to this thesis encompasses Chapter 1 and 2. In Chapter 1 a brief and relatively non-technical introduction to quantum computers is provided. One purpose of this chapter is to present the interrelated motivations for each of the two distinct lines of investigation undertaken herein: the one-way quantum computer and ancilla-based gates. Much of the work in this thesis is presented in terms of 'general quantum variables' which encompass the three different variable types a quantum computer may be constructed from - qubits, non-binary d-level qudits, and quantum continuous variables. Hence, in order to motivate the work herein, a substantial portion of Chapter 1 is dedicated to explaining why quantum computation with these systems is of interest. Chapter 2 then provides a more technical introduction to the relevant ideas and mathematics of quantum computation. This will introduce the 'general quantum variable' formalism that is used throughout this thesis and which is, in my opinion, of interest in its own right. This chapter is aided by Appendices A to G in which a range of further background topics that are needed throughout this thesis are reviewed.

Quantum circuits and the one-way quantum computer

In the second part of this thesis, which encompasses Chapters 3 and 4, the computational depth and size properties of quantum circuits and the one-way quantum computer are compared, using the general quantum variable formalism. These chapters present a range of results that are novel outside of the qubit sub-case. Although the results of these chapters do have certain implications later in the thesis, they may be read without any reference to the work on ancilla-based gates included in the latter chapters herein. The results of Chapters 3 and 4 have been presented in Proctor (2015).

Ancilla-based quantum gates

In the final part of this thesis, which encompasses Chapters 5, 6 and 7, techniques are presented for mediating gates on a well-isolated 'computational register' via ancillary systems. This work is again presented within the general quantum variable framework. Hence, these chapters rely heavily on the 'general quantum variable' formalism that is proposed in Chapter 2. However, they can be largely read without reference to the investigations into computational complexity undertaken in Chapters 3 and 4 (there are some minor exceptions to this). Much of the work in these chapters may be found in Proctor et al. (2013, 2015); Proctor and Kendon (2014, 2015, 2016).

Technical summary of the ancilla-based gates

The remainder of this thesis overview consists of a summary of the different conditions and features of the three main ancilla-based models and methods that are proposed in this thesis. This is intended to be used only as a reference to clarify the subtle differences between the underlying ideas of Chapters 5, 6 and 7. It is strongly advised that the following technical summary is *not* read except for this purpose.

The three main ancilla-based models or gate methods in this thesis are the geometric phase gates (GPGs) of Chapter 5, the ancilla-driven quantum computer (ADQC) of Chapter 6, and the minimal control models (MCMs) of Chapter 7. The controls required over the computational and ancillary QVs in these models to achieve deterministic universal quantum computation on the computational register are summarised in the following table:

	Model		
	GPG	ADQC	MCM
Chapter	5	6	7
Fixed interaction	Yes	Yes	Yes
Preparation of ancillary QVs	No	Yes	Yes
Local gates on computational QVs	Yes	No	No
Local gates on ancillary QVs	Yes	No	No
Measurements on ancillary QVs	No	Yes	No

Certain subtleties and some adaptations to these models have not been detailed by this table and are summarised below:

The GPGs are valid with ancillary and computational QVs of different types (e.g., computational qubits and ancillary qudits). Although it is not specified in Chapter 5 that only a single fixed interaction should be used between the ancillary and register QVs, the basic GPGs in that chapter may still function under the restriction to such a fixed interaction (i.e., restricted to a fixed parameter hybrid controlled Pauli gate) as long as local controls are available - as indicated in the table above. Some of the more specific gate methods presented in Chapter 5, which extend the basic GPG, require ancillas prepared in particular states. However, these gate methods are not essential for universal quantum computation and are simply methods for reducing the number of gates needed to implement certain unitaries.

The ADQC model is valid when the ancillary and computational QVs are of the same type. This model is extended to include QVs of different types in Section 6.4.1, but it is then no longer a deterministic model of computation (i.e., it uses stochastic gate sequences). In Section 6.4.3 the ADQC model is adapted so as to not require any measurements (and hence it is then globally unitary) at the cost of now needing to be able to apply local unitary gates on the ancillas to obtain universality.

The MCMs presented in Chapter 7 are universal only for qubit or qudit-based computation. The first MCM, presented in Section 7.3, is applicable when the ancillary and register QVs are of different types (i.e., different dimension qudits). However, the model presented in Section 7.5, which is in my opinion the more practical of the MCMs, is only valid when the ancillary and register systems are qudits of the same dimension (which includes the case of qubits). In Section 7.4 a model is presented which improves on the first MCM in certain senses, but uses fixed measurements (and hence does not strictly fit into the conditions of MCM, as summarised in the table above) and can only implement gate sequences stochastically.

Chapter 1

Quantum computers

1.1 Classical computers

Digital computers have had an almost unparalleled impact in shaping the modern world. They have become both ubiquitous and indispensable: computer chips are in-built into an enormous range of everyday items, from mobile phones to televisions, and much of the world's essential infrastructure is utterly dependent on complex and powerful computer networks. Although the concept of computational machines stretches back to antiquity (e.g., the abacus), the theory of computation is a relatively young field. One of the earliest pioneers was Charles Babbage in the mid-nineteenth century who is credited with designing the first programmable computer. However, the independent discipline of computer science is often considered to have begun around the 1930's with the rigorous abstract work on computability of Alan Turing and Alonzo Church [Turing (1936) Church (1936)] amongst others (e.g., Stephen Kleene, Emil Post, and Kurt Gödel).

Initially building a digital computer was a huge challenge. The first computers able to outperform humans for basic arithmetic were developed in the 1940s, with an example of such an early computer, the Harwell Dekatron, shown in Figure 1.1. Modern computers have far outstripped the power of these pioneering machines and since then there has been an exponential increase in the power of both state-of-the-art and mass produced computers, known as *Moore's Law.*[1] However, this year-on-year improvement in silicon chip technology requires ever more ingenious engineering and cannot continue indefinitely, with a variety of important limiting factors [Chien and Karamcheti (2013); Markov (2014)]. Hence, in order to continue the advance of computational power, research into a range of alternative computational paradigms has become an active field, for example, various forms of 'natural

[1] This is due to a famous prediction by Gordon Moore in 1965 that there would be a doubling of the number of the transistors on a chip approximately every two years [Moore (1998)].

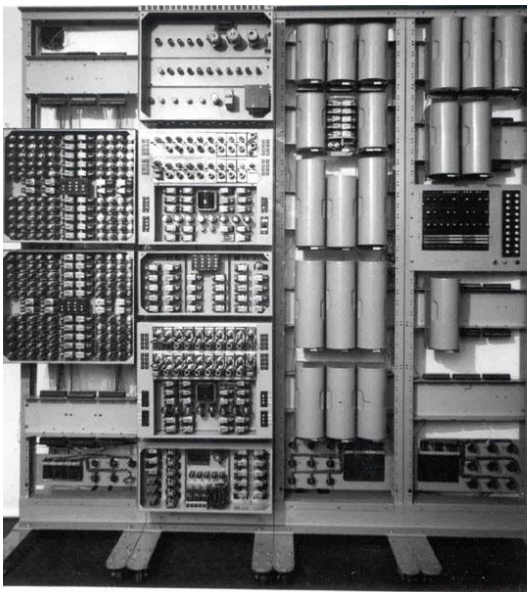


Figure 1.1: The Harwell Dekatron from 1951 which could compute basic arithmetic at a similar speed to a human. It could outperform human computers, as unlike people it did not need a break.

computation' such as molecular computers [Rozenberg et al. (2011)].

In this context, it is important to understand whether alternative computational models allow problems to be solved more quickly than with a conventional computer. To consider this, it is helpful to introduce the concept of an *efficiently solvable problem*. Most interesting computational problems may be defined for arbitrary input size N. Such a problem is called efficiently solvable if there is an algorithm that takes a number of time steps that is polynomial in N to solve it, using the elementary operations available to the computer (e.g., addition of bits). For example, the school-book algorithms for the addition and multiplication of two N-digit numbers require of order N and N^2 time steps respectively - assuming that the computer may add a single pair of one-digit numbers in a unit of time, as is the case when this is done by hand. Not all algorithms are of this sort: the time required may grow faster than any polynomial, for example it may be exponential in N (e.g., 2^N). Indeed, for many problems the obvious 'brute force' algorithm may well be of this sort. The reason that such an algorithm is considered inefficient is that it is of little practical use for anything but small input sizes (you may be willing to wait 2^{10} seconds for an algorithms output, but you should not consider waiting 2^{100} seconds as this is longer than the estimated age of the universe...). A famous example of a problem which has no known efficient (classical!) algorithm is the seemingly innocuous problem of finding the prime factors of an N-digit number. That solving this problem is strongly believed to be completely impractical is nicely illustrated by noting that widely used public-key cryptography methods, such as RSA encryption [Rivest et al. (1978)], would be rendered insecure by a fast prime factoring algorithm.

On the surface it would appear that whether an efficient algorithm exists might depend on the model of computation considered, i.e., what the basic information encoding and available operations are. One possible model to analyse these algorithm complexity issues with is the *Turing machine*, which manipulates symbols on a line of tape. Interestingly, the so-called complexity-theoretic Church-Turing (CTCT) thesis claims that it is only necessary to study whether a problem can be efficiently solved using this single model.[2] Specifically, the CTCT thesis states:

> *A Turing machine can efficiently simulate any realistic model of computation.*

There are two important points to note: firstly the 'realistic' qualifier is both essential and natural and should be taken to mean that the model is in principle physically realisable [Bernstein and Vazirani (1997)]; and secondly this does not imply that the Turing machine has a special place in computation as many models can also efficiently simulate the Turing machine. There are many examples which give support to this thesis, e.g., a Turing machine and a random-access-machine (RAM) - which is the model behind most physical computers - can simulate each other with low overhead [Katajainen et al. (1988)]. Different models may provide significant advantages in practice, but the point is that the CTCT thesis claims that whether or not a problem is fundamentally intractable is independent of the realistic computational model considered. Quantum computation presents a significant challenge to this idea and suggests the possibility that *some* problems that may never be practical on any classical computer can be solved if such a quantum device can be built.

1.2 From classical to quantum computation

At a fundamental level, nature does not obey the laws of 'classical' Newtonian physics and is instead quantum mechanical. The foundations of quantum theory were developed at the start of the 20th century and largely pre-date the abstract and practical development of computational machines. However, the suggestion that a machine based on the rules of quantum mechanics might be a useful computational device did not appear until the 1980s, with Richard Feynmann [Feynman (1982)] and David Deutsch [Deutsch (1985)] amongst the first to propose such a computer. This was initially largely inspired by, and proposed as a solution to, the

[2] The CTCT thesis is not due to either Church or Turing! It is an extension of their ideas on computability to complexity theory. It is sometimes called the strong Church-Turing thesis although this can refer to a range of slightly different statements.

inherent difficulty in using ordinary computers to simulate quantum physics [Feynman (1982)]. However, the wider ramifications of quantum computation became clear with the publication in 1994 of Shor's celebrated algorithm for efficient integer factoring using a quantum computer [Shor (1994, 1997)]. As discussed above, this is widely believed to be an intractable problem for a classical machine. Hence, Shor's algorithm suggests that quantum computers may have a larger class of efficiently solvable problems than classical computers, which directly calls into question the complexity-theoretic Church-Turing thesis.

Since 1994 there has been an explosion of interest in quantum computers, both in terms of developing the theory and attempting the daunting tasking of actually building such a device. The problem of factoring numbers is alone perhaps not of sufficient practical interest to justify building a quantum computer. However, there is an expanding range of applications for such a device, including database searching [Grover (1996)], machine-learning tasks [Schuld et al. (2015)], and techniques for simulation of quantum systems [Brown et al. (2010)]. The degree to which quantum computers may enhance classical processing is a particularly subtle and interesting area of ongoing research: it is known that many tasks are not amenable to improved efficiency using a quantum computer, and careful consideration is needed to account for the practicalities of actual computations [Aaronson (2005, 2015); Bennett et al. (1997)]. Nonetheless, the known enhancements cover a wide range of important computational processes, and it seems likely that many more applications will become apparent if a large-scale quantum computer can be engineered.

1.2.1 From classical bits to qubits

The overwhelming majority of modern classical computers are digital machines that encode information into a register of *bits*, which may each take the values 0 or 1, i.e., a bit has a state

$$\Psi_{\text{Bit}} \in \{0, 1\}. \tag{1.1}$$

The equivalent quantum system, known as a *qubit*, is a vector in a two-dimensional complex vector space with unit length, where 'length' is calculated by Pythagoras' theorem (i.e., it is defined by the Euclidean or l^2 norm). An orthonormal basis of this vector space consists of two vectors, and one such basis may be chosen to encode logical '0' and '1'. Using Dirac vector notation, we denote these basis states by $|0\rangle$ and $|1\rangle$, which hence satisfy $\langle q|q'\rangle = \delta_{q,q'}$ with $q, q' \in \{0, 1\}$, where $\langle . | . \rangle$ is the ordinary dot product of vectors and $\delta_{q,q'}$ is the Kronecker delta ($\delta_{q,q'} = 1$ if $q = q'$ and $\delta_{q,q'} = 0$ otherwise). Therefore, the allowed states of a qubit have the form

$$|\Psi_{\text{Qubit}}\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \quad \text{s.t.} \quad |\alpha|^2 + |\beta|^2 = 1, \tag{1.2}$$

which includes states that are neither definitely logical '0' nor '1' but are in a wave-like *superposition* of both. The physical interpretation of α and β is that $|\alpha|^2$ and $|\beta|^2$ are the probabilities that the qubit is projected into the states $|0\rangle$ or $|1\rangle$ respectively when measured (in this basis). The necessity for a specific concept of measurement is perhaps rather strange, and is tied up in the interpretational difficulties of quantum mechanics. However, it has a well-defined operational meaning which is entirely sufficient for the purposes of quantum computation. A perhaps more concrete representation of a qubit can be given as a column vector, as by using the natural association

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1.3}$$

which obeys the required orthonormalisation condition, then the qubit state above may be written as

$$|\Psi_{\text{Qubit}}\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{1.4}$$

A qubit may initially appear to be essentially the same as a classical bit in some probabilistic mixture of different states. Such a classical state is parameterised by two positive real numbers p_0 and p_1 which give the probabilities that the bit is 0 or 1 respectively, and hence $p_0 + p_1 = 1$. This may still be represented as a two-element column vector, e.g.,

$$\Psi_{\text{P-bit}} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}, \quad p_0, p_1 \in \mathbb{R}_{\geq 0} \quad \text{s.t.} \quad p_0 + p_1 = 1, \tag{1.5}$$

where the basis used here is such that $(1, 0)^T$ represents a bit in the state 0 and $(0, 1)^T$ represents a bit in the state 1. This demonstrates that the difference between a classical bit and a qubit is surprisingly subtle and may be largely understood as an alternative probability theory, whereby probabilities are extracted from vectors as the modulus squared of amplitudes rather than the amplitudes themselves, as summarised in Figure 1.2.

1.2.2 A register of qubits

A classical computer stores data in a 'register' of bits: for N bits there are 2^N different possible states these bits may be in, so the register can represent up to 2^N different numbers. At each step of the computation the register is in one of these states, e.g., one possible classical state is $\Psi_{N\text{-bits}} = (010100\ldots0)$. A quantum register of qubits may encode any superposition of these classical states simultaneously, as the state of this composite quantum system is some unit vector in the 2^N dimen-

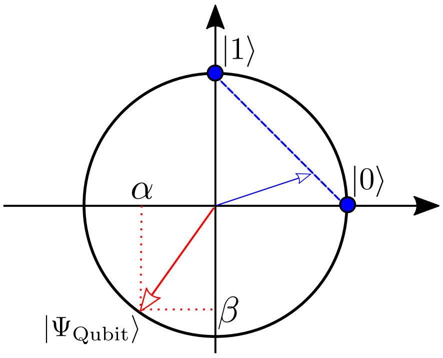


Figure 1.2: The state of a qubit $|\Psi_{\text{Qubit}}\rangle = \alpha|0\rangle + \beta|1\rangle$ for real α and β, may be represented as a point on the unit circle (red arrow) as $|\alpha|^2 + |\beta|^2 = 1$. The possible states of a classical bit are equivalent to $\alpha = 1$ or $\beta = 1$ (blue circles). A bit with classical probabilities to be 0 or 1 is parameterised by two non-negative numbers that sum to one (blue arrow and blue dashed line).

sional complex vector space obtained from a tensor product of each individual vector space. Mathematically, using the computational basis for each qubit as a basis for the whole system, the general state of a quantum register can be written as

$$|\Psi_{N\text{-qubits}}\rangle = \sum_{q_k \in \{0,1\}} \alpha_{q_1 \ldots q_N} |q_1 \ldots q_N\rangle, \tag{1.6}$$

with each $\alpha_{q_1 \ldots q_N} \in \mathbb{C}$ such that

$$\sum_{q_k \in \{0,1\}} |\alpha_{q_1 \ldots q_N}|^2 = 1. \tag{1.7}$$

To be clear, q_k is the computational basis state of the k^{th} qubit (zero or one), the sum runs over all permutations thereof, and this expression uses the shorthand notation that $|\psi, \phi\rangle \equiv |\psi\rangle \otimes |\phi\rangle$ which is used throughout (the ',' is retained or dropped for typographical convenience). This implies that a quantum register can represent a superposition of all possible N-bit numbers at once, which may seem like it has access to an unreasonable level of parallelism. However, the output of a computation is given by measuring the qubit register at the end of the computation, producing the single bit string $(q_1 q_2 \ldots q_N)$ with probability $|\alpha_{q_1 q_2 \ldots q_N}|^2$. Hence, a quantum algorithm needs to intelligently make use of the allowed superpositions to enhance the probability of the desired result, illustrating the subtlety of quantum programming [Aaronson (2015); Bacon and Van Dam (2010)]. Again, it may seem like this is similar to a classical computer with a distribution of probabilities to be in each bit string, parameterised by 2^N probabilities that sum to unity. However, the subtle difference in the allowed states (based on how probabilities are extracted) appear to make this a much more powerful model, as clearly demonstrated by Shor's algorithm [Shor (1994, 1997)] for which there is no known classical probabilistic equivalent.

1.2.3 Unitary transformations and quantum circuits

A quantum computation consists of transformations, U, that convert the total system from one allowed quantum state to another, i.e., they are maps

$$|\Psi_{N\text{-qubits}}\rangle \xrightarrow{U} |\Psi'_{N\text{-qubits}}\rangle. \tag{1.8}$$

As the state on which U acts has unit l^2 norm, i.e., $|\langle\Psi_{N\text{-qubits}}|\Psi_{N\text{-qubits}}\rangle| = 1$, and so must all quantum states, a property required of the transformations is that they preserve this norm. The relevant transformations are called *unitary operators*, which have the defining property that

$$UU^\dagger = U^\dagger U = \mathbb{I}, \tag{1.9}$$

which clearly implies that they preserve the l^2 norm, where throughout $\mathbb{I}$ will represent the identity operator of the appropriate dimension and $U^\dagger$ is the Hermitian adjoint of U. Any unitary operator acting on a d-dimensional vector may be represented by a $\mathbb{C}$-valued $d \times d$ matrix, and hence the evolution stage of a quantum computation is some global N-qubit unitary operator which may be represented by a $2^N \times 2^N$ matrix. In quantum computation, unitary operators are often called *gates*, and both terms will be used here (largely interchangeably).

To implement a quantum computation described by a given global unitary, it must be decomposed into some physically available set of basic operations. Importantly, any N-qubit unitary can be exactly composed from the tensor product and multiplicative product of gates acting on only one or two qubits at a time [DiVincenzo (1995)]. Any set of gates that can (approximately) implement any quantum computation is called a *universal gate set*, and a common example of such a set consists of the three unitaries CNOT, H and T [Boykin et al. (2000)], defined by their matrix representation in the computational basis:

$$\textsc{cnot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}. \tag{1.10}$$

A natural way to represent a quantum computation is in terms of a *circuit diagram* as shown in Figure 1.3, which uses gates from the set given above.

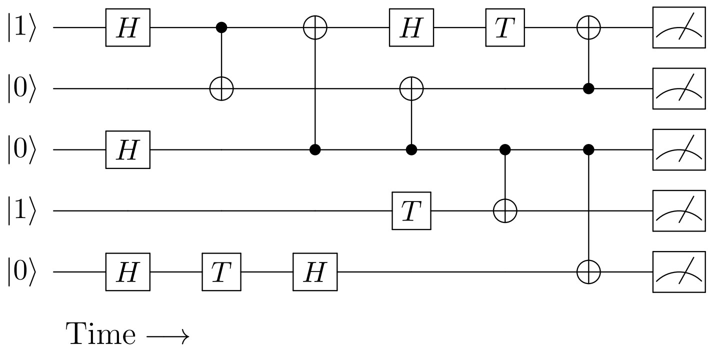


Figure 1.3: A circuit diagram may be used to represent a gate sequence, where a wire represents each qubit, time flows from left to right and symbols on or connecting wires represent gates. A box containing u denotes the unitary u acting on the wire(s) it covers (e.g., here the two gates H and T are used). The two-qubit gate here is the standard notation for CNOT. A circuit may terminate with measurements of some or all of the qubits or it may instead output a quantum state.

It is important to note that the availability of a universal gate set does *not* imply that any N-qubit unitary can be implemented efficiently: the computation is efficient only if it requires some polynomial-in-N number of gate *layers*, where a layer contains at most one gate acting on each qubit, e.g., there are six layers in the circuit of Figure 1.3. This may be clarified by an example: Shor's algorithm for an N-bit input is efficient as it can be implemented in of order N^3 gate layers using only operations that act on one and two-qubits at a time [Beckman et al. (1996)]. It may appear that which algorithms can be efficiently implemented will depend on the particular choice of universal gate set, but as long as the set is physically reasonable this is not the case. This is discussed in Chapter 2, where universal quantum computation is covered in much greater detail.

1.2.4 Quantum computing with errors

To date, a useful quantum computer is yet to be built. Given the amount of time and effort dedicated to developing such a device, this clearly indicates that this is a difficult task! The root of the problem is that accurately manipulating quantum systems and preserving their highly fragile states is inherently challenging. Furthermore, generically the difficulty grows with the size of the total quantum system, as should be expected by considering the absurdity of Schrödinger's famous dead-and-alive cat thought experiment [Schrödinger (1935)]. This might suggest that a useful quantum computer, which requires many qubits, can never be realised in the real world where imperfections exist and nothing can be controlled with infinite precision. Indeed, there are other computational models which also appear to improve on the Turing machine paradigm but which are probably not physically realistic, for example computation with perfect-precision real numbers. An interesting overview of such models is given in Aaronson (2005). However, there is good reason to be optimistic that quantum computation really can be implemented due to the theories of quantum error detection and correction, culminating in the concept of fault-tolerant quantum computation [Aharonov and Ben-Or (1997); Knill et al. (1998); Shor (1995); Steane (1996)]. A very basic outline of one of the main underlying ideas in quantum error correction is now given.

In a classical digital computer, real world imperfections can be mitigated by allowing for large error margins between the physical states encoding zero and one, e.g., substantially different voltages. Additionally, bits can be duplicated, for example by letting 0 → 000. A bit flip error can then be found and corrected by taking a majority verdict on the correct value, that is, if 000 → 010, it is corrected to 000. This cannot be directly applied to quantum computation as unknown quantum states cannot be duplicated: the transformation $|\Psi\rangle|\Phi_{\text{fixed}}\rangle \rightarrow |\Psi\rangle|\Psi\rangle$ defined for all inputs $|\Psi\rangle$ is not unitary (it is nonlinear), which is known as the *no-cloning theorem* [Wootters and Zurek (1982)]. However, rather than copying a quantum state, *logical* basis states can be encoded over many physical qubits. For example, we may associate

$$|0\rangle_{\text{logic}} \equiv |000\rangle, \qquad |1\rangle_{\text{logic}} \equiv |111\rangle, \tag{1.11}$$

and hence a logical qubit is then stored in the three-physical-qubit state

$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle. \tag{1.12}$$

Now, consider the case in which there is some (hopefully small) probability that any physical qubit may suffer a bit-flip error, (i.e., $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$). For example, an error on the first qubit gives

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow{\text{bit-flip error}} \alpha|100\rangle + \beta|011\rangle. \tag{1.13}$$

It is essential to not destroy the quantum superposition, which will happen if any individual qubit is measured to find out if it is in the state $|0\rangle$ or $|1\rangle$. However, this encoding allows such an error to be detected by instead asking only what the parity (i.e., sum modulo 2) is of both the first and second qubit pair, and the second and third qubit pair. This has four possible outcomes, 00, 01, 11 and 10, and it is easily confirmed that these correspond to no error, and an error on the first, second and third qubit respectively. Importantly, the measurement does not distinguish between the two logical basis states (with or without a bit flip error). If an error is detected it can then be corrected by flipping that qubit.

There are obvious limitations to this protocol: for example, it cannot cope with two bit flip errors or errors of a different form, and it does not protect the state from being destroyed if knowledge about whether the state of any physical qubit is $|0\rangle$ or $|1\rangle$ is leaked into the environment. Although more advanced error correcting codes do exist that allow for general single qubit errors to be corrected for [Laflamme et al. (1996)], error detection and correction needs to be accompanied by methods to implement logical gates on the logical qubits, via manipulations of the physical qubits using gates which themselves are not perfect, and whilst still maintaining the logical qubits protection from errors! Such a procedure is known as fault-tolerant quantum computation. In principle, a quantum computation of arbitrary length can be implemented using these techniques, as long as the physical error rate is below some constant threshold value (with this value depending on the techniques used) [Aharonov and Ben-Or (1997)]. There is now a vast array of ingenious methods to protect quantum states and implement robust computation, for example see Aharonov and Ben-Or (1997); Knill et al. (1998); Shor (1995); Steane (1996) for early work in this area and Brown et al. (2015); Fowler (2013); Klesse and Frank (2005); Raussendorf and Harrington (2007); Terhal (2015) for a selection of more recent work, with a clear introductory review provided by Gottesman (2010).

1.3 Beyond two-level quantum systems

Classical digital computers need not be formulated with bits but may instead use any $d \in \mathbb{N}$ base logic, with the basic d-valued unit often called a *dit*. Interestingly, in the opinion of the eminent computer scientist Donald Knuth, ternary logic is “perhaps the prettiest number system of all” [Knuth (1980)[3]]. Alternatively, computers need not be digital at all and may instead use an *analog* continuous variable encoding, where variables take values in $\mathbb{R}$ (in the ideal case). These machines predate the invention of the digital computer, with the 19th century mechanical differential analysers designed by James Thompson [Thomson (1875)] an important early example on which Claude Shannon later based the general theory of analog computation [Shannon (1941)]. In the formative years of the digital computer analog machines were still of practical importance, with an interesting example given by Enrico Fermi's ‘FERMIAC’ computer which was built in the late 1940s for Monte-Carlo simulations [Metropolis (1987)]. The different possible information encoding types, from base-2 ‘bits’ through to continuous variables, are illustrated in Figure 1.4.

As with classical computation, there is no *a priori* reason that a quantum computer must be formulated with base-2 logic and it may instead utilise any $d \in \mathbb{N}$

[3] He is referring to *balanced* ternary, which uses the values -1, 0 and 1, as opposed to standard ternary which uses 0, 1 and 2.

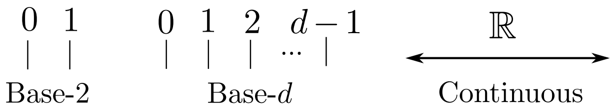


Figure 1.4: From left to right, information may be encoded into: two distinct states; d distinct states; a continuous degree of freedom.

base logic or a continuous variable information encoding. The majority of physical quantum systems have more than two levels and are not fundamentally qubits, as is the case with almost all systems being used to develop prototype quantum computers (e.g., atoms, ions, light modes, etc). To use such systems to encode a qubit they must be restricted to a two-dimensional subspace of their whole Hilbert space. Larger portions of the physically available Hilbert space may be harnessed by using a different information encoding, potentially making better use of the available quantum resources, and this provides a strong motivation for considering quantum computation beyond qubits. This may be of particular relevance to initially developing a useful quantum computer, especially given the limited numbers of quantum systems that can currently be interacted in a precisely controlled manner suitable for quantum computation.

A rigorous introduction to quantum computation with d-dimensional quantum systems, called *qudits*, and *quantum continuous variables* (QCVs) is delayed to Chapter 2, which will also cover the details of qubits not given in this introductory chapter via the special case of $d = 2$. As suggested by the title, large portions of this thesis will involve investigations of quantum computation without the restriction to qubits and therefore, to motivate the rest of this thesis, a more complete discussion of the known advantages and disadvantages of using non-qubit encodings is now given. This is then followed by a brief discussion of the experimental progress in manipulating these systems.

1.3.1 Beyond qubits: Advantages and disadvantages

Beyond the specific application of quantum computation, in quantum information there are a range of reasons for consider systems other than qubits. For example, quantum communication or entanglement sharing tasks (potentially important in a quantum computer) are likely to be most straightforward in a QCV setting [Andersen et al. (2010); Braunstein and van Loock (2005)], and an example of a concrete improvement of non-qubit encodings is the increased key rate in quantum cryptography obtained when qudits [Sheridan and Scarani (2010)] or QCVs [Jouguet et al. (2014)] are used. In the specific context of quantum computation, there are a range of known advantages (and some disadvantages) of both qudits and QCVs, which are considered in turn.

An especially striking advantage of qudits is that qudit quantum error correcting codes possess remarkable improvements with increased qudit dimension, as shown recently by a variety of authors [Andrist et al. (2015); Anwar et al. (2014); Campbell (2014); Campbell et al. (2012); Duclos-Cianci and Poulin (2013); Watson et al. (2015)]. Given the central role that error correcting will play in any eventual large-scale quantum computer (see the previous section), this is therefore a strong motivation to consider a qudit-based machine. A further advantage is that qudit algorithms have been shown to exhibit increased robustness and success probability with increased value of d [Parasa and Perkowski (2011, 2012); Zilic and Radecka (2007)]. An additional potential benefit inherent to $d > 2$ qudits is that, in comparison to a binary encoding, there is a $\log_2(d)$ reduction in the number of gates and subsystems required for a computation. The downside is that this is countered by the increased complexity of each gate (a single-qudit gate is a $d \times d$ unitary matrix) which is described by more parameters than a qubit gate, and hence any advantages would depend on the details of a given physical set-up [Muthukrishnan and Stroud Jr (2000); Stroud and Muthukrishnan (2002)].

Turning to QCVs, many problems are most naturally described using continuous parameters (e.g., most physics problems) and hence might be most directly encoded into QCVs. However, perfect-precision manipulation of QCVs is obviously impossible, and errors are generally more problematic in continuous variables (there is more to go wrong!). However, error-correction techniques have been developed for QCVs [Braunstein (2003); Lloyd and Slotine (1998); Ralph (2011); Van Loock (2010)] and despite the potential pitfalls, quantum systems which are naturally described as QCVs are some of the easiest to manipulate (see the next section). One possibility for taking advantage of QCVs is to instead use them in a *hybrid* quantum computer which employs different types of encoding simultaneously, e.g., qubits or qudits combined with QCVs. This idea has been used to construct simpler algorithms for finding eigensystems [Lloyd (2003); Travaglione and Milburn (2001)] and reduce gate-counts in quantum circuits [Brown et al. (2011)], as discussed in detail in Chapter 5.

Returning to discrete devices, hybrid qubit-qudit computers have also been previously shown to be useful for speeding up qubit-based logic [Borrelli et al. (2011); Lanyon et al. (2009); Ralph et al. (2007)]; ideas of this sort will be further developed later. Finally, a more physically grounded motivation for considering encodings beyond qubits is that if higher-dimensional systems are used as qubits, the extra unused physical levels must be considered to be part of the decoherence-inducing ‘environment’. Hence, any leakage out of the qubit computational space into these extra internal levels is a source of decoherence [Devitt et al. (2007); Ghosh et al.

(2013)], and if the natural processes of the physical system make this significantly likely, it may be better to actively use these levels rather than attempt to suppress them.

1.3.2 Beyond qubits: Physical realisations

Many quantum systems naturally allow for a $d > 2$ qudit or QCV encoding: for example, atoms and ions have many electronic energy levels and a light mode is the archetypal QCV but can also provides an obvious qudit encoding into photon number states. Focusing on qudits, it is important to note that the physical availability of more than two levels does not automatically mean that the system will be well-suited to encoding a good-quality qudit. For example, a system might have two ground states, and it might be possible to drive transitions between them using suitable laser pulse sequences. This may then provide a good-quality and controllable qubit. The other energy levels of the system could be used to encode further states for a $d > 2$ qudit, however if these quickly decay back into one of the ground states (e.g., via photon emission) such a qudit encoding would provide a very poor qudit with a very short lifetime and would be vastly inferior to the qubit logic encoding. Nevertheless, there is also no reason to suspect that there aren't systems which can provide high-quality qudits, and the very encouraging experimental progress in this direction is now discussed.

Experiments with qudits have been conducted in a variety of settings. For example, Neeley et al. (2009) have demonstrated the manipulation and measurement of a superconducting phase qudit with a dimension up to $d = 5$. A particular promising qudit experiment is that of Anderson et al. (2015); Smith et al. (2013) who in these two papers have demonstrated the control of a $d = 16$ qudit encoded into the hyperfine structure of the electronic ground state in the Caesium isotope ^{133}Cs. In particular, they have implemented very high quality state mappings [Smith et al. (2013)] and extended this to implement unitary gates with an average fidelity of over 98% as measured by randomised benchmarking [Anderson et al. (2015)]. A variety of experiments have demonstrated qudits encoded into photonic degrees of freedom [Bent et al. (2015); Lima et al. (2011); Walborn et al. (2006)] including the demonstration of techniques to create entangled photonic qudits [Dada et al. (2011); Rossi et al. (2009)] with Dada et al. (2011) creating entanglement between $d = 12$ qudits encoded into the orbital angular momentum of the photons.

Experiments that encode information into QCVs are largely based on optics. Although mainly limited to this one setting, these experiments are often some of the most impressive experimental demonstrations of various basic quantum information building blocks. For example, there are a range of experiments that demonstrate techniques for creating entangled QCVs [Menzel et al. (2012); Su et al. (2007);

Yokoyama et al. (2013); Yukawa et al. (2008)], including experiments designed to generate *cluster states*, which are a type of entangled state useful for *one-way quantum computation* - a very interesting model for implementing quantum computation introduced in Section 1.4.1. Particularly promising recent results are those of Chen et al. (2014) and Yokoyama et al. (2013) who have created entangled states useful for one-way quantum computation of 60 and 10,000 QCVs respectively. In Yokoyama et al. (2013) this is implemented using two light beams, with each QCV realised as a finite-length wave packet. However, the technique of Chen et al. (2014), in which QCVs are realised as different modes of an optical frequency comb, has the advantage that the QCVs are all simultaneously accessible and the created state is particularly well-suited to quantum computation. This state-of-the-art entanglement generation is complimented by experiments demonstrating quantum gates with QCVs, for example Ukai et al. (2011) and Su et al. (2013) have implemented basic gates in the one-way quantum computation paradigm, using four and six QCV entangled states respectively. In addition to this, there has been recent experimental progress in a range of quantum optics techniques that will be important for QCV computation, including major improvements in photon-number-resolving detectors [Calkins et al. (2013); Humphreys et al. (2015)] and matter-based quantum memories for photonic QCVs [Jensen et al. (2011)]. Finally, outside of quantum optics, there are also encouraging experiments using atomic ensembles to encode QCVs, for example see Gross et al. (2011); Krauter et al. (2013).

Before moving on, it is noted that the examples given here of qudit and QCV-based experiments can obviously be countered with many impressive qubit-based experiments showing precise controls of qubits in a huge range of systems, for example see Barends et al. (2014). The main point that I wish to emphasise here is that both qudits and QCVs are experimentally relevant, and it is likely that there will be further experimental progress made in this direction. Given that no one has yet built a quantum computer, it seems prudent to keep open the option of basing such a device on something other than qubits. As this thesis is largely concerned with avoiding any restrictions to qubit-only methods, it is convenient at this point to introduce the term *quantum variable* (QV) to encompass qubits, qudits and QCVs. This terminology, which to my knowledge is novel, and the mathematical machinery that I will develop in Chapter 2 to be applicable in this general setting, will prove highly convenient throughout this thesis.

1.4 Models for quantum computation

A basic postulate of quantum mechanics is that a closed system evolves in time via the Schrödinger equation

$$i\frac{\partial}{\partial t}|\Psi\rangle = \hat{H}|\Psi\rangle, \tag{1.14}$$

where $\hat{H}$ is the Hamiltonian of the system, which is some Hermitian operator, and where I have set $\hbar = 1$ and do so throughout. For a time-independent Hamiltonian the solution to the Schrödinger equation is

$$|\Psi(t)\rangle = e^{-i\hat{H}t}|\Psi(0)\rangle, \tag{1.15}$$

with $|\Psi(0)\rangle$ the initial state of the system. This is a unitary evolution, which follows easily from one of the defining properties of a Hermitian operator: $\hat{H}^{\dagger} = \hat{H}$. This leads to a natural and direct interpretation of a quantum circuit: Each QV in the circuit is encoded into a separate physical quantum system and to implement the gates in a layer of the circuit, the QVs are evolved in time via applying appropriate physically available Hamiltonians for precise lengths of time. I will call quantum computation in this fashion the *quantum circuit model* (QCM) [Barenco et al. (1995); Deutsch (1989)].

From a physical perspective, there are inherent challenges to implementing the quantum circuit model. Consider the generic case in which the aim is to implement some unitary

$$U = e^{-it\hat{H}_{\text{gate}}}, \tag{1.16}$$

acting on some number of QVs (e.g., a two-QV gate) where t takes a fixed value. As no experimental parameters which take values in $\mathbb{R}$ can ever be controlled exactly, the actual applied Hamiltonian will have some extra unwanted noise term acting on the system, i.e.,

$$\hat{H}_{\text{applied}} = \hat{H}_{\text{gate}} + \delta\hat{H}_{\text{noise}}, \tag{1.17}$$

and the actual evolution will be for some time $t_{\text{applied}} = t + \lambda t$, where hopefully $|\delta|$ and $|\lambda|$ are negligible. Furthermore, no quantum systems can ever be completely isolated from other nearby systems or fundamental fields with which they naturally interact. Hence, a further source of errors is interactions with this environment, i.e., the Hamiltonian applied actually has the form

$$\hat{H}'_{\text{applied}} = (\hat{H}_{\text{gate}} + \delta\hat{H}_{\text{noise}}) \otimes \mathbb{I}_{\text{environment}} + \epsilon\hat{H}_{\text{system+environment}}, \tag{1.18}$$

where $\hat{H}_{\text{system+environment}}$ represents the interactions with this environment and again hopefully $|\epsilon|$ is small. These interactions with the environment may be always active

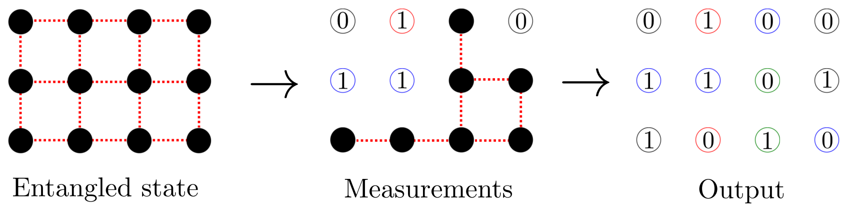


Figure 1.5: Quantum computation may be implemented by performing local measurements on a highly entangled states [Raussendorf and Briegel (2001)]. An entangled state is created, where here black circles represent QVs and dotted lines represent entanglement between QVs; measurements are then performed on individual QVs, here the outcomes are 0 and 1 and the colours represent measurements of different properties; finally, the output is obtained after all the QVs have been measured.

regardless of whether a gate is being implemented (i.e., even when $\hat{H}_{\text{gate}} = \mathbb{I}$). Although it has already been discussed that error-correction and fault-tolerance is possible in quantum computation, this only becomes applicable if the errors are below some threshold. Furthermore, if the error rate is not well below the threshold, the overhead in extra QVs and gates required for the error-correction may well be prohibitive, at least in early prototype quantum computers.

It should therefore be clear that in order for the quantum circuit model to be physically viable, each gate needs to be achieved with high enough accuracy to implement a minimal required quality of each gate whilst also maintaining sufficient lifetimes of the QVs before the environment destroys the quantum coherences. Put another way, the errors in the gates and the errors induced by the environment both need to be sufficiently small, where what is meant by 'sufficient' depends on the details of a specific task (e.g., the aim could be a small unprotected computation).

1.4.1 One-way quantum computation

One method for attempting to circumvent or minimise some of the problems in implementing the QCM is to adopt a different paradigm for quantum computation. One alternative that will be studied in this thesis is *one-way quantum computation* (1WQC), introduced by Raussendorf and Briegel (2001) with qubits and extended to qudits and QCVs by Zhou et al. (2003) and Menicucci et al. (2006) respectively. This model is also often termed *measurment-based* or *cluster-state* quantum computation. The basic idea of the 1WQC is that, rather than implementing gates on a register of QVs via Schrödinger-equation derived unitary evolution, the unitary gates of a computation are carried out on a logical level using only local (i.e., single-QV) measurements on a prepared entangled state. This is illustrated in Figure 1.5.

In the 1WQC, a time-ordering in the computation emerges because, in order to implement a useful computation, it is necessary for the choice of which measurements to perform to depend on some previous measurement outcomes. The final result may be calculated by simple classical post-processing on all the measurement outcomes. This procedure may be used to implement any desired quantum computation, and hence it may simulate any quantum circuit [Menicucci et al. (2006); Raussendorf and Briegel (2001); Zhou et al. (2003)], a fact that is not at all clear on an initial inspection. 1WQC is very promising from a physical perspective, as creating large entangled states is potentially much easier than precisely applying entangling gates to a register via unitary evolution. Consequently, there is already much experimental progress in this direction (as already mentioned in Section 1.3.2 in the context of QCVs), for example, see Bell et al. (2014); Chen et al. (2007, 2014); Lanyon et al. (2013); Su et al. (2013); Tame et al. (2014); Ukai et al. (2011); Yokoyama et al. (2013). However, it is important to note that, although the 1WQC has a range of advantages over a direct implementation of a quantum circuit, there are clearly still unavoidable difficulties related to imprecise controls: e.g., measurements and state preparation will always have errors associated with them.

The properties of qubit-based 1WQC have been extensively investigated, with Anders and Browne (2009); Broadbent and Kashefi (2009); Browne et al. (2007, 2011); Danos et al. (2007, 2009); Duncan and Perdrix (2010); Raussendorf et al. (2003) only a selection of the literature. However, there is much less known about this model in the more general case of qudits or QCVs. In Chapter 4 I present a rigorous comparison of the one-way model with quantum circuits that is applicable to all types of quantum variable. I provide mappings between quantum circuits and one-way computations and then use these to highlight the fundamental computational advantages inherent in one-way computation, which arise from its hybrid quantum-classical nature. In particular, the quantum processing part of 1WQC can in many cases be implemented in logarithmically less time than the equivalent quantum circuit. This extends results of Browne et al. (2011) to quantum computation with quantum variables of an arbitrary type.

In order to study the 1WQC with general QVs, an understanding of qudit and QCV quantum circuits will be required. As far as I am aware, the relevant circuits have to date not been studied in the literature and hence this is the subject of Chapter 3. This short chapter will include defining and exploring an *unbounded fan-out* model which will prove to be powerful for parallel quantum computation. This extends qubit-based results of Moore and Nilsson (2001) amongst others [Fang et al. (2006); Høyer and Špalek (2003, 2005); Moore (1999); Moore and Nilsson (1998, 2001); Takahashi et al. (2010)] to this more general QV setting.

1.4.2 Ancilla-based gates

Instead of departing entirely from the quantum circuit model paradigm, physically-motivated gate techniques can be layered on-top of an underlying quantum-circuit. Minimising environment-induced decoherence of computational QVs is achieved by choosing naturally well-isolated quantum systems (e.g., nuclear spins [Zhong et al. (2015)]) to encode these QVs into, but the very nature of well-isolated systems is that they are generically difficult to manipulate and it is particularly challenging to make these systems controllably interact with one another. Control and isolation are largely incompatible properties, and hence compromises must be made to optimise both properties as much as necessary. One practical method of engineering interactions between well-isolated QVs is by using an additional system to mediate the interaction. Such mediating systems are often called a *quantum bus* or an *ancilla*, and they can have different properties that optimise them for interactions, in contrast with the computational QVs optimised for isolation. Ancillas can be reset or discarded after a few gate operations, so they do not need to maintain coherence for the whole computation. This is common practice in the gate designs of a wide range of promising physical systems being developed for quantum computers. This ancillary system can have a range of different forms, for example the ancilla can be: additional collective internal degrees of freedom of the variables, e.g., vibrational modes of ions in an trap [Cirac and Zoller (1995)]; a physically distinct static system which may interact with a set of computational QVs, e.g., flux qubits coupling to a superconducting resonator [Stern et al. (2014); Wang et al. (2009); Xue (2012)]; a 'flying' quantum system which may implement gates between distant computational QVs, e.g., photons entangling spin [Carter et al. (2013); Luxmoore et al. (2013)] or atomic [Reiserer et al. (2014); Tiecke et al. (2014)] qubits. These latter two ideas are illustrated schematically in Figure 1.6.

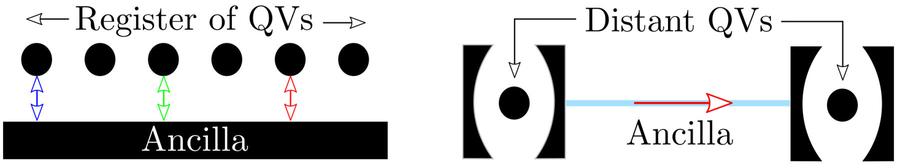


Figure 1.6: An *ancilla* or *quantum bus* may be used to implement the interactions required for a quantum computation. Left hand side (LHS): The ancilla can be a system which may interact in turn with a set of QVs. Here the different colour connections represent interactions at different times. Right hand side (RHS): Distant QVs can be coupled via a 'flying' ancilla. The schematic here represents atomic QVs trapped in separate cavities (e.g., using lasers) coupled using photons transmitted via an optical fibre.

The first important consideration is how an ancillary system may be used to mediate entangling gates on the computational QVs. An interesting and common technique consists of interacting two QVs simultaneously with an ancilla, e.g., via a Hamiltonian of the form

$$\hat{H} = \omega_a \hat{H}_a + \sum_{i=1,2} \omega_i \hat{H}_i + \sum_{i=1,2} g_i \hat{H}_{i,a}, \tag{1.19}$$

where $\hat{H}_a$, $\hat{H}_i$ and $\hat{H}_{i,a}$ represent the free ancilla Hamiltonian, the free Hamiltonian for the i^{th} QV and the interaction between the i^{th} QV and the ancilla respectively and ω_a, ω_i and g_i are constants. With particular Hamiltonians, and usually only approximately in some regime of the system (i.e., conditions on ω_a, ω_i and g_i), this may create an effective direct coupling between the two QVs. That is, in the relevant regime, $\hat{H}$ may be transformed into some effective Hamiltonian $\hat{H}_{\text{effective}} = \hat{H}_{1,2}$ which acts non-trivially on only the two QVs. For example, see Byrnes et al. (2012) where this technique is applied to coupling qubits encoded into Bose-Einstein condensates.

It is also interesting to consider the case where the ancillas may interact with different register QVs one-at-a-time via some Hamiltonian

$$\hat{H} = \omega_a \hat{H}_a + \omega_i \hat{H}_i + g_i \hat{H}_{i,a}, \tag{1.20}$$

which may be applied to any ancilla-register pair. Put another way, the QVs may interact in-turn with the ancillas via an interaction-time parameterised family of two-body unitaries $U(t) = e^{-i\hat{H}t}$ but not directly with each other. Methods to implement entangling-gates between register QVs using ancilla-mediation of this sort are the main topic of this thesis, encompassing Chapters 5, 6 and 7. The methods given will be formulated to apply as generally as possible to different quantum variable types and will cover the cases when the ancillary and register systems are either qubits, qudits or QCVs, including when the ancillas and register systems differ in QV type.

The first ancilla-based gate methods that will be introduced are the *geometric phase gates* and this is the subject of Chapter 5. The basic idea of such a gate is that by interacting with the register QVs, an ancilla picks up a phase which depends on the state of each register system:

$$|\Psi_{\text{ancilla}}\rangle \longrightarrow e^{i\theta(\Phi_{\text{register}})}|\Psi_{\text{ancilla}}\rangle, \tag{1.21}$$

where Φ_{register} schematically denotes the state of the register. The form of this phase can be chosen such that this is equivalent to an entangling gate between register QVs in conjunction with no action on the ancilla. This builds on previous work which considers using QCV ancillas to mediate gates between computational qubits, often termed the *qubus* model, see e.g., Brown et al. (2011); Proctor and Spiller (2012); Spiller et al. (2006). The novel contribution here is that it applies to registers and ancillas of all types (i.e., qubits, qudits and QCVs) and this more general construction will illuminate various interesting features of these methods. In the context of the qubus model, geometric phase gates have been shown to provide interesting advantages in terms of low gate-count circuits [Brown et al. (2011); Louis et al. (2007)]. Similar ideas will be seen to hold in the more general cases given here. This will then be used to obtain an understanding of what advantages can be gained from using higher-dimensional ancillas, and how these advantages depend on the variable types of both the computational systems and the ancillas. Both qudit and QCV ancillas will be shown to have distinct and inter-related computational advantages.

The geometric phase gate is sufficient to implement universal quantum computation on a register consisting of any variable type (i.e., qubit, qudit or QCV) when augmented with local controls of the individual ancillas and the computational QVs. However, local controls of either the register systems or the ancillas may not be easily available in some circumstances and a further disadvantage of the geometric phase gate is that it requires each computational QV involved in a gate to interact with the ancilla more than once. This latter constraint may be particularly problematic in some circumstances, such as with ancillas coupling distant QVs, e.g., photons coupling atoms in separate cavities. Hence, in Chapter 6 a method for implementing universal quantum computation on a register is presented which requires *only* sequential interactions of the register QVs (involved in the gate) with the ancillas using a *single fixed-time interaction gate* augmented with measurements of the ancillas. No further local controls of either the ancillas or the register are required. A model of this sort has been previously formulated for qubits by Anders et al. (2010), and is known as *ancilla-driven quantum computation* (ADQC). The novel contribution here is to extend this to be applicable to any variable type. A simple mapping between this model and 1WQC explored in Chapter 4 is provided for all QV types, which will show that ADQC may exploit the same computational advantages as 1WQC and is in some sense a hybrid between the QCM and 1WQC. Interestingly, deterministic gate implementation is only possible when the ancillary and computational registers are of the same QV type. However, when this is not the case I show that either quantum computation can be implemented stochastically, or determinism may be recovered by local controls on the register.

To realise the ADQC model of Chapter 6, experimental methods for implementing a range of (single-party) measurements on each ancilla are needed, and this may be challenging in some circumstances. Hence, in Chapter 7, a model is proposed whereby the required measurement is fixed. The cost of this added simplicity is that the model is again only probabilistic and requires gate sequences of indeterminate length. These ideas are similar to the recent work of Halil-Shah and Oi (2013, 2014) carried out in parallel to that herein. The probabilistic element of these models is highly undesirable and will add significant, and potentially unreasonable, overheads to the computation. Hence, the final type of gate methods proposed herein are designed to recover determinism by returning to globally unitary dynamics. The two distinct models proposed still only utilise a single fixed ancilla-register interaction gate and interestingly the *only* additional resource they require is preparation of ancillas in very simple states (from the computational basis). These deterministic models provide 'minimal control' methods for implementing universal quantum computation on a register via ancillary systems, and in my opinion have the potential to significantly simplify the realisation of a quantum computer.

In some cases, ancillas may not be required to implement basic gates, or they may use alternative techniques to those proposed herein. However, future designs for a universal, scalable and fault-tolerant quantum computer will likely be based around modular quantum processing units (QPUs) of some fixed size, e.g., a single ion-trap can hold only so many ion QVs. It will then be necessary to entangle individual QPUs via some ancillary systems, as illustrated in Figure 1.7. Hence, ancilla-based gate techniques may well be of importance to this higher-level aspect of quantum computer design, regardless of whether or not they are needed for the individual basic gates in the QPU. A recent proposal of this type is that of Nickerson et al. (2014) who aim to construct a scalable network of high fidelity quantum registers linked via more lossy optical ancillas. There are a variety of qubit register implementations that are suitable for this architecture, with one of the most advanced being ion trap technology, as suggested by Monroe et al. (2014) and recent promising experimental progress has been made in this direction [Hucul et al. (2015)].

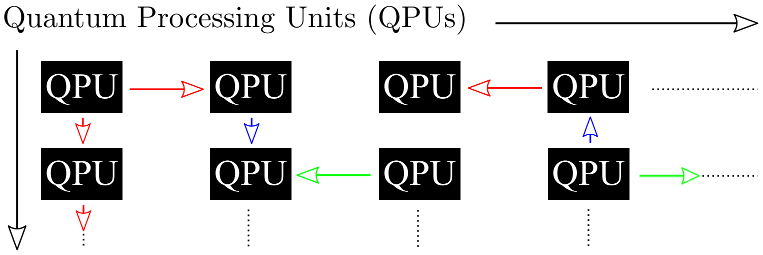


Figure 1.7: Many proposals for universal, scalable and fault-tolerant quantum computer utilise fixed-sized quantum processing units (QPUs) entangled via ancillary systems or 'quantum communication buses' [Monroe et al. (2014); Nickerson et al. (2014)]. Here the coloured arrows represent ancillas sent between different QPUs with the different colours representing different times.

1.4.3 Further models of quantum computation

Finally, before concluding this introductory chapter, it is noted that there are many different alternatives to, or adaptions of, the quantum circuit model. Although some are purely of abstract interest, e.g., the quantum Turing machine [Deutsch (1985)], as with the 1WQC and ancilla-based gates, most of these are largely designed to improve the physical viability of quantum computation. Important examples include: adiabatic quantum computing [Epstein (2012)]; spin chain models with ‘always on’ interactions [Hu et al. (2007); Lloyd (1993); Satoh et al. (2015)]; quantum walk models [Childs (2009); Childs et al. (2013)]; topological quantum computing using exotic quasi-particles [Pachos (2012)]; and a range of special purpose designs for quantum simulations [Brown et al. (2010)] or optimisation problems via quantum annealing [Das and Chakrabarti (2008); Trummer and Koch (2015)]. These ideas are not all necessarily entirely distinct, e.g. the one-way model can utilise topologically protected gates [Raussendorf et al. (2007)], and quantum annealing is closing related to adiabatic quantum computation. Each of these paradigms has its own advantages and disadvantages in the quest to overcome errors and decoherence, however these models are discussed no further herein.

1.5 Conclusions

Shor’s algorithm for efficient integer factorisation [Shor (1994, 1997)], is the most famous example from a range of evidence strongly suggesting that there are problems that are classically intractable which can be efficiently solved on a quantum computer, e.g., see Aaronson and Arkhipov (2011). Furthermore, there is a significant set of important computational problems that are expected to be amenable to a quantum-enhanced speed-up, which, beyond those related directly to integer-factoring, include machine-learning tasks [Schuld et al. (2015)], database searching [Grover (1996)] and simulation of quantum systems [Brown et al. (2010)] amongst others. Together, these provide substantial motivation for developing such a device.

The simplest basic element that a quantum computer may be constructed from is the qubit, which may exist in states that are a superposition of logical 0 and 1. However, there is no *a priori* reason that quantum computation should be formulated with two-level qubits and may instead employ d-level qudits or quantum continuous variables (QCVs). Indeed, there are good reasons for considering these more general quantum variables (QVs), ranging from their physical availability and the experimental progress made in manipulating them, to abstract computational advantages, such as improved error-correction techniques [Campbell (2014)] and improved algorithm success probabilities [Parasa and Perkowski (2012)].

The quantum circuit model (QCM), in which elementary gates are applied to

QVs via Schrödinger-equation derived unitary evolution, is the most well-known and simple model for a quantum computer. However, this requires precisely applying one and two-body Hamiltonians on-demand to a register of QVs, each of which must also be isolated to minimise environment-induced decoherence as much as required. These technical challenges motivate the exploration of alternative paradigms for quantum computation, with the one-way quantum computer (1WQC), as introduced by Raussendorf and Briegel (2001), one such model. In Chapter 4, I will give a detailed comparison of 1WQC and quantum circuits with arbitrary QV type, mainly focusing on an investigation into computational depth (a proxy for time) in these models.

One possibility which allows the register QVs in a quantum circuit to be optimised for coherence times is to use more easily controlled ancillary systems to mediate the required interactions between them. The majority of this thesis is on gate methods of this sort, with this topic encompassing Chapters 5, 6 and 7. The ideas covered range from the computational advantages available when using ancillas, as seen most clearly in Chapter 5, to minimising the required physical controls necessary to implement universal quantum computation, as considered in Chapter 6 and especially Chapter 7. In order to proceed further, a more technical introduction to quantum computation is required. This is the subject of the next chapter, which will introduce a general 'quantum variable' formulation for quantum computation that covers, in parallel, the key mathematics of qubits, qudits and QCVs that will be needed throughout this thesis.

Chapter 2

General quantum variables

In this chapter I review the terminology and mathematical tools for quantum computation using *qudits* of arbitrary finite dimension and *quantum continuous variables* (QCVs). I propose a simple unified *quantum variable* (QV) formulation that encompasses both qudits of any dimension and QCVs, which then enables a presentation of the structures in quantum computation that is valid simultaneously for each type of QV. This 'quantum variable' construction provides a succinct language for formulating further results about quantum computation with any type of QV and it will be used to this end throughout the remainder of this thesis. The underlying content introduced in this chapter, and encompassed by the general QV formalism, is almost exclusively a review of known material. However, this has previously been largely presented separately for qubits, qudits and QCVs and I am unaware of such a dimension-independent formulation of quantum computation anywhere in the literature.

2.1 Qubits, qudits and quantum continuous variables

2.1.1 Qudits: d-level quantum systems

The mathematics of qudits (i.e., finite-dimensional quantum mechanics) was initially developed by Hermann Weyl in the early decades of quantum theory [Weyl (1950)] and in the light of its relevance to quantum information it has since been extensively investigated, see e.g., the work of Gibbons et al. (2004); Klimov et al. (2009, 2005); Vourdas (2003); Wootters (1987), with Vourdas (2004) providing an excellent technical review in a broad context. The material relevant to this thesis is now covered, using the language of quantum computation. The state of a qudit is a vector of unit length in a d-dimensional complex vector space. An orthonormal basis of this vector space consists of d vectors, and such a basis may be picked out to encode the logical values $0, 1, \dots, d-1$ and denoted $|0\rangle, |1\rangle, \dots, |d-1\rangle$. The basis

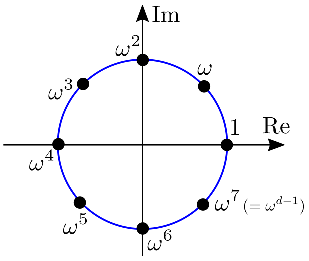


Figure 2.1: The d distinct d^{th} roots of unity are integer powers of $\omega = e^{2\pi i/d}$ and reside on the unit circle in the complex plane, illustrated here for $d = 8$.

states therefore obey $\langle q|q'\rangle = \delta_{q,q'}$. This is called the *computational basis*. Hence, the general state of a qudit may be written as

$$|\Psi_{\text{Qudit}}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{d-1}|d-1\rangle, \tag{2.1}$$

with $\alpha_q \in \mathbb{C}$ such that

$$|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{d-1}|^2 = 1. \tag{2.2}$$

As with a qubit, the physical interpretation of α_q is that $|\alpha_q|^2$ is the probability that the system is projected into the state $|q\rangle$ if measured. The d^{th} root of unity, $e^{2\pi i/d}$, will play an important role, and is denoted ω. It has the property that

$$\omega^0 + \omega^1 + \omega^2 + \cdots + \omega^{d-1} = 0, \tag{2.3}$$

as illustrated in Figure 2.1. Clearly the value of d determines the precise form of ω, as is also the case for all the objects introduced below, but everything discussed herein holds true and is presented without reference to its particular value unless otherwise stated.

The basic operators in qudit quantum computation are the (generalised) *Pauli operators* denoted X and Z, which are the natural unitary extension of two of the well-known *qubit* Pauli operators $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ respectively. They may be defined (as can any operator) by their action on the computational basis states:

$$X|q\rangle := |q+1\rangle, \qquad\qquad Z|q\rangle := \omega^q|q\rangle, \tag{2.4}$$

where the addition is modulo d, as on a clock with d hours, i.e., $(d-1)+1 = 0$. As a computation, the X gate has a clear classical analogue which simply adds 1 modulo d to a dit and is the natural extension of a bit flip ($0 \to 1$, $1 \to 1+1 = 0$ modulo 2). In contrast, the Z gate creates complex phase factors which do not have any obvious classical equivalent. Rather than using Dirac notation, these operators may be given a perhaps more familiar and concrete representation in terms of an array of numbers. Using the association

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \tag{2.5}$$

which obeys the necessary orthonormalisation condition, the Pauli operators are the $d \times d$ matrices

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix}. \tag{2.6}$$

In fact, these operators pre-date quantum theory and were originally introduced by James Sylvester in the 19th century [Sylvester (1882); Sylvester and Baker (2012)] and in other contexts are called the ‘shift’ and ‘clock’ matrices respectively. These operators have order d, obeying

$$X^d = Z^d = \mathbb{I}, \tag{2.7}$$

which, for $d = 2$, reduces to the well-known property that the qubit Pauli operators are self inverse. One important difference between the general case and the special case of a qubit is that, although the qubit Pauli operators are both Hermitian and unitary, the qudit operators for $d > 2$ are only unitary.

2.1.2 Quantum continuous variables

A *quantum continuous variable* (QCV) [Braunstein and van Loock (2005); Lloyd and Braunstein (1999)] is a quantum system with a continuous degree of freedom taking values in $\mathbb{R}$, e.g., translational position in one-dimension. A QCV is described by the Hermitian operators $\hat{x}$ and $\hat{p}$, generically termed ‘position’ and ‘momentum’, which obey the famous *canonical commutation relation*

$$[\hat{x}, \hat{p}] = i. \tag{2.8}$$

The spectrum of an operator is preserved under conjugation by a unitary operator, where $\hat{A}$ conjugated by $\hat{B}$ is the operator $\hat{C} = \hat{B}\hat{A}\hat{B}^{-1}$. Hence, the spectrum of $\hat{x}$ is the whole real line, $\mathbb{R}$, as $\hat{x}$ is Hermitian and

$$e^{-iq\hat{p}}\hat{x}e^{+iq\hat{p}} = \hat{x} + q, \tag{2.9}$$

for any $q \in \mathbb{R}$, which may be confirmed directly using the equation

$$e^{\hat{A}}\hat{B}e^{-\hat{A}} = \hat{B} + [\hat{A}, \hat{B}] + \frac{1}{2!}[\hat{A}, [\hat{A}, \hat{B}]] + \dots . \tag{2.10}$$

Therefore, the state $|q\rangle$ obeying $\hat{x}|q\rangle = q|q\rangle$ may be used to encode the logical real value $q \in \mathbb{R}$.[1] These states form the *computational basis.* The position eigenstates are not normalisable and instead obey the quasi-orthonormalisation relation $\langle q|q'\rangle = \delta(q - q')$ where $\delta(\cdot)$ is the Dirac delta function [Sakurai (1985)]. The general state of a QCV may then be written as

$$|\Psi_{\mathrm{QCV}}\rangle = \int_{-\infty}^{\infty} \mathrm{d}q \, \psi(q)|q\rangle, \tag{2.11}$$

where $\psi(q)$ is a $\mathbb{C}$-valued function obeying

$$\int_{-\infty}^{\infty} \mathrm{d}q \, |\psi(q)|^2 = 1. \tag{2.12}$$

The physical interpretation of $\psi(q)$ is that $|\psi(q)|^2$ is the probability density for q and the $\psi(q)$ function is simply the wavefunction familiar from 'elementary' wave mechanics.

Any wavefunction $\psi(q)$ such that $\int_{-\infty}^{\infty} \mathrm{d}q \, |\psi(q)|^2 < \infty$, called a square-integrable function, may be normalised and hence describes a physical state. However, not all functions are square-integrable, for example the delta function. This implies that the computational basis states (i.e., the $|q\rangle$) are themselves not physical as $|q'\rangle$ has a wavefunction $\delta(q - q')$. From an information-theoretic perspective, this is not surprising, as if such a state could be realised it would encode a perfect precision real number. However, these states can be approximated to any desired precision with a state that can be realised in principle, for example, a possible state is one which has a Gaussian wave function centred on q with a narrow peak, which is known as a *squeezed state* [Braunstein and van Loock (2005)]. This is shown in Appendix B for completeness. The exact realisation of these states is sometimes required to perfectly implement methods discussed or proposed herein. Whenever this is the case this will be explicitly commented upon.

[1] Note that these states are not part of the Hilbert space of square integrable functions and it is necessary to employ the larger structure of a 'rigged Hilbert space' to consider these states in a mathematically precise manner [De la Madrid (2005)]. Explicitly considering these technicalities is not necessary to outline the theory of QCV quantum computation - but they do provide a solid basis for these QCV manipulations.

The basic operators in QCV quantum computation are again known in this context as the Pauli operators and may be defined by their action on the computational basis

$$X(q')|q\rangle := \left|q + q'\right\rangle, \qquad Z(q')|q\rangle := e^{iqq'}|q\rangle, \qquad q, q' \in \mathbb{R}. \tag{2.13}$$

The $X(q)$ gate has the natural classical counterpart of addition in $\mathbb{R}$. The Pauli operators can also be expressed as exponentials of $\hat{x}$ and $\hat{p}$, specifically

$$X(q) = \exp(-iq\hat{p}), \qquad Z(q) = \exp(iq\hat{x}), \qquad q \in \mathbb{R}. \tag{2.14}$$

It can be confirmed that these have the required action on the position eigenstates with the aid of Equation 2.9. Outside the context of quantum information, these operators are normally termed position and momentum translations, respectively.

2.2 General quantum variables

The preceding section was structured in part to highlight that qudits and QCVs have basic properties in common. Although there are important differences, these are fairly subtle and broadly speaking these are due to the different properties of the set of integers, $\mathbb{Z}$, and the real line, $\mathbb{R}$. I now present a notational formulation of the above basic structures that encompasses both cases simultaneously and is applicable to a general *quantum variable* (QV), that is: a qubit, qudit or QCV. This formulation is novel and in my opinion will be of use in topics well beyond those considered in the remaining chapters of this thesis. Initially, this may seem overly complex and formal. However, it will allow the relevant material for qubits, qudits and QCVs that still needs to be introduced in the remainder of this chapter to be presented only once, using this general QV formulation, with any important differences between each type of QV noted. Before beginning, it is noted that there are various topics that *do* require particular variable types, e.g., some phase-space methods apply only to QCVs or prime (and power of prime) dimension qudits [Gibbons et al. (2004); Vourdas (2004); Wootters (1987)]. However, the majority of the work in this thesis will be independent of the particular type of QV.

The underlying structure on which a d-dimensional qudit is defined is the set of d integers

$$\mathbb{Z}(d) = \{0, 1, 2, ..., d-1\}, \tag{2.15}$$

along with modulo d arithmetic: this is known as the *ring* of the integers modulo d.

In contrast, the underlying structure for a QCV is the field of the real numbers $\mathbb{R}$.[2] To consider both qudits and QCVs simultaneously, it is useful to define

$$\mathbb{S}_d := \begin{cases} \mathbb{Z}(d) & \text{for a } d\text{-dimensional qudit,} \\ \mathbb{R} & \text{for a QCV.} \end{cases} \tag{2.16}$$

Using this notation, the *computational basis* for a QV may be taken to be some basis

$$\mathcal{B} := \{|q\rangle \mid q \in \mathbb{S}_d\}, \tag{2.17}$$

where the basis states obey the orthonormalisation condition that

$$\langle q|q'\rangle = \delta(q - q'), \tag{2.18}$$

where $\delta(q-q')$ represents the Kronecker delta for a qudit, normally denoted $\delta_{q,q'}$, and the Dirac delta function for QCVs.

The only further structures that have been introduced so far are the Pauli operators. In the QCV case these were continuously parameterised, and for a qudit they were simply fixed operators (i.e., constant matrices). However, for all QVs they may be taken to be a mapping from $\mathbb{S}_d$ to the unitary operators. This is achieved for qudits by defining

$$X(q) := X^q, \qquad Z(q) := Z^q, \qquad \forall q \in \mathbb{S}_d. \tag{2.19}$$

The $q = 1$ cases will appear regularly (even for QCVs), for both these and other $q \in \mathbb{S}_d$ parameterised gates introduced later. Hence, for any gate $G(q)$ with $q \in \mathbb{S}_d$ the shorthand $G \equiv G(1)$ will be used. Integer powers of the the d^{th} root of unity $\omega = e^{2\pi i/d}$ and a continuously parameterised phase factor were intrinsic to the definitions of the Pauli operators for qudits and QCVs, respectively. These can be unified into one notation by *defining* the dimensionality constant, d, for a QCV to be $d = 2\pi$. Then

$$X(q')|q\rangle = |q + q'\rangle, \qquad Z(q')|q\rangle = \omega^{qq'}|q\rangle, \qquad \forall q, q' \in \mathbb{S}_d. \tag{2.20}$$

where still $\omega = e^{2\pi i/d}$. Hence, this reduces to the required phase factor for each case, as can be seen with reference to Equations 2.4 and 2.13. Here, $q + q'$ should

[2] As an aside, the difference between a ring and a field is that every non-zero element of a ring does not necessarily have a multiplicative inverse whereas in a field it does (e.g., $1/a$ is the multiplicative inverse of non-zero $a \in \mathbb{R}$ as $a \cdot 1/a = 1$). Any element in $\mathbb{Z}(d)$ that is coprime with the dimension d has a multiplicative inverse in $\mathbb{Z}(d)$. Hence, prime dimension qudits are a special case because then every non-zero number in $\mathbb{Z}(d)$ is coprime with d and so this is precisely the cases in which the integers modulo d is a field (called a finite or Galois field).

be understood to be the appropriate arithmetic for $\mathbb{S}_d$, i.e., ordinary arithmetic in $\mathbb{R}$ for a QCV and modulo d arithmetic for a qudit. Often it will be convenient to use expressions such as $|-q\rangle$ or $X(-q)$. Whenever a value is used outside of $\mathbb{S}_d$, it should be understood to be modulo d for a d-dimensional qudit (for a QCV it is never outside the allowed values as this is all of $\mathbb{R}$). For instance, $|-1\rangle$ should be taken to mean $|-1 \text{ modulo } d\rangle = |d-1\rangle$ for a qudit. In some cases this is not strictly necessary, e.g., $X(-q)$ can be taken to mean X^{-q}, but it may always be assumed to be taken modulo d if it is unclear as to whether or not it is of consequence.

Before moving on, it is noted that in certain contexts (especially QCVs in quantum optics), the Pauli operators are often replaced by the entirely equivalent *displacement operators*, with the difference simply one of convention. The displacement operators for any QV type, denoted $\mathcal{D}(q,q')$, may be defined by their relation to the Pauli operators

$$\mathcal{D}(q,q') \propto Z(q')X(q). \tag{2.21}$$

A more detailed discussion of these operators is given in Appendix C.

2.2.1 The Fourier gate

An important unitary operator that will be required throughout is the Fourier gate, denoted F. As its name suggests, it is simply the unitary representation of the discrete and continuous Fourier transforms in the case of qudits and QCVs respectively. Explicitly,

$$F|q\rangle = \frac{1}{\sqrt{d}} \sum_{q' \in \mathbb{S}_d} \omega^{qq'} |q'\rangle, \tag{2.22}$$

where this summation notation denotes the sum or integral over all computational basis elements as appropriate. Specifically, for a d-dimensional qudit the sum runs over the values $q' = 0, \dots, d-1$, and in the QCV case this represents an integral over all computational basis elements. Hence, for a QCV

$$F|q\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dq' e^{iqq'} |q'\rangle. \tag{2.23}$$

The $\sum_{q\in\mathbb{S}_d}$ notation will be used throughout this thesis without further comment. Note that, for qubits, $F = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, which is more commonly known as the Hadamard gate and has been encountered briefly already in Equation 1.10, where following convention it was denoted H.

The Fourier gate is ubiquitous in quantum circuits, and its multi-system generalisation is a key ingredient in many quantum algorithms, e.g., Shor's algorithm [Shor (1994, 1997)], and will be encountered later. In Appendix D it is shown that this transformation is indeed unitary and that it has order 4, i.e.,

$$F^4 = \mathbb{I}. \tag{2.24}$$

Furthermore, it is also shown that for QCVs it is a particularly natural operator as it may be generated by the quantum harmonic oscillator (QHO) Hamiltonian

$$\hat{H}_{\text{QHO}} = \frac{1}{2}\left(\hat{x}^2 + \hat{p}^2\right), \tag{2.25}$$

applied for a time $t = 3\pi/2$. Many quantum systems are QHOs or may be approximated as such, e.g., a micro-mechanical resonator [Poot and van der Zant (2012)] or a single light mode [Gerry and Knight (2005); Radmore and Barnett (1997)]. As the QHO Hamiltonian is used occasionally in this thesis, the properties of $\hat{H}_{\text{QHO}}$ are considered in more depth in Appendix A.

The Fourier gate may be used to relate the Pauli operators to one another. Under conjugation by the Fourier gate, the Pauli operators are transformed with the cyclic relation

$$\begin{tikzcd} X(q) \arrow[r] & Z(q) \arrow[d] \\ Z(-q) \arrow[u] & X(-q), \arrow[l] \end{tikzcd} \tag{2.26}$$

where this represents $FX(q)F^\dagger = Z(q)$, $FZ(q)F^\dagger = X(-q)$, etc. This is also shown in Appendix D.

2.2.2 The conjugate basis

A *conjugate basis*, denoted $\mathcal{B}_+$, may be defined in terms of the action of the Fourier transform on the computational basis:

$$\mathcal{B}_+ := \{|+_q\rangle := F|q\rangle \mid q \in \mathbb{S}_d\}. \tag{2.27}$$

Each of these states is an equal superpositions of all possible computational basis states with different phase factors, e.g., for a qudit $|+_1\rangle$ is

$$|+_1\rangle = \frac{1}{\sqrt{d}}\Big(|0\rangle + \omega|1\rangle + \cdots + \omega^{d-1}|d-1\rangle\Big).$$

Note that, for qubits, the conventional notation is $|+\rangle \equiv |+_0\rangle$ and $|-\rangle \equiv |+_1\rangle$ (as $\omega = -1$ and so $|\pm\rangle \propto |0\rangle \pm |1\rangle$) and the notation here is adapted from this. The conjugate basis states have maximal uncertainty in terms of the outcomes of computational basis measurements and vice versa, which is a property inherited directly from their relationship to a Fourier transform. This is because

$$\langle q|+_{q'}\rangle = \frac{\omega^{qq'}}{\sqrt{d}}, \qquad \forall q, q' \in \mathbb{S}_d, \tag{2.28}$$

which is easily confirmed directly. This property means the bases are what is termed *mutually unbiased.*[3]

In the conjugate basis, the roles of the Pauli operators are reversed. Specifically

$$Z(q')|+_q\rangle = \left|+_{q+q'}\right\rangle, \qquad X(q')|+_q\rangle = \omega^{-qq'}|+_q\rangle, \qquad \forall q, q' \in \mathbb{S}_d, \tag{2.29}$$

which follows directly from the cyclic relation in 2.26. The reader is reminded again that for qudits this addition is modulo d. Hence, the computational and conjugate bases are eigenstates of $Z(q)$ and $X(q)$ respectively. The actions of the Pauli and Fourier gates can be intuitively summarised in a *phase space* diagram, as shown in Figure 2.2. There is a wide range of rigorous and powerful phase space methods, e.g., quasi-probability distribution functions, both for QCVs and qudits [Silberhorn (2007); Wootters (1987)]. However, herein phase space will be used only occasionally and as a schematic aid.

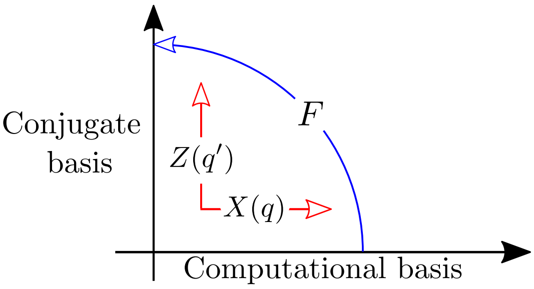


Figure 2.2: The Pauli operators may be represented as orthogonal translations in a phase space formed from the computational and conjugate bases. The Fourier transform is a $\pi/2$ rotation in phase space. The background phase space is $\mathbb{S}_d \times \mathbb{S}_d$ (e.g., for qutrits this is a 3×3 periodic lattice).

2.2.3 Entangling gates

All of the operations described so far in this chapter have applied to one QV. For quantum computing, interactions between pairs of QVs are required. The quantum

[3] A set of bases $\{\mathcal{B}_1, \mathcal{B}_2, ...\}$ for a qudit of dimension d (a QCV) which are orthonormal (quasi-orthonormal) are said to be *mutual unbiased* if for any pair of bases $\mathcal{B}_j$ and $\mathcal{B}_k$ ($j \neq k$) in this set and for any basis states $|a\rangle \in \mathcal{B}_j$ and $|b\rangle \in \mathcal{B}_k$ in these bases then $|\langle a|b\rangle| = k$ where the constant k is $k = 1/d$ (any non-zero and positive value) [Durt et al. (2010); Weigert and Wilkinson (2008)].

gate often considered is the SUM gate given by

$$\textsc{sum}|q\rangle|q'\rangle = |q\rangle|q+q'\rangle, \tag{2.30}$$

as adding the value of two QVs is naturally a useful computational resource. This is conventionally called CNOT for qubits and was encountered already in Equation 1.10. Two quantum systems (in a pure state) are *entangled* if their joint state *cannot* be written as $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, otherwise they are called *separable*. Hence, it is clear that SUM may create an entangled state of two QVs as, for example,

$$\frac{1}{\sqrt{d}}(|0\rangle + |1\rangle + |2\rangle \dots)|0\rangle \xrightarrow{\textsc{sum}} \frac{1}{\sqrt{d}}(|00\rangle + |11\rangle + |22\rangle \dots). \tag{2.31}$$

For qubits, this is one of the famous Bell-states which are at the heart of many quantum information protocols, e.g., teleportation [Bennett et al. (1993)] or dense coding [Bennett and Wiesner (1992)], and the modern formulation of the hotly-debated Einstein-Podolski-Rosen paradox [Einstein et al. (1935)].

An alternative gate to SUM, which is essentially equivalent, is the CZ gate which has the action

$$\textsc{cz}|q\rangle|q'\rangle = \omega^{qq'}|q\rangle|q'\rangle, \tag{2.32}$$

and this gate will be used frequently throughout this thesis. It is often called the controlled-phase gate but I will not use this term as 'the phase gate' will have a different specific meaning herein. The SUM and CZ gates are particular cases of an important class of gates that are ubiquitous in quantum computation: the controlled-u gates, denoted Cu, with the action

$$|q\rangle|q'\rangle \xrightarrow{\mathrm{C}u} |q\rangle u^q|q'\rangle, \tag{2.33}$$

for some unitary u. The first QV is called the *control* and the second the *target*. Note that this is still well-defined for control and target QVs of different types (e.g., a control qubit and a target QCV) and will be used as such later. When necessary, super and subscripts will be used to denote the control and target QVs respectively, i.e.

$$|q\rangle_j|q'\rangle_k \xrightarrow{\mathrm{C}^j_k u} |q\rangle_j u^q|q'\rangle_k, \tag{2.34}$$

where a subscript k on a state denote that this is the state of the QV labelled k. Finally, the circuit notation used for these controlled gates is introduced in Figure 2.3.

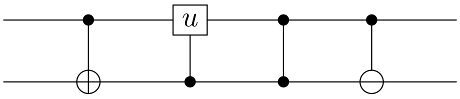


Figure 2.3: From left to right: circuit notation for SUM, a general Cu, CZ and SUM†. The black circle denotes the control QV (CZ acts symmetrically).

2.2.4 The unitary group

At this point it is convenient to take a diversion to discuss the n-QV unitary group. Considering first qudits: The unitaries that act on n-qudits form a group, which is normally denoted $U(d^n)$ and which when represented as matrices (in some basis) are $d^n \times d^n$ complex-valued matrices obeying $UU^\dagger = U^\dagger U = \mathbb{I}$, as has already been discussed briefly in Section 1.2.3. Hence, such an operator is defined by a set of $m < 2d^{2n}$ real parameters. For example, a general single-qubit unitary (a $U(2)$ operator) may be parametrised by the matrix

$$u(\theta,\phi,\varphi,\psi) = e^{i\psi}\begin{pmatrix} e^{i\phi}\cos\theta & e^{-i\varphi}\sin\theta \\ -e^{i\varphi}\sin\theta & e^{-i\phi}\cos\theta \end{pmatrix}. \tag{2.35}$$

Therefore, it is clear that the n-qudit unitary operators are easily understood in terms of matrices containing a finite number of real-valued parameters.

In contrast to this, an arbitrary unitary operator on only a single QCV requires infinitely many parameters to define [Lloyd and Braunstein (1999)]. As it is necessary to specify which transformation it will be demanded that an n-QCV quantum computer can perform, it is convenient to restrict ourselves to considering the set of all n-QCV unitaries that may be written as

$$U = e^{i\mathrm{poly}(\hat{x}_1,\hat{p}_1,\ldots,\hat{x}_n,\hat{p}_n)}, \tag{2.36}$$

where $\mathrm{poly}(\hat{x}_1,\hat{p}_1,\ldots,\hat{x}_n,\hat{p}_n)$ is any real polynomial of finite degree in the $\hat{x}$ and $\hat{p}$ operators of each of the n QCVs. For example, a possible polynomial for two QVCs is $a\hat{x}_1^3 + b\hat{p}_1^2\hat{p}_2 + c\hat{p}_2^7$ for $a, b, c \in \mathbb{R}$. Any such unitary operator is defined by a discrete set of real-valued parameters (i.e., the coefficients in the polynomial), putting this set of unitaries on a similar footing to the set of qudit unitaries. This then enables a well-defined and useful construction of universal quantum computation with QCVs, as first given by Seth Lloyd and Samuel Braunstein [Lloyd and Braunstein (1999)] and encompassed in the general construction I provide in Section 2.3. For notational simplicity, throughout I will use $U(2\pi^n)$ to denote the set of these n-QCV unitaries, so that the relevant unitary operators for a general QV are members of $U(d^n)$.

2.3 Universal quantum computation

The concept of a universal quantum computer has already been introduced briefly in Chapter 1. However, a more exact exposition of these ideas is required for the purposes of this thesis. In particular, for Chapters 3 and 4 it will be useful to have a concept of a quantum computer and universality which is not framed entirely in terms of quantum circuits. To do this I introduce the concept of a general quantum computational model (to my knowledge, this is novel), again formulated for arbitrary types of QVs.

Definition 2.1. *A quantum computational model using QVs is defined by the object* $\mathfrak{M} = (\mathfrak{o}, \mathfrak{s})$ *where* $\mathfrak{o}$ *is a set of basic allowed operations which act on QVs and* $\mathfrak{s}$ *is some set of preparable states.*

The allowed operations are not necessarily restricted to unitary gates. Operations are in general allowed to have classical outputs (i.e., they are measurements of some sort) or depend on classical inputs (e.g., measurement outcomes). Following Browne et al. (2011), a *quantum computation* in a particular model is then a quadruplet

$$\mathfrak{Q} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{q}), \tag{2.37}$$

where $\mathcal{V}$ is a set of QVs, $\mathcal{I}, \mathcal{O} \subseteq \mathcal{V}$ are *input* and *output* subsets and $\mathfrak{q}$ is a sequence of operations from $\mathfrak{o}$ which act on QVs from $\mathcal{V}$. A sequence of operations is considered to be ill-defined if any operations depend on outputs from operations occurring later in the operation sequence, as in such a case the sequence has no clear practical meaning. All non-input QVs[4], $\mathcal{V} \setminus \mathcal{I}$, are prepared in states from the preparable set $\mathfrak{s}$ and it is assumed that the input QVs may in general be in an arbitrary state $|\psi\rangle$.

A quantum computation may be considered to implement the $|\mathcal{I}|$-QV unitary U if for any input state $|\psi\rangle$, the final state of the output QVs is $U|\psi\rangle$, which requires $|\mathcal{O}| = |\mathcal{I}|$. Such a computation will be denoted $\mathfrak{Q}_U$. Here and throughout this thesis, I use the standard notation that $|s|$ is the cardinality of the set s, i.e., the number of elements it contains. QVs that are not in the input or output sets are normally termed *ancillas*, however I will term them *auxiliary* QVs. This is to avoid confusion with the ancillas considered in the latter chapters of this thesis, which play a special gate-mediating role. Computations employing ancilla-mediated gates may involve both auxiliary and gate-mediating ancillary QVs, and hence to avoid ambiguity it is preferable to have distinct terminology.

For two computations $\mathfrak{Q} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{q})$ and $\mathfrak{Q}' = (\mathcal{V}', \mathcal{I}', \mathcal{O}', \mathfrak{q}')$ such that $\mathcal{O} = \mathcal{I}'$, which may be enforced with a QV relabelling as long as $|\mathcal{O}| = |\mathcal{I}'|$, the composite 'serial' computation $\mathfrak{Q}' \circ \mathfrak{Q}$ may be defined in a natural way as [Browne et al. (2011)]

[4] $\mathcal{S}_1 \setminus \mathcal{S}_2$ is the standard notation for the set of elements that are in $\mathcal{S}_1$ and are not in $\mathcal{S}_2$.

$$\mathfrak{Q}' \circ \mathfrak{Q} := (\mathcal{V} \cup \mathcal{V}', \mathcal{I}, \mathcal{O}', \mathfrak{q}'\mathfrak{q}). \tag{2.38}$$

Here $\mathfrak{q}'\mathfrak{q}$ is the concatenated operation sequence, i.e., the $\mathfrak{q}$ command sequence followed by the $\mathfrak{q}'$ command sequence. In a similar way for $\mathcal{V} \cap \mathcal{V}' = \emptyset$, the 'parallel' tensor product of two computations may defined by [Browne et al. (2011)]

$$\mathfrak{Q} \otimes \mathfrak{Q}' := (\mathcal{V} \cup \mathcal{V}', \mathcal{I} \cup \mathcal{I}', \mathcal{O} \cup \mathcal{O}', \mathfrak{q}'\mathfrak{q}). \tag{2.39}$$

It is evident that if the two computations implement the unitaries U and U' then the serial and parallel composite computations implement the unitaries $U'U$ and $U \otimes U'$, respectively. This formalises the concept of building larger computations from smaller ones.

If in a particular model there are basic building-block computations that implement some set of unitaries, it is important to know what global unitaries these can be composed to compute, e.g., can the computer implement Shor's algorithm? A quantum computational model is considered to be *universal* if it may implement any unitary on any number of input QVs. However, there are two subtly different notions of universality: *exact* and *approximate*. Largely the difference is irrelevant, but this is covered now for clarity because here there are some subtle differences between qudits and QCVs. Furthermore, these different forms of universal computation do have some implications in Chapters 3 and 4. Following the circuit model convention, in the following I talk about the basic unitaries that can be implemented as the gate set.

2.3.1 Exact and approximate universality

An exactly universal gate set is defined in the following way:

Definition 2.2. *A set of gates is exactly universal for quantum computation on n-QVs if a finite sequence of gates from the set may be used to exactly implement any $U \in U(d^n)$.*

From a mathematical perspective, an exactly universal gate set generates the full $U(d^n)$ group. The number of elements in the group $U(d^n)$ is uncountable, which is a simply consequences of $\mathbb{R}$ being uncountable. The set of unitaries generated by combining the elements of a finite set of gates must contain a countable (although not necessarily finite) number of elements, which implies that an exactly universal gate set must have an infinite number of basic gates.

There is a weaker notion of universality which may be satisfied by finite gate sets. It is necessary to first introduce a precise meaning of gate error, considering initially only the case of qudits. Any two n-qudit gates U and V may be adapted to have the same determinant by the physically irrelevant action of choosing the global phase of either operator, as $\det(e^{i\phi/d^n}U) = e^{i\phi}\det(U)$. For two unitary operators U and V with $\det(U) = \det(V)$, the error in the approximation of $U \in U(d^n)$ by $V \in U(d^n)$ may be defined to be

$$E(U,V) = \sup_{\| |\psi\rangle \| = 1} \| (U - V) |\psi\rangle \|, \tag{2.40}$$

where $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$ is the norm of $|\psi\rangle$. The justification for this definition of error is that it is a bound on the difference in the measurement statistics for any possible measurement [Nielsen and Chuang (2010)], but there are many alternative definitions of gate error that could be used such as those based on fidelity, e.g., see Gilchrist et al. (2005) for a discussion of this. Using this definition of gate error, V is called an *ϵ-approximation* to U if $E(U,V) \leq \epsilon$. For QCVs, it is more natural to say that V is an ϵ-approximation to U when every coefficient in the generating polynomial $\text{poly}(\hat{x}_1, \hat{p}_1, \dots, \hat{x}_n, \hat{p}_n)$ of V is within ϵ (or alternatively ϵ/n) of the coefficient in the generating polynomial of U [Lloyd and Braunstein (1999)]. This facilitates the following definition:

Definition 2.3. *A set of gates is approximately universal for quantum computation on n-QVs if for any $U \in U(d^n)$ and $\epsilon > 0$ there exists a finite sequence of gates from the set that is an ϵ-approximation to U.*

From a mathematical perspective, approximate universality means that the gate set need only generate a dense subset of $U(d^n)$ and this condition can be satisfied by gate sets containing a finite number of gates.[5]

2.3.2 Approximate universality is practical universality

The definitions of exactly and approximately universal gate sets may seem reasonably straight forward, however there are some points that need addressing, particularly in the case of QCVs. Consider the notion of exact universality. In one sense, for *qudits* this is a useful concept: A unitary on n qudits is a $d^n \times d^n$ complex-valued matrix and matrix decomposition techniques can be used to express this without approximation as tensor and multiplicative products of matrices representing only two- and one-qudit gates [Bullock et al. (2005); Nielsen and Chuang (2010)]. Hence, there are reasonable gate sets for qudits which are exactly universal, with important specific sets covered in Section 2.5. However, to reiterate what I have already said above: the number of gates in the set must still be infinite (i.e., continuously parameterised). Therefore, although an exactly universal gate set is a useful abstract

[5] A finite set of gates can only generate a countable set of operators, but a countable set can be dense in an uncountable set. For example, the rational numbers are countable but are dense in $\mathbb{R}$, as there is a rational number arbitrarily close to any element of $\mathbb{R}$.

object with which to study quantum computation with qudits, in practice such a gate set still cannot exist.

For QCVs, it is not clear that *exact* universality is a useful concept at all. In general, an available gate set for QCV computation with any physical relevance will have the form

$$\mathcal{G}_{\text{QCV}} = \{e^{-i\hat{H}_1 t}, e^{-i\hat{H}_2 t}, \dots, e^{-i\hat{H}_N t}\}, \tag{2.41}$$

where the $\hat{H}_j$ are real finite-degree polynomials in the position and momentum operators of some number of QCVs and here we assume that in each case t may take any value in $\mathbb{R}$. In QCV computation, unitaries are constructed using the two relations [Braunstein and van Loock (2005); Lloyd (1995)]:

$$e^{i\hat{H}_j \delta t} e^{i\hat{H}_k \delta t} e^{-i\hat{H}_j \delta t} e^{-i\hat{H}_k \delta t} = e^{[\hat{H}_j, \hat{H}_k]\delta t^2} + O(\delta t^3), \tag{2.42}$$

$$e^{i\hat{H}_j \delta t/2} e^{i\hat{H}_k \delta t} e^{i\hat{H}_j \delta t/2} = e^{i(\hat{H}_j + \hat{H}_k)\delta t} + O(\delta t^3), \tag{2.43}$$

which may be confirmed with a Taylor expansion.[6] Using arbitrarily small δt and arbitrarily many repeated applications of these equalities, the unitaries $e^{[\hat{H}_j, \hat{H}_k]t}$ and $e^{i(\hat{H}_j + \hat{H}_k)t}$ for any desired values of $t \in \mathbb{R}$ may be constructed. Furthermore, using these gates and applying the above techniques again, we may implement any unitaries generated by the Hermitian operators $[\hat{H}_i, [\hat{H}_j, \hat{H}_k]]$, $i[\hat{H}_h, [\hat{H}_i, [\hat{H}_j, \hat{H}_k]]]$, $i[[\hat{H}_h, \hat{H}_i], [\hat{H}_j, \hat{H}_k]]$ and so on, along with those unitaries generated by real-valued linear combinations of these. That is, any gate of the form $e^{i\hat{H}t}$ where $\hat{H}$ is the sum of the $\hat{H}_j$ and of nested commutators of these operators is implementable [Lloyd (1995)], which is called the *algebra* over $\mathbb{R}$ generated by commutation of the set of operators $\{\hat{H}_1, \hat{H}_2, \dots\}$ [Humphreys (1972)].

This construction gives a sensible meaning to how a unitary may be approximated to any accuracy (an ϵ-approximation) with a finite sequence of gates from some set - simply by applying the construction above to the accuracy required. In order to be an approximately universal gate set, the algebra of the generators of the available gates must include every polynomial of the position and momentum operators for any number of QCVs. Importantly, as with qudits, only one and two-QCV gates are required to approximately generate any n-QCV unitary [Lloyd and Braunstein (1999)] meaning that physically sensible approximately universal gate sets exist, with specifics covered in Section 2.5. However, it is not clear that exact universality has any relevance to QCV computation: for finite sequences of gates the above gate composition techniques are in general intrinsically approximate (this is not to say *some* gates outside the basic gate set cannot be implemented exactly). Consequently, whenever exact universality is mentioned from now on it should be

[6] Note that there is not a missing factor of i in the exponential here. This is because $[\hat{H}_j, \hat{H}_k]$ is not a Hermitian operator, but $\pm i[\hat{H}_j, \hat{H}_k]$ is.

assumed this applies only to qudits.

2.3.3 The overhead of gate approximations

Regardless of the technicalities discussed above, in practice the relevant notion of universality is clearly approximate universality, for all types of QVs. Therefore, given a particular approximately universal gate set, it is important to understand how the length of the gate sequence required to ϵ-approximate any unitary scales with ϵ. For example, if the length scaled exponentially with the required accuracy this would be a serious problem. For qudits, a result known as the *Solovay-Kitaev theorem* shows that there is a surprisingly small overhead required - to obtain an accuracy of ϵ the gate sequence need only be of length $O(\log^c(1/\epsilon))$, where $c \geq 1$ is a small constant that depends on the details of the particular method [Harrow et al. (2002); Kitaev (1997)]. Furthermore, the standard proof of this theorem provides an efficient classical algorithm for finding the gate sequence, for example, a detailed presentation of an algorithm with $c = 3.97$ is provided by Dawson and Nielsen (2006). Note that the gate sequence length does scale exponentially in the number of qudits that the gate to be approximated acts upon, but this is to be expected as otherwise it would provide an efficient method for simulating any n-qudit unitary. As this theorem is relied upon to guarantee efficient gate simulation for the approximate gate sets used herein, it is stated formally in Appendix F.

As far as I am aware, there are no similar theorems implying that only a poly-logarithmic overhead is required for gate approximations in QCV computation. However, it is known that the length of the gate sequence need grow no faster than a small polynomial in $1/\epsilon$ [Lloyd and Braunstein (1999)]. It will be important in this thesis to have some some specific universal gate sets, however it is convenient to delay this discussion until after the next section.

2.4 The Clifford group

The *Clifford group* is of fundamental importance in quantum computation, for example, it underpins the theories of error correction and fault tolerance [Gottesman (2010)]. Furthermore, it will be central to the results of Chapters 3 and 4 and hence it is now introduced. It is first necessary to define the *Pauli group*.

2.4.1 The Pauli group

An important property of the Pauli operators is that they commute up to a phase via the relation

$$Z(q)X(q') = \omega^{qq'} X(q')Z(q), \tag{2.44}$$

which may easily be confirmed by the action of each side of the equality on the computational basis. This is often called the *Weyl commutation relation* and is perhaps the most used equality in this thesis. This relation means that under operator multiplication the Pauli operators may be used to form a strict subgroup of the single-QV unitary group called the single-QV *Pauli group*. This is denoted $\mathcal{P}_1$ and defined by

$$\mathcal{P}_1 := \{p_{\xi,q,q'} = \omega^{\xi/2} X(q) Z(q') \mid \xi \in \mathbb{S}_D,\ q, q' \in \mathbb{S}_d\}, \tag{2.45}$$

where $\mathbb{S}_D$ is defined as

$$\mathbb{S}_D := \begin{cases} \mathbb{Z}(2d) & \text{for qudits,} \\ \mathbb{R} & \text{for QCVs.} \end{cases} \tag{2.46}$$

For a QCV this is a very natural definition: it is simply the group generated by multiplication of $X(q)$ and $Z(q)$, as can be seen from the Weyl commutation relation. However, for qudits there are extra phases that are powers of $\omega^{1/2}$, and hence it is necessary to add $\omega^{1/2}\mathbb{I}$ to the $X(q)$ and $Z(q)$ operators to generate the whole group. One justification for these extra phases is that for $d = 2$ this recovers the normal qubit Pauli group, generated by the two operators X and Z along with the third ordinary Pauli operator $Y = iXZ$, which is normally introduced on an equal footing with X and Z when only qubits are considered. A more concrete reason for these extra phases is that they are required for even-dimension qudits in order for the Clifford group, introduced below, to have equivalent properties for all types of QV (i.e., for QCVs and both even and odd-dimension qudits). Including the extra phases for odd-dimension qudits, as well as even-dimension qudits, is in my opinion the most convenient choice. This is in line with some of literature, see e.g., Hostens et al. (2005), but other authors take the alternative view, see e.g., Farinholt (2014).

The n-QV Pauli group, denoted $\mathcal{P}$, is a simple generalisation of this and is the subgroup of $U(d^n)$ consisting of all operators of the form

$$p_{\xi,\vec{v}} := p_{\xi_1,v_1,v_{n+1}} \otimes p_{\xi_2,v_2,v_{n+2}} \otimes .... \otimes p_{\xi_n,v_n,v_{2n}}, \tag{2.47}$$

where $\xi = \xi_1 + \xi_2 + ... + \xi_n$ with the addition as approriate for $\mathbb{S}_D$ (i.e., modulo D for a qudit) and $\vec{v}$ is the vector $\vec{v} = (v_1, \dots, v_{2n}) \in \mathbb{S}_d^{2n}$.

2.4.2 The Clifford group

The (n-QV) Clifford group is the normaliser of the Pauli group in the group of the unitaries. Hence it is defined by [Bartlett et al. (2002); Gottesman (1999*a*,*b*)]

$$\mathcal{C} := \{U \in U(d^n) \mid UpU^\dagger \in \mathcal{P}\ \ \forall p \in \mathcal{P}\}. \tag{2.48}$$

Therefore, the Clifford gates (the elements of $\mathcal{C}$) are those unitaries which transform Pauli gates to Pauli gates under conjugation. It is easily confirmed that it is indeed a group under operator multiplication. It turns out that all of the specific gates so far introduced in this chapter ($X(q)$, $Z(q)$, F, $\textsc{cz}$ and $\textsc{sum}$) are Clifford. A further important Clifford gate is the *phase gate*, $P(p)$, defined by

$$P(p)|q\rangle := \omega^{\frac{pq}{2}(q+\varrho_d)}|q\rangle, \tag{2.49}$$

with $p \in \mathbb{S}_D$ and where $\varrho_d = 1$ for odd-dimension qudits and $\varrho_d = 0$ otherwise. For qubits, this reduces to the well-known gate $P = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$, also often denoted S in the literature.

It will be useful in this thesis to have a set of gates which generate the Clifford group. It is convenient to use the standard notation that $\mathcal{G} = \langle g_1, \dots, g_k \rangle$ represents the statement that $\mathcal{G}$ is the group generated by the elements $g_1, \dots, g_k$.

Proposition 2.1. *$\mathcal{C} = \langle \textsc{cz}, Z(q), P(q), F \rangle$ with $q \in \mathbb{S}_d$ for all QV types.*

To be clear, this is the statement that, for any QV type, any n-QV Clifford gate can be exactly decomposed into $\textsc{cz}$, $Z(q)$, $P(q)$, and F gates. Furthermore, it turns out that such a decomposition need only contain $O(n^2)$ of these basic generating gates. For qudits this follows from the work of Hostens et al. (2005) and Farinholt (2014)[7] and for QCVs it was shown by Bartlett et al. (2002). Not all of these generators are required in each case. For example, with qudits $Z(q)$ and $P(q)$ can be obtained from powers of Z and P and hence only four generators are needed, and in prime dimensions Z can be obtained from P and F.[8] However these minor differences can be largely ignored.

In Chapter 4 it will be useful to have the conjugation relations of these generators on arbitrary Pauli operators. In Appendix E it is shown that

$$p_{\xi,q,q'} \xrightarrow{Z(p)} p_{\xi+2pq,q,q'}, \tag{2.50}$$

$$p_{\xi,q,q'} \xrightarrow{F} p_{\xi-2qq',-q',q}, \tag{2.51}$$

$$p_{\xi,q,q'} \xrightarrow{P(p)} p_{\xi+pq(q+\varrho_d),q,q'+pq}, \tag{2.52}$$

$$p_{\xi,(q_1,q_2,q_1',q_2')} \xrightarrow{\textsc{cz}} p_{\xi+2q_1q_2,(q_1,q_2,q_1'+q_2,q_2'+q_1)}. \tag{2.53}$$

The changes in the phase factors are often, but not always, of no importance. Note that the arithmetic in each subscript is calculated as appropriate for the QV type,

[7] In the case of qudits, many derivations in the literature apply only in prime dimensions. E.g., see Gottesman (1999*a*); Hall (2007).

[8] In odd dimensions $F^2P^{d-1}F^2P = Z$. For qubits $P^2 = Z$. Although it is claimed by Farinholt (2014) that for all dimensions of qudits the Z generator is unnecessary, I am unaware of any proof that confirms this.

which for qudits is modulo $2d$ for the phase factor and modulo d for the $X(\cdot)$ and $Z(\cdot)$ gate variables.

2.4.3 Classical simulation of Clifford circuits

Gates from the Clifford group are alone not sufficient for universal quantum computation as they form a strict subset of the unitary group. Furthermore, quantum computations consisting of only Clifford gates acting on QVs prepared in the computational basis and which have access only to measurements of the computational basis can be efficiently exactly simulated on a classical computer. This is known generally as the Gottesman-Knill theorem, due to its original formulation for qubits by Gottesman (1999*b*) and which is accredited therein to Emanuel Knill. The generalisations to qudits and QCVs may be found in Bartlett et al. (2002); De Beaudrap (2013); Gottesman (1999*a*); Hostens et al. (2005); Van den Nest (2013). This theorem is nicely illustrated by the qubit Clifford circuit simulator programmed by Scott Aaronson [Aaronson and Gottesman (2004, 2005)]. Clifford gates can create highly entangled many-QV states from separable computational basis inputs, such as n-qubit Greenberger-Horne-Zeilinger (GHZ) states

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|00...0\rangle + |11...1\rangle), \tag{2.54}$$

and hence, the Gottesman-Knill theorem may appear surprising. However, because the theorem is only valid given strict restrictions on the allowed input states and measurements, this prevents the full array of non-classical resources available in states such as GHZ being accessed.

2.4.4 Further Clifford gates

The four gates CZ, SUM, F and $P(q)$ along with the Pauli operators are the most important Clifford gates herein. However, there are certain other Clifford unitaries which will appear regularly and hence these are now introduced. The first of these is the SWAP gate, defined by

$$\textsc{swap}|q\rangle|q'\rangle := |q'\rangle|q\rangle, \tag{2.55}$$

and which as the name suggests has the action of swapping the states of the two input QVs. It is obvious that this is Clifford. A further useful operator is the *squeezing gate* defined by

$$S(s)|q\rangle := |sq\rangle, \tag{2.56}$$

for any $s \in \mathbb{S}_d$ such that there exists $s^{-1} \in \mathbb{S}_d$. Without this condition on s it would not be unitary. This condition holds for all non-zero $s \in \mathbb{S}_d$ with QCVs and prime dimension qudits, and any non-zero s which is co-prime with the dimension of the qudits in other cases (such an s is called a unit in $\mathbb{S}_d$). This gate can be confirmed to implement the conjugation maps

$$p_{\xi,q,q'} \xrightarrow{S(s)} p_{\xi,sq,s^{-1}q'}. \tag{2.57}$$

The CZ and SUM gates are the most important special cases of the more general gates $CZ(q)$ and $CX(q)$ (the special case is $q = 1$). Again, it is easy to confirm that these gate are Clifford. For qudits, they may be obtained as powers of SUM and CZ. For QCVs, Equation 2.57 implies that they may be obtained from either CZ or SUM and the squeezing gate, as shown in Figure 2.4. Finally, Figure 2.5 presents the simple relation between $CX(q)$ and $CZ(q)$ in terms of local Fourier gates which will be used regularly throughout.

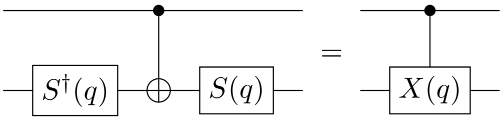


Figure 2.4: General controlled Pauli gates can be implemented via CZ or SUM and local Clifford gates. Here the squeezing gate is used to create the $CX(q)$ gate.

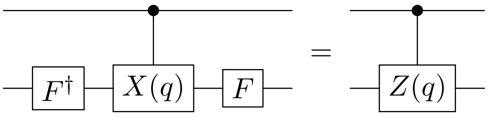


Figure 2.5: Conjugation by local Fourier gates transforms between $CZ(q)$ and $CX(q)$ gates. This includes as a special case the relation between CZ and SUM.

2.5 Universal gate sets

We are now ready to return to the subject of universal gate sets, and in particular to give certain universal sets that will be of relevance herein. A particularly important result in quantum computation is the following:

Proposition 2.2. *A gate set composed of any entangling gate in conjunction with any set of single-QV gates that is (approximately / exactly) universal for single-QV unitaries is an (approximately / exactly) universal gate set.*

For qudits, this results is due to Brylinski and Brylinski (2002), and for QCVs (where only approximate universality applies), it was shown by Lloyd and Braunstein (1999). This implies that, as long as some entangling gate can be implemented and there are sufficient local controls of each QV then universal quantum computation is possible. Clearly this leaves substantial freedom in terms of the exact gates, particularly as almost any multi-partite gate is entangling [Lloyd (1995)]. Often the entangling gate is taken to be CZ or SUM due to their convenient properties and the natural role they play in algorithms, but this is not essential.

Proposition 2.2 raises the important question of which single-QV gate sets provide single-QV universality. To consider this, it useful to introduce the *rotation gate* which is a single-QV unitary that is parameterised by a function $\vartheta : \mathbb{S}_d \to \mathbb{R}$ and is defined by

$$R(\vartheta)|q\rangle := e^{i\vartheta(q)}|q\rangle. \tag{2.58}$$

To guarantee that this is well-defined for a QCV, in this case this function is constrained to being some finite-degree real polynomial in q. There is a physically irrelevant global phase freedom in this gate, which can be removed by setting $\vartheta(0) = 0$. In the case of qudits, the gate set of all such rotation gates[9] along with the Fourier gate is an exactly universal single-qudit set. This is well-known for qubits [Nielsen and Chuang (2010)[10]] and for qudits it is implied by the results of Zhou et al. (2003). This can then be adapted to a finite gate set and approximate universality by simply picking a set containing one 'generic' rotation gate along with the Fourier gate F. This is shown in Appendix G and is again well-known for the qubit sub-case.

For *prime dimension* qudits there is a particularly elegant result that will be useful herein: the addition of *any* non-Clifford gate to a set of generators of the Clifford group elevates that set to (approximate) universality [Campbell et al. (2012); Nebe et al. (2001, 2006)]. Similarly, for QCVs it is known that the addition of continuous powers of any non-Clifford single-QCV gate to the Clifford group is sufficient for (approximate) universality [Lloyd and Braunstein (1999)]. Hence, for such QV types and a single-QV unitary $u \notin \mathcal{C}$, then

$$\mathcal{G}_{\epsilon-\text{UNI}} = \{\text{SUM}, F, P(q), Z(q), u^q \mid q \in \mathbb{S}_d\}, \tag{2.59}$$

is an approximately universal set. As far as I am aware, it is not known whether this holds for non-prime dimension qudits. However, in such cases the u gate can be taken to be a generic single-QV rotation gate, to obtain universality via the argument of

[9] For qudits, these rotation gates are parametrised by d phase angles in $\mathbb{R}$, or $d-1$ phase angles if the global phase is fixed

[10] Any single-qubit unitary may be written as $U = e^{i\phi}R(\theta)HR(\phi)HR(\gamma)$ where $R(\chi)|q\rangle = e^{i\chi q}|q\rangle$ and H is the Hadamard gate, i.e., the qubit Fourier gate. This may be shown directly via simple matrix multiplication.

Appendix G. In this thesis, it will be at times convenient to know that the Clifford gates can be generated exactly, and hence I will make substantial use of this gate set for some unspecified single-QV gate u that elevates the set to universality, and which will often be assumed to be diagonal, for convenience.

Finally, there are a range of simple choices for the non-Clifford gate in this gate set, which may be practically convenient. One option is to choose a diagonal 'cubic' gate. The T or the π-by-8 gate for qubits, as already introduced in Equation 1.10, can in a certain sense be considered cubic as $T|q\rangle = \omega^{q^3/d^3}|q\rangle$, and it is not hard to show that for all QV types that this provides a non-Clifford gate (e.g., via the results below). However, for QCVs the $k = 3$ case of the gate

$$D_k(r)|q\rangle := \omega^{rq^k/k}|q\rangle, \tag{2.60}$$

with $k \in \mathbb{N}$ and $r \in \mathbb{S}_d$ is normally considered, termed the *cubic phase gate* [Gu et al. (2009)]. Note that, for QCVs and even-dimension qudits, $k = 1$ and $k = 2$ give the Pauli $Z(r)$ gate and the phase gate $P(r)$ respectively. Again, for qudits this cubic gate will also provide a non-Clifford gate. However, Campbell (2014) suggests that a more natural generalisation for the T gate, to prime-dimension qudits with $d > 3$, is $T(r)|q\rangle = \omega^{rq^3}|q\rangle$ with $r \in \mathbb{S}_d$, which is also equivalent to the cubic phase gate for QCVs up to a rescaling of $r \in \mathbb{R}$. These gates have important applications to fault-tolerant quantum computation, due to their interesting relation to the Clifford group [Campbell (2014); Howard and Vala (2012)]. However, as this is not discussed herein, it is of no consequence which non-Clifford gate is chosen to elevate the Clifford group to universality, beyond possible practical considerations of what the simplest non-Clifford gate is to implement.

2.6 Conclusions

In this chapter I have reviewed the terminology and mathematical tools for quantum computation using qubits, qudits of arbitrary finite dimension and quantum continuous variables. A simple unified formulation of the fundamental state spaces, bases, operators, groups and concepts necessary to the theory of quantum computation has been proposed. This will be utilised throughout the remainder of this thesis to succinctly present results in a manner that is applicable to all types of QVs.

Chapter 3

Unbounded fan-out circuits with general quantum variables

This chapter introduces and investigates the computational power of the *unbounded fan-out gate*, defined on general quantum variables (QVs), which may quantum-copy QVs into an arbitrary number of auxiliary QVs. I show that a circuit model in which this gate may be implemented in unit time has greater parallel computation power than quantum circuits using only gates with fixed input size. This extends results by several authors on *qubit* quantum circuit complexity into the general QV domain, which applies to quantum computation not only with qubits, but also with qudits of *any* dimension and QCVs. This chapter is based on Proctor (2015).

3.1 Introduction

Understanding which problems are fundamentally efficient to solve and which are not is a question that has clear practical implications and has interested many researchers in computer science and beyond. The answers to such computational complexity questions have, broadly speaking, proven particularly challenging to solve. Perhaps the most famous question of this sort is the 'P *versus* NP' problem, which asks whether the set of classically efficiently *solvable* problems (the complexity class P), and the set of problems for which a given solution can be classically efficiently *verified* (the complexity class NP), are the same [Arora and Barak (2009)]. It is widely believed that P $\neq$ NP [Hemaspaandra (2012)], and there is plenty of motivation to settle this question either way (including a $1,000,000 prize). However, to date no one has been able to prove it.

In light of this, it is sensible to consider simpler problems in the hope that progress on these will shed light on the more over-arching open questions in complexity theory. One avenue of research is into the power of *Boolean circuits* with access to limited resources of some sort, where Boolean circuits are essentially the (irreversible) classical version of quantum circuits [Arora and Barak (2009)]. A natural resource to restrict is computational time, called *depth* in the context of circuits. For example, this can be restricted to a constant or poly-logarithmic growth as a function of input size. There are a range of interesting results known about the power of such restricted-depth Boolean circuits [Arora and Barak (2009); Furst et al. (1984); Goldreich (2008)].

The study of quantum circuit complexity is a natural extension of these classical complexity ideas into the realm of quantum computation, providing insights into both the power of quantum computation and the differences between closely related quantum and classical circuit classes. As far as I am aware, the first explicit definitions and investigations of constant and restricted-depth quantum circuits are due to Moore and Nilsson (1998) and this work has since been extended by a range of authors [Fang et al. (2006); Moore (1999); Moore and Nilsson (2001); Takahashi et al. (2010)], with Høyer and Špalek (2003, 2005) providing a detailed investigation of the power of unbounded fan-out gates. However, to my knowledge, up until now all of the literature on this topic has exclusively considered qubits and any extension to either qudits or QCVs is lacking.

In this chapter I present investigations into constant and poly-logarithmic depth quantum circuits with general QVs. This therefore includes the previously neglected cases of $d > 2$ qudits and QCVs. The gates and models that I define and the propositions that I prove in this chapter will provide the basis for linking the computational properties of quantum circuits and the one-way quantum computer for all QV types, which is the subject of Chapter 4. However, they are also interesting in their own right as a study of non-binary qudit and QCV circuit depth and size complexity. To keep the presentation concise and because the results given here extend previous qubit-based work into the general QV domain, rather than beginning this chapter with an extensive review of the qubit literature, I will discuss if and where the qubit special case of each result I present in this chapter can be found in the literature when appropriate. The remainder of this chapter is structured as follows: In Section 3.2 quantum depth and size are introduced. In Section 3.3 definitions are proposed for the fan-out gate, standard quantum circuits, and unbounded fan-out circuits for general QVs. It is then shown that, when restricted to constant depth, unbounded fan-out circuits are more powerful than standard quantum circuits. In Section 3.4 it is shown that constant depth unbounded fan-out gates can compute sequences of commuting unitaries and any Clifford circuit. Section 3.5 includes a brief discussion of certain technical issues that arise in the setting of QCV quantum circuits, along with a resolution to these problems. In Section 3.6 the physical relevance of unbounded fan-out circuits is briefly considered and the chapter is then concluded in Section 3.7.

3.2 Depth and size in quantum computation

In order to study computational depth and size complexity in quantum circuits, formal definitions of these concepts are required. These are expressed in terms of a general quantum computational model so that they can also be immediately applied in Chapter 4 to the one-way quantum computer.

Definition 3.1. *For a quantum computation* $\mathfrak{Q} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{q})$, *a path of dependent operations is a sub-sequence* (q_j) *of* $\mathfrak{q}$ *such that each operation either*

(a) acts on a QV in common with, or

(b) depends upon the outcome of,

the previous operation in the subsequence.

This facilitates the following definition of the (quantum) depth of a computation:

Definition 3.2. *The quantum depth of a quantum computation* $\mathfrak{Q}$, *denoted* $\mathrm{depth}(\mathfrak{Q})$, *is the number of operations in the longest path of dependent operations.*

The depth represents the number of steps required for the computation, and hence such a definition of depth encodes the standard assumption that two operations cannot be performed simultaneously on a QV and that an operation may not be performed simultaneously with one whose output it depends upon. For a quantum circuit the depth is simply the number of layers in the circuit, but this definition also encompasses the more subtle concept of depth in one-way quantum computation.

Definition 3.3. *The quantum size of a quantum computation, denoted* $\mathrm{size}(\mathfrak{Q})$, *is the sum of the size of each operation it contains, where the size of an operation is defined to be the number of QVs on which it acts.*

For example, the SUM gate has a size of 2. The concepts of size and depth may be clarified further by reference to the circuit given in Figure 3.1 which has a size of 17 and depth of 9. These quantities are referred to as *quantum* size and depth as they take no account of any classical computational resources required for any manipulations of any classical outputs. However, this is physically well-motivated given the relative practical difficulties of classical and quantum computation.[1] Note that the quantum depth does not tell you how long a computation need be, but rather how long a given computation is. For example, the two circuits in Figure 3.2 have the same action, but have a different depth. In this case it is obvious that the

[1] This is of course assuming that the model does not use unreasonable classical resources.

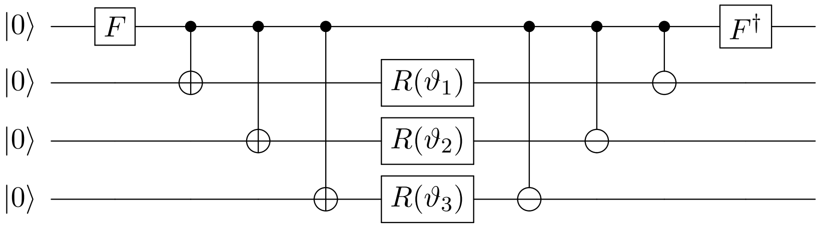


Figure 3.1: This quantum circuit has a depth of 9 and a size of 17.

greater depth circuit can be compressed, but in general it is a highly non-trivial task to confirm whether or not a particular decomposition is optimal. Serial and parallel computations (see Equations 2.38 and 2.39) obey

$$\text{depth}(\mathfrak{Q}_1 \circ \mathfrak{Q}_0) \leq \text{depth}(\mathfrak{Q}_1) + \text{depth}(\mathfrak{Q}_0), \tag{3.1}$$

$$\text{depth}(\mathfrak{Q}_1 \otimes \mathfrak{Q}_0) = \max(\text{depth}(\mathfrak{Q}_1), \text{depth}(\mathfrak{Q}_0)), \tag{3.2}$$

as is to be expected. In both cases sizes simply add.

In the rest of this chapter, the main topics of study are asymptotic depth and size scalings of quantum circuits. Hence, although the standard asymptotic notation has already been used herein without an explicit definition, it is crucial for the following that its precise meaning is understood. A function $f(n)$ is $O(g(n))$ if, for some constants $C > 0$ and n_0, then $f(n) < Cg(n)$ for all $n > n_0$. A function $f(n)$ is $\Omega(g(n))$ if, for some constants $C > 0$ and n_0, then $f(n) > Cg(n)$ for all $n > n_0$. For example, $n^2 + 10n$ is $O(n^2)$ and $\Omega(n^2)$; it is also $O(n^3)$ and $\Omega(\log n)$, but it is *not* $O(n)$.

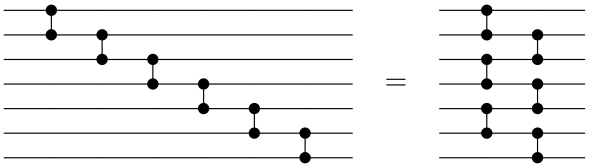


Figure 3.2: The depth of the circuit on the LHS is 6. The depth of the equivalent circuit on the RHS is 2.

3.3 Standard and unbounded fan-out circuits

For any type of QV, a *quantum circuit model* (QCM) is any quantum computational model $\mathfrak{M} = (\mathfrak{o}, \mathfrak{s})$ in which the allowed operations, $\mathfrak{o}$, is some set of unitary operators (quantum gates). It is conventional to restrict the set of preparable auxiliary QV states to $\mathfrak{s} = \{|0\rangle\}$, and this will be taken to be the case herein. It it often also required that the input and output QV subsets in any computation are equal, and this will happen to be true in all cases in this chapter, but this is not strictly necessary. A gate that acts on a constant number of QVs is a unitary that transforms some fixed number of QVs, e.g., SUM takes two QVs as an input.

Definition 3.4. *The 'standard quantum circuit model' is a QCM with some universal gate set that contains only gates that act on a constant number of QVs.*

A *standard quantum circuit* is then a particular computation in this model. Roughly speaking, the exact specification of the gate set is not necessary in order to consider only how computational depth and size *scale* with the number of input QVs for the implementation of n-QV unitary families, and for this reason no particular gate set was mentioned in this definition. However, there are certain issues related to whether the gate set is approximately or exactly universal. More specifically, for exact universality, which is relevant only for qudits, then any exactly universal set (with fixed-size gates) is completely equivalent to any other, in this context. This is because any unitary acting on k qudits may be exactly decomposed into $O(d^{2k})$ gates from any exactly universal gate set [Bullock et al. (2005); Lloyd (1995)] and so one universal gate set may simulate another with only constant size and depth overhead (as each gate in the set to simulate acts on no more than k-qudits for some constant k). For concreteness, we may consider the exactly universal set of SUM along with all single-qudit gates, which we denote $\mathcal{G}_{\text{UNI}}$.

In the case of approximate universality, as one approximately universal gate set cannot necessarily exactly simulate the gates from another approximately universal set, there can be more subtle issues related to how the overhead to simulate one gate set depends on the systematic gate-error level that may be tolerated (e.g., polynomial or poly-logarithmic overheads). However, these issues will not have any direct implications for the results of this chapter as long as the gate set can exactly generate any Clifford gate. Hence, for concreteness, in the case of approximate universality we consider the set $\mathcal{G}_{\epsilon-\text{UNI}}$, which was already introduced in Equation 2.59 as

$$\mathcal{G}_{\epsilon-\text{UNI}} = \{\text{SUM}, F, P(q), Z(q), u^q \mid q \in \mathbb{S}_d\}, \tag{3.3}$$

with non-Clifford single-QV unitary u which may be taken to be a diagonal gate. This may exactly generate any Clifford gate, and is appropriate for all QV types. Instead of this particular set, for qudits and for the purposes of this chapter, any gate set containing any other set of Clifford group generators is completely equivalent. However, in the case of QCVs this is not entirely true due to a slightly subtle issue that arises from the non-periodic nature of the QCV Pauli gates: a discussion of this is delayed until Section 3.5. In summary, the following results on standard quantum circuits are valid with either: any exactly universal qudit gate set including only fixed-input-size gates (e.g., $\mathcal{G}_{\text{UNI}}$), or with the approximate universal set $\mathcal{G}_{\epsilon-\text{UNI}}$ for all types of QVs.

3.3.1 Unbounded fan-out circuits

An alternative circuit model, which I will show does not have the same depth complexity as standard quantum circuits, can be defined by first introducing the n-QV 'fan-out' gate. To my knowledge, outside of the qubit sub-case such a gate has not been defined in the literature. I will denote this gate by FANOUT and define it by the action

$$\textsc{fanout}|q\rangle|q_1,\dots,q_n\rangle := |q\rangle\,|q_1+q,\dots,q_n+q\rangle\,. \tag{3.4}$$

Unlike for the qubit sub-case, for general QVs the fan-out gate is not self-inverse - for a d-dimensional qudit it has order d (this is because $q_k + d = q_k$ modulo d). A circuit notation for this gate is defined in the circuit on the LHS of Figure 3.3. It is obvious that this gate may be composed from a sequence of n SUM gates, as shown in the middle circuit diagram of Figure 3.3. The fan-out gate is named as such as it may be used to copy computational basis states into n QVs, specifically[2]

$$|q\rangle|0,\dots,0\rangle \xrightarrow{\textsc{fanout}} |q\rangle\,|q,\dots,q\rangle\,. \tag{3.5}$$

Hence, it may be used to delocalise a logical QV in a single QV over $n+1$ QVs, which will prove to be a useful resource for parallel computations.

Definition 3.5. *The 'unbounded fan-out model' is a QCM with some universal gate set that contains only gates that act on a constant number of QVs along with fan-out gates acting on any number of QVs.*

Again, an *unbounded fan-out circuit* is then a particular computation in this model. The gate set discussions below Definition 3.4 are directly applicable again here. Hence, for the same reasons as given there, the gate set may be taken to be

$$\mathcal{G}_{\text{FANOUT}} = \mathcal{G}_{\epsilon-\text{UNI}} \cup \{\textsc{fanout}\}, \tag{3.6}$$

or alternatively, the exactly universal set obtained by replacing $\mathcal{G}_{\epsilon-\text{UNI}} \to \mathcal{G}_{\text{UNI}}$ in this equation. It does not really matter which, except that a fair comparison between the two circuit models herein is given by considering the exact or universal set in both cases.

[2] Note that this does *not* violate the no-cloning theorem as it only copies basis states - it does not copy a QV, but instead creates a highly entangled multi-QV state for a general input.

Proposition 3.1. *Any standard quantum circuit for the n-QV fan-out gate has a depth of $\Omega(\log n)$. There is a standard quantum circuit for this gate with a depth of $O(\log n)$ and a size of $O(n)$.*

Proof: A circuit for the n-QV fan-out gate with a depth of $O(\log n)$ and size of $O(n)$ is presented in the RHS of Figure 3.3. This uses a standard 'divide-and-conquer' strategy, via SUM and SUM† gates. All the output QVs of the fan-out gate depend on the state of the control QV. With l circuit layers composed of gates that act on at most m QVs for some constant m, at most m^l QVs can depend on the state of the control QV. Hence, for n QVs to depend on the control QV it is necessary for at least $l = \log_m n$ layers. Therefore, any standard quantum circuit for the fan-out gate must have a depth of $\Omega(\log n)$, which concludes the proof. This proof is essentially identical to that for the qubit sub-case, originally presented by Fang et al. (2006).

This proposition shows that the ability to implement the fan-out gate on an unbounded number of QVs in unit depth allows for lower depth circuits in comparison to standard quantum circuits, which require logarithmic depth to simulate an n-QV fan-out gate. In the next section, it will be shown that unbounded fan-out gates facilitates interesting circuit-depth reductions. A simple lemma of Proposition 3.1 is the following complexity relation between standard and unbounded fan-out circuits:

Lemma 3.1. *Any n-QV unbounded fan-out circuit $\mathfrak{F}$ may be implemented with a standard quantum circuit that has a size of $O(\text{size}(\mathfrak{F}))$ and a depth of $O(\text{depth}(\mathfrak{F}) \log n)$.*

This lemma may be used to convert the remaining results of this chapter, which will be stated in terms of unbounded fan-out circuits, into statements about standard quantum circuits. It may be also used to the same end with regard to the results of Chapter 4, in which relationships between the 1WQC and the quantum circuit model will be derived.

3.4 Constant depth unbounded fan-out circuits

It is now shown that certain operators may be implemented in constant depth with an unbounded fan-out circuit. The main purpose of presenting the following results is that they will be required to derive many of the results in Chapter 4. However, they are also of independent interest in terms of quantum circuit complexity questions.

3.4.1 Commuting circuits

Consider the circuit diagram of Figure 3.4, which shows k pair-wise commuting unitaries acting in series on a set of n QVs. An interesting property of the unbounded

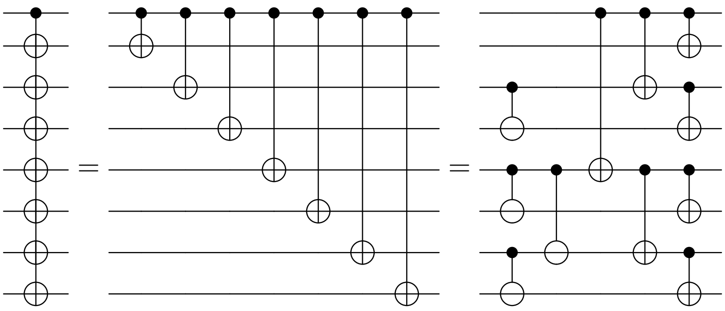


Figure 3.3: LHS: A circuit notation for the n-QV fan-out gate. Middle: The fan-out gate decomposition into n SUM gates with a circuit size and depth of $O(n)$. RHS: An alternative circuit decomposition implementing the fan-out gate with a depth of $O(\log n)$ and size $O(n)$. The case shown here is for $n = 2^3 - 1$. The same structure may be used for all $n = 2^m - 1$ and for other cases the structure for $2^{\lceil \log(n+1) \rceil} - 1$ may be used with the gates omitted which would act on non-existent QVs. The circuit notation used here for SUM and SUM† gates was introduced in Figure 2.3.

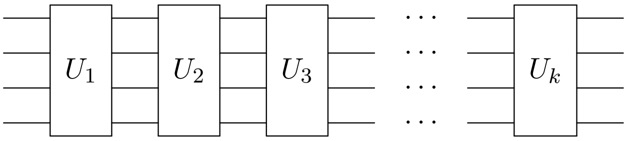


Figure 3.4: A sequence of k mutually commuting unitaries U_i, with $i = 1, \dots, k$, acting on a set of n QVs. Commutation implies that they are all diagonalised by some n-QV unitary B, i.e., $D_i = BU_iB^\dagger$ for some diagonal unitaries D_i.

fan-out gate is that it facilitates the application of commuting gates on a set of QVs in parallel, whenever the basis in which they are all diagonal can be transformed into with a sufficiently low depth circuit. More precisely:

Proposition 3.2. *Consider a sequence of k mutually commuting unitaries U_i that act on n QVs, which are therefore diagonalised by the same n-QV operator B, i.e., $BU_iB^\dagger = D_i$ where D_i is some diagonal unitary for each i. Such an operator sequence may be implemented with an unbounded fan-out circuit that has a depth of* $\max_i(\mathit{depth}(D_i)) + 2\mathit{depth}(B) + 6$*, and a size of* $\max(O(n^2), O(\mathit{size}(B)), O(\sum_i \mathit{size}(D_i)))$.

Proof: The proof precedes by providing such a circuit. The first stage of the circuit is to apply a B gate to the n-QVs, changing into the basis in which all of the gates are diagonal. Next, copy the n-QVs into $k-1$ sets of n auxiliary QVs, using n fan-out gates in parallel and $n(k-1)$ auxiliary QVs (prepared, as always, in $|0\rangle$). The diagonal unitary D_i is applied to the i^{th} register and these may be implemented in parallel (distinct QVs). This creates the required total phases because phases

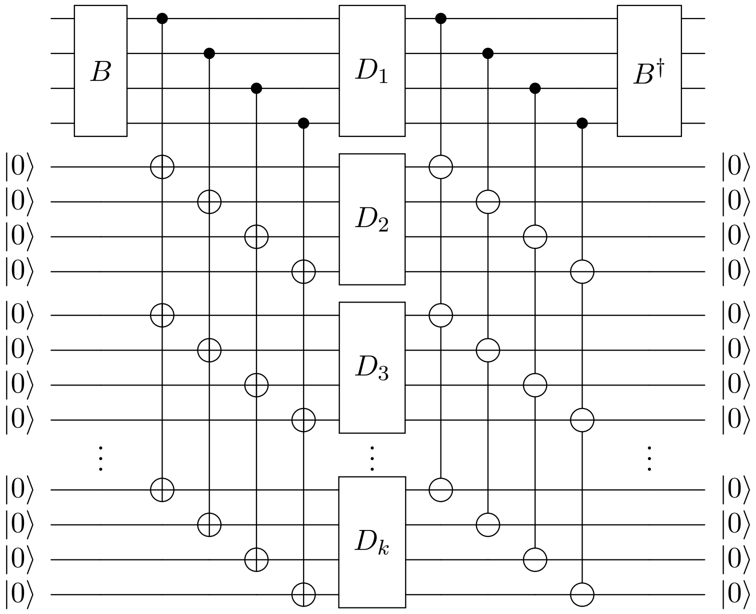


Figure 3.5: This circuit implements, in parallel and with the aid of fan-out gates, any sequence of k mutually commuting unitaries $U_i = B^\dagger D_i B$ (with $i = 1, \ldots, k$) that act on a set of n QVs. The case shown here is with $n = 4$. This circuit has constant depth (as a function of both k and n) if B, FANOUT and D_i for all i may be implemented in constant depth. This circuit requires $n(k-1)$ auxiliary QVs. Each inverse fan-out gate may be implemented with one FANOUT and four F gates.

add, i.e., $e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)}$. Inverse fan-out gates are applied to return the auxiliary QVs to the $|0\rangle$ state (this requires F, $F^\dagger$ and fan-out gates). Finally, the QVs are rotated back into the computational basis by $B^\dagger$. A careful counting of the depth and size of each stage provides the total depth and size stated above, concluding the proof. The fan-out circuit from this proof is shown in Figure 3.5.

In the special case of qubits, this proposition can be found in the literature and is due to Moore and Nilsson (2001). This result will be of use later, both in Section 3.4.2 and in Chapter 4. Moreover, it may also be applied to reduce the depth of a variety of interesting quantum circuits. One example is now considered: an arbitrary polynomial-size circuit on n-QVs, consisting of one- and two-QV diagonal gates. Such a circuit can be easily (and efficiently) rearranged into a circuit of the form given in Figure 3.6. This circuit has a depth of $2n-1$ (ignoring the overhead in decomposing these gates into those from the available set), but it is not clear how it can be computed with a lower depth than this without fan-out based techniques and utilising auxiliary QVs. By applying the technique of Figure 3.5, each layer can be implemented in parallel using auxiliary QVs and unbounded fan-out gates.

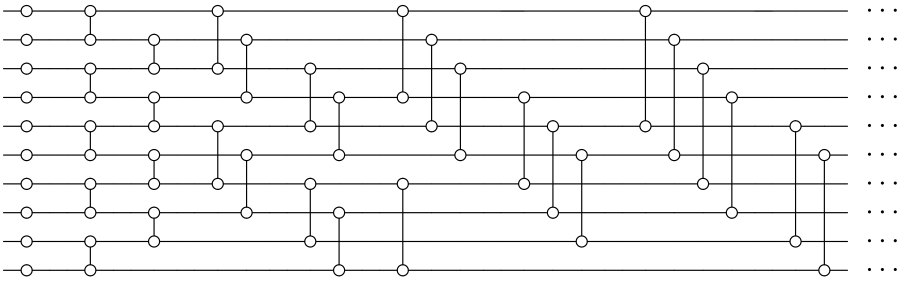


Figure 3.6: A polynomial-size circuit on n-QVs consisting of arbitrary one- and two-QV diagonal gates can be arranged into a circuit of this form, which contains $2n-1$ layers. This is achieved by writing it as a layer of local gates, followed by a sequence of two layers for nearest-neighbour interactions, then two layers for next-nearest-neighbour interactions and so on. This is partially shown here for $n = 10$, where the gates in this circuit represent generic one- and two-QV diagonal gates, and gaps are shown between layers for clarity.

This requires only constant depth with an unbounded fan-out circuit.[3] Without unbounded fan-out gates it seems unlikely to me that this can be implemented in less than $\log(n)$ depth, which can be obtained via a direct simulation of the unbounded fan-out circuit, e.g., via the method in Figure 3.3.

3.4.2 Clifford circuits

Two novel adaptions of the fan-out gate that will be useful herein are the $\textsc{fanout}(\vec{v})$ and $\textsc{multisum}(\vec{v})$ gates, which are both parameterised by a vector $\vec{v} = (v_1, \ldots, v_n) \in \mathbb{S}_d^n$, and I define by

$$|q\rangle|q_1, \ldots, q_n\rangle \xrightarrow{\textsc{fanout}(\vec{v})} |q\rangle\,|q_1 + v_1 q, \ldots, q_n + v_n q\rangle\,, \tag{3.7}$$

$$|q\rangle|q_1, \ldots, q_n\rangle \xrightarrow{\textsc{multisum}(\vec{v})} |q + v_1 q_1 + \cdots + v_n q_n\rangle\,|q_1, \ldots, q_n\rangle, \tag{3.8}$$

respectively. The latter of these gates is the natural extension to general QVs of what is called the qubit *parity* gate (the parity gate, denoted $\textsc{parity}$, is the $\textsc{multisum}(\vec{v})$ gate for qubits with $\vec{v} = (1, \ldots, 1)$). Using the conjugation action of the Fourier gate on the Pauli operators, it is easy to confirm the conjugation relation

$$\textsc{fanout}(\vec{v}) \xrightarrow{F \otimes F \otimes \cdots \otimes F} \textsc{multisum}(-\vec{v}). \tag{3.9}$$

[3] Again, this is ignoring any overhead of decomposing the unitaries, in each parallel part of the computation, into the available one and two-QV gates - in many cases this will not scale with n, and if it does this will also apply to the original fan-out free 'serial' circuit as well.

This has a similar form, and reduces to, the well-known relationship between the qubit fan-out and parity gates

$$\textsc{fanout} \xrightarrow{H\otimes H\otimes\cdots\otimes H} \textsc{parity}, \tag{3.10}$$

first noted by Moore (1999), where H is the qubit Fourier gate more often known as the Hadamard gate.

Lemma 3.2. *Any n-QV* $\textsc{fanout}(\vec{v})$ *or* $\textsc{multisum}(\vec{v})$ *gate may be implemented with an unbounded fan-out circuit that has a depth of $O(1)$ and a size of $O(n)$.*

Proof: It is only necessary to show how to implement any $\textsc{fanout}(\vec{v})$ gate as then a $\textsc{multisum}(\vec{v})$ gate may be implemented by the relation in Equation 3.10. Any $\textsc{fanout}(\vec{v})$ gate may be implemented using standard fan-out gates and $\mathrm{C}X(q)$ gates as follows: Let c_1 label the control QV and $1,\ldots,n$ label the target QVs of the $\textsc{fanout}(v)$ gate. Fan-out the control QV into $n-1$ copies using $n-1$ auxiliary QVs, labelled $c_2,\ldots,c_n$. Next, implement $\mathrm{C}_j^{c_j}X(v_j)$ gates in parallel ($j=1,\ldots,n$, each gate is on distinct QVs). Such gates can be easily obtained from the generators of the Clifford group (which have been assumed to be in the available gate set), either as powers of $\textsc{sum}$ for qudits, or using $\textsc{sum}$ and the squeezing gate for QCVs, as shown in Figure 2.4. Applying inverse fan-out gates (in parallel) disentangles the auxiliary QVs and completes the gate. Each stage has a constant depth and $O(n)$ size.[4]

Lemma 3.3. *Any polynomial-size n-QV circuit consisting of only controlled and local $Z(q)$ gates may be implemented with a constant depth and $O(n^2)$ size unbounded fan-out circuit.*

This circuits consists of commuting gates, and hence this lemma is implied by Proposition 3.2. In particular, it is a special case of the application of Proposition 3.2 to circuits consisting of only one- and two-QV diagonal gates which was discussed below that proposition and in Figure 3.6.

Proposition 3.3. *Any polynomial-size circuit consisting of only controlled and local $Z(q)$ and $X(q)$ gates may be efficiently rearranged into a polynomial-size circuit consisting of only controlled and local $Z(q)$ gates, followed by a polynomial-size circuit consisting of only controlled and local $X(q)$ gates.*

Proof: Gates on distinct QVs commute and hence it is only necessary to provide a rule for commuting gates which act on at least one QV in common. Consider commuting controlled $Z(q)$ and controlled $X(q)$ gates. As controlled $Z(q)$ is symmetric,

[4] There is a simpler method for simulating any $\textsc{fanout}(\vec{v})$, valid for QCVs and prime dimension qudits, which uses one ordinary fan-out gate and local squeezing gates on each of the target QVs.

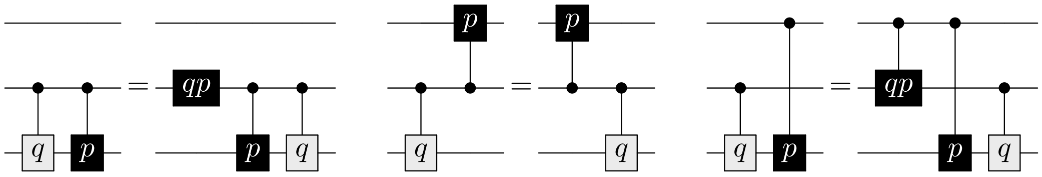


Figure 3.7: Commutation rules for reordering controlled $X(q)$ and $Z(p)$ gates. A black (grey) box containing q denotes $Z(q)$ $(X(q))$. This covers all cases as the controlled $Z(p)$ gate acts symmetrically on its input QVs.

there are only three cases to consider. Commutation rules for rearranging all three cases so that $\mathrm{C}Z(q)$ gates act before $\mathrm{C}X(q)$ gates are given in Figure 3.7. Rules for commuting the local gates, and combinations of local and controlled gates, can be obtained from these. E.g., $Z(q)$ may be commuted past a controlled $X(q)$ gate via the relation obtained by considering the input $|1\rangle$ to the top QV in the middle and RHS circuits of this figure. That the resulting circuits are still of polynomial size is obvious.

Proposition 3.4. *Any polynomial-size n-QV circuit consisting of only controlled and local $Z(q)$ and $X(q)$ gates may be implemented with an unbounded fan-out circuit of $O(n^2)$ size and $O(1)$ depth.*

Proof: By Proposition 3.3, such a circuit may be rearranged into a polynomial-size circuit consisting of only controlled and local $Z(q)$ gates, followed by a polynomial-size circuit consisting of only controlled and local $X(q)$ gates. The first part of the circuit may be implemented with a constant depth and $O(n^2)$ size unbounded fan-out circuit, by Lemma 3.3. Hence, it only remains to show that a polynomial-size circuit consisting of only controlled and local $X(q)$ gates can be implemented with a constant depth and quadratic size unbounded fan-out circuit.

The controlled and local $X(q)$ gates map computational basis states to computational basis states. Hence, for each computational basis input $|q_1, \dots, q_n\rangle$, this controlled and local $X(q)$ circuit maps

$$|q_1, \dots, q_n\rangle \to |f_1, \dots, f_n\rangle, \tag{3.11}$$

for some output computational basis state $|f_1, \dots, f_n\rangle$. Consider the first layer of the circuit: It is not hard to confirm that this maps $|q_1, \dots, q_n\rangle \to |q_1', \dots, q_n'\rangle$, where, if the layer contains the gate $X(p)$ acting on the k^{th} QV then $q_k' = q_k + p$, if the layer contains the gate $\mathrm{C}_k^j X(p)$ then $q_k' = q_k + pq_j$, and if k is either a control QV of a $\mathrm{C}X(q)$ gate, or it has no gate act on it in the layer, then $q_k' = q_k$. Hence, by writing

$\vec{q} = (q_1, \dots, q_n)^T$, and $\vec{q'} = (q'_1, \dots, q'_n)^T$, the first layer of circuit has the action

$$\vec{q'} = M^{[1]}\vec{q} + \vec{v}^{[1]}, \tag{3.12}$$

where $M^{[1]}$ is the identity matrix which is altered by letting $M^{[1]}_{k,j} = p$ if the gate $\mathrm{C}^j_k X(p)$ is in the layer, and $\vec{v}^{[1]}$ is the vector with $v^{[1]}_k = p$ if the layer contains the gate $X(p)$, and $v^{[1]}_k = 0$ otherwise. A matrix $M^{[a]}$ and a vector $\vec{v}^{[a]}$, representing each layer $a = 1, \dots, l$ of the l-layer circuit, can be found in exactly the same way. Then, by writing the final output as $\vec{f} = (f_1, \dots, f_n)^T$, and repeatedly applying Equation 3.12, the output vector is related to the input by

$$\vec{f} = M^{[l]}\left(\dots\left(M^{[2]}\left(M^{[1]}\vec{q} + \vec{v}^{[1]}\right) + \vec{v}^{[2]}\right)\dots\right) + \vec{v}^{[l]}. \tag{3.13}$$

By expanding this, the total action of the circuit may be expressed as

$$\vec{f} = M\vec{q} + \vec{v}, \tag{3.14}$$

where $M \in \mathbb{S}^n_d \times \mathbb{S}^n_d$ is given by $M = M^{[l]} \dots M^{[2]} M^{[1]}$, and $\vec{v} \in \mathbb{S}^n_d$ is given by

$$\vec{v} = M^{[l]} \dots M^{[3]} M^{[2]} \vec{v}^{[1]} + M^{[l]} \dots M^{[3]} \vec{v}^{[2]} + \dots + \vec{v}^{[l]}, \tag{3.15}$$

noting that all arithmetic is that for $\mathbb{S}_d$. Hence, the action of the circuit is entirely described by this $n \times n$ matrix M and n element vector $\vec{v}$, which can be efficiently found from a given circuit.[5]

For any given M and $\vec{v}$ pair, it is now shown how to simulate the controlled and local $X(q)$ gate circuit they describe. This requires mapping an arbitrary computational basis input state $|q_1, \dots, q_n\rangle$ to $|f_1, \dots, f_n\rangle$, where the f_k are given by $(f_1, \dots, f_n)^T = M(q_1, \dots, q_n)^T + \vec{v}$. To do this we use an additional auxiliary 'result' register (and further work auxiliary registers). The method is split into four steps, the first of which is to implement the map

$$|q_1 \dots q_n\rangle|0 \dots 0\rangle \to |q_1 \dots q_n\rangle|f'_1 \dots f'_n\rangle, \tag{3.16}$$

where the second register is this result register and $f'_k = f_k - v_k$ (so $\vec{f'} = M\vec{q}$). To begin, fan-out the main register into n auxiliary registers using n fan-out gates in parallel and n^2 auxiliary QVs (initialised to $|0\rangle$). In the k^{th} auxiliary register the k^{th} QV is mapped from $q_k \to f'_k$ using a $\mathrm{C}X(M_{kk})$ gate, with the control the k^{th} QV in the original register, and a MULTISUM gate. Specifically, for the MULTISUM gate the

[5] The matrix and vector for each layer can be easily found as above, and then the total M and $\vec{v}$ for the circuit are obtained via matrix multiplication. As the circuit is polynomial size, this is efficient.

k^{th} QV in that register is the target and the remaining $n-1$ QVs are the control QVs. The gate is MULTISUM($\vec{m}_k$) where $\vec{m}_k \in \mathbb{S}_d^{n-1}$ is the k^{th} row of M with the M_{kk} element removed. These gates may be implemented on each auxiliary register in parallel and, by Lemma 3.2, the MULTISUM gates may be implemented via fan-out gates in constant depth and linear size. The value of each f_k' may be written into the 'result' auxiliary register in a depth of 1 using n SUM gates. The next step is to disentangle the n auxiliary work registers from the main and result registers, by *uncomputing* each f_k'. This is achieved by applying the entire circuit (except the copying into the result register) backwards, with gates replaced with their inverses. This leaves n^2 clean auxiliary registers along with the original and result registers in the state $|q_1, \dots, q_n\rangle|f_1', \dots, f_n'\rangle$ for each input computational basis state $|q_1, \dots, q_n\rangle$. In order to clarify this method a circuit diagram is provided in Figure 3.8.

The second stage is to clean the original register, performing the transformation

$$|q_1 \dots q_n\rangle|f_1' \dots f_n'\rangle \to |0 \dots 0\rangle|f_1' \dots f_n'\rangle. \tag{3.17}$$

To do this, $|q_1 \dots q_n\rangle$ is calculated from $|f_1' \dots f_n'\rangle$ using the above method again (i.e., via the n auxiliary registers), but with the changes now described: The roles of the original and result registers are reversed and M is replaced with M^{-1} (which may be found by directly inverting M, or by using the same the method as used for finding M). This then computes q_k on the k^{th} QV of the k^{th} auxiliary register. A SUM† gate, with the target the k^{th} QV of the original register and the control the k^{th} QV of the k^{th} auxiliary register, maps the target to $|q_k - q_k\rangle = |0\rangle$. As above, the inverse computation is implemented to disentangle the n auxiliary registers, leaving the original and result registers in the state $|0, 0 \dots 0\rangle|f_1', f_2', \dots, f_n'\rangle$.

The third stage of the circuit swaps the states of the original and result registers, i.e., the mapping

$$|0 \dots 0\rangle|f_1' \dots f_n'\rangle \to |f_1' \dots f_n'\rangle|0 \dots 0\rangle. \tag{3.18}$$

This may be implemented by n SWAP gates in parallel, where SWAP was defined in Equation 2.55, or alternatively, simply using one SUM and one SUM† gate per QV pair. Hence, swapping the registers requires constant depth and linear size. Finally, the mapping $|f_1' \dots f_n'\rangle \to |f_1 \dots f_n\rangle$ is implemented via a $X(q)$ gate on each QV (the required gate on the k^{th} QV is $X(v_k)$, as $f_k' = f_k - v_k$). Hence, the total mapping $|q_1, \dots, q_n\rangle \to |f_1, \dots, f_n\rangle$ has been performed, as required. A careful consideration confirms that this unbounded fan-out circuit, which implements a polynomial size circuit consisting of only controlled and local $X(q)$ gates, has a depth of $O(1)$ and size of $O(n^2)$ which concludes the proof.

A similar proposition to this was proven for the qubit sub-case by Moore and Nilsson (2001). Proposition 3.4 will be crucial in the Chapter 4. It also facilitates

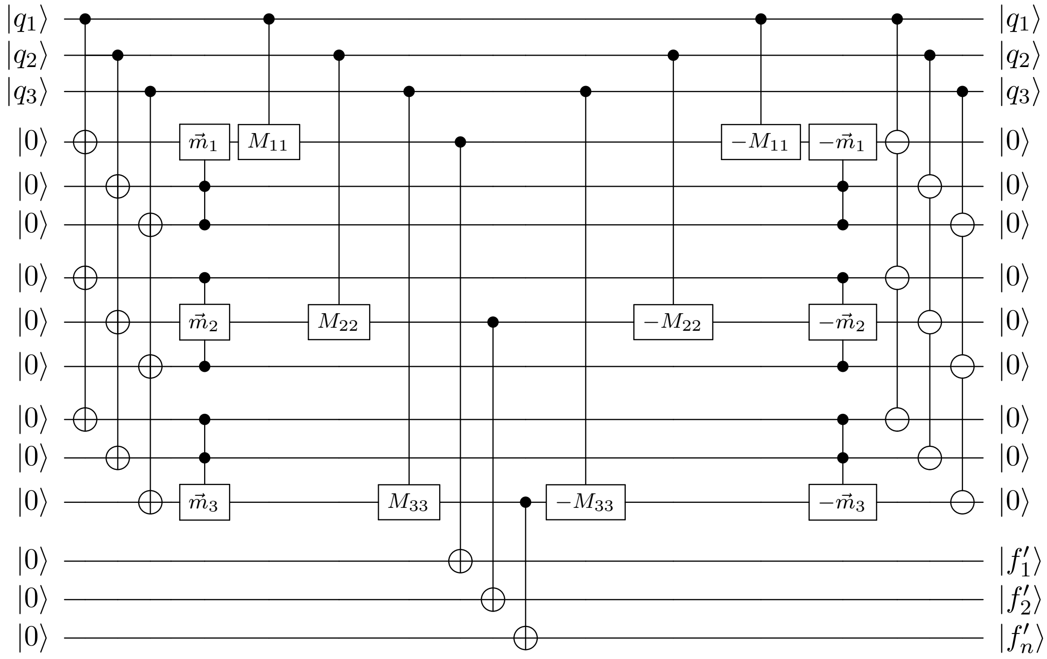


Figure 3.8: The first stage of a constant depth and quadratic size unbounded fan-out circuit simulating any polynomial-size n-QV circuit of controlled and local $X(q)$ gates. The details of this circuit are described in the proof of Proposition 3.4, which also defines the parameters in the gates. Here the case of $n = 3$ is shown.

the proof of the following:

Proposition 3.5. *Any n-QV Clifford operator may be implemented with an unbounded fan-out circuit of $O(n^4)$ size and $O(1)$ depth.*

This proposition could be obtained by directly adapting Proposition 3.4 to also include Fourier and phase gates. However, this results in an unnecessarily cumbersome proof (it is the Fourier gates which cause the main complications), hence I will instead prove it indirectly via the relationship between the one-way quantum computer and the unbounded fan-out model that is derived in the next chapter (and which requires Proposition 3.4 to obtain). It will be noted when the results presented are sufficient to directly imply Proposition 3.5.

3.5 Physically reasonable Clifford group generators

In this section, a possible criticism of the gate set used throughout this chapter is discussed which is relevant only in the case of QCVs. This is perhaps rather technical, but it is covered for clarity and because it will be important again for an observation made in Chapter 5. The results presented so far in this chapter have assumed that a set of generators for the Clifford group are included in the basic gate set. Specifically, it has been assumed that the set includes the SUM (or CZ), F, $P(p)$ and $Z(q)$ gates, for all $q, p \in \mathbb{S}_d$.[6] For qudits, the general phase and $Z(q)$ gates can be replaced with P and Z, as $P(p) = P^p$ and $Z(q) = Z^q$ for integer p and q, and the overhead of simulating any such $Z(q)$ or $P(p)$ gate with P and Z is less than d. This is a constant, and hence all the results throughout this chapter equally apply when considering this more restricted basic gate set, which is likely to be more physically relevant.

This may seem rather obvious, however, there is a more subtle technical issue in the case of QCVs. In this case, it has been assumed that $P(p)$ and $Z(q)$ for any $p, q \in \mathbb{R}$ are in the available gate set. However, the assumption inherent in including a gate in the basic gate set is that it is valid to claim it may be implemented in a depth of one, or at the very least, constant depth. As depth is meant to be a simple proxy for computational time, it is important that this is physically justifiable. However, it can be argued that this is not the case for $Z(q)$ and $P(p)$ with any $p, q \in \mathbb{R}$. To see this, note that

$$Z(q) = e^{iq\hat{x}}, \qquad P(p) = e^{ip\hat{x}^2/2}, \tag{3.19}$$

where $\hat{x}$ is the position operator. Hence, q and p are essentially the time that the Hamiltonians $-\hat{x}$ and $-\hat{x}^2/2$ need to be applied for, in order to implement these gates (up to a rescaling by any physical constants). It is therefore hard to physically justify the claim that a $Z(q)$ or $P(p)$ gate can be implemented in a unit of time (and hence a depth of one) for *all* q and p in $\mathbb{R}$ (or $\mathbb{R}_{\geq 0}$). If this argument is accepted, a natural solution to this problem is to restrict the Clifford gate generators in the basic gate set to CZ, F, $Z(q)$ and $P(p)$ where now $q, p \in [0, a]$ for some constant $a \in \mathbb{R}$ with $a \neq 0$, for example, $a = 1$ or $a = 2\pi$ are obvious possible choices, and I consider the former choice, for concreteness. It is easily confirmed that these operators still generate the Clifford group, and it is now justified in claiming that each of these gates can be implemented in a unit of time.

There are consequences in changing to this more physically motivated gate set which, if adopted, necessitates some minor adaptions to the lemmas and propositions of this chapter. For example, consider the n-QCV family of unitaries

$$U_n = Z(q) \otimes Z(2) \otimes Z(3) \otimes \cdots \otimes Z(n). \tag{3.20}$$

With the full gate set used earlier in this chapter this can obviously be implemented in a depth of 1, but using only $Z(q)$ gates with $q \in [0, 1]$ this has a depth of n, which is a linear rather than constant scaling. However, by using fan-out parallelisation techniques, it is possible to recover constant depth unbounded fan-out implementa-

[6] See the start of Section 3.3 for a discussion of this.

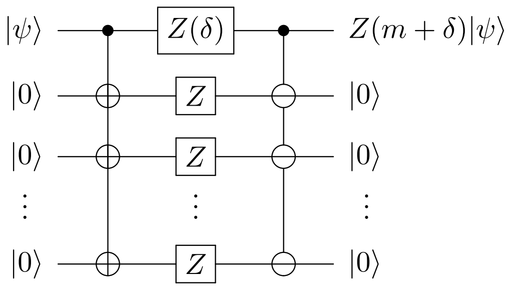


Figure 3.9: The gate $Z(m+\delta)$ for $m \in \mathbb{N}$ and $\delta \in [0,1]$, may be implemented in constant depth and $O(m)$ size via unbounded fan-out gates, m auxiliary QCVs and $Z(q)$ gates with $q \in [0,1]$. The same method may be used to implement $P(m+\delta)$ gates.

tions of the operators $Z(q)$ and $P(q)$ for any $q \in \mathbb{R}_{\geq 0}$. Implementing such a $Z(q)$ or $P(q)$ gate is achieved by writing $q = m + \delta$ for some $m \in \mathbb{N}$, and $\delta \in [0,1]$, and then using an m-QCV fan-out gate, and m auxiliary QCVs, as shown in Figure 3.9.[7] The one further issue that this raises is that now care must be taken to make sure that the unbounded fan-out circuit implementing $Z(q)$ or $P(q)$ is polynomial size - which it is if the q parameters are only polynomially large.[8] By using these ideas, then all of the lemmas and propositions of this chapter can be adapted to apply to this more physically realistic QCV gate set whilst still achieving constant depth unbounded fan-out circuits, as claimed previously in these statements. The exact required technical changes to the results of this chapter, for this different QCV gate set, are listed in the following final paragraph in this section in the interest of completeness. This may be skipped if these details are of no interest to the reader.

For QCVs and the gate set restricted as discussed above, Lemma 3.2 must be adapted to only apply to $\textsc{fanout}(\vec{v})$ and $\textsc{multisum}(\vec{v})$ gates with a vector $\vec{v} \in \mathbb{R}^n$ for which the modulus of each element in $\vec{v}$ is a polynomial in n, i.e., $O(|v_k|) = f(n)$ where $f(n)$ is a polynomial. The resulting unbounded fan-out simulation of such gates still has constant depth, but now has $O(nf(n))$ size. In Lemma 3.3 and Proposition 3.4, the $q \in \mathbb{R}$ parameters in the local and controlled $Z(q)$ and $X(q)$ gates (as appropriate for each statement) must all have $O(|q|) = f(n)$, where $f(n)$ is a polynomial. The resultant constant depth unbounded fan-out circuit is now no longer guaranteed to be quadratic size, but it will be polynomial size. Proposition 3.5 must be adapted to no longer apply to any Clifford operator, but rather a Clifford operator composed from (or that may be decomposed into) polynomially many $\textsc{cz}$,

[7] $Z(q)$ and $P(q)$ with any $q \in \mathbb{R}_{<0}$ can then be obtained via Fourier gates.

[8] E.g., the circuit for parallelising the unitary U_n in Equation 3.20 via unbounded fan-out gates would be expoentially large if the parameter in the $Z(\cdot)$ gate on the k^{th} QCV was not k but instead c^k for some constant c.

F, $Z(q)$ and $P(q)$ gates where all the parameters $q \in \mathbb{R}$ are $O(f(n))$, for a polynomial $f(n)$. Again, the unbounded fan-out circuit simulating this is still constant depth, but it is now only guaranteed to be polynomial size rather than quartic.

3.6 Implementing unbounded fan-out gates

For the purposes of this section and later chapters, it is useful to introduce the two Hermitian operators

$$\hat{x} := \sum_{q \in \mathbb{S}_d} q|q\rangle\langle q|, \qquad \hat{p} := \sum_{q \in \mathbb{S}_d} q|+_q\rangle\langle +_q|, \tag{3.21}$$

where this notation is used because they are the position and momentum operators for a QCV. Hence, the 'position' and 'momentum' terminology will be used for all QV types. The powerful nature of unbounded fan-out circuits for parallel quantum computation raises the question: *is the unbounded fan-out gate physically implementable in a single time-step?* The model that unbounded fan-out circuits has been compared to here is one in which SUM gates can be applied on-demand between arbitrary pairs of QVs and more than one SUM gate can be applied simultaneously, if acting on distinct QVs. One simple way that this might be achieved is if it is possible to turn on and off the Hamiltonians

$$\hat{H}^{\text{SUM}}_{j,k} = \hat{x}_j \otimes \hat{p}_k, \tag{3.22}$$

for arbitrary QVs j and k. This implements the SUM gate, with control QV j and target QV k, if applied for a time $t = 2\pi/d$. Dropping the j and k labels, that is: $\text{SUM} = e^{-2\pi i \hat{H}^{\text{SUM}}/d}$.

If each of these Hamiltonians can be turned on and off on demand, and if they can also be turned on and off simultaneously on distinct pairs of QVs, there is no obvious reason why it would not be possible to turn on the n commuting Hamiltonians $\hat{H}^{\text{SUM}}_{c,1}$, $\hat{H}^{\text{SUM}}_{c,2}$, ..., $\hat{H}^{\text{SUM}}_{c,n}$ simultaneously. This would implement the total Hamiltonian

$$\hat{H}_{\text{FANOUT}} = \hat{x}_c \otimes (\hat{p}_1 + \hat{p}_2 + \cdots + \hat{p}_n), \tag{3.23}$$

where this notation includes $n-1$ implicit identity operators in each of the terms in the sum. The application of this Hamiltonian, for a time $t = 2\pi/d$, implements the n-QV FANOUT gate. By this argument, it would appear that FANOUT is as physically plausible as on-demand SUM gates between arbitrary QVs.

There are a few potential problems with this idea: Firstly, the physical detail of how SUM gates are actually implemented could (and probably would) differ from simply applying $\hat{H}^{\text{SUM}}$, and the reasoning given above might not apply. This would depend on the specific physics of any given set-up. The second issue is that, in many of the proposed architectures for a quantum computer, SUM gates between arbitrary pairs of QVs are *not* directly possible, and interactions are only implementable between nearest-neighbour QVs in some geometry, e.g., a linear array [Fowler et al. (2004); Ladd et al. (2002)] or a 2D square lattice [Hollenberg et al. (2006)]. When this is the case there are significant over-heads associated with shuttling logical QVs around through different physical QVs (or using other techniques) in order to implement the required gates in a circuit. As such, in this setting even SUM cannot be considered to have unit depth between arbitrary QVs [Saeedi et al. (2011)].

One possible method for implementing entangling gates between arbitrary pairs of QVs in unit time is via ancilla-mediated gates: if the ancillas are highly mobile it may be possible to use them to interact distant QVs in a unit of time (i.e., in essentially one gate layer). This is further motivation for the ancilla-based gate methods investigated in the latter chapters of this thesis. Interestingly, these may also provide a method for implementing n-QV fan-out gates in constant depth, as is briefly discussed in Chapter 5. The final point that I would like to make is that, regardless of whether the Hamiltonian of Equation 3.23 or some other method may be used to implement fan-out gates, in all cases it seems clear that a fan-out gate of *unbounded* input size is hard to justify physically.[9] Finite input-size FANOUT gates can still potentially provide very significant parallel power, but crucially they cannot provide any *asymptotic* advantages. However, although not irrelevant, asymptotics are certainly not the only important consideration.

3.7 Conclusions

In this chapter I have introduced the general QV fan-out gate and investigated the computational power of circuits in which this may be implemented in unit depth on an unbounded number of QVs. In particular, it was shown that this gate can be used for constant depth implementations of commuting circuits, and it was claimed that this is also the case for any Clifford circuit. This latter statement will be confirmed in the following chapter. It is interesting that the ability to apply the single n-QV Clifford gate FANOUT in unit depth substantially reduces the depth required to implement any n-QV Clifford gate. Finally, I discussed whether the unbounded fan-out gate can be implemented in unit depth in practice. The results presented in this chapter will be crucial to the investigation of the one-way model for general QVs undertaken in the next chapter.

For the qubit sub-case, logarithmic and constant depth unbounded fan-out circuits have been previously investigated in detail by Høyer and Špalek (2003, 2005)

[9] Causal influences can only travel at the speed of light.

and other authors [Moore and Nilsson (2001); Takahashi and Tani (2013); Takahashi et al. (2010)]. There are a range of low-depth qubit unbounded fan-out circuits that are not included as a sub-case of any of the general QV results I have presented. For example, there is a constant depth qubit unbounded fan-out circuit that can approximate the quantum Fourier transform (QFT) [Høyer and Špalek (2005)], which is an important component in many quantum algorithms. In future work, it would be interesting to consider whether this can be extended to the QFT on a qudit register, particularly as Parasa and Perkowski (2011, 2012) have shown that the qudit QFT circuit has a range of advantages over the binary version.

Chapter 4

One-way quantum computation with general quantum variables

In this chapter the parallel power of the one-way quantum computer (1WQC) is investigated using the general quantum variable formalism, which is simultaneously applicable to qubits, qudits of any dimension and QCVs. To facilitate this, a formulation of the 1WQC is proposed in terms of general *measurement patterns* which go beyond a model focused exclusively on measurements on pre-prepared many-body entangled states. I introduce a depth-reduction procedure that can be applied to composite measurement patterns, which will then be used to highlight the differences between quantum circuits and the 1WQC. In particular, it is shown that for all types of quantum variables the computational depth complexity of the 1WQC is exactly equivalent to that of unbounded fan-out circuits. This implies that the inherent parallel power of the unbounded fan-out model is also available to the 1WQC. As such, the 1WQC is not only a physically practical model for quantum computation, but it has computational advantages over standard quantum circuits. This chapter extends a range of qubit-based results to the general QV domain, especially those of Broadbent and Kashefi (2009); Danos et al. (2007) and Browne et al. (2011). This chapter is based upon Proctor (2015).

4.1 Introduction

It has been known since Raussendorf and Briegel (2001) introduced the *one-way quantum computer* (1WQC) that adaptive local measurements of qubits prepared in an entangled state are sufficient for universal quantum computation. Not long after this it was shown that this can be extended to models defined on qudits [Zhou et al. (2003)] and QCVs [Menicucci et al. (2006)], and hence the 1WQC provides an alternative to quantum circuits for quantum computation with any type of QVs.

This remarkable computational paradigm is particularly appealing from a physical perspective as it allows the creation of entanglement to be separated into an initial off-line procedure, which is potentially much simpler than on-demand application of unitary entangling gates. Indeed, entangled resource states have been generated in a variety of settings, with a particularly impressive example given by the recent QCV-based experiments of Chen et al. (2014) and Yokoyama et al. (2013) in which 60 and 10,000 QCVs have been entangled, respectively. Furthermore, there are a range of promising experiments demonstrating the basic measurement-induced gates required to compute in this model [Bell et al. (2014); Chen et al. (2007); Lanyon et al. (2013); Su et al. (2013); Tame et al. (2014); Ukai et al. (2011)].

The one-way quantum computer, often also termed *measurement-based quantum computation*[1], may appear to have very little in common with the quantum circuit model. As such, it is perhaps surprising that it is capable of universal quantum computation. However, for *qubits* the relationship between the 1WQC and quantum circuits has been extensively researched and is now well understood [Broadbent and Kashefi (2009); Danos et al. (2007, 2009); Raussendorf et al. (2003)], with one interesting conclusion that the one-way model requires less quantum computational steps to implement certain operator sequences than standard quantum circuits [Broadbent and Kashefi (2009); Browne et al. (2011)].

Although there has been some investigations of the computational properties of the 1WQC in the more general setting of qudits [Hall (2007)] and QCVs [Gu et al. (2009)], a detailed and unified understanding of the qudit and QCV 1WQC models, and their relationship to quantum circuits, remains to be developed: This is the topic of this chapter. In the following, I will provide mappings between quantum circuits and one-way computations for general QVs. This will then be used to show that the 1WQC has exactly the same parallel power as the unbounded fan-out model, which was introduced and investigated in the previous chapter. This extends a qubit-based result of Browne et al. (2011) to the setting of general QVs. The results of this chapter highlight that, for all types of QVs, the 1WQC is especially powerful for parallel quantum computation, whilst also being a particularly physically appealing model for realising a quantum computer. I would argue that the $d > 2$ qudit-based model is especially promising as, along with this parallelism, it may also benefit from the improvements in error-correction codes and algorithm success probabilities associated with moving from a binary encoding to higher-dimensional qudits [Andrist et al. (2015); Anwar et al. (2014); Campbell (2014); Campbell et al. (2012); Duclos-Cianci and Poulin (2013); Parasa and Perkowski (2011, 2012); Watson et al. (2015); Zilic and Radecka (2007)].

The remainder of this chapter is structured as follows: Section 4.2 provides an

[1] I will only refer to this model as one-way quantum computation in this thesis.

introduction to ‘quantum teleportation’ - which is the underlying technique that the 1WQC is based upon. Section 4.3 introduces the 1WQC, within the general QV framework, and confirms the universality of this model for quantum computation. A procedure for reducing computational depth in a 1WQC is formulated in Section 4.4, which extends qubit-based work of Danos et al. (2007). In Section 4.5 I present mappings between the 1WQC and quantum circuits, which are used to derive the relationship between unbounded fan-out circuits and the 1WQC. The relationships between 1WQC, unbounded fan-out circuits and standard quantum circuits are then expressed in terms of complexity classes in Section 4.6. In Section 4.7, these complexity classes are used to show that there are a large range of quantum computational models which the 1WQC can simulate with no increase in depth scaling. Section 4.8 will briefly comment on the classical computations required in the 1WQC and the role of quantum resources in enhancing classical computations. Finally, the experimental progress in implementing 1WQC is discussed in Section 4.9 and the chapter concludes in Section 4.10.

4.2 Logical gates via projective measurements

Projective measurements generically destroy quantum superpositions, and hence it may seem strange that they can be used to drive unitary evolution. Therefore, before considering the 1WQC more formally, it is useful to begin by demonstrating the basic underlying idea on which this model rests: quantum teleportation. Consider two QVs, the first of which is in some computational basis state $|q\rangle$, and the second of which is prepared in the conjugate basis state $|+_0\rangle$. If a CZ gate is applied to this pair of QVs, they are mapped to

$$|q\rangle|+_0\rangle \xrightarrow{\text{CZ}} |q\rangle|+_q\rangle. \tag{4.1}$$

This has imprinted the value of q into the second QV. Next, apply an $R(\vartheta)$ gate (which is defined in Equation 2.58) to the first QV, for some arbitrary function ϑ, and then an F gate also to this QV. This is the mapping

$$|q\rangle|+_q\rangle \xrightarrow{FR(\vartheta)\otimes\mathbb{I}} e^{i\vartheta(q)}|+_q\rangle|+_q\rangle. \tag{4.2}$$

The key point to note is that this phase factor is no more associated with one QV than the other.

Now, consider performing a destructive measurement on the first QV which projects it onto the computational basis state $|m\rangle$, with associated outcome $m \in \mathbb{S}_d$. By a *destructive* measurement it is meant that the measured QV is destroyed in the measurement process; mathematically it is traced-out, leaving a one-QV state.

Hence, the effect of the measurement on the second QV is:

$$e^{i\vartheta(q)}|+_q\rangle|+_q\rangle \xrightarrow{\text{measurement}} \frac{\langle m|+_q\rangle}{|\langle m|+_q\rangle|}e^{i\vartheta(q)}|+_q\rangle, \tag{4.3}$$

for known $m \in \mathbb{S}_d$, where the denominator in the fraction is the required renormalisation term. The overlap of a computational and conjugate basis state is $\langle m|+_q\rangle = \omega^{mq}/\sqrt{d}$, as stated in Equation 2.28, and so this state may be written as

$$\frac{\langle m|+_q\rangle}{|\langle m|+_q\rangle|}e^{i\vartheta(q)}|+_q\rangle = \omega^{mq}e^{i\vartheta(q)}|+_q\rangle. \tag{4.4}$$

Therefore, the measurement has induced a phase factor which depends on both m and q. As $X(-m)|+_q\rangle = \omega^{mq}|+_q\rangle$ via Equation 2.29, then from the action of $R(\vartheta)$ and F on the computational basis it follows that

$$\omega^{mq}e^{i\vartheta(q)}|+_q\rangle = X(-m)FR(\vartheta)|q\rangle. \tag{4.5}$$

As such, the effect so far has been to 'teleport' $|q\rangle$ from the first to the second QV and in the process apply the gate $FR(\vartheta)$ and the probabilistic measurement-induced $X(-m)$ 'error', where every $m \in \mathbb{S}_d$ is equally likely to be the actualised value. This error can be removed by applying $X(m)$, leaving the final state

$$X(-m)FR(\vartheta)|q\rangle \xrightarrow{\text{correction}} FR(\vartheta)|q\rangle. \tag{4.6}$$

The $X(m)$ gate can be considered a hybrid quantum-classical SUM gate, as m is the value of a classical variable. By linearity, if the first QV is in the general input state $|\psi\rangle = \sum_{q\in\mathbb{S}_d} c_q|q\rangle$, this whole procedure maps

$$|\psi\rangle|+_0\rangle \longrightarrow FR(\vartheta)|\psi\rangle. \tag{4.7}$$

This is summarised in Figure 4.1 as a quantum-classical hybrid circuit, where double wires represent classical variables of the same type as the QVs (i.e., for qubits they are bits, for qudits they are dits, and for QCVs they are classical continuous variables).

A projection onto a computational basis state is only one possible measurement and the local gates on the first QV, in the above protocol, may be absorbed into a more general ϑ-parameterised measurement. In order to introduce these measurements, it is useful to define the u-parameterised Hermitian operator

$$\hat{x}_u := \sum_{q\in\mathbb{S}_d} q\left(u^\dagger|q\rangle\langle q|u\right) = u^\dagger\hat{x}u, \tag{4.8}$$

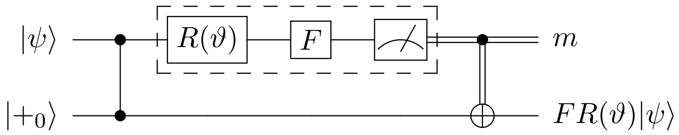


Figure 4.1: A hybrid quantum-classical circuit which implements the gate $FR(\vartheta)$ and teleports a QV in an unknown state $|\psi\rangle$ to a second QV initialised to $|+_0\rangle$. In addition to unitary gates, this circuit uses a destructive measurement and classical controls. The operations enclosed by a dashed box can be combined into a general ϑ-parameterised measurement.

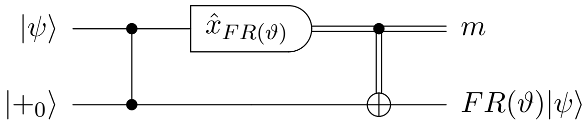


Figure 4.2: Local unitary controls can be absorbed into a change in measurement basis. This gate implementation protocol is the basis of the 1WQC.

where $\hat{x}$ is the 'position' operator for a general QV, as introduced in Equation 3.21. In practice, a measurement of this operator does not need to actually have the outcome q associated with a projection onto $u^\dagger|q\rangle$ in the sense that, as long as the measurement outcome for each basis state is distinct, the outcomes can be mapped onto these values. It is sometimes a useful shorthand to discuss 'measuring in a basis'. Consider the basis

$$\mathcal{B}_u := \{u^\dagger|q\rangle \mid q \in \mathbb{S}_d\}. \tag{4.9}$$

By the statement '*a measurement in the basis* $\mathcal{B}_u$' what will be meant is a measurement of the Hermitian operator $\hat{x}_u$. For a destructive measurement, the application of u followed by a computational basis measurement is exactly equivalent to a measurement in the $\mathcal{B}_u$ basis. Therefore, the procedure of Figure 4.1 can implemented without any single-QV gates by instead using a ϑ-parameterised $\mathcal{B}_{FR(\vartheta)}$ basis measurement, as shown in Figure 4.2. Note that performing variable measurements may in practice be no easier than implementing local gates and a fixed measurement - but it is at least no harder, as it can always be decomposed as such.

There is no *a priori* reason that a measurement of one of a pair of entangled QVs, encoding a shared logical QV, will result in a unitary action on this logical QV. For example, consider the two-QV state

$$|\Psi\rangle = \sum_{q\in\mathbb{S}_d} c_q|q,q\rangle, \tag{4.10}$$

which encodes the $|\psi\rangle = \sum_{q\in\mathbb{S}_d} c_q|q\rangle$ logical QV. A destructive computational basis measurement of either QV will implement the mapping

$$\sum_{q\in\mathbb{S}_d} c_q|q,q\rangle \xrightarrow{\mathcal{B}-\text{measurement}} |m\rangle, \tag{4.11}$$

with probability $|c_m|^2$, which is not a logical unitary: it has destroyed the logical QV and extracted some information about the values of c_q. The key to the scheme of Figure 4.2 is that the measurement is in a basis that is conjugate to the basis in which the shared QV is encoded: if either QV in Equation 4.2 is measured in the conjugate basis then the value of q is revealed, but a measurement of either QV in the computational basis reveals nothing about this value. The inherent element of randomness in the measurement outcomes is then realised as the random phase error.

The protocol presented above is the basic building block of one-way quantum computation. It may seem like this method has involved quite a lot of hard work simply to implement a single-QV unitary gate, however, the 1WQC model based on this has a range of advantages over quantum computation with unitary evolution (and final measurements) alone. In my opinion, a particularly intuitive way to think of the 1WQC is as a structured method for turning fully quantum circuits into quantum-classical hybrid circuits. In doing so, it transfers some of the computation to the classical domain, which is highly preferable in practice. Bearing this in mind throughout the remainder of this chapter can help to clarify the results presented. However, from other points of view the one-way quantum computer is radically different to quantum circuits.

4.3 The one-way quantum computer for general quantum variables

The 1WQC for general QVs is now defined. This will include cluster state computation (i.e., measurements on a lattice entangled state) as a sub-case, which is the standard formulation for the qudit [Zhou et al. (2003)] and QCV [Menicucci et al. (2006)] models, but it is more general than this. As the formalism I propose here largely extends previous qubit-based work, the notation and terminology I use in the remainder of this chapter is chosen to closely match that in common use for the qubit sub-case, see e.g., Danos et al. (2007). It will be useful in this chapter, and throughout this thesis, to use a subscript on an operator to denote the QV it acts upon, e.g., u_jv_k represents u and v acting on QVs j and k, respectively. In the following, I will define the 1WQC in terms of a quantum computational model $\mathfrak{M}$, and I will use the associated notation and concepts (e.g., serial and parallel compositions), which were introduced in Section 2.3.

I define the general quantum variable 1WQC to be a quantum computational model $\mathfrak{M} = \{\mathfrak{o}, \mathfrak{s}\}$ in which the allowed set of operations $\mathfrak{o}$ are the *entangling operations*, *Pauli corrections* and *dependent* and *independent measurements* which will be defined in-turn below. The set of preparable states, $\mathfrak{s}$, which non-input QVs can be initialised to, is taken to be $\mathfrak{s} = \{|+_0\rangle\}$. Each operation type is now introduced:

1. *Entangling operations:* The entangling operation, denoted $E_{i,j}$, where i and j are the QVs on which it acts, is defined by

$$E_{i,j} := \mathrm{C}^i_j Z, \tag{4.12}$$

which is simply the CZ operator.[2]

2. *Pauli corrections:* The Pauli corrections are classically-controlled X and Z operators, specifically they are $X_i(s)$ and $Z_i(t)$ operators where $s, t \in \mathbb{S}_d$ are classical variables (CLVs) calculated from constants and measurement outcomes (see below) using the arithmetic of $\mathbb{S}_d$.

3. *Dependent measurements:* A dependent measurement, denoted ${}_t\big[M_i^\vartheta\big]^s$, is defined to be a destructive measurement on the i^{th} QV of the operator

$$\hat{x}_{FR(\vartheta)X(s)Z(t)}, \tag{4.13}$$

for some $\vartheta : \mathbb{S}_d \to \mathbb{R}$ and $s, t \in \mathbb{S}_d$. The measurement outputs a CLV, and this is denoted by $m_i \in \mathbb{S}_d$. A phase function, ϑ, and values for the s and t CLVs must be provided to completely specify a dependent measurement.

4. *Independent measurements:* This is a measurement which does not require input CLVs to define. It is a measurement of $\hat{x}_{FR(\vartheta)}$. Such a measurement is denoted M_i^ϑ.

Because a destructive measurement of $\hat{x}_{vu}$ is equivalent to a u gate followed by a measurement of $\hat{x}_v$ and because $\hat{x}_{e^{i\phi}u} = \hat{x}_u$, it follows that

$${}_{t+t'}\Big[M_i^\vartheta\Big]^{s+s'} = {}_t\Big[M_i^\vartheta\Big]^s X_i(s')Z_i(t') = M_i^\vartheta X_i(s+s')Z_i(t+t'). \tag{4.14}$$

Hence, it is simple to convert between dependent measurements and independent measurements preceded by Pauli corrections. To implement a dependent measurement the values of the CLVs may be accounted for by altering the phase function ϑ,

[2] This uses the $\mathrm{C}^i_j u$ notation for CZ as it is more convenient for explicitly denoting which the control and target QVs are. It might also seem questionable whether there is any need for this extra $E_{i,j}$ notation. However, it will make the similarities between this and another model, with an alternative entangling operation, more obvious when discussed later in this thesis.

as we now see. By noting that $X(s)$ maps $|q\rangle \to |q+s\rangle$ and that $Z(t) = R(\varphi)$ with $\varphi(q) = 2\pi tq/d$, it follows that

$$R(\vartheta)X(s)Z(t) = X(s)R\left(\vartheta_{s,t}\right), \tag{4.15}$$

where $\vartheta_{s,t}$ is the s and t adapted phase function

$$\vartheta_{s,t}(q) = \vartheta(q+s) + 2\pi tq/d. \tag{4.16}$$

Using this, it may then be shown that

$$\langle q|FR(\vartheta)X(s)Z(t) = \langle q|FX(s)R\left(\vartheta_{s,t}\right) = \omega^{sq}\langle q|FR\left(\vartheta_{s,t}\right). \tag{4.17}$$

This implies that

$$\hat{x}_{FR(\vartheta)X(s)Z(t)} = \hat{x}_{FR(\vartheta_{s,t})}. \tag{4.18}$$

and hence a dependent measurement can be accounted for by adapting the ϑ parameterised measurement dependent on the CLVs s and t, via $\vartheta \to \vartheta_{s,t}$. This encompasses the adaptive element of the 1WQC. The formalism that has been introduced above will be particular useful for comparing quantum circuits and the 1WQC.

4.3.1 Basic measurement patterns

A computation in the one way model will be called a *measurement pattern*. A particular pattern is specified by giving a quadruplet

$$\mathfrak{P} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{p}), \tag{4.19}$$

where $\mathfrak{p}$ is a sequence of operations on the set of QVs $\mathcal{V}$ (and $\mathcal{I}$ and $\mathcal{O}$ are input and output subsets of QVs). The definitions of the allowed operations in the model may appear rather technical and hence, in order to illustrate how a measurement pattern implements a quantum computation and to demonstrate the universality of the model, examples of patterns are now given.

It is essentially trivial to give a pattern that implements the CZ gate. As the entangling operation is a CZ operator, this can be implemented with the measurement-free pattern

$$\mathfrak{P}_{\text{CZ}} = (\{1,2\}, \{1,2\}, \{1,2\}, E_{1,2}), \tag{4.20}$$

in which $\mathcal{V} = \mathcal{I} = \mathcal{O}$. To be clear, there are two QVs in total on which the measurement pattern acts, labelled ‘1’ and ‘2’ (the set $\{1,2\}$), and these are also the input and output subsets.

In Section 4.2 it has already been shown how a $FR(\vartheta)$ gate may be implemented via an entangling operation and a variable measurement, as summarised by Figure 4.2. The procedure of Figure 4.2 may be expressed as the measurement pattern

$$\mathfrak{P}_{FR(\vartheta)} = (\{1,2\},\{1\},\{2\},X_2(m_1)M_1^{\vartheta}E_{1,2}), \tag{4.21}$$

in which there is one input QV, labelled 1, and one output QV, labelled 2, and the first QV is destroyed in the process.[3] This demonstrates the utility of this notation: this expression is a fairly compact representation of a non-trivial procedure. From this measurement pattern it is possible to generate F and any $R(\vartheta)$ using composition of measurement patterns. Specifically, using the 'zero function' $\vartheta_0(q) = 0$ for all q, then[4]

$$\mathfrak{P}_F = \mathfrak{P}_{FR(\vartheta_0)}, \qquad \mathfrak{P}_{R(\vartheta)} = \mathfrak{P}_F \circ \mathfrak{P}_F \circ \mathfrak{P}_F \circ \mathfrak{P}_{FR(\vartheta)}, \tag{4.22}$$

which uses relation that $F^4 = \mathbb{I}$, given in Equation 2.24. Although a special case of the $R(\vartheta)$ gate, the $Z(q)$ gate may also be implemented with the measurement-free pattern

$$\mathfrak{P}_{Z(q)} = (\{1\},\{1\},\{1\},Z_1(q)), \tag{4.23}$$

which simply uses a correction to implement the gate.

4.3.2 A universal set of measurement patterns

The measurement patterns presented above can generate logical gates that are sufficient for universal quantum computation - an entangling gate, the Fourier gate and some set of rotation gates is a universal gate set, as was discussed in Section 2.5. Hence, by composition of measurement patterns, this shows that the 1WQC is a universal quantum computer provided suitable measurements are available. Note that this has already been shown in the original papers on 1WQC, using the cluster-state formalism [Menicucci et al. (2006); Raussendorf and Briegel (2001); Zhou et al. (2003)].

One of the aims of this chapter is to compare the 1WQC and the quantum circuit models introduced in the previous chapter. Hence, to facilitate a suitable comparison, it is helpful to restrict both models to equivalent logical gate sets. If we wish to only consider approximate universality then (again) the gate set that will be considered is $\mathcal{G}_{\epsilon-\text{UNI}}$, as introduced in Equation 2.59, which includes the generators of the Clifford group CZ, F, $P(p)$ and $Z(q)$ for $q \in \mathbb{S}_d$, along with $q \in \mathbb{S}_d$ powers of

[3] Alternatively, a nice way to think of this is that the measured QV is being transformed into a classical variable by the measurement.

[4] This uses the idea of a serial computation as given in Equation 2.38, denoted by the composition symbol '$\circ$'. The idea is that the output of one computation is the input to the next. With measurement patterns this is less trivial than with quantum circuits, but is still fairly straight forward.

some single-QV non-Clifford gate u that is sufficient for universality. We again take this u gate to be diagonal, with its phase function denoted ϑ_f, and this may be the relevant 'cubic' gate for the QV type, as discussed in Section 2.5, if a specific choice is needed.[5]

To implement the Clifford gates in this set, it is sufficient to demand that measurements of $\hat{x}_\vartheta$ can be performed for phase-functions $\vartheta_0(q)$ and $\vartheta_{P(p)}$ given by

$$\vartheta_0(q) = 0, \tag{4.24}$$

$$\vartheta_{P(p)}(q) = \pi pq(q+\varrho_d)/d, \tag{4.25}$$

where $\varrho_d = 1$ for odd-dimension qudits, and $\varrho = 0$ otherwise. This is because these phase functions in the pattern $\mathfrak{P}_{FR(\vartheta)}$ implement logical F and $FP(p)$ (as the phase gate acts as $P(p)|q\rangle = e^{\pi i pq(q+\varrho_d)/d}|q\rangle$) and the other generators are obtained from the measurement-free patterns $\mathfrak{P}_{\text{CZ}}$ and $\mathfrak{P}_{Z(q)}$. The availability of an $\hat{x}_{\vartheta_f}$ measurement is then essential to access a universal gate set, and furthermore, for some purposes, it is also essential to be able to measure the classically-adapted version of this, as given by Equation 4.17. Finally, if it is instead desirable to consider exact universality (relevant only for qudits), the set of all ϑ phase-functions is sufficient for this (see Section 2.5). For most of the following the exact gate set, or rather the measurement-basis set, is not explicitly relevant. However, some results rely on the implicit assumption that Clifford gates can be implemented exactly.

4.3.3 Depth and size in measurement patterns

The main aim of this chapter is to study depth and size complexity in measurement patterns, and compare this to quantum circuits. The definitions of quantum depth and size given in Section 3.2 can be immediately applied to measurement patterns and compositions of measurement patterns. However, the concept of depth is in this case rather more subtle than with quantum circuits and therefore an example is now given. Consider the measurement pattern

$$\mathfrak{P} = (\{1,2,3,4\}, \{1\}, \{4\}, \mathfrak{p}), \tag{4.26}$$

with the operation sequence $\mathfrak{p}$ given by

$$\mathfrak{p} = X_4(m_3 - q - m_1 - pm_2)Z_4(m_2)M_3^{\vartheta_{P(p)}}[M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}. \tag{4.27}$$

This is a sequence of three entangling operations, followed by three measurements (two independent, one dependent), and finally, a pair of corrections on the output.

[5] This is appropriate for QCVs and prime dimension qudits. For non-prime dimensions a generic rotation gate will suffice (see Appendix G).

The size of a pattern is no more complex to understand than with a circuit: this pattern has a size of eleven (with a contribution of two from each entangling operation, as they act on two QVs, and one from each of the other operations).

The (quantum) depth of a computation is defined as the longest subsequence of dependent operations from its command sequence $\mathfrak{p}$: a subsequence of dependent operations is one in which each operation acts on a QV in common with, or depends on the outcome of, the previous operation in the sequence (see Definitions 3.1 and 3.2). It is easy to find dependent subsequences in a measurement pattern, for example, take the first and third operations in $\mathfrak{p}$. This is the subsequence $E_{2,3}E_{1,2}$ and this satisfies these criteria: $E_{2,3}$ acts on a QV in common with $E_{1,2}$. However, the subsequence of the first and second operation $E_{3,4}E_{1,2}$ is *not* a dependent subsequence - encoding the idea that they can be implemented simultaneously. In this pattern the depth is five, as this is length of the longest dependent subsequence. For example, one such subsequence is highlighted in cyan below:

$$\mathfrak{p} = X_4(m_3 - q - m_1 - pm_2)Z_4(m_2)M_3^{\vartheta_{P(p)}}[M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}. \tag{4.28}$$

The $[M_2^{\varphi}]^{m_1}$ measurement does not act on the same QV as the operation before it in this subsequence, but it does depend on the outcome of that operation. An alternative dependent subsequence of the same length is obtained by removing M_1^{ϑ} and including $E_{2,3}$, but both operations cannot be included as they act on no QVs in common, and M_1^{ϑ} does not depend on an outcome of $E_{2,3}$ (which is not even a measurement). The measurement pattern used here to illustrate size and depth may seem rather arbitrary. However, it is a useful computation which implements the unitary $FP(p)Z(q)FR(\varphi)FR(\vartheta)$ and, as will be seen in the next section, this can be obtained by composition of the individual basic patterns for the $FP(\vartheta)$ gate and the $Z(q)$ gate, which were given in Equation 4.21 and Equation 4.23.

4.4 Standard measurement patterns

The presentation of the 1WQC given so far does not highlight the advantages over quantum circuits inherent in measurement patterns. These can be illuminated by introducing an operation rearranging process that can be applied to composite measurement patterns, and which will be called *standardisation*. This extends ideas developed for qubits by Danos et al. (2007).

4.4.1 Entangle → measure → correct

Composite measurement patterns can be rearranged so that they consist of an initial sequence of entangling operations, followed by measurements, and then finally Pauli corrections only on the output QVs. This then links general measurement patterns to computation with cluster states, in which dependent measurements are performed on pre-prepared entangled states. Let the i^{th} QV, along with the classical variable m_i this is converted to by a measurement (if any), be termed *variable i*. Operations acting on, or depending on, distinct variables commute and may be freely rearranged. Hence, the operations in any pattern may be reordered into entangling operations, measurements and then corrections, with the aid of the equalities

$$E_{ij} \cdot X_i(s) Z_i(t) = X_i(s) Z_i(t) Z_j(s) \cdot E_{ij}, \tag{4.29}$$

$$_t[M_i^{\vartheta}]^s \cdot X_i(s') Z_i(t') = {}_{t+t'}[M_i^{\vartheta}]^{s+s'}. \tag{4.30}$$

The first of these equalities follows from the conjugation rule for CZ on Pauli gates, given in Equation 2.53, and the second equality was already stated in Equation 4.14. Notice that the rearrangement of the entangling operation to precede the corrections, whilst maintaining the corrections as Pauli gates, is only possible because the entangling operation is Clifford.

4.4.2 Removing dependencies for Clifford gates

In the case of patterns including Clifford operators, a further stage of pattern rewriting can be implemented, which will be called *Pauli simplification*. The only patterns for generating the Clifford group that require measurements are those for F and $FP(p)$, with associated measurement phase functions θ_0 and $\vartheta_{P(p)}$, introduced in Equations 4.24 and 4.25. Using the phase and Fourier gate conjugation rules given in Equations 2.51 and 2.52, it follows that

$$\langle q| FP(p) X(s) Z(t) = \omega^{sp(s+\varrho_d)/2 - qs} \langle q| FP(p) Z(t+sp), \tag{4.31}$$

and similarly, $\langle q|FX(s)Z(t) = \omega^{-qs}\langle q|FZ(t)$, which respectively imply that

$$\hat{x}_{FR(\vartheta_{P(p)})X(s)Z(t)} = \hat{x}_{FR(\vartheta_{P(p)})Z(t+sp)}, \tag{4.32}$$

$$\hat{x}_{FR(\vartheta_0)X(s)Z(t)} = \hat{x}_{FR(\vartheta_0)Z(t)}. \tag{4.33}$$

Written in terms of the measurement operations notation, this says that

$$_t\left[M_i^{\vartheta_{P(p)}}\right]^s = {}_{t+sp}\left[M_i^{\vartheta_{P(p)}}\right], \tag{4.34}$$

$$_t\left[M_i^{\vartheta_0}\right]^s = {}_t\left[M_i^{\vartheta_0}\right], \tag{4.35}$$

where dropping one dependency super-script (or sub-script) is a natural way to denote that the measurement no longer has this dependency type (we could equivalently put a 0 superscript here). Hence, by using these equations after standardisation has been applied to a pattern, all the X-type dependencies can be removed from these Clifford measurements in a pattern.

4.4.3 Removing all Z-type dependencies

The final stage of pattern rewriting to be introduced will be called *signal shifting* and this removes *all* Z-type dependencies in *all* the measurements. Again, using the conjugation relation in Equation 2.51, it follows that

$$\langle q|FR(\vartheta)X(s)Z(t) = \omega^{-st}\langle q|X(-t)FR(\vartheta)X(s) = \omega^{-st}\langle q+t|FR(\vartheta)X(s). \quad (4.36)$$

Therefore, a general $s, t \in \mathbb{S}_d$ classically-adapted measurement operator may be rewritten as

$$\hat{x}_{FR(\vartheta)X(s)Z(t)} = \sum_{q\in\mathbb{S}_d}(q-t)\left(X(-s)R(-\vartheta)F^{\dagger}|q\rangle\langle q|FR(\vartheta)X(s)\right). \quad (4.37)$$

Such a measurement is equivalent to instead measuring $\hat{x}_{FR(\vartheta)X(s)}$ and then subtracting t from the measurement outcome.[6] In terms of measurement operations, this can then be understood as the equality

$$\left(m_i, {}_t[M_i^{\vartheta}]^s\right) = \left(m_i - t, [M_i^{\vartheta}]^s\right). \quad (4.38)$$

This denotes that the measurement outcome m_i is classically post-processed if the change in the measurement basis is dropped, and hence, anywhere in the pattern that m_i appeared, now $m_i - t$ appears.

4.4.4 Applying the standardisation procedure

The composite process of standardisation, Pauli simplification and then signal shifting will be called *complete standardisation*, and a pattern on which this has been applied is called *completely standard*. A completely standard measurement pattern for a Clifford circuit will have no dependent measurements, and hence all of the measurements may be performed simultaneously. To clarify the process of complete standardisation, an example of applying this to a composite pattern is now given.

Consider the composite patten for the single-QV unitary $FR(\gamma)Z(q)FR(\varphi)FR(\vartheta)$ for some arbitrary functions ϑ, φ and γ and $q \in \mathbb{S}_d$, as obtained from the basic patterns $\mathfrak{P}_{FR(\vartheta)}$ and $\mathfrak{P}_{Z(q)}$, which are given in Equation 4.21 and Equation 4.23,

[6] For qudits, note that subtraction of t means adding $d-t$ modulo d.

respectively. Via the definition of serial composition, this is the pattern

$$\mathfrak{P}_{FR(\gamma)Z(q)FR(\varphi)FR(\vartheta)} = (\{1,2,3,4\},\{1\},\{4\},\mathfrak{p}), \tag{4.39}$$

where $\mathfrak{p}$ is given by

$$\mathfrak{p} = \Big(X_4(m_3)M_3^{\gamma}E_{3,4}\Big)Z_3(q)\Big(X_3(m_2)M_2^{\varphi}E_{2,3}\Big)\Big(X_2(m_1)M_1^{\vartheta}E_{1,2}\Big), \tag{4.40}$$

where the brackets are used to clearly distinguish the operation sequence obtained from each of the four basic patterns. First we apply standardisation to this sequence of operations. This procedure gives

$$\begin{aligned}
\mathfrak{p} &= X_4(m_3)M_3^{\gamma}E_{3,4}Z_3(q)X_3(m_2)M_2^{\varphi}E_{2,3}X_2(m_1)M_1^{\vartheta}E_{1,2}, && (4.41)\\
&\Rightarrow X_4(m_3)M_3^{\gamma}Z_3(q)X_3(m_2)Z_4(m_2)E_{3,4}M_2^{\varphi}X_2(m_1)Z_3(m_1)E_{2,3}M_1^{\vartheta}E_{1,2}, && (4.42)\\
&\Rightarrow X_4(m_3)Z_4(m_2)\,{}_q[M_3^{\gamma}]^{m_2}M_2^{\varphi}X_2(m_1)Z_3(m_1)M_1^{\vartheta}E_{3,4}E_{2,3}E_{1,2}, && (4.43)\\
&\Rightarrow X_4(m_3)Z_4(m_2)\,{}_{q+m_1}[M_3^{\gamma}]^{m_2}[M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}, && (4.44)\\
&= \mathfrak{p}^{(s)}. && (4.45)
\end{aligned}$$

This pattern is now standardised. It is clear that it now consists first of entangling operations, then measurements, and finally corrections on the output QV. In this case, as there are no Clifford gate measurements, the Pauli simplification stage changes nothing. Signal-shifting is then applied, which results in the transformation

$$\mathfrak{p}^{(s)} \Rightarrow X_4(m_3 - q - m_1)Z_4(m_2)[M_3^{\gamma}]^{m_2}[M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}. \tag{4.46}$$

This sequence is then completely standardised. Notice that, although this procedure has (slightly) reduced the depth of the pattern, none of the measurements have lost their dependencies, and so they still have to be performed in sequence.

To demonstrate the procedure when some of the gates are Clifford, return to the standardised pattern $\mathfrak{p}^s$ and set $\gamma = \vartheta_{P(p)}$. The Pauli simplification procedure obtains the pattern

$$\begin{aligned}
\tilde{\mathfrak{p}}^{(s)} &= X_4(m_3)Z_4(m_2)\,{}_{q+m_1}[M_3^{\vartheta_{P(p)}}]^{m_2}[M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}, && (4.47)\\
&\Rightarrow X_4(m_3)Z_4(m_2)\,{}_{q+m_1+pm_2}[M_3^{\vartheta_{P(p)}}][M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}, && (4.48)\\
&= \tilde{\mathfrak{p}}^{(ps)}. && (4.49)
\end{aligned}$$

Applying signal shifting to this new operation sequence then results in the pattern

$$\tilde{\mathfrak{p}}^{(ps)} \Rightarrow X_4(m_3 - q - m_1 - pm_2)Z_4(m_2)M_3^{\vartheta_{P(p)}}[M_2^{\varphi}]^{m_1}M_1^{\vartheta}E_{2,3}E_{3,4}E_{1,2}. \tag{4.50}$$

This pattern is now completely standard. Notice that the Clifford measurement now has no dependencies, and hence, it may be implemented in the first round of measurements. This is the pattern that was used in Section 4.3.3 to demonstrate depth and size in the 1WQC.

It can be shown that complete standardisation never increases the (quantum) size or depth of a pattern[7], and in many cases it can substantially reduce it. The cost of this is the addition of simple classical processing - the exact requirements of this classical side-processing are discussed Section 4.8.

4.4.5 Entanglement graphs

The complete standardisation procedure results in a computation in which classically controlled measurements are implemented on an entangled state, and explicit corrections are only applied on the output (if at all[8]). This is exactly the idea of cluster state computation. The entanglement stage of a pattern may be represented uniquely as a graph in which the nodes are the QVs and the number of edges between nodes represents the number of entangling operations acting on each QV pair (for qudits, this may be restricted to being in $\mathbb{Z}(d)$). The graph may also be labelled with measurement bases, along with their dependencies, to completely define a standard measurement pattern. This is shown in Figure 4.3.

Definition 4.1. *The entanglement depth is the minimum depth of the entanglement operations in a standardised pattern.*

It is defined to be the *minimum* depth because, by arranging the entangling operations in a particularly inconvenient order, the depth can (in most cases) obviously be increased. However, as the entangling operations can be freely commuted, it is more useful to know what the minimum depth can be by a judicious rearrangement of these operations. For example, consider the 'cascade' of CZ gates, which may be arranged for the depth to be either two or the same as the number of gates, shown in Figure 3.2. The entanglement depth of a standard pattern can be easily extracted from its graph representation:

Lemma 4.1. *[Broadbent and Kashefi (2009) Lemma 3.1] Let G be the entanglement graph of a standardised pattern $\mathfrak{P}$ and let $\Delta(G)$ be the maximum degree of G. The entanglement depth of $\mathfrak{P}$ is either $\Delta(G)$ or $\Delta(G) + 1$.*

[7] Broadbent and Kashefi (2009) have shown that this is the case for standardisation with qubits. Essentially the same derivation will hold here.

[8] Corrections on the output do not actually need to be applied: either they can be absorbed into the next stage of a measurement pattern, or, if the QV is then measured, they can be absorbed into a re-interpretation of the result. The exception to this is if the output of a measurement pattern is to be input into something other than another measurement pattern, e.g., a quantum circuit.

The lemma of Broadbent and Kashefi (2009) is presented in the context of qubit measurement patterns, but as it only relates to the properties of the entanglement graph it is easily confirmed that it also applies here. To be clear, the degree of a node in a graph is the number of edges attached to the node, and the maximum degree of the graph is the maximum over all the nodes (e.g., a square 2D lattice has maximum degree 4, a linear chain has maximum degree 2).

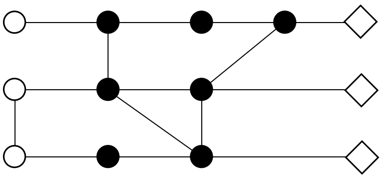


Figure 4.3: A standard measurement pattern may be represented in terms of a graph. The nodes represent QVs and the edges represent entangling operations between QVs. White circles represent input QVs, prepared in an arbitrary input state; black circles represent auxiliary QVs prepared in $|+_0\rangle$; diamonds represent output QVs, prepared in $|+_0\rangle$ and which are not measured. A phase function and any dependencies may be written by each node that represents a QV that is measured in the pattern (normally all non-output QVs) to completely define a standard pattern.

4.5 Quantum circuits and measurement patterns

Mappings in both directions between quantum circuits and measurement patterns are now provided (see Broadbent and Kashefi (2009) for similar work for the qubit sub-case). This will then be used to provide depth-preserving mappings between measurement patterns and unbounded fan-out circuits, extending a result of Browne et al. (2011) to the general quantum variable domain.

4.5.1 Measurement patterns simulating quantum circuits

Definition 4.2. *The standard measurement pattern simulation of a quantum circuit is obtained by*

1. *Rewriting the circuit as the composition of the single-gate circuits $\mathfrak{C}_{\mathrm{CZ}}$, $\mathfrak{C}_F$, $\mathfrak{C}_{R(\vartheta)}$ and $\mathfrak{C}_{Z(q)}$.*
2. *Replacing each basic circuit in the decomposition with the equivalent basic measurement patterns $\mathfrak{P}_{\mathrm{CZ}}$, $\mathfrak{P}_F$, $\mathfrak{P}_{R(\vartheta)}$ and $\mathfrak{P}_{Z(q)}$.*
3. *Completely standardising the resultant measurement pattern.*

It is noted that this procedure introduces additional auxiliary QVs. The number of additional auxiliary QVs required generically scales with the size of the quantum circuit.

Lemma 4.2. *Any standard quantum circuit $\mathfrak{C}$ may be implemented with a measurement pattern $\mathfrak{P}$ that has a depth of $O(depth(\mathfrak{C}))$ and a size of $O(size(\mathfrak{C}))$.*

Proof: Consider the standard measurement pattern implementation of the circuit, as given by Definition 4.2. Each basic measurement pattern replacing each basic gate is at most a small constant increase in size and depth. Hence, after (and before) standardisation, this pattern will have, at most, a constant increase in size and depth over the original quantum circuit.

This method of converting a quantum circuit into a measurement pattern is, in general, not optimal in terms of the depth of the pattern, and it will not always give constant depth patterns for Clifford circuits. Consider, for example, any circuit consisting of only CZ gates, in which case the measurement pattern will include no measurements and have an identical depth to the circuit. Hence, an alternative circuit-simulation procedure is now given which will produce constant depth patterns for Clifford circuits.

Definition 4.3. *The cluster-state measurement pattern simulation of a quantum circuit is found using an identical procedure to the standard measurement pattern except that, before conversion to a measurement pattern, four $\mathfrak{C}_F$ basic circuits are inserted between any $\mathfrak{C}_{\text{CZ}}$ gates that act consecutively on the same QV.*

This has no effect on the unitary implemented by the circuit (and hence the unitary implemented by the resultant measurement pattern) because $F^4 = \mathbb{I}$, and this procedure will increase the depth and size of the circuit, and hence the pattern, by less than a factor of four. However, it may be shown that now the entanglement graph of the pattern has nodes of at most degree three. This is important in proving the following proposition:

Proposition 4.1. *Any n-QV Clifford operator may be implemented with an $O(n^2)$ size and constant depth measurement pattern.*

Proof: Any n-QV Clifford gate may be decomposed into an $O(n^2)$ size circuit with no auxiliary QVs consisting of only F, $P(q)$, $Z(q)$ and CZ gates, using the efficient algorithm of Farinholt (2014) and Hostens et al. (2005).[9] Consider the cluster-state measurement pattern simulation of this circuit. This pattern still has a size of $O(n^2)$. Such a pattern has a constant depth for the entanglement operations (of at most 4) by Lemma 4.1, as its entanglement graph has a maximum degree of three. As the pattern is completely standard, and the measurement phase functions are only those for implementing F and $FP(p)$, all the measurements are independent

[9] The work of Hostens et al. (2005) and Farinholt (2014) is in the context of qudits, but can be easily applied to QCVs (which, in this context, are simpler than general dimension qudits as all non-zero elements of $\mathbb{R}$ are invertible).

and hence may all be implemented simultaneously. This therefore requires only unit depth. The corrections all apply to different QVs in the output and hence may be applied in a depth of 2. Hence, the measurement pattern has a total size of $O(n^2)$ and the depth is a constant (more specifically, the depth is 7 or less).

Lemma 4.3. *The n-QV fan-out gate can be implemented with an $O(n)$ size and constant depth measurement pattern.*

Proof: The n-QV fan-out gate is Clifford, as can be seen from its decomposition into n SUM gates in Figure 3.3. Hence, by Proposition 4.1, this may be implemented in constant depth. The $O(n)$ size scaling is because the SUM gate circuit for fan-out, as given in Figure 3.3, has a size of $O(n)$.

Lemma 4.4. *Any unbounded fan-out circuit $\mathfrak{F}$ may be implemented with a measurement pattern $\mathfrak{P}$ that has a depth of $O(depth(\mathfrak{F}))$ and a size of $O(size(\mathfrak{F}))$.*

This follows from Lemmas 4.2 and 4.3. The consequences of this are that the 1WQC has access to the parallel computation power of the unbounded fan-out model: this includes all of the results shown in Chapter 3. Furthermore, it is likely that general-QV unbounded fan-out circuits are substantially more powerful for parallel computation than shown in this thesis as there are a range of further known results in the qubit sub-case [Høyer and Špalek (2003, 2005); Moore and Nilsson (2001); Takahashi and Tani (2013); Takahashi et al. (2010)], as discussed briefly in the conclusions to Chapter 3. Hence, this provides a further motivation for future extensions to the studies of Chapter 3.

4.5.2 Circuit simulations of measurements patterns

It is now shown how a quantum circuit may simulate a measurement pattern. In the complete standardisation procedure, the Pauli corrections that are obtained have the general form $Z_j\left(q_j + \sum_i c_i m_i\right)$ and $X_j\left(q_j + \sum_i c_i m_i\right)$, where the sum is over the measurement outcomes of different QVs (the m_i), and where each measurement outcome may be added or subtracted to the other values (i.e., $c_i = \pm 1$), or may also have more general multiplicative factors, which come from dependencies removed from phase gates (see Equation 4.34). The $q_j \in \mathbb{S}_d$ parameters are obtained from any Pauli gates in the pattern implemented directly via corrections (see Equation 4.23). This is used in the following definition:

Definition 4.4. *The coherent circuit simulation of the measurement pattern $\mathfrak{P} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{p})$ is the circuit $\mathfrak{C} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{c}(\mathfrak{p}))$, where $\mathfrak{c}(\mathfrak{p})$ consists of an initial layer of F gates on all QVs in $\mathcal{V} \setminus \mathcal{I}$, followed by the operations of $\mathfrak{p}$ in order using the replacements*

1. $M_i^{\vartheta} \Rightarrow F_i R_i(\vartheta)$,

2. $X_j\left(q_j + \sum_{i\in\mathbb{M}_j} c_i m_i\right) \Rightarrow X_j(q_j)\prod_{i\in\mathbb{M}_j} \mathrm{C}_j^i X(c_i)$,

3. $Z_j\left(q_j + \sum_{i\in\mathbb{M}_j} c_i m_i\right) \Rightarrow Z_j(q_j)\prod_{i\in\mathbb{M}_j} \mathrm{C}_j^i Z(c_i)$.

Here, each $\mathbb{M}_j \subset \mathcal{V}$ is the set of measured QVs on which the correction on the j^{th} QV depends, and c_i is the value that the m_i outcome is multiplied by in that correction in the pattern (e.g., $c_i = \pm 1$ or c_i is a phase gate parameter).

No replacement rule is needed for entangling operations as the $E_{i,j}$ operation is simply the $\mathrm{C}_j^i Z$ gate. This procedure may be used to turn any measurement pattern into a quantum circuit by decomposing any dependent measurements into Pauli corrections followed by independent measurements. This quantum circuit implements the same operation as the measurement pattern by the principle of deferred measurement - a measurement can always be delayed until later and classical controls replaced with quantum control, see e.g., [Nielsen and Chuang (2010)].[10] This method for the coherent implementation of a measurement pattern explicitly highlights the intrinsic role of classical computation in the one-way model: Local gates controlled by *classically computed* CLV sums are replaced by a sequence of two-QV gates in which these sums are *quantum computed*. Hence, the power of the one-way model is in using classical computation instead of quantum computation when the quantum element is superfluous.

Proposition 4.2. *Any polynomial-size measurement pattern, $\mathfrak{P}$, may be implemented with an unbounded fan-out circuit that has a depth of $O(\mathrm{depth}(\mathfrak{P}))$ and a size of $O(\mathrm{size}(\mathfrak{P})^2\mathrm{depth}(\mathfrak{P}))$.*

Proof: Without lose of generality, consider a completely standard pattern $\mathfrak{P}$. The operation sequence of $\mathfrak{P}$ consists of three sequential stages: I. Entanglement operations; II. A sequence of measurements that may each be either X-type error dependent ($[M_i^{\vartheta}]^s$ operations) or independent (M_i^{ϑ} operations); III. Pauli corrections on the output QVs. Consider the coherent circuit implementation of $\mathfrak{P}$, as given by Definition 4.4. The preliminary stage of this circuit consists of F gates on the QVs in the non-input set $\mathcal{V} \setminus \mathcal{I}$. This may be implemented by an unbounded fan-out circuit that has unit depth and a size no greater than size($\mathfrak{P}$). Consider stage I: This consists of CZ gates and, as these are the same operations as in the measurement pattern, this requires a quantum circuit of no greater depth or size than the entangling stage of the measurement pattern. Consider stage II: This circuit subsection consists of no more than depth($\mathfrak{P}$) layers each of which consists of

[10] Moreover, here there is no need to perform the delayed measurements. This is because, the auxiliary QVs in the circuit which would have been measured in the measurement pattern, will each just be in the state $|+_0\rangle$ at the end of the circuit.

first a $CX(q)$ and $X(q)$ gate circuit, acting on at most size($\mathfrak{P}$) QVs (and obtained from the X-type corrections, which come from expanding the X-type error dependent measurements into corrections and independent measurements), followed by some local F and $R(\vartheta)$ gates on these QVs, which all act on distinct QVs (and are obtained from the independent measurements). This polynomial-size circuit acting on size($\mathfrak{P}$) QVs and consisting of only controlled and local $X(q)$ gates may be implemented with an unbounded fan-out circuit of size $O(\text{size}(\mathfrak{P})^2)$ and depth of $O(1)$, by Proposition 3.4. The following local F and $R(\vartheta)$ gates may be implemented with unit depth. As there are at most depth($\mathfrak{P}$) such layers, this results in a total size for this stage of the circuit of $O(\text{size}(\mathfrak{P})^2\text{depth}(\mathfrak{P}))$ and a depth of $O(\text{depth}(\mathfrak{P}))$. Consider stage III: This is a polynomial-size circuit consisting of only $CX(q)$, $X(q)$, $CZ(q)$ and $Z(q)$ gates, which acts on at most size($\mathfrak{P}$) QVs. By Proposition 3.4, this may also be implemented by an unbounded fan-out circuit with a size of $O(\text{size}(\mathfrak{P})^2)$ and depth of $O(1)$. Hence, the unbounded fan-out circuit simulation of $\mathfrak{P}$ has a size of $O(\text{size}(\mathfrak{P})^2\text{depth}(\mathfrak{P}))$ and a depth of $O(\text{depth}(\mathfrak{P}))$.

This proposition, in combination with Proposition 4.1, proves the claim in Chapter 3 that unbounded fan-out circuits can implement any Clifford gate in constant depth, which was stated in Proposition 3.5. As a slightly technical aside, note that, for QCVs, if the basic gate set in the quantum circuits is restricted to only include $Z(q)$ and $P(q)$ gates with $q \in [0, 1]$, which it was suggested in Section 3.5 might be necessary from a physically perspective, then this proposition must be slightly adapted. In particular, consider a measurement pattern that has a polynomial size and only contains measurements that implement $P(q)$ gates with polynomially large q and 'gate-like' Pauli corrections $Z(q)$ (i.e., those $Z(q)$ 'corrections' which are not corrections as such, but have been inserted to implement a $Z(q)$ gate, and hence q is a constant rather than a measurement outcome) also with only polynomially large q. A QCV unbounded fan-out circuit that uses this more restricted gate set can be found that simulates such a measurement pattern and which has the same depth as the measurement pattern and a polynomial size.

4.6 Depth complexity classes

Quantum and classical circuits are both *non-uniform* models of computation. What is meant by this is that for an n-variable input problem there is a different circuit, and hence a different computational device, for each size of n. When we consider a circuit to implement the unitary U_n, defined for arbitrary $n \in \mathbb{N}$, e.g., n-QV FANOUT, what is really meant by this is that we are considering a *family* of circuits $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3, \dots$, where circuit $\mathfrak{C}_n$ computes U_n for input size n. Therefore, it is possible for completely unrelated circuits to be picked for each value of n, and this can allow for powerful computational properties to be hidden in the circuit description [Goldreich (2008)]. Hence, it is often useful to consider *uniform* families of circuits, which are those circuit families which, for each n, the associated circuit can be found efficiently using a Turing machine.[11] This technical restriction to uniformly generated circuits (and measurement patterns) is used below.

A concise way in which to summarise the results of both this and the previous chapter is in terms of complexity classes. For quantum circuits with *qubits*, the complexity class QNC^k of operators (or alternatively decision problems) that may be computed by poly-logarithmic depth ($O(\log^k n)$) standard quantum circuits was first introduced by Moore and Nilsson (2001), as the quantum analog of the equivalent classical circuit class NC^k. Extensions of this complexity class for qubit unbounded fan-out circuits, denoted QNC^k_f, and measurement patterns, denoted QMNC^k, have also been defined [Browne et al. (2011); Høyer and Špalek (2003)]. I now further extend these classes to general QVs.

Definition 4.5. *The complexity classes* QNC^k_d*,* $\mathrm{QNC}^k_{f,d}$ *and* QMNC^k_d *contain operators computed exactly by uniform families of standard quantum circuits, unbounded fan-out circuits and measurement patterns, respectively, which have input size* n*, a depth of* $O(\log^k n)$*, and polynomial size.*

Naturally, the class of operators depends on the QV type, which the subscript d in the complexity class notation is used to denote, and the qubit case recovers the previously defined and studied classes.[12] Note that the classes depend to some degree on the universal gate set available, and it may be assumed that each model has the relevant basic set built from $\mathcal{G}_{\epsilon-\textsc{uni}}$ in each case, as has been largely the case throughout (i.e., the standard circuit model has this exact gate set, the unbounded fan-out model has this set along with FANOUT, and the allowed measurements in the 1WQC are those to implement $\mathcal{G}_{\epsilon-\textsc{uni}}$).

The relationship between unbounded fan-out circuits and measurement patterns, that I have proven in Lemma 4.4 and Proposition 4.2, can be summarised by

$$\mathrm{QNC}^k_{f,d} = \mathrm{QMNC}^k_d, \tag{4.51}$$

which holds for all k. This is an extension of a theorem of Browne et al. (2011) to general QVs. Proposition 3.1 then implies the complexity class inclusion

$$\mathrm{QNC}^0_d \subset \mathrm{QNC}^0_{f,d} = \mathrm{QMNC}^0_d \subseteq \mathrm{QNC}^1_d, \tag{4.52}$$

[11] The classical computation required to find the circuit may be restricted in size and depth: e.g., a poly-logarithmic time and space Turing machine.

[12] Sometimes these complexity classes are instead defined in terms of decision problems, e.g., in Browne et al. (2011). However, in much of the literature the classes are defined to contain unitary operators (as here), e.g., see Moore and Nilsson (2001).

which summarises the difference in depth complexity between standard quantum circuits and unbounded fan-out circuits: unbounded fan-out gates cannot be computed in constant depth with a standard quantum circuit, but can be computed in $\log(n)$ depth. For all k, Equation 4.51 and Proposition 3.1 also imply that

$$\mathrm{QNC}_d^k \subseteq \mathrm{QNC}_{f,d}^k = \mathrm{QMNC}_d^k \subseteq \mathrm{QNC}_d^{k+1}. \tag{4.53}$$

However, except for $k = 0$, none of these inclusions have been shown to be strict.[13] This mirrors the situation for the qubit sub-case [Browne et al. (2011)].

4.7 Measurement patterns have optimal depth

I now shown that there are a large range of quantum computational models which cannot have a lower depth complexity than measurement patterns. This will be useful for understanding the computational model introduced in Chapter 6.

Proposition 4.3. *Consider a quantum model $\mathfrak{M} = (\mathfrak{o}, \mathfrak{s})$ in which the set of allowed operations $\mathfrak{o}$ consists only of*

1. *Unitary operators in QMNC_d^0,*
2. *Destructive measurements of Hermitian operators, $\hat{O}$, that act on any number of QVs and which have outcomes in $\mathbb{S}_d$, such that $U\hat{O}U^\dagger$ is diagonal in the conjugate basis for some $U \in \mathrm{QMNC}_d^0$,*
3. *Unitary operators $u(n) \in \mathrm{QMNC}_d^0$ with $n \in \mathbb{S}_d$, where n is the value of a CLV calculated from arithmetic in $\mathbb{S}_d$ on previous measurement outcomes and constants in $\mathbb{S}_d$,*

and where the set of preparable states for the non-input QVs, $\mathfrak{s}$, is such that

4. *For each $|\psi\rangle \in \mathfrak{s}$, $|\psi\rangle = U|+_0\rangle$ for some $U \in \mathrm{QMNC}_d^0$.*

For any computation $\mathfrak{Q}$ in $\mathfrak{M}$, there exists a measurement pattern $\mathfrak{P}$ that simulates $\mathfrak{Q}$ in a depth of $O(\mathrm{depth}(\mathfrak{Q}))$.

Proof: The preparation of all non-input QVs in states from $\mathfrak{s}$ can be achieved with initial measurement patterns of constant depth from QVs prepared in $|+_0\rangle$, by condition 4 of the proposition. $\mathfrak{Q}$ may be decomposed into $\mathrm{depth}(\mathfrak{Q})$ sub-computations, each of unit depth. In each sub-computation there is at most one operation on each QV. The unitaries in this layer that are not classically controlled may be implemented with constant depth measurement patterns, due to condition 1.

[13] For $k \neq 0$, showing that these inclusions are strict, or conversely that they are actually equalities, is likely to be very difficult.

Each (in general, many-QV) measurement in the layer may be simulated by first applying the unitary that diagonalises the measurement in the conjugate basis, which may be done with a constant depth measurement pattern by condition 2, and then implementing $M_i^{\vartheta_0}$ operations (which are conjugate basis measurements) on each QV that the measurement acts on. The appropriate measurement outcome of $\hat{O}$, associated with the projection onto the resultant conjugate basis state of the QV(s), can then be calculated from the individual measurement outcome(s). Note that, although this is in general different to a measurement of $\hat{O}$ (as $\hat{O}$ has outcomes in $\mathbb{S}_d$ rather than $\mathbb{S}_d^k$ where k is the number of measured QVs), as the measured QVs are discarded (the measurement is destructive) these procedures are identical under the assumption that only the CLV calculated from the individual measurement outcomes is retained. As the procedure for each measurement in the layer is of constant depth, and all the measurements in the layer must act on distinct QVs, the measurements may be implemented by a constant depth measurement pattern.

The classically controlled unitaries may implemented with a constant depth measurement pattern, as they all act on distinct QVs and, by condition 3, all of these unitaries may be implemented in constant depth measurement patterns, regardless of the CLV input. Furthermore, the CLV on which they depend may be calculated with the classical computations that have been assumed to be available to the 1WQC: arithmetic in $\mathbb{S}_d$. Therefore, each component in a layer of $\mathfrak{Q}$ may be implemented with a constant depth measurement pattern and, as each operation in the layer acts on distinct QVs (and may only depend on outcomes from previous layers), the composite measurement pattern for the entire layer has constant depth. Hence, the total pattern simulating $\mathfrak{Q}$ has a depth of $O(\text{depth}(\mathfrak{Q}))$, which concludes the proof.

This proposition is similar to one proven for qubits by Browne et al. (2011) (see Theorem 4 therein). Any model using only Clifford operators, single-QV measurements, Pauli corrections and preparation in states preparable by Clifford circuits from the computational basis satisfies the constraints of this proposition. This will therefore cover the model introduced in Chapter 6.

4.8 Quantum resources for classical computation

The considerations so far in this chapter have largely overlooked the classical side-processing required to implement the 1WQC. There is good physical justification for this, given that simple classical computations can be considered to be essentially free in comparison to the difficulties inherent in implementing quantum operations. This may not always be entirely true: if the time required to implement any classical calculations between quantum layers results in any significant wait time this may have some implications. However, this would depend on the particular measurement and coherence times in any physical device and there are many other layers of classical controls in an experiment which would also need to be considered in such an analysis.

4.8.1 Classical processing introduced via complete standardisation

In order to obtain an understanding of both the 1WQC and quantum computation more generally, it is interesting to consider what *classical* resources are required in addition to measurements of an entangled state, to obtain deterministic and universal quantum computation. This may be understood by considering the classical computations introduced via complete standardisation, as is done below. Here, and particular in Section 4.8.2, it will be helpful to distinguish between ordinary arithmetic (i.e., arithmetic on $\mathbb{R}$) and the arithmetic defined on the ring $\mathbb{S}_d$. This is achieved by denoting addition, subtraction and multiplication in $\mathbb{S}_d$ by $\oplus$, $\ominus$ and $\otimes$ respectively.

The standardisation procedure on a measurement pattern requires $\oplus$ addition of measurement outcomes and constants, for all QV types, as implied by Equation 4.30. Standardisation is sufficient to turn any measurement pattern into one consisting of measurements on an entangled state, and hence, addition of measurement outcomes is all that is necessary for deterministic universal quantum computation in this fashion. However, the removal of any unnecessary dependencies, via Pauli simplification and signal shifting, adds further classical computations: Pauli simplification in general uses both $\oplus$ and $\otimes$ operations on measurement outcomes, due to the phase gate relation given in Equation 4.34, and signal shifting uses the $\ominus$ operation, as seen in Equation 4.38.

For qudits, the variable $p \in \mathbb{S}_d$ parameterised phase gates are not actually required (CZ, F, P and Z generate the Clifford group), and if the parameter p is set to unity in Equation 4.34, then no multiplication of measurement outcomes by constants is needed. Furthermore, modulo subtraction can be obtained from $d-1$ applications of modulo addition. Hence, for qudits the classical control computer for the 1WQC requires only the SUM gate, or with irreversible logic it may use the gate

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

demonstrated here for $d = 4$. For bits, this is known as XOR (exclusive or). The classical computer that uses only SUM gates, I will refer to as a SUM computer, and for bits this is known as the *parity computer* [Aaronson and Gottesman (2004)]. In contrast to qudits, with QCVs the continuously parameterised $P(p)$ gate is necessary to generate the Clifford group and subtraction cannot be obtained via addition. Hence, in this case, if 1WQC is to be implemented without unnecessary dependencies then addition, subtraction and multiplication in $\mathbb{R}$ are all required to be available to the classical control computer.[14]

Interestingly, for all QV types, it appears that the full power of classical computation is not required for controlling the 1WQC: it is well known that XOR is not a universal gate for Boolean logic [Pelletier and Martin (1990)], and similar considerations apply to the modulo addition gate for d-valued logic.[15] For example, modulo addition cannot be used to implement the modulo multiplication gate

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

again demonstrated for $d = 4$ and known as AND for bits. Similarly, although the control classical computer for the QCV 1WQC requires addition, subtraction and multiplication, this is *not* sufficient for universal classical analog computation: such a device requires access to some further operations, with universality achievable via the inclusion of an integrator and a constant function in the basic operations set [Bournez et al. (2006)]. Note that here I mean analog computation in the sense of Claude Shannon's general-purpose analog computer based on differential analysers.

4.8.2 GHZ states as a resource for a classical processor

An intriguing way to look at 1WQC is in terms of a quantum resource (a cluster state) giving a very limited classical computer access to the power to solve problems presumed to be intractable with any classical machine. Extending this idea, Anders and Browne (2009) considered if there are more limited quantum resources that can increase the power of the parity computer and they showed that access to single-qubit measurements on three-qubit GHZ states allows the calculation of the AND gate with the parity computer, which along with XOR is universal for Boolean logic

[14] Note that exact real-valued arithmetic is not required - it is only of any benefit to calculate the values to the precision that the quantum operations can be performed.

[15] XOR is not functionally complete as its truth table contains the same number of 0's as 1's. Hence it can only implement Boolean functions $f : \{0,1\}^n \to \{0,1\}$ which output 1 for half of the input strings and 0 for the other half (even when using auxiliary fixed 0 and 1 bits). Similarly, the $\oplus$ logic gate for general d can only implement functions $f : \mathbb{Z}(d)^n \to \mathbb{Z}(d)$ which give each value in $\mathbb{Z}(d)$ for a fraction of 1/d of the possible inputs.

[Pelletier and Martin (1990)]. I now briefly show how this idea can be extended to qudits of any *even dimension*, and hopefully in doing so shed some light on the binary special case. Interestingly, it would not be expected that this can be extended to also include odd dimension qudits as it is known that there is a local hidden variable model for odd-dimension qudit Stabilizer quantum mechanics [Gross (2006)]. In the following, it will be necessary to use the equality[16]

$$\frac{1}{d}\sum_{r\in\mathbb{Z}(d)}\omega^{r(q+q')}=\delta(q\oplus q'). \tag{4.54}$$

Given two classical dits a, b, the SUM computer may compute $a\oplus b$ using a single SUM gate. Take the 3-qudit GHZ state

$$|\text{GHZ}\rangle=\frac{1}{\sqrt{d}}\sum_{q\in\mathbb{Z}(d)}|q,q,q\rangle. \tag{4.55}$$

Now, consider performing a measurement on the qudits in this state of the operators $\hat{x}_{FP(a)}$, $\hat{x}_{FP(b)}$ and $\hat{x}_{FP^{\dagger}(a\oplus b)}$, noting that the measurements to be performed can be controlled by this restricted-power SUM computer. This is equivalent to applying the operator $FP(a)\otimes FP(b)\otimes FP^{\dagger}(a\oplus b)$, followed by a computational basis measurement. Hence, the measurement outcome triplet $(m,n,p)\in\mathbb{Z}(d)^3$ is obtained with the probability

$$\begin{aligned}\text{Prob}(m,n,p)&=\left|\frac{1}{\sqrt{d}}\sum_{q\in\mathbb{Z}(d)}\omega^{q^2(a+b-a\oplus b)/2}\langle m,n,p|+_q,+_q,+_q\rangle\right|^2, &(4.56)\\ &=\left|\frac{1}{d^2}\sum_{q\in\mathbb{Z}(d)}\omega^{q^2(a+b-a\oplus b)/2+q(m+n+p)}\right|^2, &(4.57)\end{aligned}$$

where $\langle q|+_{q'}\rangle=\omega^{qq'}/\sqrt{d}$ has been used. Now consider the case when $a+b<d$, which implies that $a+b-(a\oplus b)=0$. Hence, using Equation 4.54, it follows that

$$\text{Prob}(m,n,p|a+b<d)=\left|\frac{1}{d^2}\sum_{q\in\mathbb{Z}(d)}\omega^{q(m+n+p)}\right|^2=\frac{1}{d^2}\delta(m\oplus n\oplus p). \tag{4.58}$$

That is, the probability is only non-zero if $m\oplus n\oplus p=0$. In other words, each possible outcome $q\in\mathbb{Z}(d)$ is equally likely for each measurement but they must all add up to zero modulo d.

Consider now the remaining cases not covered above, which are when $a+b\geq d$.

[16] This may be proven using the formula for a geometric series: see Appendix D, where this formula is also stated and a brief proof is given (for all QV types).

It then follows that $a + b - a \oplus b = d$. Now in this case

$$\omega^{q^2(a+b-a\oplus b)/2} = e^{i\pi q^2} = (-1)^{q^2} = (-1)^q = \omega^{qd/2}, \tag{4.59}$$

as the square of an odd (even) number is odd (even). Therefore, using this equality and Equation 4.54, it follows that

$$\text{Prob}(m,n,p|a+b \geq d) = \left| \frac{1}{d^2} \sum_{q \in \mathbb{Z}(d)} \omega^{q(m+n+p+d/2)} \right|^2 = \frac{1}{d^2} \delta(m \oplus n \oplus p \oplus d/2), \tag{4.60}$$

noting that this is well-defined because, as d is even, $d/2$ is an integer. Therefore, again, any outcome for each measurement is equally likely in isolation, however, now they must obey $m \oplus n \oplus p = d/2$ (as then $m \oplus n \oplus p \oplus d/2 = 0$).

The consequence of this is that by first calculating $a \oplus b$, then performing this measurement procedure and finally using further SUM gates to calculate the modulo sum of these measurement outcomes, a SUM computer with access to GHZ states can calculate the function

$$\text{THRESHOLD}(a,b) = \begin{cases} 0 & \text{if } a+b < d, \\ d/2 & \text{if } a+b \geq d. \end{cases} \tag{4.61}$$

Alternatively, it may be written as a truth table, for example, with $d = 4$ it has the form

THRESHOLD	0	1	2	3
0	0	0	0	0
1	0	0	0	2
2	0	0	2	2
3	0	2	2	2

The binary special case (bits and three-qubit GHZ) reproduces the result of Anders and Browne (2009), up to minor differences.[17] In the binary case, this technique has provided the parity computer with the ability to implement the AND function. As AND and XOR can together implement any Boolean function, this GHZ state resource has elevated the parity computer to universal classical computation.

More generally, for computation with dits of even dimension $d > 2$, it is not obvious what significance the THRESHOLD gate has as an additional resource for a SUM computer beyond the observation that it is indeed an additional resource as it cannot be constructed from $\oplus$. One issue with dealing with higher-base logics is that the number of different two-input irreversible gates is d^{d^2} (this is the number

[17] In Anders and Browne (2009) the measurements are of Pauli operators. Note that the qubit Y Pauli operator is given by $Y = PFX$.

of unique truth tables), and while for bits this is only $2^4 = 16$, for d only as large as 4 this is $4^{16} = 4,294,967,296$. However, the point stands that, with dits of even dimension, a quantum 3-qudit GHZ resource state can provide further power to a classical SUM computer. As an aside, the complexity class of problems that can be efficiently solved by the parity computer is what is known as Parity-L or $\oplus$L [Aaronson and Gottesman (2004)]. I suspect that the relevant class for the SUM computer is Mod$_d$L, defined as the set of decision problems solvable by a log-space Turing machine such that the number of accepting paths is divisible by d if and only if the answer is 'no'.[18] However, my limited knowledge of Turing machines prevents me from claiming this with any certainty. It is only a conjecture that $\oplus$L and Mod$_d$L are strict subsets of the full class of classically efficiently solvable decision problems P. Finally, I wish to emphasise that I am not suggesting that GHZ resources are useful in practice for implementing classical computation - the ideas here are merely observations on the nature of entangled quantum resources in computation.

4.9 Physical implementation

Entanglement generation is often simpler to achieve in practice than the application of on-demand unitary gates, and this is one of the main reasons why the 1WQC has such great potential for a physical realisation of universal quantum computation. In this final section before concluding the chapter, the experimental progress and the prospects for 1WQC are briefly discussed.

There have been a range of physical systems proposed for implementing 1WQC with qubits, and to date the most well-developed experiments are with ion-trap and optical technologies [Bell et al. (2014); Chen et al. (2007); Lanyon et al. (2013); Tame et al. (2014)]. Specifically, Lanyon et al. (2013) have implemented a universal set of operations on up to seven entangled ion-trap qubits, and Bell et al. (2014); Tame et al. (2014) have entangled and performed computations on up to five qubits encoded into photons, with Chen et al. (2007) presenting a alternative technique whereby 1WQC was performed on four logic qubits encoded over two photons. Furthermore, there have been a variety of proposals for creating the many-qubit resource states that are required for a useful 1WQC, for example, such states may be realised as the ground state of certain many-body Hamiltonians [Bartlett and Rudolph (2006); Brennen and Miyake (2008); Chen et al. (2009)]. However, as of yet no such large-scale states have been realised that allow for individual qubit addressability, which is a requirement for computation.

In this regard, 1WQC with QCVs is an especially promising paradigm, as demonstrated by the spectacular recent experiments of Yokoyama et al. (2013) who have

[18] For a more detailed definition, see the complexity zoo at https://complexityzoo.uwaterloo.ca.

entangled 10,000 individually addressable QCVs encoded into finite-length wave packets in two light beams. Complementing this is the alternative technique of Chen et al. (2014) who have created resources states of 60 QCVs, realised as different modes of an optical frequency comb, and where all the encoded QCVs are simultaneously accessible. To implement 1WQC, measurement techniques are required that implement a universal gate set. In order to implement any Clifford gate - called a *Gaussian transformation* in this context - it is only necessary to employ homodyne detection, which is a measurement of the operator $\hat{x}\sin\theta + \hat{p}\cos\theta$ for some θ.[19] This has been experimentally demonstrated by Ukai et al. (2011) and Su et al. (2013), who have implemented one and two-mode Gaussian transformations, using four and six QCV entangled states, respectively. However, this is not sufficient for universal quantum computation and the difficulty in extending this to a universal set of operations is that this requires a non-linear optical element of some sort. The cubic phase gate, as introduced in Equation 2.60, is sufficient to obtain universality and one method for approximately implementing this gate is via photon-number counting and some additional Gaussian resources [Gottesman et al. (2001); Gu et al. (2009)]. Moreover, recent experimental improvements in photon-number-resolving detectors suggest that this may well be feasible [Calkins et al. (2013); Humphreys et al. (2015)].

The 1WQC with qudits of dimension $d > 2$ has seen only limited attention in the literature to date, but it has been noted that (as with qubits) suitable resource states can be obtained as the ground states of many-body Hamiltonians for spin $(d-1)/2$ particles [Zhou et al. (2003)] and a method has been suggested for creating $d = 4$ photonic cluster states [Joo et al. (2007)]. Although, to my knowledge, there have been no experiments directly implementing a proof-of-principle qudit-based 1WQC, there have been a range of experiments that have shown impressive control and high quality measurements of qudits in a variety of systems. In particular, qudits have been encoded into photonic degrees of freedom [Bent et al. (2015); Lima et al. (2011); Walborn et al. (2006)] and multiple photonic qudits have been entangled [Dada et al. (2011); Rossi et al. (2009)]. Particularly interesting is the experiment of Dada et al. (2011) in which they generate entanglement between $d = 12$ qudits encoded into the orbital angular momentum of the photons. Given that there is no fundamental limit on the dimensionality of the qudit that may be encoded into this degree of freedom, and a range of high-quality measurements have been demonstrated on orbital angular momentum encoded qudits [Bent et al. (2015)], systems of this sort

[19] By reference to Section 4.3, it follows that the measurement to implement F for a QCV is simply $-\hat{p}$. To implement $FP(q)$ the measurement required is then $-P(-q)\hat{p}P(q) = -\hat{p} - q\hat{x} = -(\hat{p}\cos\theta + \hat{x}\sin\theta)/\cos\theta$ where $\theta = \tan^{-1}(q)$. Hence, to implement the phase gate a homodyne measurement may be performed along with a rescaling of the measurement output [Menicucci et al. (2006)].

may have the potential for future progress on 1WQC with qudits.

Outside the optical regime, a particular promising experiment is that of Anderson et al. (2015); Smith et al. (2013) who have reported high-quality control and measurement of a $d = 16$ qudit encoded into the hyperfine structure of the electronic ground state in the Caesium isotope ^{133}Cs. Note that, although many atom-based experiments use fundamentally binary measurements (e.g., via pumping only one basis-state-encoding level to a photon-emitting state and detecting any emitted photons), such measurements can be used to simulate a d-outcome measurement via multiple binary measurements in conjunction with permuting the different basis states in between these measurements. Furthermore, varied basis measurements may always be simulated via local unitary controls along with a fixed d-outcome measurement.

One potential problem with QCV 1WQC is that it cannot be implemented perfectly even in principle: it requires the realisation of conjugate basis states which are not normalisable and are unphysical. In practice they are realised by finitely squeezed vacuum states (see Appendix B for the formal relation) and until recently it had not been shown that this did not cause uncorrectable errors in the computation. However, Menicucci (2014) showed that by encoding a logical qubit into each QCV, using the scheme of Gottesman, Kitaev and Preskill (GKP) [Gottesman et al. (2001)], these errors due to finite squeezing can be corrected for. Because of the universality of QCV 1WQC, it is immediately implied that universal computation can be implemented on the encoded qubit. Furthermore, due to the nature of the encoding, the qubit-encoded Clifford operators can be implemented via only QCV Clifford operators [Menicucci (2014)]. Interestingly, the GKP encoding scheme could also be used to embed qudits into each QCV and hence this may provide a promising route for an optical implementation of qudit 1WQC. A more detailed investigation of this idea, including looking into whether this qudit encoding can be made fault-tolerant using the same ideas employed by Menicucci (2014), would be an interesting future avenue of research.

4.10 Conclusions

In this chapter, the computational power of the one-way quantum computer with arbitrary QV type has been investigated. To do this I have introduced a general ‘measurement pattern’ formulation of the 1WQC, which extends the cluster state paradigm [Menicucci et al. (2006); Zhou et al. (2003)] to a more flexible setting that is well-suited to a comparison with the gate model. Depth reduction ‘standardisation’ protocols were then developed, following the qubit-based work of Danos et al. (2007), and using this a simple procedure for mapping between quantum circuits and measurement patterns was provided. The implication of these mappings is that the depth complexity of the 1WQC is exactly equivalent to that of the unbounded fan-out model investigated in Chapter 3. This confirms and makes precise the parallelism inherent in 1WQC and extends a qubit-based result of Browne et al. (2011) to the setting of more general QVs. Possible future work could investigate how the full range of highly-developed concepts in the qubit 1WQC, e.g., information flow notions [Browne et al. (2007); Duncan and Perdrix (2010)], may be extended to the general QV setting. It would also be interesting to continue the investigations into the interplay between classical and quantum resources in higher-dimensional 1WQC which was briefly touched upon in Section 4.8.

Chapter 5

Geometric phase gates for general quantum variables

In this chapter *geometric phase gates* for general quantum variables are proposed and investigated. These gates employ an ancilla to entangle QVs in a computational register via a sequence of register-QV controlled Pauli operators on the ancilla. The construction given will be applicable both when the computational elements and ancillas are QVs of the same and of different types. This will include elements of what is known as *qubus* computation [Spiller et al. (2006)] as a special case, given when the register consists of qubits and the ancillas are QCVs, but is applicable in a broader setting. The computational advantages associated with having access to ancillas of a different dimension to the computational QVs are investigated. In particular, this will include a proposal for a practical and highly efficient method for implementing generalised Toffoli gates and also a comment showing that a previous method proposed for implementing the quantum Fourier transform via a QCV ancilla [Brown et al. (2011)] is infeasible. Finally, the physical relevance of these gate methods is discussed. This chapter is partially based on Proctor et al. (2015).

5.1 Introduction

The elements of the computational register in a quantum-circuit-model computer need to be well-isolated in order to minimise the destructive effects of decoherence. On the other hand, it is also essential to implement two-body entangling gates to perform any computation. The tension between these demands is one motivation for sidestepping direct interactions and instead mediating entangling gates via an ancillary system. This allows the register to be specifically tailored for long coherence times, and interactions are only required with some physically distinct ancillary systems. These ancillas may be chosen to optimise the interactions with the elements of the main register and moreover, as the quantum information is stored in the main register, the coherence time of these ancillary systems is not as critical as for the computational systems. Hence, they may exhibit complementary properties to the register systems, such as being comparatively easy to manipulate. Indeed, ancillas are used in a range of experiments, such as superconducting flux qubits coupled via transmission line resonators [Majer et al. (2007); Stern et al. (2014); Wang et al. (2009); Xue (2012)], spin qubits coupled via ancillary photonic qubits [Carter et al. (2013); Luxmoore et al. (2013); Yamamoto et al. (2009)] or nuclear spins coupled to electron spins [Taminiau et al. (2014, 2012)].

In light of this, it is of both practical and theoretical interest to study the effect of incorporating the ancillary system into the computational model, hence to date there has been a range of literature on this subject: for a selection see Anders et al. (2010); Halil-Shah and Oi (2014); Ionicioiu et al. (2008); Spiller et al. (2006). There is no obvious physical reason why the ancillary system should be the same type of QV as the computational elements in the register. For example, photons couple to a range of systems and hence they are a natural candidate as an ancillary system and they can be employed as either qubits (e.g., via a polarisation encoding), qudits (e.g., using the number states as a basis) or QCVs (using the quadratures eigenstates as a basis). Furthermore, as has been argued in Section 1.3.2, it also seems pertinent to avoid assuming that the computational elements in a quantum computer will necessarily be qubits. Therefore, it is preferable to develop schemes relevant to the full range of encodings whenever possible. In the remainder of this thesis I propose and investigate a variety of methods for implementing quantum computation via interaction-mediating ancillary systems, with much of the work applicable to all types of QVs. In this chapter, I propose what will be called *geometric phase gates* for general quantum variables, with this terminology due to their relationship to closed phase-space paths. Interestingly, many of the methods encountered later in this thesis can be understood as adaptations of this gate.

The remainder of this chapter is arranged as follows: In the Section 5.2 the basic gate is introduced. Although (to my knowledge) this is novel in all other cases, for a qubit register and QCV ancilla this gate has been previously proposed [Milburn (1999)] and investigated in detail, see e.g., Spiller et al. (2006). In this qubit-QCV setting, there have been a range of interesting results showing that this basic gate can be adapted for low gate-count implementations of certain qubit-based circuits [Brown et al. (2011); Louis et al. (2007)]. Hence, in Section 5.3 efficient gate decompositions using the more general geometric phase gate proposed herein are investigated. This will include a proposal for an efficient implementation of generalised Toffoli gates (on qubits) via qudit ancillas. In Section 5.4 I outline the links between geometric phase gates and *hybrid quantum computation* - in which quantum

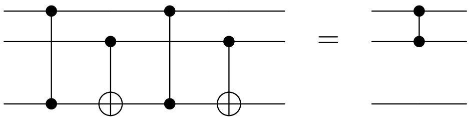


Figure 5.1: Two qubits may be entangled without any direct interactions via CZ and CNOT gates acting on a target ancillary qubit.

computation is implemented on more than one type of QV simultaneously. Finally, the possibilities for physical implementations of the gate methods proposed in this chapter are discussed in Section 5.5 and the chapter then concludes in Section 5.6.

5.2 The geometric phase gate

To begin the geometric phase gate is illustrated in the simplest case: mediating a gate between two computational qubits via a third ancillary qubit. Consider the gate sequence shown in the LHS circuit of Figure 5.1, which consists of CNOT and CZ gates. If the two computational qubits are in the states $|q\rangle$ and $|q'\rangle$ respectively, then the operator applied to the ancilla is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{q'} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{q} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{q'} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{q} = (-1)^{qq'} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \tag{5.1}$$

Hence, it has no net effect (i.e., an identity) on the ancilla, but, regardless of the ancilla state, it creates a -1 phase factor on the composite system if $q = q' = 1$. This is exactly the action of CZ on the two register qubits (for qubits, $\textsc{cz}|q\rangle|q'\rangle = (-1)^{qq'}|q\rangle|q'\rangle$), as denoted by the RHS circuit of Figure 5.1. Therefore, by interacting each qubit with an ancillary qubit twice, an entangling gate between the two register qubits has been mediated.[1]

Before introducing this gate in the more general case it is necessary to take a diversion to discuss what may be termed *hybrid* controlled Pauli gates. Up to this point in this thesis two-QV gates have always acted on two QVs of the same type: either two qudits of the same dimension or two QCVs. In this chapter the ancilla will not generally be assumed to be of the same type as the computational QVs it is used to mediate gates between. Therefore, it is necessary to use two-QV gates which act on systems that may be of different types. A general control gate Cu, as

[1] Given the simplicity of this relation it seems likely that this has been noted somewhere in the literature (prior to its discussion in Proctor et al. (2015)).

defined first in Equation 2.33, has the action

$$\mathrm{C}u(|q\rangle \otimes |q'\rangle) = |q\rangle \otimes u^q|q'\rangle, \tag{5.2}$$

and this is still valid for control and target QVs of different types - it is only necessary for u to be a unitary that acts upon the target QV type. In this chapter, the interactions that will be largely considered are the (hybrid-QV) controlled Pauli operators, $\mathrm{C}Z(p)$ and $\mathrm{C}X(p)$. Consider the action of $\mathrm{C}X(p)$:

$$\mathrm{C}X(p)\left(|q\rangle \otimes |q'\rangle\right) = |q\rangle \otimes X(p)^q|q'\rangle. \tag{5.3}$$

Now, this is perfectly well-defined for all combinations of QV types. However, the gate enacted on the target system is only a Pauli gate if

$$X(p)^q = X(qp), \tag{5.4}$$

for all $q \in \mathbb{S}_d$, where $\mathbb{S}_d$ is the relevant set for the control system, and clearly the same considerations apply to $\mathrm{C}Z(p)$. This equation holds for all combinations of QVs except if the control system is a QCV and the target system is not. In this case, q takes all values in $\mathbb{R}$, and a continuous power of a qudit Pauli operator is not a Pauli operator (see Equation 2.20). Hence, in the remainder of this chapter all cases are considered *except* a register of QCVs mediated via ancillary qudits. In order to keep the presentation as simple as possible, this will not be explicitly accounted for in the formulas and it should be assumed that the relations given will *not* hold in this particular case.

The qubit-mediated gate of Equation 5.1 is possible only because the qubit Pauli operators commute up to a phase (of -1) and $X^2 = Z^2 = \mathbb{I}$. The first of these is a property shared with the Pauli operators for all QV types, which commute up to a phase of ω, as was seen in the Weyl commutation relation of Equation 2.44. This relation directly implies that

$$X(p')Z(-p)X(-p')Z(p) = \omega^{pp'}\mathbb{I}. \tag{5.5}$$

This may be understood pictorially in phase space in terms of a closed loop of translations creating an area-dependent phase, as shown in Figure 5.2. As such, this can be thought of as a geometric phase which motivates the ‘geometric phase gate’ terminology for the gate now introduced.

Global phases have no physical consequence in quantum mechanics, however, as in Equation 5.1, *controlled* Pauli gates can utilise the geometric phase of Equation 5.5 to entangle QVs. Specifically, consider the circuit diagram on the LHS of Figure 5.3 for two computational QVs and an ancilla of an arbitrary QV type (given

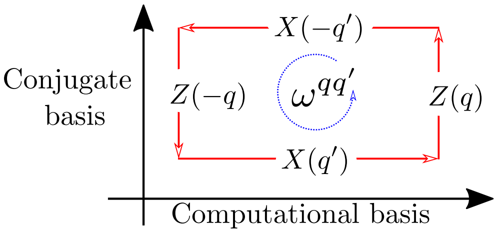


Figure 5.2: A closed loop of translations generated by Pauli operators creates an area-dependent geometric phase.

the restriction discussed above). For the computational QVs in the states $|q\rangle$ and $|q'\rangle$ respectively, the action on the ancilla is

$$X(q'p')Z(-qp)X(-q'p')Z(qp) = \omega_a^{pp'qq'}\mathbb{I}, \tag{5.6}$$

where the subscript a denotes that the phase is dependent on the ancilla QV type, that is, $\omega_a = e^{2\pi i/d_a}$ where d_a is the dimension of the ancilla, as it will be throughout this and later chapters. The q and q' dependent phase, on the RHS of this equality, is equivalent to the controlled rotation gate $CR(2\pi pp'/d_a)$ on the computational QV pair, with

$$R(\theta)|q\rangle = e^{i\theta q}|q\rangle. \tag{5.7}$$

This $R(\theta)$ notation is used as a short-hand for the linear and scalar-parameterised case of the more general phase-function parameterised rotation gate introduced in Equation 2.58 and used throughout the previous two chapters. Note that, in all cases, if the dimensions of the computational and ancilla QVs match this is the CZ gate (when $p = p' = 1$). For clarity, the cases of a qudit and a QCV ancilla are considered individually:

1. *Qudit ancilla:* The gate parameters are restricted to $p, p' \in \mathbb{Z}(d_a)$ and d_a is the dimension of the ancillary qudit. By varying p and p' then $d_a - 1$ distinct non-trivial gates may be implemented, which are the $d_a - 1$ integer powers of the gate given by $p = p' = 1$. The exact gate implemented depends on the QV type of the register.

2. *QCV ancilla:* The gate parameters may take any values $p, p' \in \mathbb{R}$ and $d_a = 2\pi$. By varying p and p', any $CR(\theta)$ gate for any phase parameter $\theta \in \mathbb{R}$ can be implemented. For any type of computational QVs this may be chosen to implement CZ, with the appropriate choice of phase angle depending on the computational QV type (e.g., $pp' = \pi$ gives the CZ gate for qubits, and more generally take $pp' = 2\pi/d$).

For all types of ancillas and computational QVs, this gate method may implement

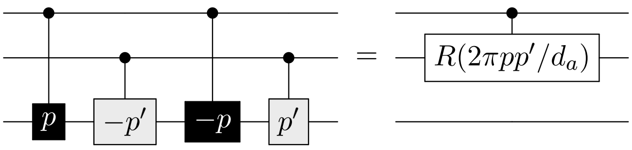


Figure 5.3: An entangling gate on two computational QVs may be mediated via an ancilla using controlled Pauli gates. A black (grey) box containing a variable p denotes the gate $Z(p)$ ($X(p)$). The induced gate on the computational QVs is the symmetric controlled $R(2\pi pp'/d_a)$ gate, where d_a is the dimension of the ancilla and $R(\theta)|q\rangle = e^{iq\theta}|q\rangle$.

an entangling gate on the register and is therefore sufficient for universal quantum computation when augmented with local controls of the computational register. As the action of the gate leaves the ancilla unchanged, the ancilla may be either reused, discarded or reset to remove any residual entanglement from imperfect operation.

For QCV ancillas and computational qubits the gate method introduced above is not novel - to my knowledge it was originally proposed by Milburn (1999). This has been followed by a large literature, investigating both the possibilities for physical realisations and the computational properties of both this and closely related schemes, for example see Brown et al. (2011); Horsman et al. (2011); Khosla et al. (2013); Louis et al. (2008, 2007); Milburn et al. (2000); Munro, Nemoto and Spiller (2005); Proctor and Spiller (2012); Spiller et al. (2006); Van Loock et al. (2008); Wang and Zanardi (2002). There is one notable difference between the literature on this QCV-ancilla mediated entangling qubit gate and the presentation here: the literature is phrased in terms of controlled displacement operators. These notational differences can be bridged via the relations between complex-parameterised displacement operators and the QCV Pauli operators given in Appendix C. As far as I am aware, this ancilla-based geometric phase gate is novel in all cases outside the qubit-QCV setting.

5.3 Size-reducing circuit decompositions

The geometric phase gate described above is sufficient for universal quantum computation on the register (assuming the addition of local controls), and hence any gate sequence can be implemented by many applications of such gates. Moreover, I will now show that the gate can be adapted to implement some common gate sequences in a more efficient fashion. Consider the gate sequence in Figure 5.4, in which many computational QVs, separated into 'control' and 'target' sub-registers of n and m

QVs respectively, interact in turn with an ancilla (demonstrated in Figure 5.4 for $n = 3$ and $m = 2$). Let the control and target sub-registers contain QVs labelled $1, \dots, n$ and $n+1, \dots, m+n$, respectively. As it is essentially trivial that

$$Z(z_n) \dots Z(z_2) Z(z_1) = Z(z_n + \dots + z_2 + z_1), \tag{5.8}$$

$$X(x_{n+m}) \dots X(x_{n+2}) X(x_{n+1}) = X(x_{n+m} + \dots + x_{n+1} + x_{n+1}), \tag{5.9}$$

then using these equations and applying Equation 5.5, it may be confirmed that if the j^{th} QV is in the state $|q_j\rangle$ then the gate sequence of Figure 5.4 maps the ancilla as

$$|\phi_{\text{ancilla}}\rangle \to \omega_a^{(z_1 q_1 + \dots + z_n q_n)(x_{n+1} q_{n+1} + \dots + x_{n+m} q_{n+m})} |\phi_{\text{ancilla}}\rangle. \tag{5.10}$$

Here $|\phi_{\text{ancilla}}\rangle$ is some arbitrary initial state of the ancilla and, as always, ω_a is dependent on the QV type of the ancilla. Expanding the brackets confirms that this is equivalent to $m \times n$ controlled rotation gates: one between each of the systems in the control register and each of those in the target register - noting that this has been achieved using only $2(n+m)$ gates. Consequently, this is a gate-count reduction from the obvious (but not necessarily optimal) quantum circuit to implement this unitary without the aid of an ancilla. In the context of a qubit register and QCV ancilla these gate-count reduction ideas were originally developed by Brown et al. (2011, 2012); Horsman et al. (2011); Louis et al. (2007)[2] but to my knowledge the result is novel in all other cases.

One important feature of this gate method is that the controlled rotation gates induced on the register by this sequence do not all have independent rotation parameters – this would not be possible as there are only $n + m$ parameters in the ancilla-mediated gate sequence. This gate method is a particularly clear setting for considering any efficiency gains obtained from using ancillas of a different dimension to the main register to aid a computation: the phase parameter in the controlled rotation enacted on the j^{th} control and k^{th} target QV pair is $e^{2\pi i z_j x_k / d_a}$ with $z_j, x_k \in \mathbb{S}_{d_a}$, and hence, higher dimensional ancillas give greater freedom in the implemented rotation angles. For example, with a QCV ancilla the phase may take any value in $\mathbb{R}$, but for a qubit ancilla every phase is either 0 or π. Whether there are any fundamental advantages associated with combining ancillary and computational registers of different QV type is discussed further in Section 5.4. However, before turning to this, some specific highly-efficient ancilla-mediated gate decompositions are considered, which may be of practical interest. These are essentially extensions of the gate method given above, and, in the interesting cases, will employ ancillas of a different dimension to the register QVs.

[2] The techniques used in these papers are all special cases or adaptions of this.

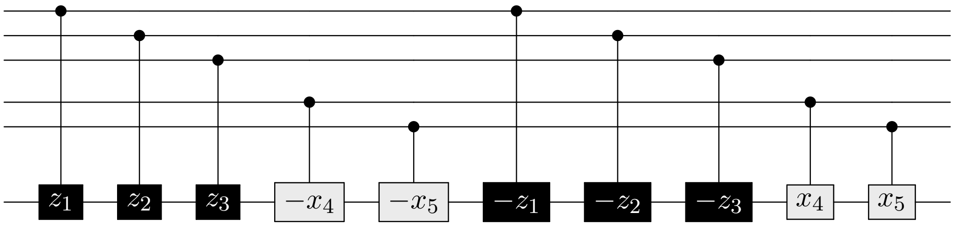


Figure 5.4: An ancilla-mediated gate sequence that enacts a controlled rotation gate between every control-target pair of QVs from ‘control’ and ‘target’ sub-registers. The specific circuit demonstrated here is for three QVs in the control sub-register (top three quantum wires), and two QVs in the target sub-register (quantum wires four and five). The lowest quantum wire represents the ancilla.

5.3.1 The quantum Fourier transform

The ancilla-based gate-count reduction method given above has been adapted to implement the quantum Fourier transform (QFT) on a qubit register using a QCV ancilla by Brown et al. (2011). I now point out a problem with this method. In the interest of generality and in keeping with the majority of this thesis, I will not show this directly for the qubit-based QFT method of Brown et al. (2011), but for a simple and natural extension to a technique for implementing a qudit-based QFT via a QCV ancilla - which hence includes the binary version as a special case.[3] To clarify, this is a *negative* result showing that the previous method proposed by Brown et al. (2011) (and the simple extension here) is not of any practical use. Any readers uninterested in such a result are encouraged to skip ahead to Section 5.3.2. To begin, the QFT is introduced.

The Fourier transform has already been encountered in this thesis - as the single-QV Fourier gate F, which was first introduced in Section 2.2.1. More generally, what is conventionally termed the *quantum Fourier transform* (QFT) modulo k is a unitary which acts on k orthonormal basis states $|0\rangle, |1\rangle, \dots, |k-1\rangle$, encoding the numbers $0, 1, \dots, k-1$. Here it will be denoted $\textsc{qft}_k$, and it is defined by the mapping

$$|q\rangle \xrightarrow{\textsc{qft}_k} \frac{1}{\sqrt{k}} \sum_{q'=0}^{k-1} e^{2\pi i q q'/k} |q'\rangle. \tag{5.11}$$

Therefore, as with the F gate, it is exactly the unitary representation of the discrete Fourier transform, but it is now defined as a family of operators where for each value

[3] Although it may seem strange to extend a method I am going to show is infeasible, given the material already covered in this thesis, it essentially requires no additional effort to present this more general case.

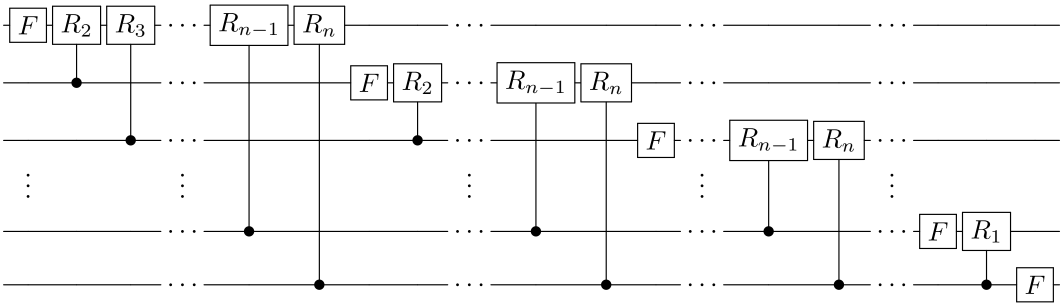


Figure 5.5: An n-qudit circuit to implement the quantum Fourier transform modulus d^n, where d is the dimension of the qudits [Cao et al. (2011); Zilic and Radecka (2007)]. This circuit also inverts the ordering of the qudits, and hence to implement precisely QFT_{d^n}, as given by Equation 5.13, is is necessary to swap the output qudit ordering: that is, swap qudit 1 with qudit n, qudit 2 with qudit $n-2$, etc. Here R_k is the gate with the action $R_k|q\rangle = e^{2\pi i q/d^k}|q\rangle$.

of k it acts on a different sized Hilbert space.

The QFT for modulus $k \leq d^n$ is an operator that can be implemented using n qudits of dimension d, and it is particularly simple to perform QFT_{d^n} using n qudits. The most natural way to embed QFT_{d^n} as an operator on n qudits is to use the association

$$\left|q_1 d^{n-1} + q_2 d^{n-2} + \cdots + q_n d^0\right\rangle \equiv |q_1, q_2, \ldots, q_n\rangle, \tag{5.12}$$

which is the d-nary encoding of the numbers 0 to $d^n - 1$ into n qudits. Using this representation, the QFT modulus d^n is then found by replacing each q in Equation 5.11 with the d-nary representation of q. Hence, it is the mapping

$$|q_1, q_2, \ldots, q_n\rangle \xrightarrow{\text{QFT}_{d^n}} \frac{1}{\sqrt{d^n}} \sum_{q'_1, q'_2, \ldots, q'_n = 0}^{d-1} e^{2\pi i \sum_{a,b=1}^{n} (q_a q'_b d^{n-a-b})} \left|q'_1, q'_2, \ldots, q'_n\right\rangle. \tag{5.13}$$

For a single qudit ($n = 1$) this reduces to a single local Fourier transform F, as it should. The QFT is a critical sub-routine in a significant proportion of algorithms that exhibit a quantum speedup [Nielsen and Chuang (2010)], including Shor's algorithm [Shor (1997)] and related problems. In most of the literature the implementation of the QFT over a register of qubits has been considered (either with modulus 2^n or more generally). However, the non-binary QFT may have certain advantages, including reduced errors when the smaller rotations are not implemented [Zilic and Radecka (2007)]. Furthermore, in direct analogy to the binary sub-case, it is an important component in qudit algorithms, such as the qudit phase estimation algorithm [Cao et al. (2011); Parasa and Perkowski (2011)].

An expansion of the phase terms in Equation 5.13 can be used to show that the qudit QFT can be implemented by the quantum circuit given in Figure 5.5, consisting of single-qudit Fourier gates and controlled rotations. This decomposition is originally due to Coppersmith (1994) for qubits, and this qudit circuit may be found in Cao et al. (2011); Zilic and Radecka (2007).[4] The qudit QFT circuit of Figure 5.5 has a size of $O(n^2)$ and, with a careful pairing of controlled gates,[5] it has a depth of $O(n)$.

A method for a low-gate count implementation of a 'QFT-like' unitary on a register of qudits via a QCV ancilla is now presented, which includes the technique of Brown et al. (2011) as a special case. Define the 'QFT-like' unitary $U_{\vec{u},\theta}$, which is parameterised by n single-qudit gates $u_1, \ldots, u_n$ and a matrix of phase angles θ, by the product of basic single and two-qudit gates

$$U_{\vec{u},\theta} = u_n \left(\mathrm{C}^n_{n-1} R(\theta_{n-1,l})\right) u_{n-1} \ldots \left(\prod_{l=3}^{n} \mathrm{C}^l_2 R(\theta_{2,l})\right) u_2 \left(\prod_{l=2}^{n} \mathrm{C}^l_1 R(\theta_{1,l})\right) u_1, \quad (5.14)$$

where $\theta_{j,k} \in \mathbb{R}$, $j = 1, \ldots, n-1$ and $k = j+1, \ldots, n$.[6] The natural circuit representation for this unitary is given in Figure 5.10, which should hopefully clarify why it is termed 'QFT-like': it is has the same circuit structure as the standard circuit for the QFT modulus d^n. Indeed, it reduces to the $\textsc{qft}_{d^n}$ when $u_k = F$ for all k and if the phase angles are given by

$$\theta_{j,k} = 2\pi d^{j-(k+1)}. \quad (5.15)$$

As with the QFT, the circuit given in Figure 5.10 has a size of $O(n^2)$ and a depth of $O(n)$, via a suitable pairing of controlled rotations.

Now, consider the ancilla-mediated gate sequence given in Figure 5.11. This is probably simpler to comprehend as a circuit diagram, but for completeness the gate

[4] See Nielsen and Chuang (2010) for a clear derivation in the binary case, which may be easily adapted to the qudit QFT.

[5] This may be achieved using a similar, but slightly more subtle, method to that already encountered in Figure 3.6.

[6] In this expression, the subscript k on u_k is used to denote that these are in general different unitaries for each k, and also to denote which unitary the operators acts on (i.e., u_k denotes the unitary u_k acting on qudit k.). Although perhaps slightly vague, I consider this preferable to a more complication notation.

sequence is

$$U_{\text{QFT-seq}} = \left(\prod_{l=2}^{n-1} \mathrm{C}_a^l Z(-z_l)\right) \cdot v_n \mathrm{C}_a^n X(x_n) \cdot \left(\mathrm{C}_a^{n-1} Z(z_{n-1}) v_{n-1} \mathrm{C}_a^{n-1} X(x_{n-1})\right) \dots$$
$$\dots \left(\mathrm{C}_a^3 Z(z_3) v_3 \mathrm{C}_a^3 X(x_3)\right) \cdot \left(\mathrm{C}_a^2 Z(z_2) v_2 \mathrm{C}_a^2 X(x_2)\right) \cdot \mathrm{C}_a^1 Z(-z_1) \cdot \left(\prod_{l=2}^{n} \mathrm{C}_a^l X(-x_l)\right)$$
$$\mathrm{C}_a^1 Z(z_1) v_1, \quad (5.16)$$

where the 'a' subscript denotes the ancillary system. Via a careful consideration of this sequence, or the circuit of Figure 5.11, and with the aid of the Weyl commutation relation of Equation 5.6, it may be confirmed that this implements the QFT-like unitary $U_{\vec{u},\theta}$ with $u_k = v_k$ and with the controlled rotation parameters in the matrix θ given by

$$\theta_{j,k} = 2\pi z_j x_k / d_a, \quad (5.17)$$

where as always d_a is the dimension of the ancilla, and $z_j, x_k \in \mathbb{S}_{d_a}$. On an initial inspection, the ancilla-mediated circuit of Figure 5.11 has a size of $9n-8$ and a depth of $5n-4$, which are both $O(n)$. Hence, this provides a reduction from quadratic size to a linear size scaling in comparison to the defining circuit for a general $U_{\vec{u},\theta}$ unitary, as given in Figure 5.10.

Consider now the case of a QCV ancilla, whence $\theta_{j,k} = z_j x_k$ and $z_j, x_k \in \mathbb{R}$. If the aim is to apply the QFT_{d^n} then it is necessary to implement the phases given in Equation 5.15. Leaving z_1 as some arbitrary value, which may be chosen later for convenience, in order to satisfy Equation 5.15 for $j = 1$ and $1 < k \leq n$, it is necessary to take

$$x_k = 2\pi d^{-k} / z_1. \quad (5.18)$$

This then gives $z_1 x_k = 2\pi d^{-k}$, as required. Now, to satisfy Equation 5.15 for $j = 2, \dots, n-1$ and general $k = j+1, \dots, n$, it is necessary to take

$$z_j = z_1 d^{j-1}. \quad (5.19)$$

This gives $z_j x_k = 2\pi d^{j-1-k}$, as required. Hence, the QCV ancilla-mediated gate sequence of Figure 5.11 implements the QFT modulus d^n on the n-qudit register if we take the the values for the z_j and x_k parameters given above (z_1 may be fixed to any non-zero value, say $z_1 = 1$) and with $u_m = F$ for all m. As such, this provides a method for implementing the QFT modulus d^n, via a QCV ancilla, with a circuit depth and size of $O(n)$. This is in contrast to the standard circuit decomposition for the (exact) QFT, which has a size of $O(n^2)$ and depth of $O(n)$.

However, there is a problem with this ancilla-based circuit decomposition for the QFT, as now explained. The assumption in the analysis of the circuit depth and size in this circuit is that controlled Pauli $X(q)$ and $Z(q)$ operators with *any* parameters $q \in \mathbb{R}$ are available in the basic gate set, and hence may be implemented in unit depth. As has already been argued in Section 3.5, the claim that all such gates may be implemented in a unit of time cannot be physically justified.[7] Hence, in order for depth to be an accurate proxy for computational time, it is necessary to restrict the values of $q \in \mathbb{R}$ for which $\mathrm{C}Z(q)$ and $\mathrm{C}X(q)$ gates are assumed to be implementable in a unit depth by considering only $q \in [0, a]$ for some (non-zero) constant $a \in \mathbb{R}$. However, the controlled Pauli gates in this QFT-implementing sequence contain parameters which grow *exponentially large* as a function of input size n, which can be confirmed via Equation 5.19.[8] Therefore, with the more physically appropriate gate set of bounded-magnitude controlled Pauli gates, some of the gates in this sequence require exponential depth (and time), which renders this QFT implementation technique impractical, and vastly inferior to the ordinary $O(n^2)$ size and $O(n)$ depth decomposition, given in Figure 5.5 (which may be implemented via ancilla in a gate-by-gate fashion, if required). It might appear as though the exponential resource-scaling in this ancilla-based method can be removed with the aid of local squeezing gates on the QCV ancilla, but although these gates can transfer the exponential parameter scaling from the ancilla-register interaction gates to local squeezing gates (see Figure 2.4), exponential scaling in such gates is essentially just as problematic and unphysical. Finally, before moving on it is noted that this ancilla-based technique for implementing a QFT-like unitary *is* valid in certain other cases that are *not* the QFT, by which I mean that, even under the restriction of bounded-magnitude controlled Pauli gates, it will have the depth and size scaling initially claimed. However, it is not clear that it implements any unitaries of interest in such cases, except those also covered by the simpler technique of Figure 5.4.

5.3.2 Modulo controlled gates via qudit ancilla

So far in this chapter, only register-controlled Pauli gates have been considered as the ancilla-register interactions. The reason for this is that Pauli operators have convenient properties that make them easy to manipulate, and which also allow for an analysis that can be applied simultaneously to each type of QV. When only considering operations of this sort, a qudit ancilla has strictly less power to enhance a computation than is available with a QCV, as inferred by the discussions near

[7] The discussion in Section 3.5 largely considers local Pauli gates, but the conclusions given obviously extend to controlled Pauli gates.

[8] This exponential parameter scaling cannot be removed by taking z_1 to be exponentially small, that is by choosing $z_1 \propto d^{-n}$. This is because if $z_1 \propto d^{-n}$ then the biggest x_k parameter grows exponentially with increasing n, as then Equation 5.18 implies that $x_2 \propto d^n$. Hence, either the controlled $X(x_2)$ or controlled $Z(z_{n-1})$ gate has a parameter which grows exponentially with n.

the beginning of this section. However, the restriction to controlled Pauli gates is perhaps rather unnatural for a qudit ancilla, and it can be argued it is more physically well-motivated to consider a general controlled rotation interaction gate, which maps

$$|q\rangle_r|q'\rangle_a \xrightarrow{\mathrm{C}_a^r R(\theta)} e^{i\theta qq'}|q\rangle_r|q'\rangle_a, \tag{5.20}$$

where $\theta \in \mathbb{R}$. For $\theta = 2\pi z/d_a$ with $z \in \mathbb{S}_{d_a}$, this gives the $\mathrm{C}Z(z)$ gate. Hence, this operator is only a generalisation from $\mathrm{C}Z(q)$ for the case of qudits, as with a QCV target system then $\mathrm{C}R(\theta) = \mathrm{C}Z(\theta)$. This is a natural extension of the allowed interactions for qudit ancillas as it is easy to confirm that this operator is generated by the same Hamiltonian as the controlled Pauli operator, with the interaction time controlling θ, as will be shown in Section 5.5. This gate allows for continuous parameters in qudit ancilla-based sequences, but also means that the periodicity of a qudits phase space can be harnessed to efficiently implement some interesting gates, as I now show. In the following, the ancilla and register are restricted to being qudits and, as always, the ancilla and register dimensions are denoted d_a and d, respectively.

Controlled rotation operators along with ancilla preparation may be used to implement a controlled rotation gate on the register of arbitrary phase angle, by adapting the geometric phase gate of Figure 5.3. This is because the $\mathrm{C}X$ gate maps a register system in an arbitrary computational basis state $|q\rangle$, and an ancillary qudit in the state $|0\rangle$, to

$$|q\rangle|0\rangle \xrightarrow{\mathrm{C}X} |q\rangle|q \bmod d_a\rangle. \tag{5.21}$$

Hence, as long as $d_a \geq d$, then for two register qudits c and t, this implies that

$$\langle 0|_a \mathrm{C}_a^c X^\dagger \cdot \mathrm{C}_a^t R(\theta) \cdot \mathrm{C}_a^c X |0\rangle_a = \mathrm{C}_t^c R(\theta). \tag{5.22}$$

Note that $\langle 0|$ appears in the LHS of this equation so that the RHS is simply a gate acting on the register, but equivalently it could be dropped and then the final ancilla state on the RHS would be $|0\rangle$. The circuit diagram for this gate is given in Figure 5.6. In contrast to when the gates are all controlled Pauli operators, ancilla preparation is now essential in order for the qudit not to remain entangled with the register. This is because the overall operation on the ancilla is a register-controlled phase, which acts as the identity if the ancilla is prepared in the state $|0\rangle$ (or a constant phase multiplied by the identity if initialised in any other computational basis state). This gate method may not seem of much consequence, but it provides the basis for the more interesting gates introduced below.

Before going any further, it will be useful to introduce a succinct notation for

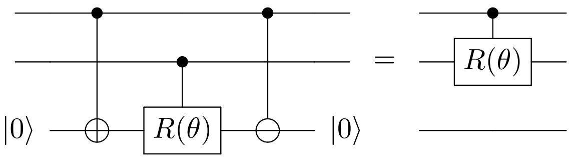


Figure 5.6: A circuit which implements a general controlled rotation gate between register qudits of dimension d via an ancilla qudit of dimension $d_a \geq d$. The SUM and SUM† gate circuit notation (the $\oplus$ and $\ominus$ symbols, respectively) is used to denote the CX and $CX^\dagger$ gates, because these can be considered to be hybrid SUM and SUM† gates respectively.

controlled gates with multiple control and target QVs. Consider two sets of QVs, $\mathcal{Q}$ and $\mathcal{Q}'$, with no elements in common (i.e., $\mathcal{Q} \cup \mathcal{Q}' = \emptyset$). Then, for a scalar-parameterised unitary $u(p)$ with $p \in \mathbb{S} \subseteq \mathbb{R}$ and $u(a)u(b) = u(b)u(a)$ for all $a, b \in \mathbb{S}$, and a map $\theta : \mathcal{Q}' \times \mathcal{Q} \to \mathbb{S}$, define

$$\mathrm{C}_{\mathcal{Q}}^{\mathcal{Q}'} u(\theta) := \prod_{q' \in \mathcal{Q}'} \prod_{q \in \mathcal{Q}} \mathrm{C}_q^{q'} u(\theta(q', q)). \tag{5.23}$$

That is, this unitary is equivalent to a controlled $u(\cdot)$ gate between each QV in $\mathcal{Q}$ and each QV in $\mathcal{Q}'$, with $u(\cdot)$ taking a potentially different parameter for each control-target pair. This is well defined as the ordering of the gates in Equation 5.23 is irrelevant, due to the commutativity of each $\mathrm{C}u(\cdot)$ gate. This notation is a simple way to denote many multi-QV gates that are defined naturally in terms of controlled gates without explicit and cumbersome expansions. For example, the utility of this notation can be seen by observing that the ancilla-based circuit of Figure 5.4 can be succinctly expressed as

$$\mathrm{C}_a^{\mathcal{Q}'} X(x) \cdot \mathrm{C}_a^{\mathcal{Q}} Z(-z) \cdot \mathrm{C}_a^{\mathcal{Q}'} X(-x) \cdot \mathrm{C}_a^{\mathcal{Q}} Z(z) = \mathrm{C}_{\mathcal{Q}'}^{\mathcal{Q}} R(2\pi z x / d_a), \tag{5.24}$$

where $z : \mathcal{Q} \to \mathbb{S}_{d_a}$ and $x : \mathcal{Q}' \to \mathbb{S}_{d_a}$. It will also be useful to have a simple notation for an arbitrary diagonal gate on a set of QVs, $\mathcal{Q}$. Such a gate is parameterised by a potentially different phase for each computational basis state, and hence it may be defined by the unitary $D_{\mathcal{Q}}(\phi)$ with the action on the computational basis

$$\big|q_1, \dots, q_{|\mathcal{Q}|}\big\rangle \xrightarrow{D_{\mathcal{Q}}(\phi)} e^{i\phi(q_1, \dots, q_{|\mathcal{Q}|})} \big|q_1, \dots, q_{|\mathcal{Q}|}\big\rangle, \tag{5.25}$$

where ϕ is a function $\phi : \mathbb{S}_d^{|\mathcal{Q}|} \to \mathbb{R}$, and the reader is reminded that $|\mathcal{Q}|$ denotes the number of elements in the set $\mathcal{Q}$.

We are now ready to consider interesting qudit ancilla-mediated gates that utilise the periodicity of the ancillary qudit's phase space. Consider two sets of register qudits $\mathcal{Q} = \{1, \dots, n\}$ and $\mathcal{Q}' = \{n+1, \dots, m+n\}$. Then, if the first set of qudits interact with an ancilla prepared in $|0\rangle$ via the n-gate sequence $\mathrm{C}_a^{\mathcal{Q}} X(x)$, where $x : \mathcal{Q} \to \mathbb{S}_{d_a}$, then the affected register qudits and the ancilla are mapped as

$$|q_1, \dots, q_n\rangle|0\rangle \xrightarrow{\mathrm{C}_a^{\mathcal{Q}} X(x)} |q_1, \dots, q_n\rangle|x(1)q_1 \oplus \dots \oplus x(n)q_n\rangle. \tag{5.26}$$

The $\oplus$ notation is used here, and throughout the rest of this section, to explicitly denote that this arithmetic must be taken modulo d_a, and that this is in general not the same modularity as if a similar summation was implemented in a register qudit (which would only be true if $d_a = d$). From Equation 5.26, and using the action of a controlled scalar-parameterised rotation given in Equation 5.20, it follows that

$$\langle 0|\mathrm{C}_a^{\mathcal{Q}} X(-x) \cdot \mathrm{C}_a^{\mathcal{Q}'} R(\theta) \cdot \mathrm{C}_a^{\mathcal{Q}} X(x)|0\rangle = D_{\mathcal{Q} \cup \mathcal{Q}'}(\phi), \tag{5.27}$$

where the phases of the diagonal gate, which acts on all $n+m$ of the register qudits, are given by

$$\phi(q_1, \dots, q_{n+m}) = (\theta(n+m)q_{n+m} + \dots + \theta(n+1)q_{n+1})\,(x(n)q_n \oplus \dots \oplus x(1)q_1)\,. \tag{5.28}$$

When $d_a > (d_r - 1)\sum_{k \in \mathcal{Q}} x(k)$, then the modulo arithmetic is equivalent to ordinary arithmetic. In this case, this implements the unitary $\mathrm{C}_{\mathcal{Q}'}^{\mathcal{Q}} R(\theta)$ where $\theta(j,k) = x(j)\theta(k)$, which is almost identical to what can be achieved with controlled Pauli operators and a QCV ancilla, as given in Equation 5.10 and discussed below that equation. Although this is an extension on what can be achieved with a qudit ancilla in Equation 5.10 (which allows only phases that are integer multiples of the d_a^{th} root of unity for a qudit ancilla), a much more interesting case is when

$$d_a \leq (d_r - 1) \sum_{k \in \mathcal{Q}} x(k), \tag{5.29}$$

which is when the modularity of the arithmetic is central to the effect of the gate. It is perhaps not entirely obvious whether this gate has any uses in quantum computation, when written in this general form. However I now give a simple adaption of this to implement a novel 'step' gate, which I now introduce and which includes the important generalised Toffoli gate as a particular case for qubits. Before presenting the method, this 'step' gate is defined and the importance of generalised Toffoli gates is briefly discussed.

Define the step gate, denoted $\textsc{step}_D(u)$, by the action:

$$|q_1, \dots, q_n\rangle|q\rangle \xrightarrow{\textsc{step}_D(u)} |q_1, \dots, q_n\rangle \otimes u^{\lfloor (q_1 + \dots + q_n)/D \rfloor}|q\rangle, \tag{5.30}$$

where $\lfloor x \rfloor$ is the floor function, which returns the largest $k \in \mathbb{N}$ with $k \leq x$. Therefore, this gate applies the unitary u^m on the target qudit, when

$$D(m+1) > q_1 + \cdots + q_n \geq Dm. \tag{5.31}$$

Hence, the step gate is a family of unitaries (i.e., it is defined for a general input size $n+1$) which require a unitary u and a value $D \in \mathbb{N}$ to be fully defined, noting that D may be chosen to scale with n if desired. For qubits, this includes the generalised Toffoli gate as a special case, which maps

$$|q_1 \dots q_n\rangle|q\rangle \xrightarrow{\text{TOFFOLI}_n(u)} |q_1 \dots q_n\rangle \otimes u^{q_1 \cdot q_2 \cdots q_n}|q\rangle, \tag{5.32}$$

and hence applies the unitary u to the target system if and only if all of the n control qubits are in the state $|1\rangle$. Specifically, it is the special case of the qubit step gate, $\text{STEP}_D(u)$, with $D = n$. The Toffoli gate plays an important role in quantum computation, for example, it appears in many error correcting codes [Fedorov et al. (2011); Gottesman (1997)] and it is a natural component in a variety of quantum algorithms [Nielsen and Chuang (2010)]. The importance of this gate is in part because the ordinary Toffoli gate ($n = 2$, $u = X$) is a valid classical 3-bit gate, and alone is universal for classical reversible computation [Toffoli (1980)[9]]. Hence, efficient decompositions of Toffoli gates into physically realistic primitive gates are of interest.

Consider the sub-case of Equation 5.27 where $\mathcal{Q}' = \{t\}$. From this equation it follows that

$$\langle 0|\mathrm{C}_a^{\mathcal{Q}}X \cdot \mathrm{C}_a^t R(-\theta/d_a) \cdot \mathrm{C}_a^{\mathcal{Q}}X|0\rangle = D_{\mathcal{Q}\cup\{t\}}(\phi), \tag{5.33}$$

where the phases of the diagonal gate are given by

$$\phi'(q_1, \dots, q_n, q_t) = -\frac{\theta}{d_a} q_t \left(q_1 \oplus \cdots \oplus q_n\right). \tag{5.34}$$

As long as $d_a \geq d$, then individual additional control rotation gates of $\mathrm{C}_t^k R(\theta/d_a)$, for $k = 1, \dots, n$, can be applied via n applications of the ancilla-based gate sequence in Figure 5.6, which uses a total of $3n$ gates. If these additional gates are appended to the sequence of Equation 5.33, the total unitary effected is

$$\mathrm{C}_t^{\mathcal{Q}} R(\theta/d_a) D_{\mathcal{Q}\cup\{t\}}(\phi) = D_{\mathcal{Q}\cup\{t\}}(\phi'), \tag{5.35}$$

[9] Interestingly, the addition of only the Hadamard gate, or indeed *any* basis changing gate, is enough to make this universal classical set become universal for quantum computation [Shi (2002)].

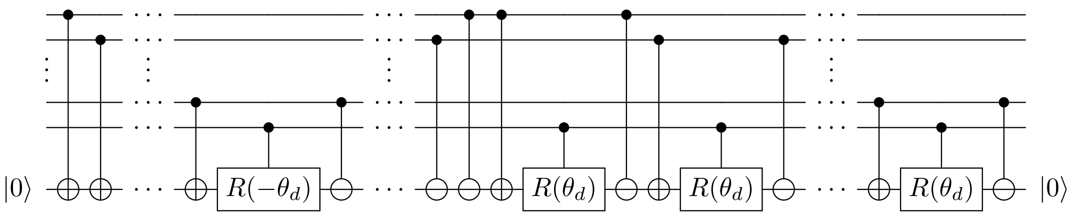


Figure 5.7: This circuit implements the gate $\text{STEP}_{d_a}(R(\theta))$ on one target and n control register qudits of dimension d, via an ancilla of dimension $d_a \geq d$ prepared in the state $|0\rangle$. The lowest wire of the main register is the target of the step gate and $\theta_d = \theta/d_a$. This circuit has a size of $10n + 2$ and a depth of $5n + 1$.

where the resultant gate has the phase factor function ϕ' given by

$$\phi'(q_1, \dots, q_n, q_t) = \theta q_t \left((q_1 + \dots + q_n) - (q_1 \oplus \dots \oplus q_n) \right) / d_a, \tag{5.36}$$

$$= \theta q_t \lfloor (q_1 + \dots + q_n) / d_a \rfloor. \tag{5.37}$$

The latter equality follows via considering the difference between the same ordinary and modulo arithmetic sums. Hence, $D(\phi')$ is exactly the gate $\text{STEP}_{d_a}(R(\theta))$, where θ can take any value in $\mathbb{R}$. Therefore, this ancilla-based sequence gives a method for implementing a subset of step gates using only $5n+1$ basic gates. The complete circuit is given in Figure 5.7.

For a register of qubits, this may be converted via local gates to a step gate with any unitary u, as for all $u \in U(2)$ there is a $v \in U(2)$ and $\theta, \phi \in \mathbb{R}$ such that $u = e^{i\phi} v R(\theta) v^\dagger$, which is simply u expressed in terms of its eigenvectors (columns of v) and eigenvalues (which are $e^{i\phi}$ and $e^{i(\phi+\theta)}$). As the n-qubit Toffoli gate is the special case of the qubit step gate, $\text{STEP}_D(u)$, with $D = n$, then this gives a method for implementing any generalised Toffoli gate on n qubits via $5n + 1$ interactions with an ancilla of dimension n. Moreover, this method may be adapted slightly to reduce the gate-count for the generalised Toffoli gate, with a circuit given in Figure 5.8 which requires only $2n+5$ gates (a saving of $\approx 3n$).[10] Although the most well-known decomposition of generalised Toffoli gates into two-qubit gates, due to Barenco et al. (1995), requires a number of gates quadratic in n, it is known that this can be reduced to a linear scaling without the need for higher-dimensional ancilla [Barenco et al. (1995); Maslov et al. (2008); Saeedi and Pedram (2013)]. This is the same scaling with input size n as the qudit-mediated scheme I have proposed here, however (to my knowledge) all known decompositions into two-qubit gates require more than $2n + 5$ elementary gates. As far as I am aware, the optimal qubit-only

[10] Similar adaptions apply more generally for step gates, but have been ignored for simplicity.

construction in the literature (in terms of both size and depth) is due to Saeedi and Pedram (2013) and requires $12n - 22$ gates.[11]

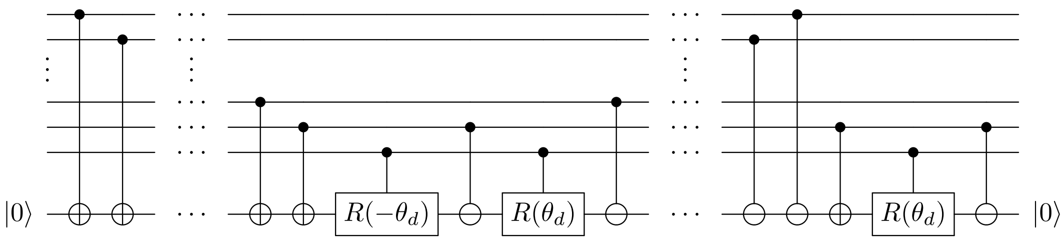


Figure 5.8: A circuit acting on $n+1$ qubits and an ancillary qudit of dimension n initialised to $|0\rangle$ which implements the gate $R(\theta)$ on the the qubit $n+1$ if and only if all of the other control qubits are in the state $|1\rangle$. This is the generalised Toffoli gate $\text{TOFFOLI}_n(u)$ with $u = R(\theta)$, where the Toffoli gate is defined in Equation 5.32. From this a generalised Toffoli gate with any $u \in U(2)$ can be implemented via local controls. This circuit has a size of $4n+10$ and a depth of $2n+5$. The parameter θ_d is given by $\theta_d = \theta/n$.

An alternative method for implementing generalised Toffoli gates in a highly efficient manner via a qudit ancilla has been proposed previously by Ionicioiu et al. (2009). I now present a (slightly improved version) of this method to compare to the technique introduced above. Consider a qudit ancilla with dimension $d_a > n$ that is initialised to $|\ominus n\rangle$ (i.e., $|d_a - n\rangle$). Then, as with the method above, if the interaction sequence $\mathrm{C}_a^{\Omega} X$ is applied, this maps

$$|q_1 \dots q_n\rangle |q_t\rangle |\ominus n\rangle \xrightarrow{\mathrm{C}_a^{\Omega} X} |q_1 \dots q_n\rangle |q_t\rangle |q_1 \oplus \dots \oplus q_n \ominus n\rangle. \tag{5.38}$$

Hence, the ancilla is in the state $|0\rangle$ only when all of the qubits are in the $|1\rangle$ state (as $d_a > n$). Therefore, if the gate u is then implemented on the target subsystem controlled on whether the ancilla is in the state $|0\rangle$, i.e., the unitary

$$U_0(u) = |0\rangle\langle 0| \otimes u + \sum_{k=1}^{d_a-1} |k\rangle\langle k| \otimes \mathbb{I}, \tag{5.39}$$

this implements a u gate on the target qubit only if all of the n control qubits are in the state $|1\rangle$, as required of the generalised Toffoli gate. As in the method proposed above, applying $\mathrm{C}_a^{\Omega} X^{\dagger}$ disentangles the control qubits, finishing the gate.[12]

[11] This uses $n-2$ auxiliary qubits. With only one auxiliary qubit then $24n-64$ gates are required.

[12] The gate that is implemented if the input size n is allowed to scale independently of d_a is what might naturally be called a $\text{MOD}_{d_a}(u)$ gate, which applies u to the target qubit if and only if $q_1 \oplus \dots \oplus q_n = 0$, where the summation is modulo d_a.

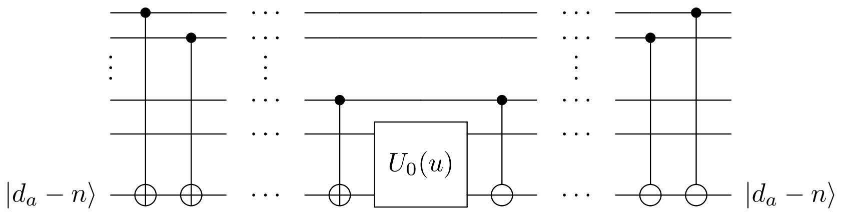


Figure 5.9: The method of Ionicioiu et al. (2009) for implementing a generalised Toffoli gate on $n+1$ qubits via a qudit ancilla of dimension $d_a > n$. The $U_0(u)$ gate applies the gate u to the target register qubit if the ancillary qudit is in the state $|0\rangle$, and applies the identity otherwise.

This method for implementing the generalised Toffoli gate is summarised in Figure 5.9 and requires only $2n+1$ gates, which is a reduction of four gates from the method I have proposed herein, as given in the circuit diagram of Figure 5.8. However, the circuit of Figure 5.9 has a substantial disadvantage: it contains a $U_0(u)$ gate. A direct implementation of this gate requires an additional ancilla-register interaction Hamiltonian, as it is not generated by the same Hamiltonian as the $\mathrm{C}R(\theta)$ gate, and it cannot be obtained from such a gate and local controls alone. For this reason, I would argue that the method proposed herein is substantially more practical, as it uses only $\mathrm{C}R(\theta)$ and $\mathrm{C}X(\pm 1)$ gates (which can all be easily obtained from $\mathrm{C}R(\theta)$ and local F gates, as discussed further in Section 5.5). Finally, one nice feature of (the adaption of) the scheme of Ionicioiu et al. (2009) given here is that it can be used to implement generalised Toffoli gates on different sized inputs, n, as long as $n < d_a$, with the only change for different input sizes being a different initial ancilla state. This can also be achieved with the method proposed herein simply by changing the ancilla input state in the circuit of Figure 5.8 to $|n - d_a\rangle$, which facilitates the implementation of a generalised Toffoli for any input size $n \leq d_a$.

5.4 Hybrid quantum computation

The ancilla-based gates discussed in this chapter use (in general) hybrid variables, and hence are clearly *hybrid quantum computation* in one sense. However, the focus has been entirely on implementing gates on the register and has not considered whether some computation may also be implemented explicitly in the ancillary register (there will necessarily be many ancillas in practice, i.e, a ‘register’ of ancillas). If universal quantum computation can be performed in both registers, when they are of different QV types, then the computational model can be considered a hybrid quantum computer in a much stronger sense. I will now show that the physical primitives used in the geometric phases gates of this chapter allow for truly hybrid quantum computation with all pairings of different types of QVs for the computational and ancillary systems. The following discussion will then be useful for understanding to what degree ancillas of a different dimension can provide efficiencies in quantum computation and, as such, may be used to put the results of Section 5.3 into a more general context.

To begin, consider the case when the register and ancillary systems are all qudits, which may in general be of different dimensions. The interaction gate we have been considering is the $\mathrm{C}R(\theta)$ gate ($\theta \in \mathbb{R}$), which is completely symmetric as[13]

$$\mathrm{C}^r_a R(\theta)|q\rangle_r|q'\rangle_a = e^{i\theta qq'}|q\rangle_r|q'\rangle_a = \mathrm{C}^a_r R(\theta)|q\rangle_r|q'\rangle_a. \tag{5.40}$$

Hence, the ancilla can be equally considered to be the control system in such a gate.[14] As such, it is clear that, along with local controls on both ancillary and register systems, an interaction gate of this sort allows for universal quantum computation on both the ancillary and computational registers (geometric phase gates, etc, may be implemented on the ancillary register, via computational QVs).

Essentially the same considerations hold true for a qudit register combined with QCV ancillas, although it is less straightforward to see. In the following, and in the next section, it be useful to use the 'position' and 'momentum' operators for a general QV, given by $\hat{x} = \sum_{q\in\mathbb{S}_d} q|q\rangle\langle q|$ and $\hat{p} = \sum_{q\in\mathbb{S}_d} q|+_q\rangle\langle +_q|$ respectively, as first introduced in Equation 3.21. In this qudit-QCV context, the implicit assumption throughout this chapter has been that it is possible to implement $\mathrm{C}Z(q)$ gates, for arbitrary $q \in \mathbb{R}$ (or at least, arbitrary $q \in [0,a]$ for some non-zero $a \in \mathbb{R}$), between any register-ancilla pair, where the register QV is the control system. This operator can be expressed in terms of the position operators of the two systems, specifically $\mathrm{C}^r_a Z(q) = e^{iq\hat{x}_r\otimes\hat{x}_a}$. Hence, as $F\hat{x}F^\dagger = \hat{p}$, then via local Fourier gates it is also possible to implement the gate

$$(F_r \otimes \mathbb{I}_a)\cdot \mathrm{C}^r_a Z(q) \cdot (F^\dagger_r \otimes \mathbb{I}_a) = e^{iq\hat{p}_r\otimes\hat{x}_a}, \tag{5.41}$$

between any register qudit, r, and ancillary QCV, a. Therefore, for a single register system, r, and two ancillary QCVs, a and b, it is possible to implement the operation

[13] Note that, in this equation, the $R(\theta)$ gate on the LHS is not exactly the same gate as on the RHS. That is, on the LHS it is the $R(\theta)$ gate for a d_a-dimensional qudit, and on the RHS it is a $R(\theta)$ gate for a d-dimensional qudit. Obviously, if this was not the case this equality would not make sense.

[14] For example, taking $\theta = 2\pi q/d$ with $q \in \mathbb{S}_d$, can be interpreted as implementing an ancilla-controlled Pauli $Z(q)$ gate on the register qudit.

sequence

$$e^{iq\hat{p}_r\otimes\hat{x}_b}e^{iq\hat{x}_r\otimes\hat{x}_a}e^{-iq\hat{p}_r\otimes\hat{x}_b}e^{-iq\hat{x}_r\otimes\hat{x}_a} = e^{q^2[\hat{p}_r,\hat{x}_r]\otimes\hat{x}_a\otimes\hat{x}_b} + O(q^3), \tag{5.42}$$

where this equality follows from the general relation

$$e^{i\hat{H}_j\delta t}e^{i\hat{H}_k\delta t}e^{-i\hat{H}_j\delta t}e^{-i\hat{H}_k\delta t} = e^{[\hat{H}_j,\hat{H}_k]\delta t^2} + O(\delta t^3), \tag{5.43}$$

for Hermitian $\hat{H}_k$ and $\hat{H}_j$ [Braunstein and van Loock (2005); Lloyd (1995)], which has already been stated in Equation 2.42. As discussed in Section 2.3.2, this means that via repeated applications of this sequence the unitary

$$U = e^{\phi[\hat{p}_r,\hat{x}_r]\otimes\hat{x}_a\otimes\hat{x}_b}, \tag{5.44}$$

can be built up to arbitrary accuracy for any finite $\phi \in \mathbb{R}$. Now, if the register qudit is prepared in an eigenstate of the Hermitian operator $i[\hat{p}_r,\hat{x}_r]$, then this implements the gate $U(\theta) = e^{i\theta\hat{x}_a\otimes\hat{x}_b}$, for some $\theta \in \mathbb{R}$, which is the two-QCV controlled $Z(\theta)$ gate.[15] Hence, a register qudit has been used to entangle two ancillary QCVs, implying that along with local controls of both the ancillary and register systems, this interaction is sufficient to implement universal quantum computation in both the main and the ancillary registers. This derivation is very closely related to the work of Lloyd (2003) in which the concept of hybrid discrete-continuous quantum computation was introduced. Interestingly, this qudit-mediated two-QCV gate can be understood as an infinitesimally constructed version of the geometric phase gate.[16]

The discussions up to this point have explicitly shown the close link between ancilla-mediated geometric phase gate techniques and hybrid quantum computation, but have not shed any light on the degree to which such different-dimension ancillary systems can provide additional efficiencies in quantum computation. To consider this question, the case in which the register and ancillary systems are both qudits is first discussed. An ancillary qudit may be simulated with $k = \lceil \log_d d_a \rceil$ many register qudits, which is a constant (given that the dimension of the ancillas is a constant, which is a physically appropriate constraint). To implement any local gate on this encoded d_a-dimensional qudit requires only $O(d^{2k}) = O(d_a^2)$ gates and a similarly small number are needed to simulate an interaction gate between an ‘ordinary’ single register qudit and this d_a-dimensional encoded qudit. The simulation is particularly simple when the ancilla has a dimension that is an integer power of d, i.e., $d_a = d^k$,

[15] Exactly what the eigenstates of $i[\hat{p}_r,\hat{x}_r]$ are, is not that important - it is not being suggested here that this is an especially practically method for implementing an entangling gate on two QCVs. For qubits, the eigenstates of this operators are those of the Pauli $Y = iXY$ gate.

[16] The geometric phase gate does not work in an exact sense for qudits mediating an interaction between QCVs, which is the case that has been excluded throughout this chapter.

and this is discussed briefly for clarity.

Consider the case when $d_a = d^k$. The most natural encoding of a d_a-dimensional qudit into $k = \log_d(d_a)$ qudits of dimension d, is given by taking the computational basis states of the encoded qudit to be

$$\left| d^{k-1}q_1 + d^{k-2}q_2 + \cdots + q_k \right\rangle = |q_1, \ldots, q_k\rangle. \tag{5.45}$$

With this representation, an encoded rotation gate $\bar{R}(\theta)$ (a $\bar{u}$ is used to denote a unitary u that acts on the emulated qudit) is simply the tensor product of single-qudit rotation gates, specifically,

$$\bar{R}(\theta) = R\left(d^{k-1}\theta\right) \otimes R\left(d^{k-2}\theta\right) \otimes \cdots \otimes R(d\theta) \otimes R(\theta). \tag{5.46}$$

As a circuit on the physical qudits, this has a depth of one, and a size of k. To achieve the single d-dimensional qudit controlled version of this gate, $\mathrm{C}R(\theta)$, each of these gates simply needs to be controlled by the control system, and hence this need have a depth of no more than k and a size of $2k$. The encoded local Fourier gate, $\bar{F}$, is simply the QFT modulus $d_a = d^k$ on the k physical qudits, and hence may be implemented with a circuit of $O(k^2) = O(\log_d(d_a)^2)$ size, and $O(k) = O(\log_d(d_a))$ depth (see Section 5.3.1). From this, $\bar{X}(q)$ (and controlled $\bar{X}(q)$) gates can be obtained, via $\bar{R}(\theta)$ gates (or $\mathrm{C}\bar{R}(\theta)$ gates) along with Fourier gates.

In summary, the overhead of simulating ancillary qudits of a different dimension to the register qudits is low for physically relevant dimensions and in scaling terms it is irrelevant. Hence, it is clear that the advantages associated with aiding a d-dimensional qudit-based computer with d'-dimensional ancillary qudits are reasonably limited. However, an argument in favour of such devices, and the qudit-aided proposals of Section 5.3.2 such as that for the generalised Toffoli gate, is that even relatively small efficiency savings may still be of practical utility - particularly in prototype quantum computers.

The advantages that QCV ancillas can provide for a qudit (or qubit) based quantum computer are less easily understood. However, there are certain conclusions that can be drawn. Perhaps the simplest way to understand why QCVs may have the potential to aid a computation (in theory, at least), is that they can employ intrinsically real-valued, rather than integer, arithmetic. E.g., for a set of n qudits, labelled $1, \ldots, n$, then an ancillary QCV can be mapped to the state $|r_1q_1 + \ldots r_nq_n\rangle$, where q_k is the computational basis state of the k^{th} qudit, and the r_k parameters are *real numbers*. Such arithmetic is fundamentally not available to a discrete-only encoding.[17] The conclusion that this real-valued arithmetic is key to any advantages associated with QCV ancillas may be further reinforced by the simple observation that, if the computation uses only controlled QCV Pauli gates with parameters that all have the form $2\pi q/k$ for some constant $k \in \mathbb{N}$ and integer values of q, then these operations may be simulated with a k-dimensional ancillary qudit. Hence, in such cases, there can be no benefits to using QCV ancillas, beyond those limited benefits associated with qudit ancillas. Furthermore, it is important to note that, in practice, any advantages that QCV ancillary systems can provide are likely to be illusionary to some degree: finite precision essential reduces a QCV to a discrete set of accessible states and operators. Adding further weight to this point of view is the observation that, if error correction is to be layered on-top of the ancillary system, then some discrete encoding of information into the QCVs will be essential (e.g., via the GKP encoding scheme of Gottesman et al. (2001)).[18] This is because error-correction of even a classical (logical) continuous variable appears not to be possible.

5.5 Physical implementation

In this penultimate section, the physical implementation of the gate methods that have been proposed throughout this chapter is discussed. Moreover, much of what follows will also be applicable to the models and gate methods introduced in the next two chapters. Consider the ancilla-register interaction Hamiltonian

$$\hat{H}^{\text{CZ}}_{r,a} = \hat{x}_r \otimes \hat{x}_a, \tag{5.47}$$

where the first system, denoted with a subscript r, and the second system, denoted with a subscript a, are a register and ancillary QV respectively. Note that the ancillary and register QVs may be of different types and, as in the previous section, the $\hat{x}$ operator is again the 'position' operator for a general QV (see Equation 3.21). It is easily confirmed that such a Hamiltonian, applied for a time t, generates the interaction gate

$$\text{C}^r_a R(-t) = \exp\left(-it\hat{H}^{\text{CZ}}_{r,a}\right), \tag{5.48}$$

[17] Encoding $r_1q_1 + \ldots r_nq_n$ into the QCV computational basis state $|r_1q_1 + \ldots r_nq_n\rangle$ is very different to possible encodings of this value into qudits or qubits, such as encoding it into a phase. For example, a qubit state can be easily created of the form $|0\rangle + e^{i(r_1q_1+\ldots r_nq_n)}|1\rangle$, but here the value of $r_1q_1 + \ldots r_nq_n$ is not physically accessible in the same sense as the QCV encoding, in which case this value has been mapped into orthogonal basis states. Orthogonal states can in-principle be distinguished with a one-shot measurement, whereas a continuous phase parameter cannot.

[18] Note that such quantum error correction of the ancillary systems would be necessary in a full-scale and fault-tolerant quantum computer *if* the ancillary systems are to remain entangled with the register for extended periods of the computation.

which for $t = 2\pi q/d_a$, with $q \in \mathbb{S}_{d_a}$, is the $CZ(-q)$ gate. Register-QV controlled $X(q)$ gates on the ancilla, and $CR(\theta)$ gates with positive $\theta \in \mathbb{R}$, can be generated from $CR(-t)$ gates (with $t \geq 0$) and local Fourier gates on the ancilla, via the relation given in Figure 2.5 and using the equality $F^2 R(\theta) F^2 = R(-\theta)$, respectively. Hence, the interaction Hamiltonian in Equation 5.47, augmented with local Fourier gates, is sufficient to implement all of the ancilla gate methods proposed in this chapter (although not the generalised Toffoli gate method of Ionicioiu et al. (2009)).[19]

In the context of qubits, or more general dimension qudits, 'position' and 'momentum' operators are not commonly used, and it is more conventional to consider 'spin' operators. A qudit of dimension d may be considered to be a spin $s = (d-1)/2$ particle, which has a Hermitian z-spin operator defined by[20]

$$\hat{S}_z = \begin{pmatrix} s & 0 & \cdots & 0 & 0 \\ 0 & s-1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -s+1 & 0 \\ 0 & 0 & \cdots & 0 & -s \end{pmatrix}. \tag{5.49}$$

Observe that, when $s = 1/2$, this reduces to the qubit Pauli Z operator (up to a factor of $1/2$) but this is not the case more generally as it is only for qubits that the Pauli operators are both unitary and Hermitian. Replacing the position operator, $\hat{x}$, with the z-spin operator, $\hat{S}_z$, in the Hamiltonian of Equation 5.47, when either the ancillary or register systems are qubits or qudits, will still generate the required interaction $CR(\theta)$, up to local rotation gates. Hence, this provides a perhaps more familiar Hamiltonian from a physics perspective, for generating the relevant interactions. E.g., for a qubit register and a QCV ancilla, this is the commonly encountered Hamiltonian

$$\hat{H} = \sigma_z \otimes \hat{x} = \sigma_z \otimes \frac{1}{\sqrt{2}}(\hat{a} + \hat{a}^\dagger), \tag{5.50}$$

[19] Moreover, for a QCV ancilla local controls (in the form of squeezing gates) allow the interaction time to be fixed to any non-zero value, as can be confirmed with reference to Figure 2.4. For qudits it may be fixed to an irrational multiple of π, or, if only those gate methods which use controlled Pauli operators are to be used, it may be fixed to $2\pi/d_a$. Obviously, an interaction time that is an irrational multiple of π is not something that can be achieved in practice - in the realistic setting of finite precision a fixed-time interaction is still sufficient, but a more careful analysis would be needed for how this should be fixed.

[20] That the z-spin operator is diagonal in the computational basis is essentially an arbitrary choice that has been made here, i.e., the particles spin eigenstates in the z-direction can be considered to define the computational basis. Defining the computational basis is always in a sense arbitrary, without the grounding of a specific physical context.

where the subscripts have been dropped for typographical simplicity, and with

$$\hat{a}^{\dagger} = \frac{1}{\sqrt{2}}(\hat{x} - i\hat{p}), \qquad \hat{a} = \frac{1}{\sqrt{2}}(\hat{x} + i\hat{p}), \tag{5.51}$$

which are termed the ‘creation’ and ‘annihilation’ operators, respectively. These operators will be preferred to the QCV position and momentum operators throughout this section, in keeping with the majority of the literature relevant here.

Before moving on to discussing physical systems in which interaction Hamiltonians of this form might be engineered or have been realised, because the Fourier gate on the ancilla is key in implementing the schemes discussed in this chapter without recourse to more than one ancilla-register interaction Hamiltonian, it is important to first discuss how this gate may be generated. It has already been mentioned in Section 2.2.1 that this is a particularly natural operator for a QCV. This is because it is generated by the quantum harmonic oscillator (QHO) hamiltonian

$$\hat{H}_{\text{QHO}} = \hat{a}^{\dagger}\hat{a} + \frac{1}{2}, \tag{5.52}$$

which is the free hamiltonian in a range of systems, such as micro-mechanical resonators [Poot and van der Zant (2012)] or single light modes [Gerry and Knight (2005); Radmore and Barnett (1997)].[21] As such, the Fourier gate is easily implemented in these settings (e.g., with a light mode, it may be implemented with a suitable length phase/time-delay).

In the context of qudits, Stroud and Muthukrishnan (2002) have claimed that the local Fourier gate is a particular natural unitary evolution in atomic systems. However, regardless of whether or not this is an especially straightforward gate to implement directly in the particular qudit-encoding physical system in question, it can always be composed from a small number of physically reasonable operations. In particular, any local gate on a qudit of dimension d can be composed from approximately d^2 operations that couple only two levels of the qudit at a time [Brennen et al. (2005)]. Moreover, the implementation-time overhead associated with this decomposition is reduced if these couplings can be implemented in parallel [O’Leary et al. (2006)], as may well be the case in some systems, e.g., with atoms multiple couplings can be achieved with additional control fields [O’Leary et al. (2006)]. Hence, implementing local Fourier gates on qudits can be considered to be relatively straightforward, at least in comparison to the inherent difficultly in achieving strong and high-quality couplings between physically distinct systems. This is supported by some impressive experimental progress on local gates in non-binary systems. E.g., $d = 16$ qudits encoded into the hyperfine structure of the electronic ground state

[21] See Appendix D for a derivation of the equality $F = e^{-3\pi i \hat{H}_{\text{QHO}}/2}$ and Appendix A for further discussions on the properties of the well-known QHO hamiltonian.

in the Caesium isotope ^{133}Cs have been demonstrated to be a particularly promising setting for non-binary quantum computation by Anderson et al. (2015); Smith et al. (2013), with Anderson et al. (2015) reporting high-quality local gates with an average fidelity of over 98%, as measured by randomised benchmarking. Having discussed local operations, we now turn back to two-QV interactions.

To begin, consider first the case in which either the ancillary or register systems are qubits. One common Hamiltonian, which it will be seen can generate appropriate gates to implement the methods of this chapter, is that of the Jaynes-Cummings model [Jaynes and Cummings (1963)]. This model describes the coupling of a qubit to a QHO, and (in the rotating wave approximation [Gerry and Knight (2005)]) is given by

$$\hat{H}_{\text{JC}} = \omega \left(\hat{a}^{\dagger}\hat{a} + \frac{1}{2} \right) + \frac{\Omega}{2} Z + g(\sigma_{-}\hat{a}^{\dagger} + \sigma_{+}\hat{a}), \tag{5.53}$$

where $\sigma_{+} = |0\rangle\langle 1|$ and $\sigma_{-} = |1\rangle\langle 0|$, ω is the frequency of the QHO, Ω is the frequency of the qubit, and g is the qubit-oscillator coupling strength. The Jaynes-Cummings model describes a wide range of physical systems, for example, qubit-oscillator couplings in a cavity [Shore and Knight (1993)] and circuit QED [Blais et al. (2004); Deppe et al. (2008)], and for a variety of qubit types coupling to mechanical oscillators [Gröblacher et al. (2009); Wallquist et al. (2009)]. In the dispersive limit ($g/\Delta \ll 1$ where $\Delta = \Omega - \omega$) of the Jaynes-Cummings model, $\hat{H}_{\text{JC}}$ may be shown to be approximated by [Blais et al. (2004)][22]

$$\hat{H}^{\text{disp}}_{\text{JC}} \approx \omega \hat{a}^{\dagger}\hat{a} + \left(\frac{\Omega}{2} + \frac{g^2}{\Delta} \right) Z + \frac{g^2}{\Delta} Z \otimes \hat{a}^{\dagger}\hat{a}. \tag{5.54}$$

Importantly, this limit of the Jaynes-Cummings model has been experimentally realised with a large enough coupling strength, g, to implement an entangling gate within the decoherence time of the system (referred to as the strong coupling regime) [Schuster et al. (2007); Wallraff et al. (2004)].

Clearly, a QHO naturally lends itself to a QCV encoding. However, one possible way to encode a d-dimensional qudit into a QHO is by using the first d energy eigenstates of the free QHO Hamiltonian (the eigenstates of $\hat{a}^{\dagger}\hat{a}$) as the qudits computational basis, often called the *number states*. With this encoding, the Jaynes-Cummings model describes a qubit-qudit coupling, and in particular, the dispersive limit Hamiltonian, given above, generates controlled rotations gates, $\text{C}R(\theta)$, and controlled Pauli $Z(q)$ gates, on this qubit-qudit pair (up to local rotation gates[23]).

[22] This can be derived by considering the conjugation transformation $\hat{H}_{\text{JC}} \to U\hat{H}_{\text{JC}}U^{\dagger}$, with U the unitary given by $U = \exp(\frac{g}{\Omega-\omega}(\sigma_{+}\hat{a} - \sigma_{-}\hat{a}^{\dagger}))$, and then expanding to first order in g/Δ.

[23] The single-system terms in the Hamiltonian of Equation 5.54 create only local gates on each system and do not effect the non-local gate implemented by this Hamiltonian, as they commute with the interaction term.

Interestingly, using the Jaynes-Cummings Hamiltonian to implement qubit-qudit interactions has been proposed elsewhere by Mischuck and Mølmer (2013) in the context of implementing qudit-based quantum computation via control-field pulse-sequence techniques. Alternatively, if we do not consider encoding a qudit into the QHO but instead treat it as a QCV, the dispersive limit of the Jaynes-Cummings Hamiltonian generates what may be termed qubit-controlled *phase-space rotations* on the QCV.[24] This is a different qubit-QCV interaction gate to the qubit-controlled QCV Pauli operators that have been considered throughout this chapter, and there are a range of interesting ancilla-based gate methods that have been developed that directly use interactions of this sort, e.g., see Louis et al. (2007); Munro, Nemoto, Spiller, Barrett, Kok and Beausoleil (2005); Proctor and Spiller (2012); Spiller et al. (2006). However, by multiple interactions and local controls of the QCV, controlled phase-space rotations may be converted into controlled QCV Pauli operators [Van Loock et al. (2008); Wang and Zanardi (2002)[25]], and hence these interactions may also be used for the gate methods discussed herein.

There are a range of physical systems and interactions, in addition to the Jaynes-Cummings model, that can provide suitable ancilla-register interactions for the methods given in this chapter. The qubit-controlled QCV Pauli operator is generated by the Hamiltonian of Equation 5.47 which can be realised in superconducting systems [Spiller et al. (2006); Wang et al. (2009); Xue (2012)]. This has been demonstrated experimentally, for example, a very recent experiment by Yoshihara et al. (2016) implemented such controlled QCV Pauli operators (called controlled phase-space displacements therein), and confirmed that they can create large amounts of entanglement between the qubit and QCV, as would be expected in the ideal case. In order to consider qudit-qudit or qudit-QCV couplings it is obviously necessary to go beyond couplings between single two-level systems and oscillators. One possible interaction, that is relevant to photonics, is the coupling between two oscillators given by

$$\hat{H}_{\text{KERR}} = \hat{a}^\dagger \hat{a} \otimes \hat{b}^\dagger \hat{b}. \tag{5.55}$$

This is often called the *cross-Kerr* Hamiltonian, and may be engineered using electromagnetically induced transparencies [Sun et al. (2008); Yang et al. (2009)], optical fibres [Li et al. (2005); Matsuda et al. (2009)] and cavity QED systems [Mücke et al. (2010); Zhu (2010)]. With qudits encoded into both of the QHOs this describes a

[24] In the literature, these are normally simply called controlled rotations. The addition of 'phase-space' to the name, is used herein to avoid confusion with $CR(\theta)$ gates, which are *not* the same as this gate.

[25] From Appendix D, it follows that $\exp(-3\pi i \sigma_z \hat{a}^\dagger \hat{a}/2) = e^{3\pi i/4}|0\rangle\langle 0| \otimes F + e^{-3\pi i/4}|1\rangle\langle 1| \otimes F^\dagger$. Using the relation $FZ(q/2)F^\dagger = X(-q/2)$, it may then be confirmed that $CX(q) = (\mathbb{I} \otimes X\,(q/2)) \cdot \exp(-3\pi i \sigma_z \hat{a}^\dagger \hat{a}/2) \cdot (\mathbb{I} \otimes Z\,(q/2)) \cdot \exp(+3\pi i \sigma_z \hat{a}^\dagger \hat{a}/2)$. See Van Loock et al. (2008) for a more general relation, which is not dependent on large controlled rotations, i.e., it may use $\exp(i\theta\sigma_z \hat{a}^\dagger \hat{a})$ gates with general $\theta \in \mathbb{R}$.

qudit-qudit coupling that implements a controlled $R(\theta)$ gate (if the encoding considered above is used). Moreover, this provides another method for implementing qubit-controlled phase-space rotations on a QCV ancilla, as discussed above, which may be achieved by encoding the qubit into the the lowest and first energy eigenstates of $\hat{a}^{\dagger}\hat{a}$, in which case $\hat{a}^{\dagger}\hat{a}$ is equivalent to the qubit position operator (for photons, this is encoding the qubit in terms of whether or not there is a photon in the mode). A further possibility was suggested by Ionicioiu et al. (2009) who proposed that qubit-controlled qudit Pauli operators may be realisable with a qubit encoded into a field mode and a qudit encoded into a spin $s = (d-1)/2$ particle interacting via the generalised Jaynes-Cummings (GJC) model in the dispersive limit, where the GJC model describes a coupling of a spin-s particle to a field mode analogous to that in the ordinary Jaynes-Cummings model. Alternatively, this model can obviously describe the coupling of a qudit with a qudit or QCV and in these cases it may also provide relevant interactions for the gate methods herein.

Qudits have been experimentally realised in a wide range of physical systems, including superconducting [Neeley et al. (2009)], atomic [Smith et al. (2013)] and photonic systems, where in the latter the qudit is encoded in the linear [Lima et al. (2011); Rossi et al. (2009)] or orbital angular momentum [Dada et al. (2011)] of a single photon. Hence, there are likely to be many further alternatives setting in which the gate methods considered herein will be relevant. One possible alternative encoding for a qudit is in the collective excitations of an ensemble of *qubits*. Such systems are an active area of research [Byrnes et al. (2012); Dooley et al. (2015, 2013); Lü et al. (2013); Ma et al. (2015); Marcos et al. (2010); Stanwix et al. (2010)] and experiments have been conducted in a range of physical settings, including ensembles of caesium atoms [Christensen et al. (2014)] and nitrogen-vacancy (NV) centres in diamond [Zhu et al. (2011)]. One appealing property of such N-qubit ensembles is that the coupling strength between these ensembles and other physical systems generically exhibits a $\sqrt{N}$ enhancement [Lukin (2003); Rabl et al. (2006)], providing a means for obtaining strong coupling even when the individual interactions are relatively weak. Qubit ensembles have been investigated as a possible long-life quantum memory for logical qubits [Lü et al. (2013); Marcos et al. (2010); Petrosyan et al. (2009); Rabl et al. (2006)], however, to my knowledge, encoding non-binary qudits into these systems has not been explored in detail and hence I now briefly outline how this might be achieved in a physically appealing manner.

Qubit ensembles are naturally described by the *collective spin operators*. Define the collective z-spin operator, for an ensemble of N qubits, by

$$J_z := Z_1 + Z_2 + \cdots + Z_N, \tag{5.56}$$

noting the implicit identity operators on the remaining $N-1$ qubits in each term of this sum. Collective J_x and J_y operators may be defined analogously (where the Y qubit operator may be defined as $Y = iXZ$), and using these, the *total spin* operator may be defined by $J^2 := J_x^2 + J_y^2 + J_z^2$. By showing that $[J_x, J_y] = 2iJ_z$, along with cyclic permutations, it follows that $[J^2, J_k] = 0$, for $k = x, y, z$. As these operators commute, an orthonormal basis for the total N-qubit Hilbert space can be found consisting of the joint eigenstates of J^2 and J_z, with these known as the *Dicke states* [Dicke (1954)]. The subspace of maximal total angular momentum (which is N), is spanned by the $N+1$ eigenstates of J_z in this subspace, given by

$$|n_D\rangle = \binom{N}{n}^{-1/2} \sum_{\text{perm}} \left|1^{\otimes(N-n)} 0^{\otimes n}\right\rangle, \tag{5.57}$$

with $n = 0, \ldots, N$, and where the sum is over all possible arrangements of the n excitations.[26] Hence, a $d = N+1$ dimensional qudit may be encoded into this subspace of the ensemble, with a convenient choice for the computational basis of the qudit given by these Dicke states, i.e., $\mathcal{B} = \{|n_D\rangle \mid n = 0, \ldots, N\}$. Because the states in this subspace are symmetric with respect to exchange of qubits, they are physically accessible by operations that act symmetrically on all the qubits, i.e., there is no need for individual qubit addressability.

To use a qudit encoded in this way for the gate methods proposed herein, or indeed, any useful quantum information processing, it is necessary to be able to couple such spin ensembles to either qubits, qudits or QCVs. Considering the gate methods herein, the spin-ensemble-encoded qudits may play the role of either computational or ancillary systems and, given the large coherence times of spin ensembles, they may be particular well-suited to providing long-life computational qudits. As already mentioned, ensemble-qubit couplings have already been proposed in the context of utilising the collective ensemble states as a quantum memory [Lü et al. (2013); Marcos et al. (2010); Petrosyan et al. (2009); Rabl et al. (2006)], with a computational qubit stored in the ground and first excited Dicke states. These proposals provide methods for interacting spin ensembles and qubits, suggesting that it may be possible to entangle qudits encoded into ensembles via ancillary qubits. More specifically, given the encoding discussed above, an interaction Hamiltonian of the form $\hat{H}_{\text{SE}} = Z \otimes J_z$ would be appropriate for implementing controlled rotation gates and controlled $Z(q)$ gates, as used throughout this chapter.[27] One specific physical system that may be relevant for this proposal is an ensemble of NV centers coupled to a superconducting flux qubit. Couplings of this sort have been proposed by Lü et al. (2013); Marcos et al. (2010) and experimentally realised by Zhu et al.

[26] The $|n_D\rangle$ state is the eigenstate of J_z with eigenvalue $2n - N$, i.e., $J_z|n_D\rangle = (2n-N)|n_D\rangle$.

[27] These gates are symmetric, so it is not necessary to specify which system is the control.

(2011). This setting has the advantage that the NV centers have an energy spectrum that may allow for gap-tuneable flux qubits to sequentially interact with the spin-ensemble by bring them into resonance in turn.

Alternatively, it might also be of interest to consider using this spin-ensemble-encoded qudit as an ancillary system for mediating gates and aiding computation on some register of qubits or qudits. The above discussions are also relevant in this case and in Proctor et al. (2015) we have proposed an alternative method for using such an ensemble as an ancillary system to mediate entangling gates on qubits via controlled '$SU(2)$ displacements'. Although linked to the ideas presented in this chapter, this gate method is notably different to the techniques used in the rest of this thesis and hence, in the aid of continuity, this has not been included in the main text and may instead be found in Appendix K. This appendix also provides a much more detailed introduction to the spin operators that have been used here.

5.6 Conclusions

To protect the quantum information in a quantum computation it is necessary for the computational QVs to have long coherence times, but to implement a useful computation it is essential to be able to implement high-quality entangling gates on these QVs. A naturally solution to fulfilling these competing requirements is to use highly-controllable, but perhaps short-lived, ancillary systems to mediate the interactions between well-isolated QVs in a computational register. Moreover, as discussed in Section 5.1, there are a range of additional advantages associated with implementing quantum computation in this fashion, e.g., if the ancillas are highly mobile (e.g., states of light), they may be used to implement gates between distant computational QVs in some static array (e.g., a 2D square lattice, or linear array) without any overheads. In this chapter, ancilla-mediated *geometric phase gates* have been proposed and investigated. These two-QV entangling gates, introduced in Section 5.2, are implemented on a pair of computational QVs via a sequence of controlled Pauli operators acting on a target ancilla, which may be of a different QV type to the register systems. The particular case of this gate with computational qubits mediated via ancillary QCVs has been considered previously in literature, e.g., see Louis et al. (2008); Milburn (1999); Munro, Nemoto and Spiller (2005); Spiller et al. (2006), and is often called 'qubus' computation. However, the construction given here applies to computation with more general QV types and where the ancillas can be qubits, qudits or QCVs: to my knowledge it is novel in all cases outside the qubit-QCV setting.

The ancilla-mediated geometric phase gate, when augmented with local gates on the computational systems, is sufficient to implement any quantum computation.

As such, any quantum circuit can be decomposed into a sequence of these basic gates. However, by adapting the gate to keep some register systems entangled with the ancilla for extended periods of the computation, it was shown in Section 5.3 that the number of ancilla-register interactions required to achieve certain unitaries may be reduced. These ideas have been developed previously in the 'qubus' sub-case (i.e., qubit register, QCV ancillas), by Brown et al. (2011, 2012); Horsman et al. (2011); Louis et al. (2007) and, in particular, Brown et al. (2011) have given a method for implementing the quantum Fourier transform (QFT) on a qubit register with a reduced number of gates. However, in Section 5.3.1 it was shown that this method for implementing the QFT requires exponential time, and as such, is much worse than the ordinary decomposition of the QFT. Highly efficient methods for implementing a range of modulo-arithmetic based gates, via a qudit ancilla, were then developed in Section 5.3.2, including a simple scheme for implementing generalised Toffoli gates (on qubits). Furthermore, in Section 5.4, the links between these gate methods and full hybrid quantum computation were investigated and finally, in Section 5.5, the possibilities for the physical implementation of these gate methods were discussed.

The analysis throughout this chapter has assumed that all operations are performed perfectly and no decoherence is present. In any physical realisation of ancilla-based gates this will not be the case, hence an interesting extension of this work would be to assess the impact of physically realistic noise and gate errors to the operation of the geometric phase gate and its extensions. In the previously studied 'qubus' model this has already been considered by Louis et al. (2008), in the context of a photonic ancilla and photon losses during the gate implementation, and they have shown that high fidelity computations can still be achieved in the presence of moderate dissipation. It seems likely that similar considerations will carry over to the further gate methods introduced herein, although the relevant decoherence mechanisms will be depend on physical systems in question. The circuit-size reducing techniques proposed in this chapter rely on many computational QVs being entangled with an ancillary system simultaneously, and hence, any errors on this ancilla may cause correlated errors on these QVs. Such correlated errors can cause problems for quantum error-correction [Terhal (2015)] and there will then be a trade-off between reducing gate counts and introducing these problematic errors. For the 'qubus' case this optimisation has been considered by Horsman et al. (2011), confirming that gate-count reductions of this sort may indeed prove useful in practice. Again, it is likely that similar results hold for the more general gate methods introduced herein and a careful analysis of this would also be interesting to investigate in the future.

One unfortunate feature of the geometric phase gate is that each QV involved in the gate must interact with the ancilla twice, which in some settings may be particularly inconvenient (e.g., a ‘flying’ ancilla implementing a gate on distant QVs). This then provides one motivation for the ancilla-based model proposed in the next chapter, which minimises the required number of interactions per gate to a single interaction with each computational QV. This model will employ gate methods that are closely related to the geometric phase gate and it will also be seen to have many similarities to the one-way quantum computer (1WQC). Hence, it will provide an interesting conceptual link between the ideas in this chapter and the 1WQC.

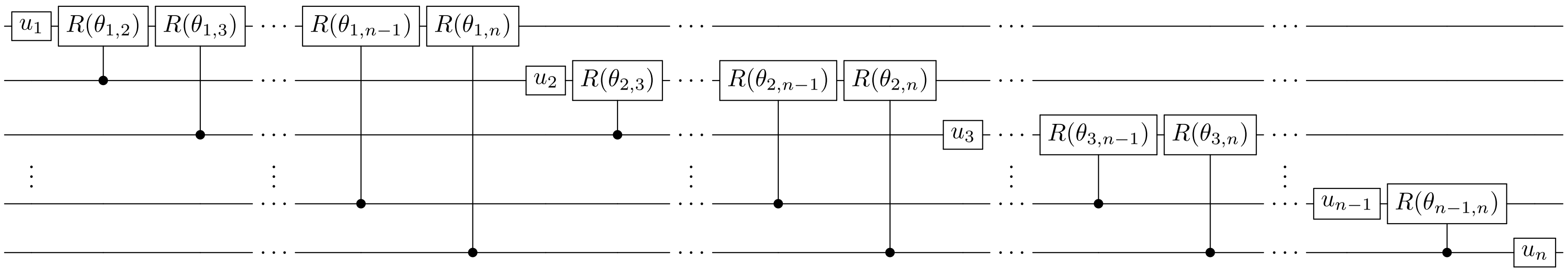


Figure 5.10: A quantum circuit acting on n qudits of dimension d and implementing a QFT-like unitary. The special case of $u_k = F$ for all k and $\theta_{j,k} = 2\pi d^{j-k-1}$ is the QFT modulus d^n. The $R(\theta)$ gate is a scalar-parameterised rotation defined by $R(\theta)|q\rangle = e^{iq\theta}|q\rangle$. This circuits has a size of $O(n^2)$ and a depth of $O(n)$ if controlled rotations on distinct qudits are paired suitably.

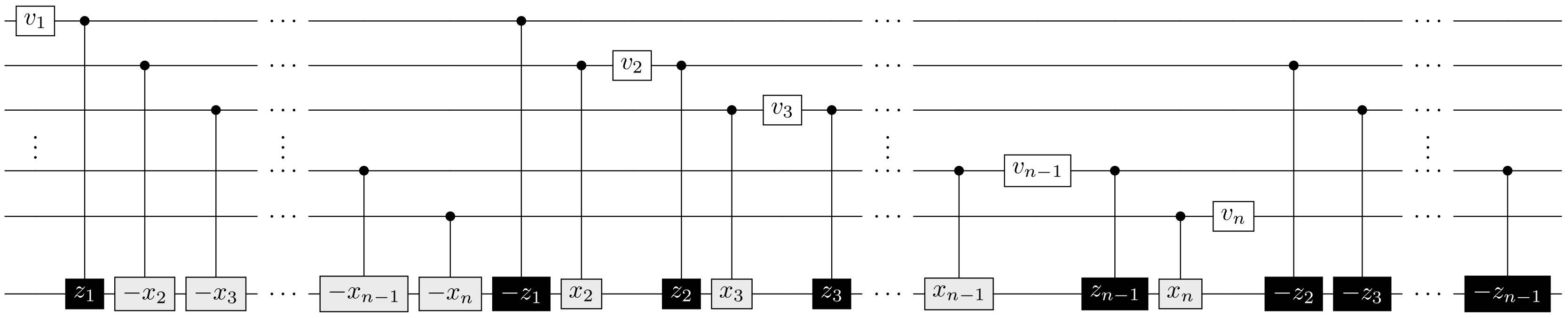


Figure 5.11: An ancilla-mediated sequence that implements a QFT-like circuit on a register of d-dimensional qudits. A circuit representation of the unitary this induces on the register is shown in Figure 5.10, where the phase parameters and local gates therein are related to those of this circuit via $\theta_{j,k} = 2\pi z_j x_k / d_a$ and $u_k = v_k$, where d_a is the dimension of the ancilla. For a QCV ancilla and with $z_j = 2\pi d^{j-1}$, $x_k = d^{-k}$ and $v_k = F$ for all k, this circuit implements the QFT with modulus d^n on the n-qudits. This circuit contains $4(n-1)$ ancilla-register interaction gates, as each register qudit interacts with the ancilla four times except qudits 1 and n, which interact with the ancilla only once. Hence, this circuit has a size of $9n-8$ and a depth of $5n-4$.

Chapter 6

Quantum computation driven by measurements of ancillas

In this chapter a model of quantum computation for general quantum variables is proposed in which universal quantum computation is implemented on a register using *only*: repeated applications of a single fixed two-body ancilla-register interaction gate, ancillas prepared in a single state, and variable basis measurements of these ancillas. Driving the computation via measurements of the ancillas introduces a fundamentally probabilistic aspect to the computation, but step-wise determinism can be maintained via classical feed-forward of measurement outcomes in a similar fashion to the general quantum variable one-way quantum computer (1WQC), which was investigated in Chapter 4. A method for simulating the 1WQC within this model is provided, which is used to demonstrate that the hybrid quantum-classical advantages of 1WQC are also inherent in the model presented here, including the ability to implement any Clifford gate in constant depth. Hence, the model proposed here not only requires highly limited physical controls but is also powerful for parallel quantum computation. The links between this model and the geometric phase gate of the previous chapter are explored and an adaptation of the model to globally unitary dynamics is given. The main measurement-based model presented in this chapter is novel in the case of non-binary qudits and QCVs, with the qubit subcase previously proposed by Anders et al. (2010); Kashefi et al. (2009), and the adaptation of this model to unitary dynamics given herein is novel in all cases. This chapter is based upon Proctor et al. (2013); Proctor and Kendon (2015).

6.1 Introduction

Decoherence is the major obstacle that is currently preventing the realisation of a useful quantum computer. In order to minimise the destructive effects of decoherence it is essential that each quantum variable in the register of a quantum computer is isolated as effectively as possible. Indeed, this is the key motivation for the development of ancilla-based techniques for quantum computation, as they remove the necessity for direct interactions between the register QVs, allowing them to be more effectively isolated. Continuing in this line of thought, it is well-motivated to consider ways in which the access needed to the register, in order to implement universal quantum computation on it, can be further reduced to a minimum. This is the subject of both this and the next chapter.

One perspective on minimising access to the register might be to try and minimise the total number of operations, or perhaps only the number of two-body gates, that need to be applied to the register in a particular quantum computation. This can be understood in terms of decomposing algorithms into an operation sequence (i.e., a sequence of gates and possibly measurements) over some operation set with a minimal computational size. In both this and the next chapter an alternative perspective is considered in which the number of different operations in the basic operations set is to be minimised. More precisely, as the priority is optimising the computational register for long coherence times, it is of utmost importance to minimise the number of operations in the basic set that *act on register systems*, leaving the possibility of manipulations on the ancillas to compensate for such restricted access to the register. Motivated by this, in both this and the next chapter, general quantum variable models will be proposed that require *only* a single fixed two-body ancilla-register interaction gate, along with certain controls on individual ancillas, for universal quantum computation on the register. Quantum computation with a scheme of this sort then allows the register systems to be optimised for long coherence times, with only a single fixed two-body gate needing to be engineered.

In the interests of physical simplicity, it is also natural to minimise the number of interactions between an ancilla and a pair of register elements required to implement an entangling gate. It is obviously necessary for the ancilla to interact with each register QV at least once and it will be seen that this minimum is indeed possible - with the aid of single-party measurements on the ancillas. To be more specific, the main model that is proposed and studied in this chapter will require *only* a single two-body ancilla-register interaction gate, ancillas prepared in a fixed state, and measurements of the ancillas in a variable basis, and furthermore, each entangling gate will be implemented via sequential interactions of an ancilla with the pair of register QVs on which it is to act. This model can be understood as an extension, to the setting of general QVs, of the qubit-based *ancilla-driven quantum computation* (ADQC) model developed by Anders et al. (2010) and Kashefi et al. (2009). For this reason, the same name will be used for the more general model proposed herein, which is introduced in Section 6.2.

Measurement outcomes are fundamentally probabilistic, hence the measurements on the ancillas must create errors in the computation. However, it will be shown that the ADQC model may achieve (step-wise) determinism via adapting measurement bases using classical feed-forward of previous measurement results, in direct analogy to the 1WQC investigated in Chapter 4. It will then be shown that the general QV 1WQC may be embedded inside the ancilla-driven model proposed herein. In particular, this will be used to demonstrate that the parallelism of the 1WQC is also available in ADQC. Hence, this ADQC model is not only interesting from a physical perspective, but also because it has access to a level of parallelism which is not present in any purely gate-based globally-unitary scheme (which uses only bounded input-size gates).

General variable-basis measurements may well be challenging in practice, particularly in the case of QCVs. Hence, in Section 6.3 sets of measurements which are sufficient to guarantee that the model may implement universal quantum computation are discussed - it will be shown that for the QCV-based model, with ancillas realised as optical states, homodyne detection and photon-number counting on these ancillas is sufficient for universality. In Section 6.4 a range of adaptions to the ADQC model are presented, including a proposal for an alternative ancilla-based model of quantum computation which removes the need for high-quality measurements of each ancilla at the cost of now requiring local unitary gates *on the ancillas*. To be precise, to achieve universal quantum computation this alternative model requires only a fixed ancilla-register interaction gate, ancillas prepared in a single state, and access to a universal set of single-QV gates which need act only on the ancillas. As such, this model provides a globally unitary counterpoint to the measurement-based ADQC model and may be of relevance in physical settings in which high-quality measurements are not available. In the interests of clarity, the constraints of the models in this chapter and how they compare to both the gate methods of the previous chapter and those that will be introduced in the following chapter have been summarised in the thesis overview, on pages 2-3 of this thesis: the reader is referred there for a concise summary of the different ancilla-based models herein.

6.2 Ancilla-driven quantum computation

To begin, the main model of study in this chapter is introduced. This model is defined on general quantum variables, and as already noted in the introduction, this will include as the qubit sub-case the so-called *ancilla-driven quantum computation* (ADQC) model which was introduced by Anders et al. (2010) and Kashefi et al.

(2009).[1] For this reason, the more general model proposed here will also be referred to by this term. This 'ADQC' model provides an ancilla-based method for implementing deterministic universal quantum computation on a register of QVs using only a fixed ancilla-register interaction gate, ancillas prepared in a fixed state, and single-party measurements on the ancillas, where the ancillas are of *the same QV type* as the register QVs.

It is clearly necessary to carefully chose the ancilla-register interaction, as universal quantum computation will not be possible in this fashion with just any fixed two-QV gate (e.g., it must be entangling), as discussed again later. Furthermore, it is also important to consider which measurements will be permissible in the model, as they will not all be equally difficult in practice, and hence, it is preferable if these are as limited as possible. Specifically, consider:

1. The fixed ancilla-register interaction gate, $\check{E}_{ar}$, defined by $\check{E}_{ar} := F_r F_a^{\dagger} \mathrm{C}_a^r Z$.

2. Measurements on ancillas of the operators $\hat{x}$ and $\hat{x}_{FR(\vartheta)}$, for variable phase-function $\vartheta : \mathbb{S}_d \to \mathbb{R}$.

3. The fixed ancilla preparation state, $|+_0\rangle$.

The exact measurements allowed will be restricted no further than this at this point - which measurements are necessary for universality will be discussed again later. Note that, as in the previous chapter, a subscript a will be used to refer to an ancillary QV and other subscripts to refer to register QVs. Furthermore, here a measurement of the Hermitian operator $\hat{x}_u$ has been used, which is defined by

$$\hat{x}_u = \sum_{q \in \mathbb{S}_d} q \left(u^{\dagger} |q\rangle\langle q| u \right) = u^{\dagger} \hat{x} u, \tag{6.1}$$

as already introduced in Equation 4.8, where $\hat{x} = \sum_{q \in \mathbb{S}} q |q\rangle\langle q|$ is the general QV 'position' operator. Finally, note that $R(\vartheta)$ with $\vartheta : \mathbb{S}_d \to \mathbb{R}$ is the gate used throughout Chapters 3 and 4 and defined in Equation 2.58 as $R(\vartheta)|q\rangle = e^{i\vartheta(q)}|q\rangle$.

6.2.1 A universal gate set on the register

It is now shown how universal quantum computation can be implemented in this 'ADQC' model. It is simple to confirm, via the equality $Z(q)|+_0\rangle = |+_q\rangle$, that the action of the fixed interaction, $\check{E}_{ar}$, on a register QV in the state $|q\rangle$ and an initialised ancilla is

$$|q\rangle|+_0\rangle \xrightarrow{\check{E}_{ar}} |+_q\rangle|q\rangle. \tag{6.2}$$

[1] The qubit sub-case of the model herein is the same as the model of Anders et al. (2010) and Kashefi et al. (2009) up to a very minor alteration, which is noted later.

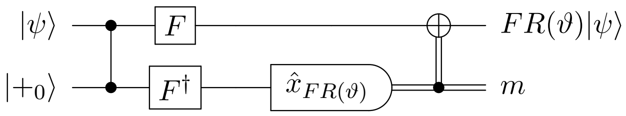


Figure 6.1: Any $FR(\vartheta)$ gate may be implemented on a register QV, via an interaction with an ancilla prepared in the state $|+_0\rangle$, using the fixed gate $\check{E} = (F \otimes F^\dagger) \cdot \textsc{cz}$ followed by a measurement of the ancilla in the ϑ-parameterised basis $\mathcal{B}_{FR(\vartheta)}$. The intended gate is followed by a probabilistic error gate $X(-m)$, where m is the measurement outcome. This error may be removed with local controls, as shown here, or instead it may be accounted for via feed-forward, as will be shown in the main text.

Hence, an interaction of a register QV with an ancilla will delocalise a logical QV in the register over the two physical QVs. Therefore, any subsequent manipulations (i.e., gates or measurements) on the ancilla will implement transformations on the logical QV, and measurements of the ancilla will destroy this delocalisation. It is this delocalisation which enables the following universal gate set implementation.

Local single-QV gates can be implemented via a measurement in almost exactly the same fashion as in the 1WQC, which was covered in detail in Section 4.3. In particular, after an ancilla-register interaction, a measurement on the ancilla of the operator $\hat{x}_{FR(\vartheta)}$ implements the gate $FR(\vartheta)$ on the register QV up to a Pauli error of $X(-m)$, where $m \in \mathbb{S}_d$ is the measurement outcome. Formally, this gate method is confirmed to act on the register as claimed by showing that

$$\frac{\langle m|F_a R_a(\vartheta)\check{E}_{ar}|+_0\rangle}{\|\langle m|F_a R_a(\vartheta)\check{E}_{ar}|+_0\rangle\|} = X_r(-m)F_r R_r(\vartheta). \tag{6.3}$$

A more detailed derivation is not given as it follows in a very similar fashion to the 1WQC teleportation calculation of Section 4.3. This gate method is summarised in the quantum-classical circuit diagram of Figure 6.1 which explicitly corrects for the error. However, as with the 1WQC, it will be shown in Section 6.2.2 that these errors do not need to be directly corrected for - which would require local gates on the register, which have been assumed to be unavailable in this model - and can instead be accounted for with classical feed-forward. Gates of the form $FR(\vartheta)$ are sufficient for implementing any single-QV gate for all types of QV, as discussed in Section 2.5.

In order to elevate any set of universal single-QV gates to full universality, all that is necessary is a method for implementing some entangling gate (see Proposition 2.2), hence it is only now required to show how such an entangling gate may be applied to the register via an ancilla. Sequential interactions between an ancilla and two register QVs, r and s, followed by a computational basis measurement of the ancilla implements such an entangling gate on this pair of register QVs.[2] This is because, if the QVs r and s are in the states $|q\rangle$ and $|q'\rangle$ respectively, then, with reference to Equation 6.2 and using $F^{\dagger}|n\rangle = |+_{-n}\rangle$, it follows that

$$|q\rangle_r|q'\rangle_s|+_0\rangle \xrightarrow{\check{E}_{as}\check{E}_{ar}} \omega^{qq'}\left|+_q\right\rangle_r\left|+_{q'}\right\rangle_s|+_{-q}\rangle. \tag{6.4}$$

Note that the $\omega^{qq'}$ phase is exactly the phase that would by created by a CZ gate acting on these two register QVs. Therefore, given that the measurement outcome is $m \in \mathbb{S}_d$, the gate implemented after the ancilla has been measured may be confirmed to be

$$\frac{\langle m|\check{E}_{as}\check{E}_{ar}|+_0\rangle}{\|\langle m|\check{E}_{as}\check{E}_{ar}|+_0\rangle\|} = X_r(m)\tilde{E}_{rs}, \tag{6.5}$$

where $\tilde{E}_{rs}$ is the symmetric entangling gate given by

$$\tilde{E}_{rs} = F_r F_s \mathrm{C}^r_s Z. \tag{6.6}$$

Notice that the phase that creates the CZ gate (i.e., the $\omega^{qq'}$ factor) is not obtained from the measurement-induced phase. The role of the measurement is simply to relocalise the logical QV, which is achieved via a measurement in a basis which reveals no information about which conjugate basis state the ancilla was in. A circuit diagram of this gate method is given in Fig. 6.2, where again the measurement-induced error is explicitly corrected for.

6.2.2 Adaptive measurements for determinism

It has now been shown that the gate methods given in Figures 6.1 and 6.2 are sufficient to implement (step-wise) deterministic universal quantum computation on the register using the fixed ancilla-register interaction $\check{E}$, along with ancilla preparation and measurement, *if* local corrections can be applied to the register after each gate. Moreover, it is now shown how these errors can be accounted for without local controls via a simple classical feed-forward process that uses classical computation and some adaptive measurements, with the technique analogous to that for the 1WQC

[2] Here there is one minor difference between the model herein in the qubit sub-case and the qubit-based model of Anders et al. (2010) and Kashefi et al. (2009). Specifically, the measurement basis for the entangling gate is not the same, with Anders *et al.* using a measurement in the basis constructed from the eigenstates of the Pauli operator $Y = iXZ = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$. Implementing the entangling gate in the general QV model herein with a measurement in a basis which is an extension of this is possible (see the 'phase basis' introduced in Section 7.4.1, which consists of the eigenstates of $Y = \omega^{(1+\varrho_d)/2}XZ$, defined for a general QV). However, the mathematical details are substantially more complicated and as this is unnecessary it is therefore avoided.

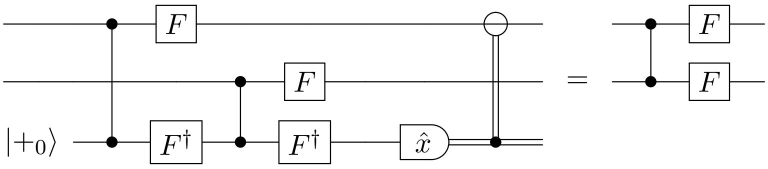


Figure 6.2: Sequential interactions between an ancilla and two register QVs, using the fixed ancilla-register gate $\breve{E} = (F \otimes F^\dagger) \cdot \textsc{cz}$, followed by a computational basis measurement of the ancilla may be used to implement an entangling gate $\tilde{E} = F \otimes F \cdot \textsc{cz}$ on the register up to a probabilistic $X(m)$ error, where $m \in \mathbb{S}_d$ is the measurement outcome. This error may be removed via a classically-controlled local $X(-m)$ gate, as shown here, or may be accounted for using feed-forward and adapting later measurement bases.

given in Chapter 4. One method for achieving this would be to introduce ADQC 'measurement patterns' and then give an ADQC 'standardisation procedure' in a very similar manner to the work for 1WQC in Section 4.4. However, a less formal approach is taken here, which in my opinion is more helpful for gaining an understanding of the ADQC model.

Consider an n-QV computational register and write the state it is in as $p_{\zeta,\vec{v}}|\psi\rangle$, where $p_{\zeta,\vec{v}} = \omega^{\zeta/2} X_1(v_1) Z_1(v_{n+1}) \dots X_n(v_n) Z_n(v_{2n})$ as defined in Equation 2.47. In other words, the register is in the state $|\psi\rangle$, up to Pauli errors on all of the QVs (and a global phase). It will be useful to let the elements of the vector $\vec{v}$ be denoted $\vec{v} = (x_1, \dots, x_n, z_1, \dots, z_n)^T$, as then the error on k^{th} QV is $X_k(x_k) Z_k(z_k)$. It is now shown how, given the vector $\vec{v}$, we may implement either of the two mappings

$$p_{\zeta,\vec{v}}|\psi\rangle \to p_{\zeta',\vec{v}'} F_r R_r(\vartheta)|\psi\rangle, \qquad p_{\zeta,\vec{v}}|\psi\rangle \to p_{\zeta',\vec{v}'} \tilde{E}_{rs}|\psi\rangle, \tag{6.7}$$

for any register QVs r and s, using the available operations in ADQC - and hence *without* recourse to directly implementing local gates on the register. Furthermore, it is also shown how the new Pauli error vector $\vec{v}'$ may be calculated in each case, using simple classical side-processing. By repeated applications of these processes it is then possible to deterministically implement any quantum computation (by decomposing it into $\tilde{E}$ and $FR(\vartheta)$ gates) up to final Pauli errors on each QV. Pauli errors on the final output state can then be accounted for in classical post-processing of final measurement outcomes (or absorbed into further computations). Note that the natural way to think of the vector $\vec{v}$ is as $2n$ classical variables (CLVs) which computations are implemented on in parallel to the quantum computation on the n QVs.

First consider the case when the aim is to apply an $\tilde{E}_{rs}$ gate to the r and s

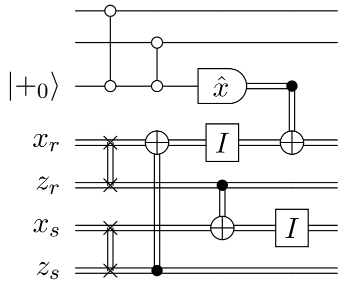
QVs in the register. By implementing the procedure of Equation 6.5, or Figure 6.2 *without* the explicit correction, the actual gate implemented is $X_r(m)\tilde{E}_{rs}$, where m is the outcome of the measurement on the ancilla. Now, as the entangling gate $\tilde{E}$ is Clifford, the Pauli errors on r and s may simply be commuted past $\tilde{E}$ whilst remaining Pauli errors (of a different form). Specifically, the relation is

$$\begin{aligned} &X_r(m)\tilde{E}_{rs}X_r(x_r)Z_r(z_r)X_s(x_s)Z_s(z_s) = \\ &\qquad \omega^{-(x_r x_s + x_r z_r + x_s z_s)} X_r(m - z_r - x_s)Z_r(x_r)X_s(-z_s - x_r)Z_s(x_s)\tilde{E}_{rs}, \end{aligned} \tag{6.8}$$

which is found via Equations 2.51 and 2.53. Using this relation, the procedure to keep track of these errors upon application of an $\tilde{E}$ gate simply requires an updating of the CLVs associated with QVs r and s (i.e, four elements from $\vec{v}$). Specifically, for measurement outcome m, the classical computation required is

$$(x_r, x_s, z_r, z_s) \to (m - z_r - x_s, -z_s - x_r, x_r, x_s), \tag{6.9}$$

which can be achieved with classical SUM, SWAP and inversion ($x \to -x$) gates.[3] To clarify this process, it may be written as a quantum-classical circuit which acts on two register QVs, one ancillary QV and four CLVs. Specifically, this process to implement $\check{E}$ and update the classical CLVs is summarised with the circuit



where the first and second quantum wires represent the r and s QVs respectively, a register QV connected to an ancilla with '$\circ$' symbols denotes the fixed ancilla-register interaction $\check{E}$, a box containing I denotes the inversion operator $x \to -x$, and wires connected via a line and '$\times$' is the standard notation for the SWAP gate, which maps $(x, z) \to (z, x)$. Using a further CLV, it would be possible to keep track of the change in the global phase at each stage of the computation, but such phases are of no physical consequence and as such this may be ignored.

Consider now the second scenario, whereby the aim is to apply a $FR(\vartheta)$ on one of the QVs, for some $\vartheta : \mathbb{S}_d \to \mathbb{R}$. The Pauli $X(x)$ maps $|q\rangle \to |q + x\rangle$, and hence,

[3] As always, $-x$ is taken modulo d for dits.

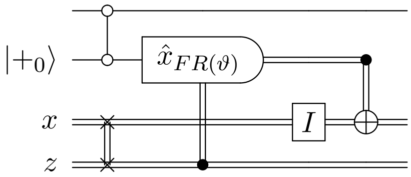
by taking ϑ_x to be the x-adapted phase-function with $\vartheta_x(q) = \vartheta(q+x)$, then

$$X(-m)FR(\vartheta_x)X(x)Z(z) = \omega^{-xz}X(-z-m)Z(x)FR(\vartheta), \tag{6.10}$$

where this has used the conjugate relations for F on Pauli operators, given in Equation 2.26. Hence, to implement this gate on the r^{th} QV without recourse to local corrections, the measurement of the ancilla should be of the x_r-adapted operator $\hat{x}_{FR(\vartheta_{x_r})}$, so that the $X(-m)FR(\vartheta_{x_r})$ gate is implemented on the register, with m the measurement outcome. Hence, this procedure implements the intended $FR(\vartheta)$ gate, and the CLV update required is

$$(x_r, z_r) \to (-z_r - m, x_r), \tag{6.11}$$

where m is the outcome of the measurement of the ancilla. This may also be written as the quantum-classical circuit module

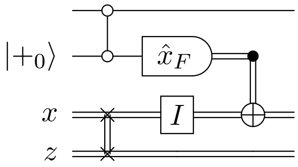


where the adaption to the measurement basis is shown schematically via the classical control wire to the measurement device.

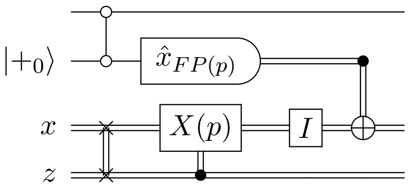
For exactly the same reasons as with the 1WQC, when the $FR(\vartheta)$ operator is a Clifford gate then the dependencies can be removed from this procedure - at the cost of further classical computation. The error up-date procedures for the F and $FP(p)$ gates on the r^{th} QV, when no classical control is used, can be found from Equations 2.51 and 2.52, to be

$$(x_r, z_r) \xrightarrow{F} (-z_r - m, x_r), \qquad (x_r, z_r) \xrightarrow{FP(p)} (-z_r - px_r - m, x_r), \tag{6.12}$$

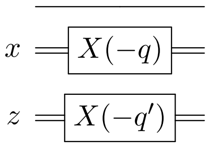
respectively. When written as quantum-classical circuit modules, the Fourier gate is implemented via the circuit



and the Fourier-phase gate, $FP(p)$, is implemented via the circuit



Finally, it is interesting to note that $Z(q)$ and $X(q)$ gates can be implemented with only classical processing, e.g., to implement the gate $X_r(q)Z_r(q')$ gate simply map the CLVs for the r^{th} QV as $(x_r, z_r) \to (x_r - q, z_r - q')$. Written as a circuit module this is the almost trivial circuit



As has already been stated many times in this thesis, CZ, F, $FP(p)$ and $Z(q)$ are sufficient to implement any Clifford gate (see Proposition 2.1), hence, as methods for implementing these operators have been given which require no classically-adapted measurements, then no measurement dependencies are required for any Clifford gates. This should not be surprising given the closely related analysis of the 1WQC in Chapter 4.

6.2.3 Simulating the one-way quantum computer

The analysis given above does not immediately imply that Clifford gates can be implemented in constant depth on the register. For example, consider the obvious procedure for implementing a sequence of m single-QV Clifford gates on one register QV, which uses m ancillas which must each be entangled with the register QV and can only be implemented sequentially.[4] Despite this, the ADQC model does contain exactly the same parallel power as the 1WQC (and therefore also the parallel power of unbounded fan-out circuits). As such, it can implement any Clifford unitary in constant depth - which is just one of the parallel features of the 1WQC (see Chapters 3 and 4). The way that I will show this is by providing a method for simulating any 1WQC using ADQC with only a constant increase in computational depth. In the following, it will be assumed that the measurement bases available in each model are equivalent in the sense that they allow the implementation of the same set of $FR(\vartheta)$ gates, i.e., the same phase-functions $\vartheta : \mathbb{S}_d \to \mathbb{R}$. This is a natural assumption to ensure that the models being compared use similar resources.

[4] Although the analysis of the previous section does imply that all the ancillas could all be measured simultaneously after they have been entangled with the register QV in sequence.

Proposition 6.1. *Any ADQC computation, $\mathfrak{A}$, can be simulated by a 1WQC measurement pattern, $\mathfrak{P}$, that has a depth of $O(depth(\mathfrak{A}))$. Any 1WQC measurement pattern, $\mathfrak{P}$, can be simulated by a ADQC computation, $\mathfrak{A}$, that has a depth of $O(depth(\mathfrak{P}))$.*

Proof: Consider any computation in the ADQC model. The allowed operations in ADQC are a Clifford entangling gate, $\check{E}$, single-QV measurements (of the ancillas) which are either computational basis measurements, or equivalent to $FR(\vartheta)$ gates (for some set of ϑ functions) followed by computational basis measurements, where ϑ may in general be classically adapted by a sum of measurement outcomes, constants, and measurement outcomes multiplied by constants. By proposition 4.3, such a model can be simulated in the 1WQC with no scaling increase in depth, i.e., there is a measurement pattern $\mathfrak{P}$ for any ADQC computation $\mathfrak{A}$ such that $\mathfrak{P}$ has a depth of $O(\text{depth}(\mathfrak{A}))$. This proves the first part of this proposition.

Without loss of generality, consider a completely standard measurement pattern $\mathfrak{P} = (\mathcal{V}, \mathcal{I}, \mathcal{O}, \mathfrak{p})$, which consists of a sequence of entangling operations (which are CZ gates), followed by a sequence of measurements, and finally a set of corrections on the output QVs (see Section 4.4, and Chapter 4 more generally, for further details on completely standard measurement patterns). Treat the total set of QVs in the measurement pattern, $\mathcal{V}$, as the register in ADQC (i.e., this includes any auxiliary QVs in the measurement pattern), and ancillas will be used to drive 1WQC on this register. All register QVs which are not inputs to the pattern ($\mathcal{V} \setminus \mathcal{I}$) must be initialised to $|+_0\rangle$. If they cannot be prepared directly in this state, this can be achieved via ancilla-driven F gates on QVs prepared in $|0\rangle$, which are the conventional auxiliary states in the quantum circuit model[5], and this requires only constant depth. The entangling stage of the measurement pattern consists of layers of CZ gates on distinct QVs. The CZ gates in each layer can be implemented (up to Pauli errors) in constant depth, as $\text{CZ} = F^3 \otimes F^3 \cdot \tilde{E}$ and all measurements of ancillas to implement these gates have no dependencies. Hence, the entire entangling stage can be implemented with only a constant increase in depth (of at most six) in comparison to that stage of the measurement pattern. Note that the entangled state created here is only equivalent to that created in the measurement pattern up to Pauli corrections on each QV (due to the measurements of the ancillas). These may be accounted for via additional changes to the following stage, which simulates the dependent and independent measurements in the measurement pattern, but will not add any increase in depth as these measurement outcomes are obviously already known at the end of this stage.

It is now shown how to simulate the measurement stage of the measurement

[5] The preparable auxiliary states of the main register in the ADQC model has not been specified, but it is perhaps natural to restrict them to the $|0\rangle$ state.

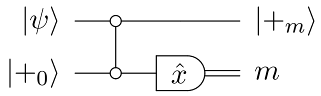


Figure 6.3: A computational basis measurement of a register QV may be simulated via an interaction with an ancilla, followed by a computational basis measurement of this ancilla. The register QV is projected onto $|+_m\rangle$, but if it is discarded, this is irrelevant.

pattern. The key to this is introducing a method for driving the non-unitary measurement dynamics on the register via ancillas. All of the measurements in the measurement pattern are of the operator $\hat{x}_{FR(\vartheta)}$, where ϑ may be classically adapted, and hence there may be a time-ordering induced by these dependencies. Hence, to simulate this in ADQC, it is necessary to be able to implement these measurements on any register QV using only the operations allowed in ADQC. A measurement of $\hat{x}_{FR(\vartheta)}$ on register QV is equivalent to $FR(\vartheta)$, where ϑ may have dependencies, followed by a computational basis measurement. A local $FR(\vartheta)$ gate is easily applied via an ancilla, using the method of Equation 6.3. A computational basis measurements on a register QV can be simulated by interacting the register QV to be measured with an ancilla and then measuring *the ancilla* in the computational basis. This is because

$$\| \langle m|_a \check{E}_{ar} |\psi\rangle_r |+_0\rangle_a \| = |\langle m|\psi\rangle|, \tag{6.13}$$

which may be confirmed from Equation 6.2. Hence, a post-interaction measurement of the ancilla is equivalent to a (non-destructive) pre-interaction measurement of the register QV,[6] or stated another way, the measurement of the ancilla performs a computational basis measurement of the logical QV that was stored in the register QV, as required. The circuit to implement this measurement is given in Figure 6.3. The only reason that this $\hat{x}_{FR(\vartheta)}$ measurement simulation procedure cannot be performed simultaneously, on all the register QVs that are to be measured, is because there is a time-ordering structure (encoded in dependencies of ϑ on other measurement outcomes) inherited directly from the measurement pattern. Hence, the depth of the measurement stage is only increased by a constant factor (of at most four) in the ADQC simulation of the measurement pattern.

The final stage of the measurement pattern is the corrections on the output.

[6] Followed by a Fourier gate on the register QV. This is irrelevant in this context as this QV has now been removed from the 1WQC as it is no-longer entangled with any other QVs and its state does not matter.

Strictly speaking, these cannot be simulated in ADQC unless we allow final local corrections on the register in ADQC. However, in neither model are these actually required, in the sense that they can be absorbed into classical post-processing. Either way this requires the same depth in each model, as it is either only a depth of two or is only a classical computation and hence does not contribute to the depth. Hence, the total measurement pattern has been simulated with a ADQC with only a constant increase in depth (at most, a multiplicative factor of six), which concludes the proof.

This proposition implies that all of the depth complexity results of Chapters 3 and 4, for unbounded fan-out circuits and the 1WQC, also apply to the ADQC model with general QV type. Therefore, although the primary motivation for introducing the ADQC model for general QVs is its potential for simplifying the requirements for a physical realisation of a quantum computer, it also has very interesting computational advantages over a purely unitary gate-based model. Finally, note that Kashefi et al. (2009) proved that the qubit ADQC model had at least the same parallel computational power as the 1WQC, using so-called 'twisted graph states'. Hence, combining the results of Kashefi et al. (2009) with the qubit 1WQC depth complexity theorems of Browne et al. (2011) provides an alternative proof of Proposition 6.1 in the *qubit* sub-case. However, the depth-preserving ADQC simulation of a 1WQC provided here is very different to that of Kashefi et al. (2009), hence the result herein still has some utility even in the qubit sub-case as it provides a different perspective on the known results.

6.3 Universal sets of measurements

The gate methods given so far are sufficient for universal quantum computation on the register. However, these techniques include $\hat{x}_{FR(\vartheta)}$ measurements for unspecified phase-functions $\vartheta : \mathbb{S}_d \to \mathbb{R}$ and not all such measurements will be equally straightforward in practice. This can be restricted to a similar set of measurement bases to those needed in the 1WQC, which was discussed in Section 4.3.2. As summarised by Figures 6.2 and 6.1, the measurements required for the entangling and local gates are

$$\tilde{E} \text{ gate } \leftrightarrow \text{ measurement operator: } \hat{x}, \tag{6.14}$$

$$FR(\vartheta) \text{ gate } \leftrightarrow \text{ measurement operator: } \hat{x}_{FR(\vartheta)}, \tag{6.15}$$

respectively. Furthermore, to implement any Clifford gate it is only necessary to implement measurements of the operators $\hat{x}$ and $\hat{x}_{FP(q)}$ for $q \in \mathbb{S}_d$, which are used for implementing $\tilde{E}$ and $FP(q)$, respectively. In order to discuss this in more detail it is convenient to consider qudits and QCVs in turn.

For qudits only three measurement operators are required to implement any Clifford gate because F, FP, Z and $\tilde{E}$ generate the Clifford group for qudits (this follows from Propostion 2.1). Hence, only measurements of $\hat{x}$, $\hat{x}_F$ and $\hat{x}_{FP}$ are necessary to implement any Clifford gate. For a qubit, a direct calculation can be used to confirm that these are equivalent to measurements of the Pauli Z, X and Y operators, respectively, up to a post-processing on the measurement outcomes of $+1 \to 0$, and $-1 \to 1$. As an aside, these qubit operators define a set of three mutually unbiased bases (i.e., the bases formed from their eigenstates), and this is is similarly true for the non-binary qudit measurement operators, as can be inferred from results which are presented later in Section 7.4.1.[7] To implement universal quantum computation, it is necessary to also have access to some non-Clifford gate, which in prime dimensions may be *any* non-Clifford gate [Campbell et al. (2012); Nebe et al. (2001, 2006)], e.g., the qudit cubic 'T' gate (see Section 2.5), and in any dimension this gate may be some $FR(\vartheta)$ with a generic phase vector (see Appendix G). Alternatively, by the same arguments as given in Appendix G, the phase function with $\vartheta(d-1) = \theta$ for some generic θ and $\vartheta(q) = 0$ if $q \neq d-1$ is also appropriate for obtaining universality when added to the Clifford group and this may be more convenient in practice. Variable-basis measurements of this sort, or equivalently, variable local gates followed by a fixed-basis measurement, have been implemented in a range of physical systems encoding non-binary qudits, e.g., see Anderson et al. (2015); Neeley et al. (2009), and are common practice in qubit systems, e.g., see Barz et al. (2014); Gao et al. (2011); Lanyon et al. (2013).

Turn now to QCVs. In the following, it will be useful to use the diagonal gate $D_k(q) = e^{iq\hat{x}^k/k}$, as introduced in Equation 2.60. The conjugation relations of this gate on the position and momentum operators are given by

$$\hat{x} \xrightarrow{D_k(q)} \hat{x}, \qquad \hat{p} \xrightarrow{D_k(q)} \hat{p} = \hat{p} - q\hat{x}^{k-1}, \tag{6.16}$$

respectively, which may be derived with the aid of Equation B.2 and by showing that $[\hat{x}^k, \hat{p}] = ik\hat{x}^{k-1}$ with $k \in \mathbb{N}$. Now, in order to implement any Clifford gate in the QCV-based ADQC model, it is only necessary to be able to measure the quadrature operator $X(\phi) = (\hat{p}\cos\phi + \hat{x}\sin\phi)$ for variable $\phi \in [0, 2\pi)$, although this must be aided with additional post-processing on the measurement outcomes. This is because

$$X(\pi/2) = \hat{x}, \qquad X(\pi) = F^\dagger \hat{x} F, \tag{6.17}$$

with the later relation holding because $-\hat{p} = F^\dagger \hat{x} F$, and a measurement of these

[7] In Section 7.4.1, it is shown that that the eigenstates of $\hat{x}$ (i.e., the computational basis), the eigenstates of $\hat{p}$ (i.e., the conjugate basis), and the eigenstates of $\hat{x}_{F^\dagger P^\dagger}$ (which will be called the phase basis) form a set of three mutually unbiased basis. These are slightly different to the measurement operators here, but the results of Section 7.4.1 can be easily adapted to these bases.

operators is what is required to implement $\tilde{E}$ gates and the F gates, respectively. Furthermore, by noting that $P(p) = D_2(p)$ and then considering Equation 6.16, it may be confirmed that

$$X(\phi) = \cos\phi(\hat{p} + \hat{x}\tan\phi) = -1\cos\phi\left(P(\tan\phi)^{\dagger}F^{\dagger}\hat{x}FP(\tan\phi)\right). \tag{6.18}$$

Hence, a measurement of $X(\phi)$ implements the gate $FP(\tan\phi)$, with the measurement outcome m needing to be post-processed via the mapping $m \to -m/\cos\phi$. Quadrature measurements, often called homodyne detection, are now routine in quantum optics, see e.g., Su et al. (2013); Ukai et al. (2011), and are implemented by mixing the light to be measured with a strong local oscillator on a beam splitter, with the relative phase of the oscillator fixing the phase-space angle, ϕ, of the measurement [Tyc and Sanders (2004)]. Although the most natural realisation of the ancillary systems in QCV-based ADQC is probably an encoding into optical states, interestingly, homodyne detection of QCVs encoded into atoms has also been recently demonstrated [Gross et al. (2011)].

To obtain a universal gate set, it is again necessary to augment the Clifford gates with some non-Clifford unitary and this must be a gate which is generated by at least a cubic function of $\hat{x}$ and $\hat{p}$, as gates which are generated by quadratic functions of $\hat{x}$ and $\hat{p}$ are Clifford. As with the 1WQC, the natural gate to consider is the *cubic phase gate*, which is the $k = 3$ case of the $D_k(q)$ gate and hence is given by $D_3(q) = e^{iq\hat{x}^3/3}$. This cubic phase gate may be implemented via measurement of the operator

$$D_3(q)^{\dagger}F^{\dagger}\hat{x}FD_3(q) = q\hat{x}^2 - \hat{p}, \tag{6.19}$$

where this equality follows directly from Equation 6.16. The CLV-adapted version of this gate required for direct step-wise determinism is simply given by letting $q \to q + x$ in Equation 6.19, where x is CLV tracking the X-type error on the register QV, which is the operator $(q + x)\hat{x}^2 - \hat{p}$ (see the paragraph containing Equation 6.10 for more details on this). However, this can also be decomposed into a measurement of the operator in Equation 6.19 followed by x-dependent Clifford gates, as will be implied by the following discussions, and this is likely to be easier in practice.

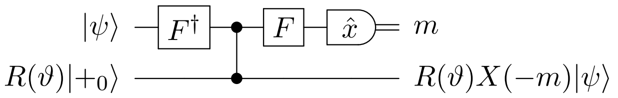
The measurement to implement the cubic phase gate is quadratic in the position operator and such a measurement is not easy to achieve experimentally as it requires a non-linear optical element. However, one alternative to these measurements is to use an auxiliary resource state, such as the so-called *cubic phase state* [Gottesman et al. (2001)]. For example, consider the state

$$|\text{cubic}(\gamma)\rangle = D_3(\gamma)|+_0\rangle, \tag{6.20}$$

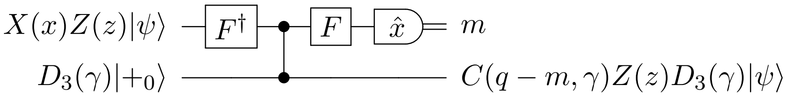
for non-zero $\gamma \in \mathbb{R}$. It is now shown how, if such states can be prepared in auxiliary register QCVs, cubic phase gates may be implemented on computational register QCVs (up to Pauli corrections) within the constraints of the ADQC model and using only homodyne detection. This uses a similar method to that proposed by Gu et al. (2009) in the context of the 1WQC. It will then be shown how these resource states can be made in a physically realistic fashion in the ADQC model, via a simple adaption of the proposals of Gottesman et al. (2001); Gu et al. (2009). To begin, via Equation 6.16 and by noting that $Ue^{i\hat{O}}U^\dagger = e^{iU\hat{O}U^\dagger}$ for any unitary U, it follows that

$$Z(q) \xrightarrow{D_3(\gamma)} Z(q), \qquad X(q) \xrightarrow{D_3(\gamma)} e^{iq(\gamma\hat{x}^2-\hat{p})} =: C(q,\gamma), \tag{6.21}$$

where $C(q,\gamma)$ is a Clifford gate as it is generated by a quadratic in $\hat{x}$ and $\hat{p}$.[8] Now, by noting that $R(\vartheta)$ commutes with CZ, it is not hard to confirm that



as this is essentially the same as the teleportation procedure that the 1WQC is based upon, which is summarised by Figure 4.1. Hence, with the aid of the conjugation relations of Equation 6.21, then it follows that



Hence, by using an auxiliary cubic phase state, the cubic phase gate has been implemented on a computational register QCV in an arbitrary state, $|\psi\rangle$, with pre-existing Pauli errors, $X(x)Z(z)$, and in the process the computational QCV has been teleported to the auxiliary QCV and a (non-Pauli) Clifford error has been created, in addition to an ordinary Pauli error. Before discussing the Clifford error, it is important to note that this circuit can be implemented with an ancilla-driven sequence: The three unitary gates in this circuit can be implemented via ancillas and homodyne detection (which will induce changes in the Pauli errors, i.e., $x \to x'(x,z,m_i)$ and $z \to z'(x,z,m_i)$, where m_i denotes that these error CLVs will also be a function of the further measurement outcomes on these additional ancillas). Furthermore, the computational basis measurement of the first register QV may be simulated via an ancilla, by the method given in Figure 6.3.

This ancilla-driven circuit has created a (non-Pauli) Clifford error and the gate

[8] This equation implies that the Pauli gates are mapped to Clifford gates under conjugation by the cubic phase gate. The set of gates with this property are in what is termed the 'third-level of the Clifford Hierarchy', see e.g., Howard and Vala (2012), and the qudit and qubit 'T' gates also have this property [Campbell (2014); Howard and Vala (2012)].

methods given so far in this Chapter are only concerned with accounting for Pauli errors. However, this Clifford error can be converted to a Pauli error via an ancilla-driven $C(m-q,\gamma)$ gate, as such a gate can be implemented up to Pauli errors by decomposing this Clifford gate into a sequence of $FP(p)$ and F Clifford gates.[9] Therefore, it has been shown how an auxiliary cubic phase state can be used to implement the mapping

$$X(x)Z(z)|\psi\rangle \to X(x')Z(z')D_3(\gamma)|\psi\rangle, \tag{6.22}$$

for any arbitrary logical register state $|\psi\rangle$, with γ fixed by the auxiliary state. Moreover, this can be converted to a cubic phase gate $D_3(q)$ with any $q \in \mathbb{R}$, by noting that $D_3(q) = S(\gamma/q)D_3(\gamma)S(q/\gamma)$, where $S(s)|q\rangle = |sq\rangle$ is the Clifford squeezing gate, which was introduced in Equation 2.56. Hence, by applying (ancilla-driven) squeezing gates before and after the protocol given above, any cubic phase gate may be implemented via ancillas using only the fixed ancilla-register interaction, homodyne detection of the ancillas, and auxiliary cubic phase states. It is important to note that this procedure requires adaptive measurements even though all of the unitary gates implemented are Clifford, as exactly which Clifford gates need to be implemented depends on one of the measurement outcomes.

Although it has been shown how auxiliary cubic phase states may be converted to cubic phase gates, no method has been given for how these states can be made. Before turning to this, it is convenient to first consider another challenge associated with the ADQC model in the setting of QCVs, which is an issue shared with all QCV-based quantum computation: the conjugate and computational basis states cannot be exactly physically realised even in principle [Lloyd and Braunstein (1999)]. In ADQC, the ancillas should be initialised to $|+_0\rangle$ in the ideal case. However, these states may be approximated by the squeezed vacuum, or more precisely $|+_0\rangle \approx S(s)|\text{vac}\rangle$ and $|0\rangle \approx S(1/s)|\text{vac}\rangle$ for $s \gg 1$, where $|\text{vac}\rangle$ is the ground state of the QHO, and this approximation becomes exact in the limit $s \to \infty$ [Radmore and Barnett (1997)], with a derivation of this included as Appendix B. The effect on the computation of preparing the ancillas in such approximations to $|+_0\rangle$ will be a distortion of the output register state from each gate, as shown for the 1WQC by Gu et al. (2009), and by analogy to the 1WQC, this distortion will build up linearly with the number of gates implemented. Squeezed states, which approximate the quadrature eigenstates, have been prepared with reasonably high levels of squeezing in the laboratory: The quantity of squeezing in a state is often expressed in terms of

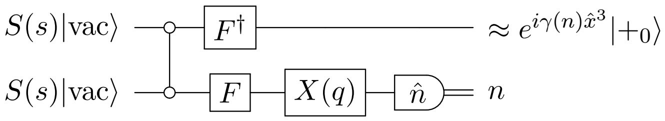
[9] The exact decomposition can be found by using the methods of Farinholt (2014). Although these are presented in the case of qudits, they are easily applied also to QCVs.

decibels (dB), where the state $S(s)|\text{vac}\rangle$ has $10\log_{10}(s^2)$ dB of squeezing,[10] and as far as I am aware, the current experimental record stands at 12.7 dB [Eberle et al. (2010); Mehmet et al. (2011)]. However, it is unlikely that these currently obtainable values are sufficient for viable computations in the QCV-based models herein - a recently established minimal squeezing threshold for error-correction in qubit-encoded QCV-based 1WQC is around 20 dB [Menicucci (2014)]. The errors associated with this finite squeezing is discussed no further here, and a full investigations of the effect of these distortions is left for future work.

It is now shown how cubic phase states may be generated with ancilla-driven gates and a physically plausible measurement. Gottesman et al. (2001) have shown how to approximately generate a cubic phase state with gaussian operations acting on squeezed vacuums, and a measurement of the *number operator*, $\hat{n}$, defined by[11]

$$\hat{n} := \frac{1}{2}(\hat{x}^2 + \hat{p}^2 - 1) = \hat{a}^\dagger \hat{a}. \tag{6.23}$$

This technique has been converted to the setting of the 1WQC by Gu et al. (2009), and by a simple manipulation of the 1WQC computation given therein (see Equation 45 of Gu et al. (2009)), it may be confirmed that



where $\gamma(n) = (6\sqrt{2n+1})^{-1}$, and where this approximation holds when $s \gg 1$ and $q \gg s$. In this circuit, the lower quantum wire represents an ancilla initialised in an approximation to $|+_0\rangle$ (which is the state that all ancilla would be initialised to in practice), the top wire represents an auxiliary register QCV initialised similarly, and it should be noted that the local $F^\dagger$ gate on the register QCV may be applied, up to a Pauli error, via an ancilla-driven gate. Although this measurement is a non-Gaussian operation, in a QHO it is very natural as it is simply a measurement of the QHO's energy. Hence, in optics, this is photon-number counting and there have been many recent improvements in the state-of-the-art in this technology [Calkins et al. (2013); Humphreys et al. (2015)]. Although photon-number resolving detectors are highly challenging to implement in comparison to homodyne detection, it is perhaps the most well-developed non-Gaussian optical component. Hence, in combination with

[10] The quantity of squeezing in any given state, with respect to the phase space angle ϕ, is often defined to be $10\log_{10}(2\Delta X(\phi)^2)$ dB, where $\Delta X(\phi)^2$ is the variance of $X(\phi)$ with respect to the state in question, i.e., $\Delta X(\phi)^2 = \langle\phi|X(\phi)^2|\phi\rangle - \langle\phi|X(\phi)|\phi\rangle^2$ [Lvovsky (2014)]. This then gives the amount of squeezing stated for the squeezed vacuum in the main text (with $\phi = 0$).

[11] The eigenvalues of $\hat{n}$ are the set of integers greater than or equal to zero, and the eigenstates are obviously those of the QHO.

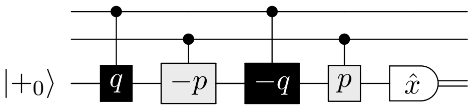
the method given above for transforming this resource state into a cubic phase gate, it has been shown that ancilla-driven gates that employ homodyne detection and number-counting measurements are sufficient for universal quantum computation.

6.4 Adapting the ancilla-driven model

In this penultimate section of the chapter interesting adaptions to the ancilla-driven model are presented. In Section 6.4.1 a generalisation of the ADQC model is considered in which the ancillary and register QVs may have different dimensions and the effect that this has on step-wise determinism is discussed. In Section 6.4.2 an alternative fixed interaction gate appropriate for the ADQC model is given, which then leads onto Section 6.4.3 where this gate is used to define an alternative completely deterministic computational model, in which the measurements of the ancillas are replaced with unitary controls.

6.4.1 Determinism and the dimension of the ancillas

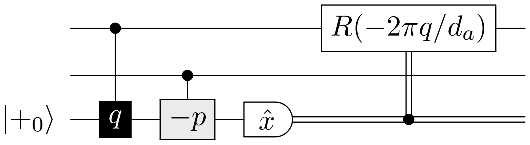
One of the first constraints imposed on the ADQC model was that the ancillary and register QVs where all of the same type. In contrast to this, the ancilla-based gates methods developed in Chapter 5, centred on the geometric phase gate, were all applicable to ancillas of a different dimension (i.e., different QV type) to the register QVs. As such, it is interesting to consider whether it is also possible to extend the ancilla-driven model to apply in this more general setting. This question can be answered by showing how the geometric phase gate can be transformed into the same form as the entangling gate of ADQC, with the added benefit of this analysis being that it will highlight the link between these two techniques. In the following, it will be assumed that the register does not consist of QCVs.[12] By considering the geometric phase gate circuit of Figure 5.2, it is clear that this gate functions independently of the ancillary input state. Hence, the circuit will have exactly the same effect if the ancilla is prepared in the state $|+_0\rangle$ and measured at the end in the computational basis, which is the quantum circuit



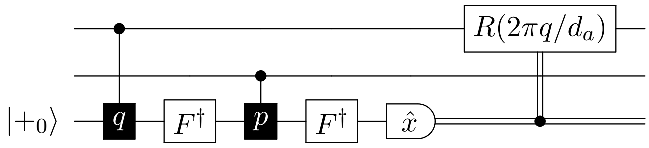
From Figure 5.2, it follows that this induces a $CR(2\pi pq/d_a)$ gate on the pair of register QVs, where d_a is the dimension of the ancilla and $R(2\pi pq/d_a)|q\rangle = e^{2\pi i pq/d_a}|q\rangle$

[12] This is because the geometric phase gate is only valid for register QCVs when the ancillas are also QCVs, and this case has already been covered in the ADQC model so may now be ignored.

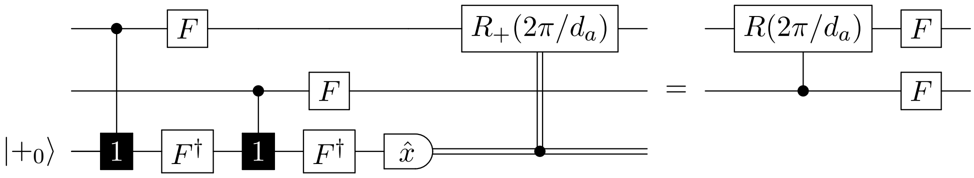
is the scalar-parameterised rotation gate. Now, after the first three gates of this sequence, the ancilla has returned to the state $|+_0\rangle$, regardless of the state of the register QVs. Furthermore, the $|+_0\rangle$ state is an eigenstate of the final gate, with an eigenvalue of unity for all values of the gate parameter p. Hence, the last gate in this circuit has the same effect as an identity operator, and can therefore be dropped. Moreover, the penultimate gate (which has now become the final gate), can equally be understood as an ancilla-controlled $R(-2\pi q/d_a)$ gate on the first register QV. Now, as a quantum-controlled gate followed by a computational basis measurement of the control system is equivalent to performing the measurement before the gate and then applying a classically controlled gate, this implies that the circuit given above can be simply rewritten as



This already looks very similar to the ADQC entangling gate. Moreover, by using the relation of Figure 2.5, (and noting that $F^2|q\rangle = |-q\rangle$) this can be further rearranged to



Hence, by setting $p = q = 1$,[13] this gate sequence requires only a fixed ancilla-register interaction gate, and by adding in a local Fourier transform to the interaction, we arrive at the sequence

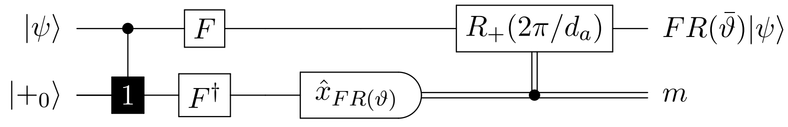


where $R_+(\theta)|+_q\rangle = e^{i\theta}|+_q\rangle$. The ancilla-register fixed interaction gate used here, and this method for implementing a two-qudit entangling gate, is the natural generalisation of the ADQC interaction and entangling gate to allow the ancillary and register QVs to be of different types.

It is clear that the gate technique given above may be used to implement an

[13] It is not essential to set the value of the two parameters to unity, but they should be set to the same value.

entangling gate on the register, but without local controls of the register this is only implemented up to the error $R_+(2m\pi/d_a)$ and with an ancilla of general dimension this is *not* in all cases a Pauli gate. The condition under which this is guaranteed to be a Pauli gate is when $d_a = d/k$ for some positive integer k, where d is the dimensionality of the register qudits, as in this case then $R_+(2m\pi/d_a) = X(-km)$. Before considering the repercussions of non-Pauli errors, consider the obvious extension of the ADQC single-qudit gates, as summarised in Figure 6.1, to this more general setting. This is the circuit



which may be easily confirmed to act as claimed via a direct calculation, where $\bar{\vartheta}$ is the phase-function given by $\bar{\vartheta}(q) = \vartheta(0 \oplus q)$ for $q \in \mathbb{S}_d$ with $\oplus$ denoting the arithmetic of $\mathbb{S}_{d_a}$. Hence, when $d_a \geq d$ or the ancilla is a QCV, any $FR(\vartheta)$ operator may be applied to the register (up to the error) by an appropriate choice of measurement basis for the ancilla. However, when $d_a < d$ then, no matter what measurement is chosen, the gate implemented has a phase function which obeys $\bar{\vartheta}(q) = \bar{\vartheta}(q \bmod d_a)$. For example, if the ancillas are qubits then each $FR(\bar{\vartheta})$ gate that can be implemented on the register has a phase-function $\bar{\vartheta}$ with $\bar{\vartheta}(q) = \vartheta(0)$ if q is even and $\bar{\vartheta}(q) = \vartheta(1)$ if q is odd for some $\vartheta : \{0,1\} \to \mathbb{R}$, which is fixed by the choice of measurement basis. Therefore, when $d_a \geq d$ it is clear that a universal set of single-qudit gates can be implemented on the register, but it is not at all obvious that this is the case for $d_a < d$.

This analysis highlights a clearly problem with this extension of the ADQC model to a setting where the ancillary and register QVs are of a different type: Still assuming a qudit register, it is necessary for the ancillas to be qudits of dimension $d_a \leq d$ for the measurement-induced errors on the register to be Pauli gates, which is required for the step-wise determinism techniques used herein. But in this case, unless $d_a = d$, it may not be possible to implement a universal gate set as the single-qudit gates that can be implemented on the register are restricted.[14] When the ancillas are qudits of dimension $d_a > d$ or QCVs, the gate set which may be applied to the register is universal (an entangling gate + a universal set of single-qudit gates), but the measurement-induced errors are non-Pauli. Hence, local corrections on the register need to be available for step-wise deterministic computation. Alternatively, without these controls the model can be said to be universal in a stochastic sense - any quantum computation can be implemented with a stochastic sequence of single-

[14] It is left for future work to confirm whether universality is achievable in this setting. It is not clear to me either way.

qudit gates of indeterminate length between each entangling gate (which can be deterministically applied, up to a single-qudit error gate). This may be considered a form of what is termed *repeat-until-success* (RUS) gate implementation [Lim et al. (2005)] and these ideas will be briefly discussed further in Chapter 7 where an additional stochastically universal model is introduced. Note however, it is my opinion that the overheads involved in quantum computation in this fashion are likely to be unreasonably large.[15]

6.4.2 An alternative interaction

Return now to the setting in which the ancillary and register QVs are of the same type. The choice to fix the ancilla-register interaction gate to $\check{E}_{ar} = F_r F_a^\dagger \mathrm{C}_a^r Z$ was made at the beginning of this chapter, and it is not obvious that this interaction has unique properties that single it out as the only possible option. Indeed, there is an alternative interaction which is suitable for ADQC, which is based on the SWAP gate and is given by

$$\check{S}_{ar} := F_a \cdot \textsc{swap} \cdot \textsc{cz}. \tag{6.24}$$

When considering this fixed interaction, there are minor changes to the gate implementation methods, which are now briefly outlined. The two-QV gate implemented by sequential interactions of an ancilla with QVs r and s followed by a computational basis measurement may easily be confirmed to be

$$\frac{\langle m|\check{S}_{as}\check{S}_{ar}|+_0\rangle}{\|\langle m|\check{S}_{as}\check{S}_{ar}|+_0\rangle\|} = X_s(-m)F_r F_s \mathrm{C}_s^r X. \tag{6.25}$$

The same set of single QV gates can be implemented by using a slightly different measurement basis. Specifically, an interaction followed by a measurement in the basis $\hat{x}_{FR(\vartheta)F^\dagger}$, implements $FR(\vartheta)$ up to Pauli error, as

$$\frac{\langle m|F_a R_a(\vartheta)F_a^\dagger \check{S}_{ar}|+_0\rangle}{\|\langle m|F_a R_a(\vartheta)F_a^\dagger \check{S}_{ar}|+_0\rangle\|} = X_r(-m)F_r R_r(\vartheta). \tag{6.26}$$

Although this gate set is not identical to the one implemented with the $\check{E}_{ar}$ interaction, the same techniques of classical-feedforward may be used to implement the computation deterministically: the details are omitted for brevity. For the qubit sub-case, it has been shown by Kashefi et al. (2009) that, up to local gates, the two interactions $\check{E}_{ar}$ and $\check{S}_{ar}$ are the only possible choices that allow for deterministic

[15] Some RUS gate methods actually have lower overheads than equivalent deterministic schemes, e.g., see Bocharov et al. (2015); Paetznick and Svore (2014). What I am claiming here, is that the sort of RUS scheme needed for the 'stochastic ADQC' model, given above, is likely to have very large overheads.

universal quantum computation within the constraints of ADQC. It is not at all clear how this could be shown more generally, if it is indeed true.

6.4.3 Replacing measurements with unitary controls

High-quality variable-basis measurements of ancillas are critical to the ancilla-driven model, and the quality of each measurement directly effects the fidelity of each gate implemented. This is challenging physically, and in some settings it may well be the case that local unitary controls of the ancillas can be enacted with much lower errors than can be achieved with measurements on these ancillas. Interestingly, the swap-based gate, $\check{S}_{ar}$, which it was shown above may be used to implement the ancilla-driven model, can also be used to implement universal quantum computation on the register if local gates, instead of measurements, can be implemented on the ancillas. To be more precise, the following model will use only: (I) a fixed ancilla-register interaction gate, (II) ancillas prepared in a single state, (III) a universal set of local gates on the ancillas.

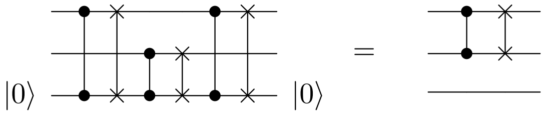
Rather than use the $\check{S}_{ar}$ interaction gate, given in Equation 6.24, it will be simpler to consider the locally-equivalent gate

$$S_{ar} := \textsc{swap} \cdot \textsc{cz}. \tag{6.27}$$

The action of this gate on two QVs in arbitrary computational basis states is

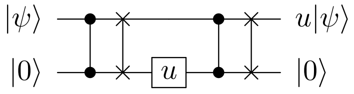
$$|q\rangle|q'\rangle \xrightarrow{S_{ar}} \omega^{qq'}|q'\rangle|q\rangle, \tag{6.28}$$

and hence, if either QV is in the state $|0\rangle$, it simply acts as a SWAP gate. Therefore, if an ancilla is initialised to $|0\rangle$, and interacts with a register QV via this gate, the logical QV in this register QV is swapped into the ancilla, i.e., $|\psi\rangle|0\rangle \rightarrow |0\rangle|\psi\rangle$. Therefore, any further gates that are applied to this ancilla will perform transformations on the $|\psi\rangle$ logical QV, and as the register QV is in the state $|0\rangle$, a further interaction of the ancilla with this QV swaps the logical state back into the register. It then immediately follows that an S_{rs} gate may be implemented between two register QVs, r and s, via the gate sequence[16]



[16] Note that two quantum wires connected via a wire with '×' symbols at each end is the notation used herein (and often in the literature) for the SWAP gate. This notation has already been encountered in this thesis, but only to represent classical SWAP gates.

which employs an ancilla initialised to $|0\rangle$ and three applications of the single fixed interaction gate S_{ar}. In exactly the same fashion, if the gate u can be applied to the ancillas this may be transferred to the register by interacting a register QV with an ancilla prepared in $|0\rangle$ both before and after a u gate is applied to this ancilla. This is the circuit



Hence, if a set of single-QV gates can be implemented on the register that is sufficient to generate any single-QV gate, then this provides a method for implementing universal quantum computation using only ancillas prepared in $|0\rangle$, the gate S_{ar} between ancillas and register QVs, and local gates on the ancillas. It is interesting to note that the entangling part of the interaction is actually only required in order to make the induced two-QV gate on the register an entangling gate, and otherwise it plays no direct role in the gate methods.

One feature of these ancilla-based gates, that make them potentially appealing from a practical point of view, is that the interaction need not have the exact form of S_{ar} and there is a range of interactions for which the above methods are applicable. Indeed, consider an ancilla-register interaction of the form

$$S_{ar}(\phi) := \textsc{swap} \cdot D_{ra}(\phi), \tag{6.29}$$

where $D_{ra}(\phi)$ is a general diagonal gate on r and a, which is parameterised by a function $\phi : \mathbb{S}_d^2 \to \mathbb{R}$ and defined as[17]

$$|q\rangle_r |q'\rangle_a \xrightarrow{D_{ra}(\phi)} e^{i\phi(q,q')} |q\rangle_r |q'\rangle_a. \tag{6.30}$$

Because the action of this more general $S_{ar}(\phi)$ gate, when either QV is in the state $|0\rangle$, is equivalent to SWAP up to local rotation gates, the gate techniques given above still apply. Hence, as long as the fixed function ϕ is chosen such that $D(\phi)$ is an entangling gate (which is almost any choice of ϕ), this gate also allows for universal quantum computation in the ancilla-based and globally unitary fashion described above. The gates implemented on the register with this more general interaction are slightly altered, in comparison to the simple case of S_{ar}, and the relevant quantum circuits are given in Figures 6.4 and 6.5.

The model of ancilla-based quantum computation presented in this section may find practical relevance in a range of settings, particularly when local unitary gates on the ancillas are straightforward but where these gates cannot be so easily ap-

[17] Note that this general two-QV diagonal gate is a special case of the many-QV diagonal gate introduced in Equation 5.25.

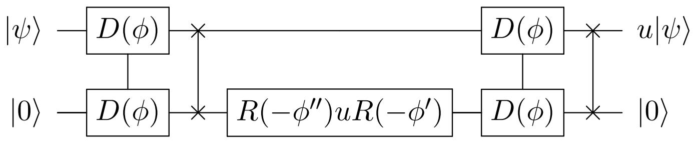


Figure 6.4: If a universal set of single-QV gates can be implemented on the ancillas, this circuit may be used to implement gates from this set on the register QVs. This circuit uses an ancilla initialised to $|0\rangle$, a single local gate on the ancilla, and two applications of the fixed interaction $S_{ar}(\phi) = \text{SWAP} \cdot D_{ar}(\phi)$, where $\phi : \mathbb{S}_d^2 \to \mathbb{R}$. Here, ϕ' and ϕ'' are the phase-functions given by $\phi'(q) = \phi(q,0)$ and $\phi''(q) = \phi(0,q)$, respectively. In this diagram, the $D(\phi)$ gate is represented schematically by the boxes containing $D(\phi)$ connected via a wire.

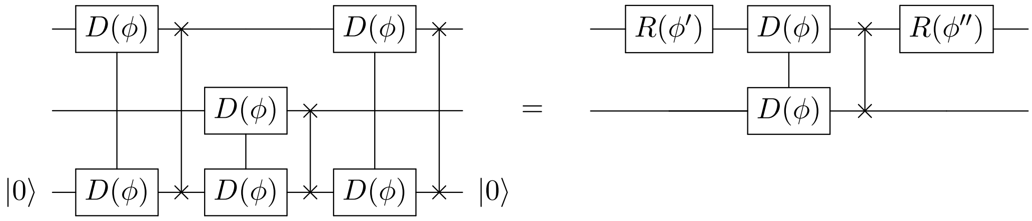


Figure 6.5: A two-QV entangling gate may be implemented on a pair of register QVs with the aid of an ancilla that has been prepared in the state $|0\rangle$, and three applications of the fixed ancilla-register interaction gate $S_{ar}(\phi)$. The circuit notation and the parameters used here are as described in Figure 6.4 and the main text.

plied directly to the well-isolated ‘memory’ register QVs and also when high-quality measurements of the ancillas are not available for implementing the ADQC model. Discussions on more specific settings in which this may be of relevance, and possible methods for generating appropriate interaction gates, are delayed until the next chapter, in which this model is extended. Before concluding this chapter, a few observations are made relating to the differences between this model and ADQC: In comparison to ADQC, one disadvantage of this globally unitary model is that to entangle two QVs it is necessary for one of the QVs to interact twice with the ancilla, and this may be highly inconvenient in some settings, e.g., with ‘flying’ photonic QVs entangling distant register QVs. However, three ancilla-register gates is actually the minimal number possible with which an entangling gate can be mediated on two QVs via an ancilla whilst using globally unitary dynamics [Lamata et al. (2008)], and hence, although the model here has this gate-count disadvantage in comparison to ADQC, this is inherent to all globally unitary models (e.g., see the geometric phase gate, which uses four interactions per gate). A further cost to using globally unitary dynamics is that the computational model can no-longer have access to the parallel power of the 1WQC.[18] It should also be made clear that, at the end of the computation, it is obviously necessary to be able to perform a measurement of each register QV. Here, this can be achieved either directly or via measurements on ancillas. Finally, note that the qubit sub-case of the model outlined in this section has been presented in Proctor et al. (2013) and this should be referred to for further details relevant only in this (perhaps most practical) special case.

6.5 Conclusions

In this chapter a model of quantum computation for general quantum variables has been developed which requires only very limited access to the computational register. This is an extension of the qubit-based *ancilla-driven quantum computation* (ADQC) model of Andersen et al. (2010) and Kashefi et al. (2009), and hence, for this reason, the same terminology has been used herein. To be more specific, in this 'ADQC' model universal quantum computation is implemented on a register using *only* repeated applications of a single fixed two-body ancilla-register interaction gate, ancillas prepared in a single state, and variable basis measurements of these ancillas. Because measurement outcomes are fundamentally probabilistic the measurements of the ancillas introduce random Pauli errors into the computation. However, it was shown that a quantum computation can still be implemented deterministically with the aid of classical feed-forward of measurement outcomes and adaptive measurement bases. It was then shown how the general quantum variable one-way quantum computer (1WQC) can be simulated within this model, which in-turn demonstrated that the hybrid quantum-classical advantages of 1WQC, as investigated in Chapter 4, are also inherent in the ADQC model presented here. Hence, ADQC not only requires highly limited physical controls, but is also powerful for parallel quantum computation. The measurement bases that are sufficient for universal quantum computation were then discussed. In particular, it was shown that in the setting of QCVs, with the ancillas realised as optical states, homodyne detection and photon-number counting are sufficient for universality. From a physical perspective this is fairly promising, as homodyne detection is now a routine quantum optics technique [Su et al. (2013); Ukai et al. (2011)] and there have been many recent improvements in photon-number-resolving detectors [Calkins et al. (2013); Humphreys et al. (2015)].

The ADQC model employs ancillas of the same dimension (i.e., the same QV type) as the register QVs, which may not be convenient in all settings. Hence, an

[18] This is true as long as the model uses only bounded input-size gates, as is the case here. This was shown in Chapter 3.

adaption of the ADQC model to the more general setting of ancillary and register QVs of different dimensions was considered and this was seen to be closely related to the geometric phase gates of Chapter 5. It was shown that when the ancillary and register dimensions do not match this either prevents step-wise determinism, or restricts the implementable gate set so that the model may no longer be universal. Finally, it was shown that the ADQC model can be implemented with a swap-like interaction gate and that this interaction can also be used for an alternative model of ancilla-based quantum computation, which requires *only* interactions between ancillary and register QVs using this single fixed gate, ancillas prepared in a single fixed state, and local unitary controls of the ancillas. This globally unitary model may be more relevant in settings in which high-quality measurements on ancillas are not possible, particularly as it has been shown that inaccurate measurements of the ancillas have a serious detrimental impact on the fidelity of the computation in the original qubit-based ADQC model [Morimae (2010); Morimae and Kahn (2010)]. Future work could include an analysis of the effects of such measurement inaccuracy to this more general model, and an additional avenue for further research could be to fully assess the effects on the QCV-based ADQC model of using finitely-squeezed vacuum states instead of ideal position and momentum eigenstates. In particular, it would be interesting to consider whether the QCV-based ADQC model can be made fault-tolerant in a similar fashion to the recent qubit-encoded QCV-based 1WQC work of Menicucci (2014).

Chapter 7

Minimal ancilla-based gates

In this chapter a quantum computer is proposed which may implement any quantum algorithm on a well-isolated register, via interactions with ancillas prepared in the computational basis, using *only* a single fixed ancilla-register interaction gate. This may be naturally termed a *minimal control* ancilla-based quantum computer, as it requires both a minimal level of access to the computational register, which can hence be optimised for long coherence times, and highly limited control over the ancillas, which may be optimised for a single high-quality interaction with the register systems. This model is applicable to the setting of both qubits and qudits of more general dimensions. Moreover, in the particular case of a qubit-based computer and a swap-like fixed interaction gate, it is shown that any quantum computation can be implemented on the register even if the ancillas can only be prepared in a *single fixed state*, which it can be argued is a completely minimal scheme for universal ancilla-based quantum computation. The models proposed in this chapter are novel for *all* types of QVs. This chapter is based upon Proctor and Kendon (2014, 2015).

7.1 Introduction

From a fundamental point of view, it is interesting to understand the minimal resources required to implement universal quantum computation. As such, this was extensively investigated by the early pioneers of the subject [Barenco (1995); Deutsch (1989)], culminating with Deutsch et al. (1995) showing that almost any two-input gate is *alone* sufficient for universality with qubits, and Lloyd (1995) independently showing that this is true for qudits of any dimension.[1] In the latter chapters of this thesis, quantum computational models have been considered in which the gates on the computational systems are mediated via ancillas, and in this more restricted setting it is not *a priori* clear, and it does not directly follow from the work of Deutsch

[1] See Childs et al. (2011) and Bauer et al. (2014) for more recent works on this subject.

et al. (1995) and Lloyd (1995), that there are fixed ancilla-register interactions which alone (i.e., with no further control of the register or ancillary QVs) can implement universal computation on the register. Indeed, the models considered so far in this thesis all require local controls of either the ancilla or the register to achieve universality: The geometric phase gates of Chapter 5 must be augmented with local gates on the register quantum variables to obtain universality, and the measurement-based ADQC model of Chapter 6 requires variable basis measurements of the ancillas, with the globally unitary adaption of ADQC proposed therein removing the necessity for these variable-basis measurements but replacing it with the need for local unitary gates on the ancillas.

In this chapter, deterministic and universal ancilla-based models will be developed which require *only* a single fixed ancilla-register interaction gate and ancillas prepared in states from a fixed orthonormal basis. Two distinct models will be presented, with distinct gate methods and forms for the fixed interaction gate - the latter of these models will be based on a swap-like gate and consume a minimal level of resources to implement each entangling gate on the register. The models proposed in this chapter will be formulated in the setting of general quantum variables and hence the gate methods will be applicable to qubits, qudits and QCVs and are novel in all of these settings. However, although highly applicable in the setting of qubits and qudits, the models will not be particularly suited to the QCV setting, largely because they fundamentally rely on preparing ancillas in computational basis states but also as the models will not be shown to be universal in this case. Due to the subtle differences between the models presented in this and the previous two chapters, the constraints and properties of each model have been summarised in the thesis overview, on pages 2-3 of this thesis: the reader is again referred there for a concise summary of the different ancilla-based models herein.

The computational models introduced in this chapter are interesting from an abstract perspective, but they also have clear practical motivations. Minimising the access needed to the computational register facilitates the optimisation of the register systems for the long coherence times that are essential for the realisation of useful computations, and this has already been discussed in detail in the introduction to Chapter 6. Going beyond this minimal-register-access paradigm, introduced in Chapter 6, the physical motivation for also minimising the control needed over the ancillary systems is clear: Implementing high-quality variable basis-measurements on any quantum system is intrinsically challenging, and in some settings it may not be straight-forward to access individual ancillas on-the-fly in order to apply local unitary gates between interactions of the ancillas with register QVs. Because the models proposed in this chapter bypass the need for on-line local controls of any kind on the register or ancillary QVs, they allow the entire set-up to be optimised for a high fidelity fixed ancilla-register interaction and long coherence times in the computational register.

7.2 Interactions via generalised controlled gates

The purpose of this chapter is to develop methods for ancilla-based universal quantum computation which require *only* a single fixed interaction gate and ancilla preparation. More precisely, with ancillas of dimension d_a and register QVs of dimension d, the idea is that the quantum computer should only requires access to

1. A single fixed ancilla-register interaction gate $U \in U(d_a \times d)$, which may be applied to any ancilla-register pair.

2. Ancillas prepared in states from a fixed orthonormal basis.

Models of quantum computation which obey these constraints will be termed *minimal control* models. As in the previous chapter, the fixed gate, U, must be chosen careful (e.g., it must be entangling) and not any interaction will do. As an aside, it is important to emphasise that although the model does not require measurements to implement the computation, some measurements will be required at the end of the computation for the final read-out. The schemes given here will allow for those measurements to be performed either directly on the register systems, or on some ancillas. Furthermore, it should also be noted that it is essential that the register QVs can be initialised to some fiducial state - or to computational inputs - at the start of the computation, as has been assumed (often implicitly) throughout this thesis.

7.2.1 Choosing an interaction for a qubit-qubit computer

In keeping with the rest of this thesis, as far as is possible the aim is to develop methods which are independent of the particular choices for the QV types of the ancillary and register systems. Hence, if the methods are to work in all cases they must work in the simplest qubit-qubit case (i.e., qubits as the ancillary and the register systems). With this in mind, we begin by considering what the conditions given above imply for the possible forms the interaction gate, U, may take in this simplest, and perhaps most physically relevant, of cases.

Given that part of the motivation for developing 'minimal control' models is physical simplicity, it is natural to demand that a single-qubit gate (from some set) can be induced on any register qubit via interactions with only a single ancilla, and using some (hopefully small) number of applications of the fixed gate U. In order for the mapping on the register implemented by some non-zero $m \in \mathbb{N}$ number of applications of the interaction gate, U, to be unitary, it is necessary for the ancilla and register to be in a product state after U^m has been applied, with the unknown quantum information still in the register.[2] This implies that, for at least some state $|\zeta_0\rangle$ that the ancillas can be prepared in, and all possible register qubit states $|\psi\rangle$, we must have

$$|\psi\rangle \otimes |\zeta_0\rangle \xrightarrow{U^m} u_0|\psi\rangle \otimes |\eta_0\rangle, \tag{7.1}$$

for at least one non-zero $m \in \mathbb{N}$, and some $|\eta_0\rangle$, and unitary u_0. Due to the unitarity of U^m, and because both systems are qubits, it is simple to show that this implies that

$$U^m = u_0 \otimes |\eta_0\rangle\langle\zeta_0| + u_1 \otimes |\eta_1\rangle\langle\zeta_1|, \tag{7.2}$$

for some $u_0, u_1 \in U(2)$ and some orthonormal qubit bases $\{|\zeta_0\rangle, |\zeta_1\rangle\}$ and $\{|\eta_0\rangle, |\eta_1\rangle\}$. Alternatively, this may be re-written as

$$U^m = c_a \cdot (u_0 \otimes |0\rangle\langle 0| + u_1 \otimes |1\rangle\langle 1|) \cdot b_a, \tag{7.3}$$

where b and c are the unitaries defined by $b|\zeta_q\rangle = |q\rangle$ and $c|q\rangle = |\eta_q\rangle$. This interaction and ancilla preparation basis pairing still contains a physically irrelevant freedom, which stems from the equivalence relation

$$\langle\psi|\hat{O}|\psi\rangle = \langle\psi|u^\dagger u \hat{O} u^\dagger u|\psi\rangle, \tag{7.4}$$

for unitary u. Hence, any transformation of the form

$$U^m \to v_a U^m v_a^\dagger = v_a U v_a^\dagger \dots v_a U v_a^\dagger, \tag{7.5}$$

for unitary v, can be accounted for by a rotation in the ancilla preparation states. Therefore, this freedom can be removed by setting the ancilla preparation basis to be the computational basis.[3] Hence, without any lose of generality, the preparation basis for the ancillas may be fixed to the computational basis, and the ancilla-register interaction must then have, as an integer power, the operator

$$U^m = \mathbb{I} \otimes l \cdot (u_0 \otimes |0\rangle\langle 0| + u_1 \otimes |1\rangle\langle 1|)\,, \tag{7.6}$$

for some unitaries $u_0, u_1, l \in U(2)$. To be clear, here the first (second) part of the tensor product acts on a register (ancilla) qubit. The non-local part of this gate can be understood as what might be termed a 'generalised controlled gate', which applies u_q to the register qubit if the ancilla qubit is in the state $|q\rangle$.

[2] This holds as measurements are not available to disentangle the ancilla and register qubits.

[3] Note that this is *not* a physical constraint, as the physical observable which defines the computational basis (i.e., what defines the Pauli Z gate) must itself be chosen by an experimentalist.

7.2.2 Choosing an interaction for general quantum variables

In order to present the natural extension to general QVs of the condition on the fixed interaction gate in the qubit-qubit case derived above, and as summarised by Equation 7.6, it is useful to first define a 'generalised controlled gate' for arbitrary QV types. For a function $\nu : \mathbb{S}_{d_c} \to U(d_t)$, where d_c and d_t are the dimensions of a control and a target QV respectively, define the *generalised controlled gate*, denoted $C[\nu]$, by the action

$$|q\rangle \otimes |q'\rangle \xrightarrow{\mathrm{C}[\nu]} |q\rangle \otimes \nu(q)|q'\rangle. \tag{7.7}$$

Note that the square parentheses in the notation have been used to clearly distinguish this gate from an ordinary controlled gate. As with ordinary controlled gates, the control and target systems will be denoted via including super- and sub-scripts in this notation when necessary, i.e., $\mathrm{C}_t^c[\nu]$ denotes that c is the control QV, and t is the target QV. This definition of a generalised controlled gate can be understood as being a notation for an arbitrary two-QV unitary that may be represented as a block-diagonal matrix, when expressed in the computational basis. To further clarify this definition, some simple examples are now given: If $\nu(q) = u$ for fixed unitary u, then $\mathrm{C}[\nu]$ is equivalent to a local u gate on the target system; if $\nu(q) = u^q$ for fixed u, then this gate is equivalent to the ordinary controlled gate $\mathrm{C}u$; finally, if $u(q)$ is diagonal for all q then this gate is an arbitrary diagonal two-QV gate, with such gates having already been encountered in this thesis (see Section 6.4.3, and in particular Equation 6.30).

The generalised controlled gate, defined above, provides a succinct notation for extending the condition derived for the fixed interaction in a qubit-qubit 'minimal control' model to the more general setting. Specifically, the natural extension of Equation 7.6 to the general QV domain is to impose the condition that, for some non-zero $m \in \mathbb{N}$, the fixed ancilla-register interaction gate, $U \in U(d_a \times d)$, obeys

$$U^m = l_a \cdot \mathrm{C}_r^a[\nu], \tag{7.8}$$

for some function $\nu : \mathbb{S}_{d_a} \to U(d)$ and $l \in U(d_a)$. Considering the m^{th} power of the fixed ancilla-register interaction to have this form immediately highlights a possible method for implementing single-QV gates on the register, and indeed, the construction was specifically designed for this purpose. In particular, it immediately follows that

$$|\psi\rangle \otimes |q\rangle \xrightarrow{U^m} \nu(q)|\psi\rangle \otimes l|q\rangle, \tag{7.9}$$

with $q \in \mathbb{S}_{d_a}$. Hence, the gate $\nu(q)$ may be applied to a register QV by m applications of the fixed interaction gate, U, to the register QV and an ancilla prepared in the state $|q\rangle$. Moreover, if the set

$$\mathcal{S}_{\nu} = \{\nu(q) \mid q \in \mathbb{S}_{d_a}\}, \tag{7.10}$$

is an (approximately[4]) universal set for single-QV gates on the register QVs, then any single-QV gate can be approximated on any register QV by repeated applications of this technique. For example, a universal set would be provided in the qubit-qubit case if $\nu(0) = H$ and $\nu(1) = T$. This will be the method used to implement single-QV gates on the register throughout this chapter. The underlying nature of this method provides one of the reasons why the models in this chapter are fairly unsuited to the setting of QCV ancillas - in the case of QCVs, the computational basis states cannot be exactly realised, and if they are imperfectly realised, via squeezed states, the ancillas will remain entangled with the register QVs and this will be a source of decoherence in the computation, even before non-ideal gate implementation, and other imperfections, are also taken into account.

7.3 The control-gate minimal control model

In the remainder of this chapter, if the register consists of QCVs it will be implicitly assumed that the ancillas are also QCVs, for the same reasons that this was assumed throughout Chapter 5. A general form for interactions that are potentially suitable for minimal control ancilla-based computation has been given in the previous section, and a simple method which may be used to implement local gates has been presented. Specifically, the fixed interaction, U, should obey $U^m = l_a \cdot \mathrm{C}_r^a[\nu]$ for some non-zero $m \in \mathbb{N}$. The simplest case is given by imposing $m = 1$, and hence $U = l_a \cdot \mathrm{C}_r^a[\nu]$. The model introduced in this section will use a fixed interaction of this form. It is not clear how, with an arbitrary gate of this sort, this interaction may be used to mediate an entangling gate on the register, which is essential for universal quantum computation. Instead, consider the slightly less general family of ancilla-register interaction operators

$$\bar{E}_{ar}(v, w, \vartheta) := F_a^{\dagger} \cdot \mathrm{C}_r^a[\nu_{v,w,\vartheta}], \tag{7.11}$$

where $\nu : \mathbb{S}_{d_a} \to U(d)$ is the function defined by

$$\nu_{v,w,\vartheta}(q) = vR(2\pi\vartheta/d_a)^q w, \tag{7.12}$$

for some $v, w \in U(d)$ and some phase-function ϑ with the restriction that $\vartheta : \mathbb{S}_d \to \mathbb{S}_{d_a}$ (the phase functions in a $R(\vartheta)$ gate can, in general, be mappings into $\mathbb{R}$). This gate still has free parameters (u, v and ϑ), that will be left undetermined for now,

[4] Only approximate universality will be relevant in this chapter. This will not always be explicitly stated.

in the interests of flexibility. This interaction is a natural generalisation of the fixed interaction gate in the ADQC model of the previous chapter, denoted $\check{E}_{ar}$, and defined by $\check{E}_{ar} = F_r F_a^{\dagger} \cdot \mathrm{C}_a^r Z$. At this point, this may not be particularly obvious, but this will be expanded upon in the following. To be clear, the quantum computational model introduced in this section will only require access to:

1. The fixed interaction $\bar{E}_{ar}(v, w, \vartheta)$, where u, v and ϑ are fixed, but yet to be specified.

2. Ancillas prepared in the computational basis, $\mathcal{B}$.

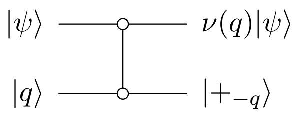
It is now shown how an (approximately) universal set of gates may be implemented on the register in this model, under a certain *assumption* about the ancilla-register interaction. It will then be shown that the parameters in the interaction gate (i.e., v, w and ϑ) can be chosen such that this assumption holds *for certain dimensions for the register and ancillary QVs.* In particular, interactions will be provided that are proven to be universal when the register consists of qubits and the ancillas are of any QV type, and when the register consists of qudits and the ancillas have a range of dimensions. Single-QV gates on the register can be applied using the method of Equation 7.9. Specifically, it immediately follows that

$$|\psi\rangle \otimes |q\rangle \xrightarrow{\bar{E}_{ar}(v,w,\vartheta)} \nu(q)|\psi\rangle \otimes |+_{-q}\rangle. \tag{7.13}$$

Therefore, via ancilla preparation in the state $|q\rangle$, the gate $\nu(q)$ is implemented with the ancilla transformed to the state $|+_{-q}\rangle$, which may be discarded. Hence, ancilla preparation may be used to deterministically implement the gates from the set

$$\mathcal{S}_{v,w,\vartheta} = \{\nu(q) = vR(2\pi q\vartheta/d_a)w \mid q \in \mathbb{S}_{d_a}\}. \tag{7.14}$$

As a circuit diagram, this is simply the single-gate circuit



where two quantum wires connected via a line and two '∘' symbols will be used to denote the fixed interaction gate, $\bar{E}_{ar}(v, w, \vartheta)$, in this section.

For now, simply *assume* that the parameters in the interaction (u, v and ϑ) may be chosen such that $\mathcal{S}_{v,w,\vartheta}$ is a universal single-QV set on the register (this is non-trivial), and this assumption is addressed in Sections 7.3.2 and 7.3.3. Given this assumption, it is now shown that it is possible to use this interaction to implement a two-QV entangling gate on any pair of register QVs, and hence the model is a universal quantum computer. Such an entangling gate may be achieved via the following protocol:

1. Sequentially interact the QVs on which the gate is to act with an ancilla prepared in any state, e.g., $|0\rangle$.
2. Using *additional ancillas* and the fixed ancilla-register interaction, implement $w^\dagger v^\dagger$ on both register QVs. The number of additional ancillas needed and the states from the computational basis they should be prepared in depends on the form of $w^\dagger v^\dagger$ and the available $\nu(q)$ single-QV gates. As such, it depends on the specific form of the interaction and the assumption that $\mathcal{S}_{v,w,\vartheta}$ is a universal set of single-QV gates (this will be returned to below).
3. Sequentially interact the QVs with the first ancilla.

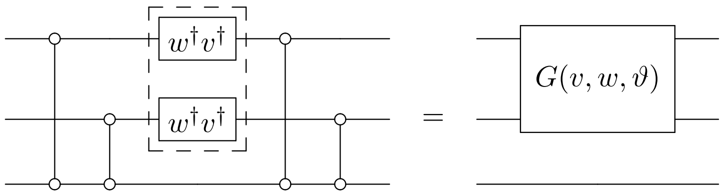
It will be shown below that the effect of this sequence on the register is the symmetric entangling gate[5]

$$G(v,w,\vartheta) = v \otimes v \cdot D\left(\phi_\vartheta\right) \cdot w \otimes w, \tag{7.15}$$

where $\phi_\vartheta : \mathbb{S}_d^2 \to \mathbb{R}$ is the two-variable phase-function given by

$$\phi_\vartheta(p,q) = 2\pi\vartheta(p)\vartheta(q)/d_a, \tag{7.16}$$

and $D(\phi)$ is the general two-QV diagonal gate, which is defined in Equation 6.30 by the mapping $|p\rangle|q\rangle \to e^{i\phi(p,q)}|p\rangle|q\rangle$. It is important to stress that this gate method requires multiple ancillas: one 'entangling' ancilla and further ancillas to implement local gates on the register (the number of which depends on the form of the gates). This method may be summarised by the circuit diagram



(7.17)

where the local gates, enclosed by the dashed box, are implemented by further ancillas prepared appropriately.

From the above presentation, it is not at all clear why (or even if) this gate functions as claimed. However, it is actually a fairly simple adaption of the geometric phase gate from Chapter 5, as is now shown. The ancilla-register interaction,

[5] $D(\phi_\vartheta)$ is entangling for most choices of ϑ, e.g., $\vartheta(q) = q$. A condition which guarantees it is entangling is given as part of Appendix J.

$\bar{E}_{ar}(v,w,\vartheta)$, may be rewritten as

$$\bar{E}_{ar}(v,w,\vartheta) := F_a^{\dagger} \cdot \mathrm{C}_r^a[\nu_{v,w,\vartheta}] = F_a^{\dagger} v_r \cdot \mathrm{C}_a^r[Z(\vartheta)] \cdot w_r, \tag{7.18}$$

which may be shown by checking the action of each side of this equality on arbitrary computational basis states. Note that this equality only makes sense because ϑ was restricted such that $\vartheta(q) \in \mathbb{S}_{d_a}$. To be clear, the non-local part of this gate maps basis states via

$$|q\rangle|q'\rangle \xrightarrow{\mathrm{C}_a^r[Z(\vartheta)]} |q\rangle \otimes Z(\vartheta(q))|q'\rangle, \tag{7.19}$$

and hence, $\bar{E}_{ar}(v,w,\vartheta)$ can be understood as a generalisation of the ADQC interaction gate $\check{E}_{ar} = F_r F_a^{\dagger} \mathrm{C}_a^r Z$, as it reduces to this case when $v = F$, $w = \mathbb{I}$ and $\vartheta(q) = q$. It is now shown why the ancilla-mediated entangling gate, given above, functions as stated. The gate sequence under consideration, given in the LHS of the quantum circuit above, is $\bar{E}_{as}\bar{E}_{ar}w_r^{\dagger}w_s^{\dagger}v_r^{\dagger}v_s^{\dagger}\bar{E}_{as}\bar{E}_{ar}$. Now, using Equation 7.18, it is straight-forward to confirm that

$$(\bar{E}_{as}\bar{E}_{ar})w_r^{\dagger}w_s^{\dagger}v_r^{\dagger}v_s^{\dagger}(\bar{E}_{as}\bar{E}_{ar}) = v_r v_s \cdot S_{rsa} \cdot w_r w_s \tag{7.20}$$

where S_{rsa} is the ancilla-register interaction gate sequence

$$S_{rsa} = F_a^{\dagger}\mathrm{C}_a^s[Z(\vartheta)] \cdot F_a^{\dagger}\mathrm{C}_a^r[Z(\vartheta)] \cdot F_a^{\dagger}\mathrm{C}_a^s[Z(\vartheta)] \cdot F_a^{\dagger}\mathrm{C}_a^r[Z(\vartheta)]. \tag{7.21}$$

By using $F^4 = \mathbb{I}$, the cyclic relation of the Pauli operators under conjugation by F, given in Equation 2.26, and the Weyl commutation relation, given in Equation 2.44, it may be shown that

$$F^{\dagger}Z(q') \cdot F^{\dagger}Z(q) \cdot F^{\dagger}Z(q') \cdot F^{\dagger}Z(q) = X(q')Z(-q)X(-q')Z(q) = \omega^{qq'}, \tag{7.22}$$

noting that this is exactly the geometric phase that the geometric phase gate, from Chapter 5, relies upon. From this relation and Equation 7.19, it follows that S_{rsa} maps register QVs in computational basis states, and an ancilla in an arbitrary state, as

$$|q\rangle|q'\rangle|\psi\rangle \xrightarrow{S_{rsa}} e^{2\pi i\vartheta(q)\vartheta(q')/d_a}|q\rangle|q'\rangle|\psi\rangle, \tag{7.23}$$

which has the action of the $D(\phi_{\vartheta})$ gate, as given in Equation 7.16, on the register QVs. Hence, by combining this with Equation 7.20, to include the effect of the local v and w gates, this has confirmed that the action of this ancilla-register interaction sequence is the $G(v,w,\vartheta)$ gate of Equation 7.15, as claimed. This gate method can be understood as a generalisation of the geometric phase gate of Figure 5.2, using a fixed interaction that includes local gates on the register systems and where the non-local part of the interaction uses a minor generalisation of a controlled Pauli gate (i.e., a C$[Z(\vartheta)]$ gate rather than simply a C$Z(z)$ gate).

7.3.1 Removing the local gates

The protocol given in Equation 7.5, for implementing an entangling gate, includes a step for implementing local gates via further ancillas and the details of this stage are now considered further. By assumption the gate set $\mathbb{S}_{v,w,\vartheta}$ is universal for single-QV gates, which implies that the required local $w^{\dagger}v^{\dagger}$ gates may be approximated to arbitrary accuracy. Hence, this step may be implemented to a given accuracy with some finite number of additional ancillas prepared suitably. In certain cases $w^{\dagger}v^{\dagger}$ may be implementable exactly and with only a small number of ancillas - this will be true in one of the examples, given in Section 7.3.2, for the qubit-qubit model. Moreover, it is not actually necessary to implement this $w^{\dagger}v^{\dagger}$ local gate on one of the two register QVs. This can be deduced by noting that, as the 'entangling' ancilla is assumed to be prepared in some computational basis state $|q\rangle$, the first gate in the entangling sequence enacts only a local $\nu(q)$ gate on the register, and hence the local $w^{\dagger}v^{\dagger}$ gate need not be applied to the first register QV (if this local gate on the first QV isn't included in the gate sequence, the local parts of the induced entangling gate are slightly altered). This raises the question: is the remaining local gate actually required? If wv could be chosen to be diagonal in the computational basis, the answer would indeed be no. However, in this case $\nu(q)$ and $\nu(q')$ commute for all $q, q' \in \mathbb{S}_{d_a}$, and hence the gate set $\mathbb{S}_{v,w,\vartheta} = \{\nu(q) \mid q \in \mathbb{S}_d\}$ cannot form an approximately universal set of single-QV gates.[6] Hence, it appears that the local gates on the second register QV are indeed necessary in this entangling gate protocol. In order to design a more elegant and practical model, in which additional ancillas are not needed to implement a single entangling gate, a different form for the fixed interaction will be used, and this is the topic of Section 7.5.

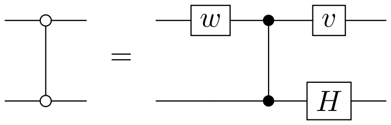
7.3.2 The qubit-qubit model

The qubit-qubit setting is perhaps the most physically relevant for implementing models of this sort, and furthermore, it is conceptually the most straight forward. For both of these reasons, and because specific interactions that can implement universal quantum computation are easily found in this case, the qubit-qubit model is now studied as an interesting special case. The ϑ phase-function parameter in the interaction gate, $\bar{E}_{ar}(v, w, \vartheta)$, is superfluous in this case, and without loss of generality, the interaction may take the form

$$\bar{E}_{ar}(v, w) = H_a v_r \cdot \text{CZ} \cdot w_r, \tag{7.24}$$

[6] This is because if wv is diagonal then $\nu(q)\nu(q') = vR(2\pi q\vartheta/d_a)wvR(2\pi q'\vartheta/d_a)w = vR(2\pi q'\vartheta/d_a)wvR(2\pi q\vartheta/d_a)w = \nu(q')\nu(q)$.

as can be obtained via considering Equation 7.11 when both systems are qubits. For clarity, the decomposition of this interaction into local and non-local parts can be summarised by the circuit



The two implementable local gates, that can be obtained by preparing an ancilla in the state $|0\rangle$ or $|1\rangle$, are $\nu(0) = vw$ and $\nu(1) = vZw$, respectively. The entangling gate implemented via the methods given above is now locally equivalent to cz. In particular, it is the gate $G(v, w) = v \otimes v \cdot \textsc{cz} \cdot w \otimes w$.

Specific choices of the gate parameters v and w are now given that result in $\nu(0)$ and $\nu(1)$ forming a universal set for single qubit gates. This then confirms that this model, using only the fixed interaction gate and ancillas prepared in the computational basis, can implement universal quantum computation on the register. Let $p(\phi)$ be the single-qubit operator defined by the action

$$p(\phi)|q\rangle = \sin\phi|q+1\rangle + (-1)^q \cos\phi|q\rangle, \tag{7.25}$$

or written as a matrix in the computational basis, it is given by

$$p(\phi) = \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix}. \tag{7.26}$$

Now, taking $v = p(\pi/8)$ and $w = p(\pi/8)R(\theta)$, it is straight-forward to show that then $\nu(0) = R(\theta)$ and $\nu(1) = HR(\theta)$, where $R(\theta)$ is the ordinary integer-parameterised rotation gate $R(\theta)|q\rangle = e^{iq\theta}|q\rangle$. This pair of gates form a universal single-qubit set if θ is a generic rotation angle and also for a range of more specific choices, such as if $\theta = \pi/4n$ for any non-zero integer n. In particular, the $n = 1$ case gives $R(\pi/4) = T$, hence $\nu(0) = T$ and $\nu(1) = HT$. The universality of this set follows from the well-known universality of T and H [Boykin et al. (2000)], as $T^7 = T^\dagger$ and so $\nu(1)\nu(0)^7 = H$.

In order to implement the entangling gate protocol of Equation 7.5, it is necessary to be able to implement $w^\dagger v^\dagger = \nu(0)^\dagger$ gates on register qubits. With the H and T-based choice for the interaction gate given above, then $\nu(0)^\dagger = \nu(0)^7$ and so $\nu(0)^\dagger$ can be implemented exactly on a register qubit using seven ancillas, initialised to the state $|0\rangle$, which each interact once with the register qubit. Therefore, the entangling gate protocol of Equation 7.5, in this case, uses a total of fifteen ancillas prepared in the state $|0\rangle$: fourteen to apply $\nu(0)^\dagger$ gates on the two register qubits, in addition to the 'entangling' ancilla that directly mediates the gate.[7] As such, it is clear that the overhead in terms of the number of ancillas and gates consumed to implement each entangling gate is fairly low with this choice for the interaction. It also then follows that the overhead to simulate gates from the set $\{\textsc{cnot}, H, T\}$ on the register, which is commonly used in algorithm decompositions, is similarly low.

7.3.3 Universality beyond the qubit-qubit model

It has now been shown that universal quantum computation can be obtained in this 'minimal control' model in the case of a qubit-qubit quantum computer, and that in this case there are a range of values that the parameters in the interaction gate may take. The case of more general QVs is now briefly considered. To begin, still restrict the register to consist of qubits, but consider the case when the ancillas may be general qudits or QCVs. The local gate that may be obtained by initialising an ancilla to $|q\rangle$ is in this case of the form $\nu(q) = vR(2\pi q\theta/d_a)w$ where $\theta \in \mathbb{S}_{d_a}$, as can be confirmed from Equation 7.14.[8] It is not hard to find choices for the parameters u, v and θ such that this set of $\nu(q)$ gates with $q \in \mathbb{S}_{d_a}$ are universal for single-qubit gates. For example, letting $\theta = 1$, in the case of QCV or even-dimension qudit ancillas $\nu(0) = vw$ and $\nu(d_a/2) = vR(\pi)w = vZw$, and hence any choices for the v and w unitaries that were sufficient for universality in the qubit-qubit case (see above), are also sufficient here. More generally, for generic gates v and w it will follow that $\nu(0) = vw$ is a rotation by an irrational multiple of π around some Bloch sphere axis and $\nu(1) = vR(2\pi/d_a)w$ is a rotation by an irrational multiple of π around some *different* Bloch sphere axis (i.e., it is not parallel to the axis that vw is a rotation around), and this is all that is required for two single-qubit gates to be a universal set for single-qubit unitaries [Nielsen and Chuang (2010)].

Moving beyond the case of a register of qubits, it is not so simple to find specific choices for the gate parameters v, w and ϑ, for which it is straight-forward to verify that $\mathcal{S}_{v,w,\vartheta} = \{\nu(q) = vR(2\pi q\vartheta/d_a)w \mid q \in \mathbb{S}_{d_a}\}$ is a universal single-QV gate set. In the case of a register of qudits and ancillas of any dimension, it seems reasonably likely to me that values for these parameters may always be found that are sufficient for universality. More specifically, it seems likely that the set will be universal for randomly chosen v and w, with an explicit proof of this possibly obtainable based on the work of Lloyd (1995). To conclude this section, a specific construction is given that guarantees universality when the register consists of qudits of any prime

[7] This may be reduced to eight ancillas if the local $\nu(0)^\dagger$ gate is only applied to the second register qubit, which is all that is actually necessary.

[8] In general, the gate $\nu(q)$ is of the form $\nu(q) = vR(2\pi q\vartheta/d_a)w$ where $\vartheta : \mathbb{S}_d \to \mathbb{S}_{d_a}$. Because the $\vartheta(0)$ phase may be always set to zero, as this is only fixing the global phase, when the register systems are qubits this gate may be written as $\nu(q) = vR(2\pi q\theta/d_a)w$ where $R(\cdot)$ is now the scalar-parameterised rotation gate, and $\theta \in \mathbb{S}_{d_a}$.

dimension, with ancillas of any dimension $d_a = nd$ for integer $n \geq 2$. Let ϑ be given by $\vartheta(q) = q(q+1)/2$ modulo d_a, and let $v = F$ and $w = \mathbb{I}$. Then $\nu(q) = FP^{\frac{q}{n}}$ and so $\nu(0) = F$ and $\nu(n) = FP$. These two gates generate the single-qudit Clifford group in prime dimensions (see Section 2.4). Now $\nu(1) = FP^{\frac{1}{n}}$ and if $n \geq 2$, as guaranteed by the condition on the dimension of the ancillas, this is not a Clifford gate. Hence, this set is universal for single-qudit gates as *any* non-Clifford unitary along with the generators of the one-qudit Clifford group is a universal single-qudit gate set in prime dimensions [Campbell et al. (2012); Nebe et al. (2001, 2006)]. This gate set, and the relation between the ancillary and register dimensions, is rather contrived. As such, if this model was to be of further interest in the non-binary case then it would be important to investigate further parameter choices that allow for universal quantum computation. Finally, note that the case of a register of QCVs has not been considered here, which is because the models in this chapter are not particular well-suited to QCVs.

7.4 Measurements for stochastic quantum computation

The 'minimal control' model presented in the previous section is appealing from a physical perspective as it may deterministically implement universal quantum computation on a register via only a single fixed gate and ancillas prepared in the computational basis. However, there are two less convenient features of the model: firstly, it requires many ancillas to implement a single entangling gate, and secondly, it cannot implement entangling gates on the register in a sequential fashion - it requires two interactions between the 'entangling' ancilla and each register QV to implement an entangling gate on the register (see Equation 7.5). In some circumstances it may be highly preferable to implement entangling gates in a sequential fashion, that is, using only one interaction with the ancilla per register QV, and as this is impossible with unitary dynamics [Lamata et al. (2008)], in order to achieve this measurements of the ancillas are required. The natural adaption of the constraints of 'minimal control' ancilla-based quantum computation (see the beginning of Section 7.2) to a measurement-based model is to consider a quantum computer restricted to using only a single fixed ancilla-register interaction, ancillas prepared in a *single state* and single-party measurements on the ancillas of a *fixed operator*. In the following, the model introduced in Section 7.3 is adapted to this measurement-based setting. In advance, it is noted that this model will have certain unappealing features which are unavoidable in a model of this sort, including being universal only in a stochastic sense, which, in my opinion, make it unlikely to be of any practical use. However, it is interesting as a conceptual link between the model of Section 7.3 and the ADQC model of Chapter 6, and also links the work herein to the (qubit-based) models of

Halil-Shah and Oi (2013, 2014), which were developed in parallel to the work here.

7.4.1 The phase basis

For the following, it is necessary to first introduce what I will call the 'phase basis'. Define the *phase basis* by

$$\mathcal{B}_{\times} := \{|\times_q\rangle := PF|q\rangle \mid q \in \mathbb{S}_d\}, \tag{7.27}$$

where P is the phase gate gate first defined in Equation 2.49 (with the parameter $p = 1$). The action of a general Pauli operators on this basis is shown in Appendix H to be

$$\omega^{\xi/2} X(a)Z(b)|\times_q\rangle = \omega^{(\xi+a(a-\varrho_d))/2-a(b+q)}|\times_{q+b-a}\rangle, \tag{7.28}$$

where $a, b \in \mathbb{S}_d$, and the reader is reminded that $\varrho_d = 1$ for odd dimension qudits and $\varrho_d = 0$ otherwise. As an interesting aside, note that $|\times_q\rangle$ is the eigenstate of the (generalised) Pauli Y operator, defined by

$$Y := \omega^{(1+\varrho_d)/2} XZ, \tag{7.29}$$

with eigenvalue ω^{-q}, where for qubits the Y operator is the standard Pauli operator $Y = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$. A measurement in either the computational, conjugate or phase bases of a QV that is in a basis state of one of the other two bases reveals no information about which basis state the QV was in before the measurement. This is because

$$\langle q|\times_{q'}\rangle = \frac{\omega^{qq'}}{\sqrt{d}}\omega^{-\frac{q}{2}(q+\varrho_d)}, \tag{7.30}$$

$$\langle +_q|\times_{q'}\rangle = \frac{\omega^{qq'}}{\sqrt{d}}\omega^{-\frac{q}{2}(q-\varrho_d)}\omega^{-\frac{q'}{2}(q'+\varrho_d)}\omega^{\frac{d-\varrho_d}{8}}, \tag{7.31}$$

and we have already seen that $\langle q|+_{q'}\rangle = \omega^{qq'}/d$. These equations are derived in Appendix H using generalised Gauss sums and integrals.

7.4.2 A stochastic minimal model

There is a natural symmetry between state preparation and projective measurements which may be used to easily transform the model presented in Section 7.3 into a measurement-based model which requires only sequential interactions and only a single ancilla to implement an entangling gate. Specifically, consider a model in which the following fixed operations are available:

1. The fixed interaction gate $\bar{E}_{ar}(v, w, \vartheta)$, as defined in Equation 7.11, where u,

v and ϑ are fixed, but yet to be specified.

2. Measurements of ancillas of the fixed operator: $\hat{x}$ (i.e., computational basis measurements).

3. Ancillas prepared in the single state: $|\psi_0\rangle = F|\times_0\rangle$.

Sequential interactions of an ancilla with two register QVs and followed by a measurement of $\hat{x}$ on the ancilla may implement an entangling gate. Specifically, the gate implemented is

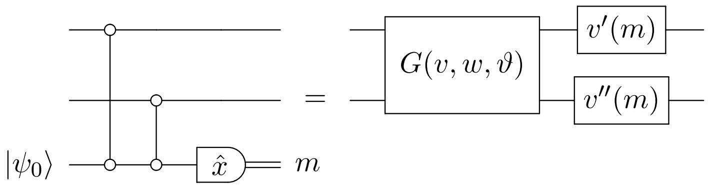
$$\frac{\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle}{\|\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle\|} = v'_r(m)v''_s(m) \cdot G(v,w,\vartheta), \tag{7.32}$$

where $G(v,w,\vartheta)$ is the entangling gate defined in Equation 7.15, and $v'(m)$ and $v''(m)$ are the measurement-outcome dependent gates

$$v'(m) = vR(-2m\pi\vartheta/d_a)v^{\dagger}, \tag{7.33}$$

$$v''(m) = vR(2m\pi\vartheta/d_a)R(-\pi\vartheta(\vartheta+\varrho_{d_a})/d_a)v^{\dagger}. \tag{7.34}$$

Hence, up to measurement-induced 'errors' this is exactly the same gate as obtained via the globally unitary sequence of Equation 7.5.[9] The substantially advantages of this gate method are that it requires only a single ancilla and a minimal number of applications of the interaction gate. It is not immediately obvious why Equation 7.32 holds, however, the intuitive reason is that the interaction gates permute the phase-basis state of the ancilla dependent on the state of the two register QVs (see Equation 7.28), encoding this information into the ancilla. The measurement induced phase is then dependent on this global property of the two QVs (see Equation 7.30), which therefore is equivalent to implementing an entangling gate on the two register QVs.[10] A formal derivation of Equation 7.32 is included in Appendix J. This measurement-based gate may be summarised by the circuit diagram



An initialised ancilla that interacts with a register QV and is then measured,

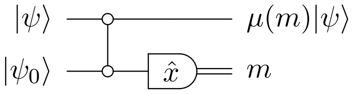
[9] In this model, it is perhaps a misnomer to term the local m-dependent gate 'errors', as will be seen below.

[10] In some ways this is quite different to the entangling gate in ADQC, in which the measurement-induced phase only creates the local error - see the discussion below Equation 6.6.

implements the single-QV gate

$$\frac{\langle m|\bar{E}_{ar}|\psi_0\rangle}{\|\langle m|\bar{E}_{ar}|\psi_0\rangle\|} = \tilde{v}R\left(-2m\pi\vartheta/d_a\right)w =: \mu(m), \tag{7.35}$$

for measurement outcome $m \in \mathbb{S}_{d_a}$, where $\tilde{v} = vR(\pi\vartheta\left(\vartheta - \varrho_{d_a}\right)/d_a)$. The derivation is simple, but is included in Appendix J for completeness. This gate method may be summarised by the circuit diagram



The gate implemented here, $\mu(m)$, is essential the same as that implemented in the global unitary model (see Equation 7.12) - and by a simple mapping in the interaction gate parameters they are identical - but with the crucial difference that now the gate that is implemented is *random* as it is controlled by the measurement outcome, rather than being deterministically fixed by the state the ancilla is prepared in. As the local gate sets are essentially the same, the universality discussions of Sections 7.3.2 and 7.3.3 also apply here and any set of parameters that provide universality for the globally unitary model can be mapped onto a set of parameters for which $\mathbb{S}'_{v,w,\vartheta} = \{\mu(m) \mid m \in \mathbb{S}_{d_a}\}$ is a universal single-QV gate set.

The gate methods given in this section, for suitable choices of the interaction parameters, allow for an entangling gate to be deterministically implemented on the register, up to measurement-outcome dependent local gates, and gates from a universal single-QV set to be stochastically applied to the register. In other words, when applying a local gate, which gate from the available set is actually implemented is entirely random and fixed by the measurement outcome - which is known after the measurement, but which cannot be predetermined. Hence, this scheme (assuming a universal gate set) can then implement universal quantum computation *stochastically*, in the sense that each single-QV gate in a gate sequence can be implemented to a given desired accuracy with a stochastic sequence of gates of indeterminate length and entangling gates can be deterministically applied. This is a form of what is called *repeat-until-success* (RUS) gate implementation [Bocharov et al. (2015); Halil-Shah and Oi (2013, 2014); Lim et al. (2005); Paetznick and Svore (2014)] but unlike in certain scenarios (i.e., see Bocharov et al. (2015); Paetznick and Svore (2014) where RUS techniques are used to achieve low-gate counts), in this case, the probabilistic nature of the gate implementation clearly creates a potentially massive gate-count (and depth) overhead, which is highly undesirable. This overhead has been considered elsewhere for a similar model with qubits, proposed by Halil-Shah and Oi (2013, 2014)[11], and is discussed no further here beyond noting that even for qubits it appears that the gate-count to achieve a target unitary via a random walk can be massive [Halil-Shah and Oi (2013)]. Hence, although this measurement-based model is interesting as it provides a conceptual link between the ADQC model of Chapter 6 and the globally unitary 'minimal control' model of Section 7.3, and also because it highlights the crucial role that *variable*-basis measurement play in ADQC, it does not appear to be a sensible model to pursue in practice. As such, it is investigated no further here.

7.5 The swap-gate minimal control model

In this section we return to the globally unitary setting of the constraints of 'minimal control', as outlined in the introduction to this chapter, and an alternative model that fits into this paradigm is presented which in many respects improves on that introduced in Section 7.3. In particular, it will require only a single ancilla to mediate an entangling gate on two register QVs, and that gate will require only three applications of the fixed ancilla-register interaction gate - which is the minimal possible with unitary dynamics [Lamata et al. (2008)]. The cost of the simplicity of this model is that it requires the ancillary and register systems to have the same dimension (denoted d), as will be assumed from now on in this section. This is because it is based on the SWAP gate. It should be noted that the following model can be understood as a simple extension of the globally unitary model presented in Section 6.4.3, but that model required local controls (in particular, local unitary gates) on the ancillas which will now no-longer be necessary.

Consider a fixed ancilla-register interaction of the form

$$\hat{E}_{ar}(u,\phi) := u_a \cdot \text{SWAP} \cdot D_{ra}(\phi), \tag{7.36}$$

with some $u \in U(d)$ and some two-parameter function $\phi : \mathbb{S}_d^2 \to \mathbb{R}$, which for now are left unspecified in the interests of flexibility. Note that the ordering of the r and a labels on the $D(\phi)$ gate is relevant as it is not in general symmetric (this has already been discussed in Section 6.4.3). To be clear, this notation is used to mean that

$$|q\rangle_r |q'\rangle_a \xrightarrow{D_{ra}(\phi)} e^{i\phi(q,q')} |q\rangle_r |q'\rangle_a, \tag{7.37}$$

that is, the first (second) label denotes the first (second) variable of ϕ. Consider now a quantum computer which only has access to:

[11] The qubit-qubit case of the model in this section has many features in common with that in Halil-Shah and Oi (2014). There are also certain differences, but the essential concept of the models is the same.

1. The fixed interaction gate $\hat{E}_{ar}(u,\phi)$, which may be applied to any ancilla-register pair, where u and ϕ are fixed, but yet to be specified.

2. Ancillas prepared in the computational basis, $\mathcal{B}$.

It is straight-forward to confirm that the fixed interaction gate, when either the ancilla or the register QV is in a computational basis state, implements the mappings

$$|\psi\rangle \otimes |q\rangle \xrightarrow{\hat{E}_{ar}(u,\phi)} |q\rangle \otimes uR(\phi(\cdot,q))|\psi\rangle, \tag{7.38}$$

$$|q\rangle \otimes |\psi\rangle \xrightarrow{\hat{E}_{ar}(u,\phi))} R(\phi(q,\cdot))|\psi\rangle \otimes u|q\rangle, \tag{7.39}$$

where $\phi(\cdot,q)$ and $\phi(q,\cdot)$ are the one-parameter phase-functions obtained from ϕ with the first and second variables fixed to q, respectively. Therefore, if either QV is in a computational basis state then the gate acts as a SWAP along with local gates. Hence, an entangling gate may be implemented on a register QV pair using only three interactions and an ancilla prepared in any computational basis state. In particular, it is simple to confirm that

$$|\psi\rangle_{rs} \otimes |0\rangle \xrightarrow{\hat{E}_{ar}\hat{E}_{as}\hat{E}_{ar}} W_{rs}(u,\phi)|\psi\rangle_{rs} \otimes u|0\rangle, \tag{7.40}$$

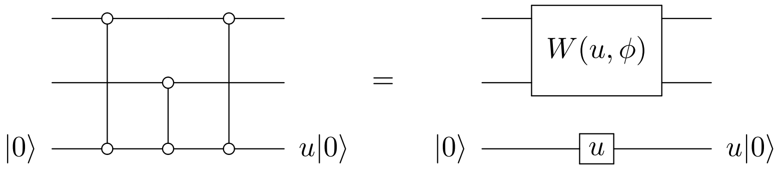
where $W_{rs}(u,\phi)$ is the (in general) entangling gate

$$W_{rs}(u,\phi) = R_r(\phi(0,\cdot)) \cdot \hat{E}_{rs}(u,\phi) \cdot u_r R_r(\phi(\cdot,0)). \tag{7.41}$$

The $W_{rs}(u,\phi)$ gate is an entangling gate except for special choices of ϕ - it may be easily confirmed that it is entangling if there is some $q,q' \in \mathbb{S}_d$ such that

$$\phi(q,q) + \phi(q',q') - \phi(q,q') - \phi(q',q) \bmod 2\pi \neq 0, \tag{7.42}$$

which is generically true. This entangling gate implementation method may be summarised by the circuit diagram



where, as in the previous sections of this chapter, two quantum wires connected via a line and two '∘' symbols are used to denote the fixed interaction gate, which is now $\hat{E}_{ar}(u,\phi)$. Note that this is essentially the same as the two-QV entangling gate method of Section 6.4.3, and in particular Figure 6.5.

It is now shown how a set of local gates can be implemented in this model via preparing ancillas in different states from the computational basis. In Section 7.2, general forms for interactions that were potentially suitable for 'minimal control' ancilla-based quantum computation were given - and in particular, it was suggested that some integer power of the interaction should be of the form $l_a \cdot \mathrm{C}_r^a[\nu]$ where $\nu : \mathbb{S}_{d_a} \to U(d)$ (see Equation 7.8). Such interactions may then be used in an obvious manner to implement local gates on the register: preparing the ancilla in $|q\rangle$ can be used to implement $\nu(q)$, as summarised in Equation 7.9. Here, this interaction is indeed of this form - it is easily confirmed that

$$\hat{E}_{ar}^2(u,\phi) = u_a \cdot \mathrm{C}_r^a[s_{u,\phi}], \tag{7.43}$$

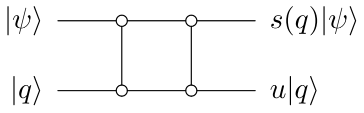
where $s_{u,\phi} : \mathbb{S}_d \to U(d)$ is given by

$$s_{u,\phi}(q) = R(\phi(q,\cdot))uR(\phi(\cdot,q)). \tag{7.44}$$

Hence, two interactions of an ancilla prepared in the state $|q\rangle$ with a single register QV may implement the gate $s(q)$, as clearly

$$|\psi\rangle \otimes |q\rangle \xrightarrow{\hat{E}_{ar}\hat{E}_{ar}} s(q)|\psi\rangle \otimes u|q\rangle. \tag{7.45}$$

This gate may be summarised in the circuit diagram



(7.46)

Note that the price of using a swap-based interaction is that two gates are required to implement the local unitaries - which is because the quantum information must be swapped back into the register. This is contrast to the single application of the (different) fixed interaction required in Section 7.3.

The two gate methods given in this section allow the deterministic implementation of the gate set

$$\mathcal{S}_{sc} = \{W(u,\phi), s_{u,\phi}(q) \mid q \in \mathbb{S}_d\}, \tag{7.47}$$

on any register QVs. This gate set is sufficient for universal quantum computation if the single-QV gates in the set are a universal set of single-QV gates, although this is not *required* for universality. Clearly, it is important to investigate whether there are choices of the interaction gate parameters, u and ϕ, that are sufficient for universal quantum computation. Because the qubit-qubit model is the simplest case, and because it is probably of most practical relevance, this special case is considered first in Section 7.5.1, before the more general QV case is covered in Section 7.5.2. However, before turning to this, one final issue is considered - how the results of the computation may be read-out from the register at the end of the computation if measurements can only be performed on the ancillas. There is a very simple method to achieve this: The computation is altered so that instead of the intended global unitary, an additional $R(-\phi(\cdot,q))u^{\dagger}$ gate is applied to each of the QVs which are to be measured. A QV is then read-out by interacting it once with an ancilla which is then measured. Clearly, as this swaps the QVs and applies a $uR(\phi(\cdot,q))$ gate, the measurement of the ancilla is identical to a direct measurement of the register QV without the unwanted additional $R(-\phi(\cdot,q))u^{\dagger}$ gate, which is the intended final state of this QV.

7.5.1 The qubit-qubit model

Consider the qubit sub-case of the model introduced in this section. Let ϕ_θ be the two-parameter phase-function given by $\phi_\theta(q,q') = qq'\theta$ for some $\theta \in \mathbb{R}$. A simple example of a specific form for the ancilla-register interaction, $\hat{E}_{ar}(u,\phi)$, such that $s(0)$ and $s(1)$ form a universal set for single-qubit gates, is given by taking $u = H$, and $\phi = \phi_{\pi/4}$. The fixed interaction then takes the form

$$\hat{E}_{ar}\left(H,\phi_{\pi/4}\right) = H_a \cdot \textsc{swap} \cdot CT, \tag{7.48}$$

and hence $s(0) = H$ and $s(1) = THT$ (from Equation 7.44). A proof of the universality of the set $\{H, THT\}$ for single-qubit gates is included as Appendix I. The entangling gate induced on a pair of register qubits in this model will then have the specific form

$$W_{rs}\left(H,\phi_{\pi/4}\right) = H_r \cdot \textsc{swap} \cdot CT \cdot H_r, \tag{7.49}$$

and this can easily simulate CNOT with four applications of this gate as

$$W_{rs}\left(H,\phi_{\pi/4}\right)^4 = \textsc{cnot}. \tag{7.50}$$

Moreover, with this particular interaction, any quantum computation can still be implemented even if only ancillas prepared in the *single state* $|0\rangle$ are available. This is because, with ancillas prepared in $|0\rangle$, the gates $s(0) = H$ and $W_{rs}\left(H,\phi_{\pi/4}\right)$ may be implemented on the register, and

$$s_r(0) \cdot W_{rs}\left(H,\phi_{\pi/4}\right)^2 \cdot s_r(0) = CP, \tag{7.51}$$

as $H^2 = \mathbb{I}$ and $W_{rs}(H,\phi_{\pi/4})^2 = H_r \cdot CP \cdot H_r$, which follows because $P = T^2$. Therefore the gates H and CP can be implemented on any register qubit using only ancillas prepared in $|0\rangle$, and this pair of gates has been shown to be sufficient for universal quantum computation by Kitaev (1997).[12]

Beyond this specific T-based gate, other suitable interactions to achieve universality in this model include $\hat{E}_{ar}(H, \phi_{\theta})$ for generic values of θ, which follows because the set $\{H, R(\theta)HR(\theta)\}$ is a universal single-qubit set for such θ - as is discussed briefly in Appendix I. Furthermore, with more general interactions of this sort, simulating CNOT is still straight-forward and requires a low gate-count overhead: suitable gate sequences for obtaining CNOT gates from any two-qubit entangling gate can be found using the method of Bremner et al. (2002).

7.5.2 Universality beyond the qubit-qubit model

It has now been confirmed that the swap-based 'minimal control' model proposed in this section can implement any quantum computation on the register in the qubit sub-case, and hence the case of d-dimensional qudits for arbitrary d is now considered. It seems highly likely that generic choices for the parameters u and ϕ will be sufficient for universality for all dimensions of qudit, and again it may be possible to confirm this using the work of Lloyd (1995). However, in the interests of completeness and to confirm that this model can implement universal quantum computation regardless of whether this conjecture is correct, a more specific choice for the interaction parameters is now given which it can be explicitly shown are sufficient for universal quantum computation.

Let $u = F$ and consider the case when ϕ is any two-parameter phase function such that $\phi(q, q') = 0$ for all $q, q' \in \mathbb{Z}(d)$ except when $q' = d-1$, in which case $\phi(q, d-1) = \theta_q$ with θ_q randomly (and independently) sampled from $\mathbb{R}$ for all non-zero $q \in \mathbb{Z}(d)$ and $\theta_0 = 0$. Because the local gate that is implemented by initialising the ancilla to $|q\rangle$, and applying the procedure of Equation 7.46, is $s_{u,\phi}(q) = R(\phi(q, \cdot))uR(\phi(\cdot, q))$, it follows that by preparing an ancilla in the state $|0\rangle$ then $s(0) = F$ can be applied to the register. It is therefore also possible to implement the gates $s(q)s(0)^3 = R(\phi(q, \cdot))$ for $0 < q < d-1$. Because $\phi(q, q') = \theta_q$ for $q' = d-1$, and $\phi(q, q') = 0$ otherwise, then this gives a method for implementing a gate which applies no phase to all the basis states except the $|d-1\rangle$ basis state, for which it applies a 'generic' phase (which is different for each q). Because these phases are generic, it is therefore possible to approximate any gate which applies only a phase to this last basis state to arbitrary accuracy. Now, $s(d-1) = R(\phi(d-1, \cdot))FR(\phi(\cdot, d-1))$, and $R(\phi(d-1, \cdot))$ is a gate which applies only a phase to the last basis state. Because with $s(q)$ gates with $q = 0, \ldots, d-2$, the gate $R(-\phi(d-1, \cdot))$ can be implemented to arbitrary accuracy and $s(0)^3 = F^{\dagger}$, it is possible to obtain the gate $s'(d-1) = R(\phi(\cdot, d-1))$ from

[12] The exact sense in which this set is universal is stated clearly by Aharonov (2003).

the available set. Now, $\phi(\cdot, d-1)$ is a generic phase function[13], as implied by the conditions on ϕ given above, and as a rotation gate with a generic phase function in combination with the F gate (obtained as $s(0)$) is a universal set of single-qudit gates, as shown in Appendix G, this confirms the universality of the available gate set with an interaction gate of this form.

The construction given above may seem rather contrived, however it represents a physically sensible gate - a $D_{ra}(\phi)$ gate with ϕ as described above is a gate which implements phases on the register qudit only if the ancilla qudit is in the state $|d-1\rangle$. However, if the model proposed in this section were to be of further interest outside the qubit-based setting, it would be important to undertake a more thorough investigation of which parameter choices in the interaction are sufficient for universality. Finally, note that universality in the QCV model has not been investigated as it does not seem likely that this model will be of practical interest in this case. One reason for this is that Gaussian (i.e., Clifford) operations are generally much simpler to implement than non-Gaussian operations in the most promising QCV setting of optics (e.g., a Gaussian entangling gate can be achieved via a beam-splitter). Hence, in this setting it makes more sense to consider a Gaussian computer aided by some non-Gaussian operator used as sparingly as possible and this does not fit into the paradigm considered here, whereby a quantum computer is based entirely on a single gate which must be non-Gaussian to achieve universality.

7.6 Physical implementation

The models proposed in this chapter are physically motived, and hence it is useful to briefly consider candidate physical systems in which they may be of interest, and Hamiltonians with which appropriate interaction gates may be generated. Consider first the model of Section 7.3, which is based on interactions that were formed from 'generalised control gates'. In particular, the interaction was a simple extension of a controlled Pauli $Z(q)$ gate, and in the most physically relevant case of qubits it reduced to an interaction that is locally equivalent to CZ (see Section 7.3.2). Generating controlled Pauli operators has been considered in detail in Section 5.5, in the context of the geometric phase gates, and these discussions largely carry over to this model. For this reason, and because the swap-based model of Section 7.5 has significant advantages, physical implementation of the 'minimal control' model of Section 7.3 is considered no further here.

The swap-based model of Section 7.5 is now considered, with the focus on the case of qubits, as this is likely to be of most practical relevance. The two-qubit

[13] Note that, although here the $\phi(0, d-1) = 0$, i.e., only the other $d-1$ values of $\phi(\cdot, d-1)$ are 'generic', this is irrelevant as this may be considered to be fixing the global phase of the rotation gate.

Hamiltonian

$$\hat{H}_{XYZ}(\theta) = \pi(X \otimes X + Y \otimes Y) + (\pi - \theta) Z \otimes Z, \tag{7.52}$$

naturally arises in spin systems [Doherty and Wardrop (2013)], and certain spin systems are potentially relevant to ancilla-based gate methods. For example, nuclear spins in diamond exhibit particularly long coherence times [Neumann et al. (2010, 2008)] as they are well isolated, and they may be interfaced via ancillary electronic spins in nitrogen-vacancy (NV) defects [Robledo et al. (2011); Taminiau et al. (2014); Waldherr et al. (2014)]. Denoting $U(\hat{H}, t) = \exp(-i\hat{H}t)$, a direct Eigen-system calculation may be used to confirm that

$$U(\hat{H}_{XYZ}(\theta), 1/4) = R(-\theta/2) \otimes R(-\theta/2) \cdot \text{SWAP} \cdot \text{C}R(\theta). \tag{7.53}$$

The unitary $U(H_{cs}(\theta), 1/4)$ followed by the fixed local gate $u' = R(\theta/2)uR(\theta/2)$ on the ancilla is an appropriate interaction for the qubit case of the swap-based model of Section 7.5 (with certain values of the parameters u and θ). In particular, it is straightforward to show that, with this interaction gate, the single-qubit gate set which can then be implemented on the register by ancilla preparation consists of $s(0) = u$ and $s(1) = R(\theta)uR(\theta)$, which is universal for a range of u and θ (see the discussions of Section 7.5.1 and 7.5.2), e.g., $u = H$ and generic θ, or $\theta = \pi/4$. Note that although this interaction is not simply generated by evolving the ancilla and register qubit via $\hat{H}_{XYZ}(\theta)$, as it also requires the implementation of a local unitary on the ancilla, this is a *fixed* gate on the ancilla after every ancilla-register interaction via $\hat{H}_{XYZ}(\theta)$, and hence this can be a fixed element in an experimental setup or incorporated into the free evolution of the ancilla between interactions. For example, if the ancillary qubit is photonic the local operation can potentially be performed by fixed linear optics after each ancilla-register interaction. Given that ancillary photons have been used to mediate gates in many experimental setups, for example with atomic [Reiserer et al. (2014); Tiecke et al. (2014)] or spin [Carter et al. (2013); Luxmoore et al. (2013)] qubits, this setting is highly relevant to models of this sort.

Although in some physical settings, such as the photonic case discussed above, the fixed local operation on the ancillary qubits after each interaction via $\hat{H}_{XYZ}(\theta)$ may be convenient or natural, in other cases it may be problematic or it may negate the benefits of the 'minimal control' models introduced in this chapter. However, it is also obviously possible to find Hamiltonians that directly implement suitable interactions for either of the models proposed in this chapter (including in the qudit case), and this can be achieved via a direct brute-force diagonalisation of any given suitable interaction unitary. Alternatively, an evolution via the Hamiltonian

$\hat{H}_{XYZ}(\theta)$, for $\theta \neq 0$ modulo 2π, generates unitaries that are directly suitable for implementing the globally-unitary swap-based model of Section 6.4.3, which relied on the application of local unitary gates on the ancillas to achieve universality. Finally, it is noted that $\hat{H}_{XYZ}(\pi)$, which is known as the two-qubit XY exchange Hamiltonian, generates the maximally entangling unitary

$$U(\hat{H}_{XYZ}(\pi), 1/4) = P^{\dagger} \otimes P^{\dagger} \cdot \textsc{swap} \cdot \textsc{cz}. \tag{7.54}$$

This gate can still be used for the fixed interaction in the globally unitary model of Section 6.4.3, but it is also locally equivalent to the swap-based interaction suitable for implementing ancilla-driven quantum computation (see Section 6.4.2), with this model relevant in settings where variable-basis measurements of the ancillas are available (e.g., this is potentially possible in optics).

7.7 Conclusions

In this chapter ancilla-based models of computation have been proposed in which universal quantum computation on a register is implemented using *only* a single fixed ancilla-register interaction and ancillas prepared in the computational basis. These models may be naturally termed *minimal control* ancilla-based quantum computers as they require both a minimal level of access to the computational register, which can hence be optimised for long coherence times, and highly limited control over the ancillas, which may be optimised for a single high-quality interaction with the register systems.

In the first part of this chapter, a minimal control model has been presented which employs an interaction based on a ‘generalised control gate’. Interestingly, the gate methods in this model are closely related to both the geometric phase gates of Chapter 5 and those of the measurement-based ancilla-driven quantum computer, as investigated in Chapter 6. Although this model has the advantages of ‘minimal control’, as outlined above, it has the serious disadvantage that it requires many ancillas and many applications of the ancilla-register interaction gate to implement a single entangling gate on a pair of register QVs. This is a particularly undesirable complication from a physical perspective. One method for removing the necessity for these additional ancillas, whilst still considering quantum computation with highly limited controls, is to adapt the model to allow measurements on the ancillas of a *fixed* operator whilst also constraining the preparation of ancillas to a singe state. However, quantum computation in this fashion results in a model that is unavoidably stochastic in nature, in the sense that gates from the universal set can only be implemented randomly, with the exact gate implemented dependent on each measurement outcome. To implement a given quantum computation requires gate sequences of an indeterminate length. A model of this sort has been proposed elsewhere (for qubits) by Halil-Shah and Oi (2014) and the stochastic nature of the computation results in a gate-count overhead [Halil-Shah and Oi (2013)], which is in my opinion highly unappealing from a practical perspective.

Hence, in the latter part of this chapter a second 'minimal control' model was developed which uses a swap-based fixed interaction (and is globally unitary). This model requires only a single ancilla, and three applications of the fixed interaction gate, to implement an entangling gate on any pair of register qubits, which is a minimal use of resources in any ancilla-based and globally unitary scheme [Lamata et al. (2008)]. Furthermore, in the qubit sub-case it was shown that, for certain fixed interaction gates, any quantum computation can be implemented on the register even if the ancillas can only be prepared in a *single fixed state*, which it can be argued is a completely minimal scheme for universal ancilla-based computation. Hence, this swap-based model is highly appealing from both a physical and theoretical perspective. In the penultimate section of this chapter, the prospects for physically implementing the models proposed in this chapter were considered. The general setting in which these minimal control models have the potential to be of particular relevance is when limited controls are available over both the register and ancillary systems, for example, the low-control setting of either qubit or qudit scatting interactions [Ciccarello et al. (2008)]. A more detailed study of physical systems which might be particularly well suited to the models proposed in this chapter would be an interesting topic for future work.

The models proposed in this chapter provide a method for realising quantum computation on a well-isolated register with a practical and simple scheme. In particular, they allow the optimisation of the physical systems entirely for coherence times and the high fidelity implementation of a single gate. Finally, these models shed a fresh light on the minimal controls that are required for a universal quantum computer and they show that such a device need only have access to a single fixed ancilla-register gate, with the computation to be implemented controlled by choosing the initial states of the ancillas.

Chapter 8

Conclusions

Quantum computers hold the potential to solve problems that are believed to be classically intractable [Aaronson and Arkhipov (2011); Shor (1994, 1997)] and there are a range of important tasks that are expected to be amenable to a quantum-enhanced speed-up, from integer-factoring [Shor (1994, 1997)] and related tasks, to machine-learning [Schuld et al. (2015)], database searching [Grover (1996)] and simulation of quantum systems [Brown et al. (2010)]. The simplest basic element that a quantum computer may be constructed from is the 2-level qubit. However, there is no *a priori* reason that quantum computation should be formulated with two-level quantum systems, and they may instead employ d-level qudits or quantum continuous variables (QCVs). Indeed, as has been covered in detail in Chapter 1, there are good reasons for considering these more general quantum variables (QVs), ranging from the physical availability of non-binary qudits and QCVs, and the experimental progress made in manipulating them, e.g., see Anderson et al. (2015); Chen et al. (2014); Smith et al. (2013); Ukai et al. (2011); Yokoyama et al. (2013), to more abstract advantages, such as improved error-correction techniques for non-binary qudits [Andrist et al. (2015); Anwar et al. (2014); Campbell (2014); Watson et al. (2015)].

Quantum computation with qubits is the simplest case in theory, and in many respects it is the most advanced experimentally (e.g., see Barends et al. (2014)). However, given that no one has yet built a useful quantum computer and that there are certain known advantages in going beyond the qubit paradigm, it seems prudent to keep open the option of basing such a device on something other than qubits. With this in mind, one contribution of this thesis has been to introduce a formulation of quantum computation that encompasses all types of quantum variables - i.e., it applies to qubits, non-binary qudits and QCVs simultaneously. This formalism, introduced in Chapter 2 and developed throughout, may be used to succinctly derive results that are applicable in all three settings which have largely been considered separately in the literature, and furthermore it may also be used to easily highlight any differences between quantum computation with the different types of QVs. Indeed, the utility of this dimension-independent formulation of quantum computation has been demonstrated by Chapters 3 to 7 of this thesis, which present results that largely apply to all types of quantum variables.

Quantum circuits and the one-way quantum computer

The *quantum circuit model*, in which elementary gates are directly applied to physical QVs via Schrödinger-equation derived unitary evolution, is the most well-known and simple model for a quantum computer. However, this requires the precise application of one and two-body Hamiltonians on-demand to a register of QVs, each of which must also be isolated to minimise environment-induced decoherence as much as is necessary. These technical challenges motivate the exploration of alternative paradigms for quantum computation. One such alternative that has been studied in this thesis is the *one-way quantum computer* (1WQC), introduced by Raussendorf and Briegel (2001) in the case of qubits, and extended to qudits and QCVs by Zhou et al. (2003) and Menicucci et al. (2006) respectively. In the 1WQC, the unitary gates of a computation are carried out on a logical level using local (i.e., single-QV) measurements on a prepared entangled state. As such, this model is very promising from a physical perspective, as creating large entangled states is potentially much easier than applying entangling gates on-demand, with this point of view backed-up by impressive experimental progress in implementing this model [Bell et al. (2014); Chen et al. (2007, 2014); Lanyon et al. (2013); Su et al. (2013); Tame et al. (2014); Ukai et al. (2011); Yokoyama et al. (2013)].

The properties of qubit-based 1WQC have been extensively investigated, for example, see Anders and Browne (2009); Broadbent and Kashefi (2009); Browne et al. (2007, 2011); Danos et al. (2007, 2009); Duncan and Perdrix (2010); Raussendorf et al. (2003). However, there is much less known about this model in the more general case of qudits or QCVs, and this has been addressed in Chapter 4 of this thesis, using the setting of general QVs. In order to study the properties of the 1WQC with general QVs, and in particular to compare it to quantum circuits, it is clear that an understanding of qudit and QCV quantum circuits is required. To my knowledge, the relevant circuits have not been studied in the literature, and hence, the necessary general QV quantum circuits were first investigated in Chapter 3.

In Chapter 3, two classes of the quantum circuit model were defined and investigated: *standard quantum circuits* and *unbounded fan-out circuits*. ‘Standard quantum circuits’ are those in which only bounded-input-size gates may be applied in a unit of depth (a proxy for time), which is in contrast to ‘unbounded fan-out circuits’, which allow QVs to be ‘quantum-copied’ into any number of auxiliary QVs in a unit of depth. More precisely, 'unbounded fan-out circuits' have access to FANOUT gates for unbounded input size, where this gate maps computational basis states as

$$|q\rangle \otimes |q_1\rangle|q_2\rangle \dots |q_n\rangle \xrightarrow{\text{FANOUT}} |q\rangle \otimes |q_1 + q\rangle|q_2 + q\rangle, \dots |q_n + q\rangle, \tag{8.1}$$

and by 'unbounded input size' it is meant that the number of input QVs to the gate, $n + 1$, may be as large as the number of QVs in the quantum circuit. This gate facilitates 'quantum copying' of a logical QV into any number of auxiliary QVs, as the above relation implies that

$$\sum_q \alpha_q |q\rangle \otimes |0\rangle|0\rangle \dots |0\rangle \xrightarrow{\text{FANOUT}} \sum_q \alpha_q |q\rangle \otimes |q\rangle|q\rangle \dots |q\rangle. \tag{8.2}$$

Given that this delocalises the quantum information in one QV over many QVs, it should perhaps not be surprising that 'unbounded fan-out circuits' are fundamentally more powerful for constant depth parallel computations than the more physically well-motivated 'standard quantum circuits'.

To be more specific, I have shown that unbounded fan-out gates can be used for constant depth implementations of certain commuting circuits and any n-QV Clifford gate.[1] Furthermore, this is a fundamental improvement on what can be achieved with 'standard quantum circuits', as it was shown that simulating the unbounded fan-out gate with bounded input-size gates *requires* logarithmic depth. For the qubit sub-case, logarithmic and constant depth unbounded fan-out circuits have been previously investigated in detail by Høyer and Špalek (2003, 2005) and others, see e.g., Moore and Nilsson (2001); Takahashi and Tani (2013); Takahashi et al. (2010). Interestingly, there are a range of logarithmic and constant depth qubit unbounded fan-out circuits that are not included as a sub-case of any of the general QV results I have presented herein. For example, for qubits, there is a constant depth unbounded fan-out circuit that can approximate the quantum Fourier transform (QFT) [Høyer and Špalek (2005)]. Because the QFT is an important component in many quantum algorithms, in future work it would be interesting to consider whether this result can be extended to the QFT on a qudit register, particularly as Parasa and Perkowski (2011, 2012) have shown that the qudit QFT circuit has a range of advantages over the binary version.

The investigations into the properties of quantum circuits with general QVs, presented in Chapter 3, laid the necessary foundations for a full comparison of the computational depth properties of the quantum circuit model and the general QV 1WQC, which was then undertaken in Chapter 4. In the first parts of this chapter a *measurement pattern* formulation of the 1WQC was given which includes

[1] Modulo certain complications in the QCV case.

and goes beyond the 'cluster state' paradigm [Menicucci et al. (2006); Zhou et al. (2003)], in which computations are implemented via measurements on a pre-prepared entangled state. These highly flexible 'measurement patterns' are well-suited to a comparison with the gate model, and using this construction a computational depth reduction protocol was then developed, extending the qubit-based work of Danos et al. (2007). A simple procedure for mapping between quantum circuits and measurement patterns was then proposed, and the implication of these mappings is that the depth complexity of the 1WQC is exactly equivalent to that of unbounded fan-out circuits. This confirms and makes precise the parallelism inherent in 1WQC and extends a qubit-based result of Browne et al. (2011) to the setting of more general QVs.

One interesting consequence of these results is that it shows that the parallel power of unbounded fan-out circuits - a model of quantum computation that is hard to justify on physical grounds - is inherently available to the physically promising 1WQC model. The root of these computational advantages associated with 1WQC is that the measurements in the computation allow parts of the computation to be moved from quantum into *classical* processing, which in the analysis given here has been assumed to be free. This classical side-processing of measurement outcomes is a crucial part of the computational model. The final contribution of Chapter 4 was to briefly comment upon the role of quantum resource states in enhancing classical processing. In particular, an extension to qudits was given of the three-qubit GHZ state protocol for elevating a 'parity' computer to universal classical processing proposed by Anders and Browne (2009). An interesting avenue for future research would be to extend these investigations into the interplay between classical and quantum resources in non-binary qudit 1WQC.

Ancilla-based quantum computation

Instead of departing entirely from the quantum circuit model paradigm, alternative gate techniques can be layered on top of an underlying quantum circuit. Minimising environment-induced decoherence of computational QVs is achieved by choosing naturally well-isolated quantum systems (e.g., nuclear spins [Zhong et al. (2015)]) to encode these QVs into, but the very nature of well-isolated systems is that they are generically difficult to manipulate and it is particularly challenging to make these systems controllable interact with one another. One practical method for engineering interactions between well-isolated QVs is by using an 'ancillary' quantum system to mediate the interaction, which can be chosen with optimisation of these interactions in mind. In Chapters 5, 6 and 7 of this thesis ancilla-based gate techniques have been developed with the formulations again designed to apply to quantum variables of different types and, wherever possible, to include the case of *hybrid* quantum variables, whereby the dimensions of the computational and ancillary systems need not match.

Although the different models and gates proposed in this thesis differ in a range of ways, they all use essentially one of two basic techniques. The first of these is *delocalising* the quantum information in a register system across that system and an ancilla. Although it appears in various guises herein, this essentially involves entangling a register QV in some arbitrary state, $\sum_{q\in\mathbb{S}_d} c_q|q\rangle$, and an ancilla, initialised to say $|0\rangle$, via the mapping

$$\sum_{q\in\mathbb{S}_d} c_q|q\rangle|0\rangle \rightarrow \sum_{q\in\mathbb{S}_d} c_q|q\rangle|q\rangle, \tag{8.3}$$

which may be achieved with a (possibly hybrid) SUM gate. The logical QV now resides non-locally in both QVs and so manipulations of the ancilla will affect the state of the *logical* QV and may therefore be used to entangle it with further register QVs and perform other logical operations on it. To complete a gate of this type the logical QV must be relocalised into the register, which could be achieved either with unitary dynamics (e.g., here an inverse SUM gate is the appropriate gate) or with a measurement of the ancilla in any basis which reveals no information about the logical QV (e.g., here a conjugate basis measurement would suffice).

Instead of delocalising the quantum information stored in a register system, the logical state of that register system, $|\psi\rangle$, can be completely *swapped* into the ancillary system. More specifically, for an ancilla in some input state $|\psi_0\rangle$, this is the mapping

$$|\psi\rangle|\psi_0\rangle \rightarrow |\psi_0\rangle|\psi\rangle, \tag{8.4}$$

which can be achieved via a SWAP gate, but also by other gates which (unlike SWAP) can be entangling and only act identically to SWAP on the input of the fixed state $|\psi_0\rangle$. Obviously, manipulations of the ancilla will then transform the logical $|\psi\rangle$ state, which must then be swapped back into the register to complete the gate, via a second SWAP or SWAP-like gate.

The first ancilla-based gate methods proposed in this thesis were the *geometric phase gates*, as introduced and investigated in Chapter 5. These gates employ an ancilla to entangle QVs in a computational register via a sequence of register-QV controlled Pauli operators on the ancilla. Interestingly, this gate functions independently of the input state of the ancilla, and is an adaption of the delocalisation technique described above so as to be applicable when the ancilla is in an unknown state - as such, the gate requires four ancilla-register interactions, which is one more than is necessary if the ancilla can be prepared in a suitable state. The geometric phase gate construction given herein is applicable both when the computational elements and ancillas are QVs of the same and of different types, and it should be noted that in the particular case of computational qubits and QCV ancillas this gate has been previously proposed by Milburn (1999); Spiller et al. (2006); Wang and Zanardi (2002). By adapting these geometric phase gates to keep some register systems entangled with an ancilla for extended periods of the computation, I have shown that, when using a qudit ancilla, a range of modulo-arithmetic based gates can be implemented on the register in a highly efficient manner in terms of gate-count (i.e., circuit size). In particular, for the case when the computational systems are qubits, this includes a proposal for a highly efficient and practical method for implementing generalised Toffoli gates.

The geometric phase gates of Chapter 5 are sufficient to implement any quantum computation on a register consisting of any quantum variable type when local unitary gates on the individual ancillas and the computational QVs are available. However, in some settings, such local gates may not be easily available and a further disadvantage of the geometric phase gate is that it requires each computational QV involved in a gate to interact with the ancilla more than once. This latter constraint may be particularly problematic in some circumstances, such as with ancillas coupling distant QVs, e.g., photons coupling atoms in separate cavities. Hence, in Chapter 6, a method for implementing universal quantum computation on a register was presented which uses *only* a single fixed ancilla-register interaction gate alongside variable-basis measurements of the ancillas and, furthermore, requires an ancilla to interact only once with each QV from a pair of register QVs in order to induce an entangling gate on them. This extends the qubit-based *ancilla-driven quantum computer* (ADQC) of Anders et al. (2010) to the setting of quantum variables of any type. This model is measurement-based, and hence clearly has many features in common with the 1WQC. The precise relationship was given in terms of a simple method for simulating a 1WQC in ADQC with no increase in computational depth, which guarantees that ADQC may exploit the same computational advantages as 1WQC, and hence the ADQC model is in some sense a hybrid between a quantum-circuit-model computer and a 1WQC.

The ADQC model of Chapter 6 relies on measurements of a range of local operators on the ancillas and this may be highly challenging in some circumstances. Hence, in Chapter 7, models of quantum computation were proposed which may implement universal quantum computation on a well-isolated register via interactions with ancillas prepared in the computational basis and in which the *only* operation used is a single fixed ancilla-register interaction gate. These may be naturally termed *minimal control* ancilla-based quantum computers as they need only a minimal level of access to the computational register, which can hence be optimised for long coherence times, and only highly limited controls over the ancillas, which may be optimised for a single high-quality interaction with the register systems. These models are applicable to the setting of both qubits and qudits of more general dimensions. Moreover, in the particular case of a qubit-based computer and a swap-like fixed interaction gate, it was shown that any quantum computation can be implemented on the register even if the ancillas can only be prepared in a *single fixed state*, which it can be argued is a completely minimal scheme for universal ancilla-based quantum computation.

The analysis of the ancilla-based models proposed herein has almost exclusively considered only the ideal case of perfect initial states, unitary controls and measurements. This leaves open the important question of what effect incorporating realistic imperfections has on the viability of each of the models. In the case of geometric phase gates with QCV ancillas and a register of qubits, it is known that, with an optical realisation of the ancillas, high fidelity computations can in-principle still be achieved in the presence of moderate dissipation on the ancillas in the form of photon losses [Louis et al. (2008)]. It seems likely that similar conclusions will hold more generally, although the dominant decoherence mechanisms will be depend on physical systems in question. Furthermore, such losses will have effects on the gate-count reduction methods discussed in Chapter 5, as if multiple register QVs are entangled with a dissipating ancilla this can induce correlated errors on the register, which can be problematic for quantum error-correction [Terhal (2015)]. Hence, there will be a trade-off between reducing gate counts and introducing these problematic errors, and for the QCV-qubit 'qubus' case, this optimisation has been considered by Horsman et al. (2011). Again, it seems likely these results will carry over to the more general models herein, but this would need investigating if these gate-count methods were to be considered further.

Going beyond considering only the effects of imperfections on individual gate fidelities, it would be interesting to consider whether error-detection, correction and fault-tolerance can be naturally in-built into any of the ancilla-based models proposed and investigated herein. From one perspective they are a natural setting for error-detection and correction, as they explicitly include the possibility for entangling the register QVs with ancillas and performing measurements on these ancillas. Finally, it is noted that future designs for a universal, scalable and fault-tolerant quantum computer will likely be based around modular quantum processing units (QPUs) of some fixed size with entangling gates between these QPUs implemented via 'flying' ancillas [Hucul et al. (2015); Nickerson et al. (2014)]. Hence, the ancilla-based gate techniques proposed herein may well be applicable to this higher-level aspect of quantum computer design, which is likely to be crucial to the long-term prospects of realising a useful quantum computer.

Bibliography

Aaronson, S. (2005), 'NP-complete problems and physical reality', *ACM Sigact News* **36**(1), 30–52. 8, 13

Aaronson, S. (2015), 'Read the fine print', *Nature Physics* **11**(4), 291–293. 8, 10

Aaronson, S. and Arkhipov, A. (2011), The computational complexity of linear optics, *in* 'Proceedings of the forty-third annual ACM symposium on Theory of computing', ACM, pp. 333–342. 26, 191

Aaronson, S. and Gottesman, D. (2004), 'Improved simulation of stabilizer circuits', *Phys. Rev. A* **70**(5), 052328. 47, 95, 98

Aaronson, S. and Gottesman, D. (2005).
URL: *http://www.scottaaronson.com/chp/* 47

Aharonov, D. (2003), 'A simple proof that toffoli and hadamard are quantum universal', *arXiv preprint quant-ph/0301040* . 185

Aharonov, D. and Ben-Or, M. (1997), Fault-tolerant quantum computation with constant error, *in* 'Proceedings of the twenty-ninth annual ACM symposium on Theory of computing', ACM, pp. 176–188. 13, 14

Anders, J. and Browne, D. E. (2009), 'Computational power of correlations', *Phys. Rev. Lett.* **102**(5), 050502. 21, 95, 97, 192, 194

Anders, J., Oi, D. K. L., Kashefi, E., Browne, D. E. and Andersson, E. (2010), 'Ancilla-driven universal quantum computation', *Phys. Rev. A* **82**(2), 020301(R). 24, 104, 137, 138, 139, 140, 142, 196

Andersen, U. L., Leuchs, G. and Silberhorn, C. (2010), 'Continuous-variable quantum information processing', *Laser &amp; Photonics Reviews* **4**(3), 337–354. 15, 162

Anderson, B. E., Sosa-Martinez, H., Riofrío, C. A., Deutsch, I. H. and Jessen, P. S. (2015), 'Accurate and robust unitary transformation of a high-dimensional quantum system', *Phys. Rev. Lett.* **114**, 240401. 17, 100, 128, 150, 191

Andrist, R. S., Wootton, J. R. and Katzgraber, H. G. (2015), 'Error thresholds for abelian quantum double models: Increasing the bit-flip stability of topological quantum memory', *Phys. Rev. A* **91**(4), 042331. 16, 72, 191

Anwar, H., Brown, B. J., Campbell, E. T. and Browne, D. E. (2014), 'Fast decoders for qudit topological codes', *New J. Phys.* **16**(6), 063038. 16, 72, 191

Arecchi, F. T., Courtens, E., Gilmore, R. and Thomas, H. (1972), 'Atomic coherent states in quantum optics', *Phys. Rev. A* **6**(6), 2211. 250, 255, 256

Arora, S. and Barak, B. (2009), *Computational Complexity: A Modern Approach*, Cambridge University Press. 51, 52

Bacon, D. and Van Dam, W. (2010), 'Recent progress in quantum algorithms', *Communications of the ACM* **53**(2), 84–93. 10

Barenco, A. (1995), 'A universal two-bit gate for quantum computation', *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* **449**(1937), 679–683. 165

Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A. and Weinfurter, H. (1995), 'Elementary gates for quantum computation', *Phys. Rev. A* **52**(5), 3457. 19, 119

Barends, R., Kelly, J., Megrant, A., Veitia, A., Sank, D., Jeffrey, E., White, T. C., Mutus, J., Fowler, A. G., Campbell, B. et al. (2014), 'Superconducting quantum circuits at the surface code threshold for fault tolerance', *Nature* **508**(7497), 500–503. 18, 191

Bartlett, S. D. and Rudolph, T. (2006), 'Simple nearest-neighbor two-body hamiltonian system for which the ground state is a universal resource for quantum computation', *Phys. Rev. A* **74**(4), 040302. 98

Bartlett, S. D., Sanders, B. C., Braunstein, S. L. and Nemoto, K. (2002), 'Efficient classical simulation of continuous variable quantum information processes.', *Phys. Rev. Lett.* **88**(9), 097904. 45, 46, 47

Barz, S., Vasconcelos, R., Greganti, C., Zwerger, M., Dür, W., Briegel, H. J. and Walther, P. (2014), 'Demonstrating elements of measurement-based quantum error correction', *Phys. Rev. A* **90**(4), 042302. 150

Bauer, B., Levaillant, C. and Freedman, M. (2014), 'Universality of single quantum gates', *arXiv preprint arXiv:1404.7822* . 165

Beckman, D., Chari, A. N., Devabhaktuni, S. and Preskill, J. (1996), 'Efficient networks for quantum factoring', *Phys. Rev. A* **54**(2), 1034. 12

Bell, B. A., Herrera-Martí, D. A., Tame, M. S., Markham, D., Wadsworth, W. J. and Rarity, J. G. (2014), 'Experimental demonstration of a graph state quantum error-correction code', *Nature Communications* **5**. 21, 72, 98, 192

Bennett, C. H., Bernstein, E., Brassard, G. and Vazirani, U. (1997), 'Strengths and weaknesses of quantum computing', *SIAM journal on Computing* **26**(5), 1510–1523. 8

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. and Wootters, W. K. (1993), 'Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels', *Phys. Rev. Lett.* **70**(13), 1895–1899. 38

Bennett, C. H. and Wiesner, S. J. (1992), 'Communication via one-and two-particle operators on einstein-podolsky-rosen states', *Phys. Rev. Lett.* **69**(20), 2881. 38

Bent, N., Qassim, H., Tahir, A. A., Sych, D., Leuchs, G., Sánchez-Soto, L. L., Karimi, E. and Boyd, R. W. (2015), 'Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures', *Phys. Rev. X* **5**(4), 041006. 17, 99

Berndt, B. C. and Evans, R. J. (1981), 'The determination of gauss sums', *Bulletin of the American Mathematical Society* **5**(2), 107–129. 242

Bernstein, E. and Vazirani, U. (1997), 'Quantum complexity theory', *SIAM Journal on Computing* **26**(5), 1411–1473. 7

Blais, A., Huang, R.-S., Wallraff, A., Girvin, S. M. and Schoelkopf, R. J. (2004), 'Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation', *Phys. Rev. A* **69**(6), 062320. 128

Bocharov, A., Roetteler, M. and Svore, K. M. (2015), 'Efficient synthesis of universal repeat-until-success circuits', *Phys. Rev. Lett.* **114**, 080502. 158, 180

Borrelli, M., Mazzola, L., Paternostro, M. and Maniscalco, S. (2011), 'Simple trapped-ion architecture for high-fidelity toffoli gates', *Phys. Rev. A* **84**(1), 012314. 16

Bournez, O., Campagnolo, M. L., Graça, D. S. and Hainry, E. (2006), The general purpose analog computer and computable analysis are two equivalent paradigms of analog computation, *in* 'Theory and Applications of Models of Computation', Springer, pp. 631–643. 95

Boykin, P. O., Mor, T., Pulver, M., Roychowdhury, V. and Vatan, F. (2000), 'A new universal and fault-tolerant quantum basis', *Inform. Process. Lett.* **75**(3), 101–107. 11, 175, 243

Braunstein, S. L. (2003), Error correction for continuous quantum variables, *in* 'Quantum Information with Continuous Variables', Springer, pp. 19–29. 16

Braunstein, S. L. and van Loock, P. (2005), 'Quantum information with continuous variables', *Rev. Mod. Phys.* **77**, 513–577. 15, 31, 32, 43, 123, 227

Bremner, M. J., Dawson, C. M., Dodd, J. L., Gilchrist, A., Harrow, A. W., Mortimer, D., Nielsen, M. A. and Osborne, T. J. (2002), 'Practical scheme for quantum computation with any two-qubit entangling gate', *Phys. Rev. Lett.* **89**(24), 247902. 185

Brennen, G. K. and Miyake, A. (2008), 'Measurement-based quantum computer in the gapped ground state of a two-body hamiltonian', *Phys. Rev. Lett.* **101**(1), 010502. 98

Brennen, G. K., O'Leary, D. P. and Bullock, S. S. (2005), 'Criteria for exact qudit universality', *Phys. Rev. A* **71**(5), 052318. 127

Broadbent, A. and Kashefi, E. (2009), 'Parallelizing quantum circuits', *Theor. Comput. Sci.* **410**(26), 2489 – 2510. 21, 71, 72, 85, 86, 192

Brown, B. J., Nickerson, N. H. and Browne, D. E. (2015), 'Fault-tolerant error correction with the gauge color code', *arXiv preprint arXiv:1503.08217* . 14

Brown, K. L., De, S., Kendon, V. M. and Munro, W. J. (2011), 'Ancilla-based quantum simulation', *New J. Phys.* **13**(9), 095007. 16, 24, 103, 104, 108, 109, 110, 112, 133

Brown, K. L., Horsman, C. and Kendon, V.and Munro, W. J. (2012), 'Layer-by-layer generation of cluster states', *Phys. Rev. A* **85**(5), 052305. 109, 133

Brown, K. L., Munro, W. J. and Kendon, V. M. (2010), 'Using quantum computers for quantum simulation', *Entropy* **12**(11), 2268–2307. 8, 26, 191

Browne, D. E., Kashefi, E., Mhalla, M. and Perdrix, S. (2007), 'Generalized flow and determinism in measurement-based quantum computation', *New J. Phys.* **9**(8), 250. 21, 101, 192

Browne, D., Kashefi, E. and Perdrix, S. (2011), Computational depth complexity of measurement-based quantum computation, *in* 'Theory of Quantum Computation, Communication, and Cryptography', Springer, pp. 35–46. 21, 40, 41, 71, 72, 86, 91, 92, 93, 101, 149, 192, 194

Brylinski, J.-L. and Brylinski, R. (2002), *Universal quantum gates*, Chapman & Hall / CRC Press. 49, 239

Bullock, S. S., O'Leary, D. P. and Brennen, G. K. (2005), 'Asymptotically optimal quantum circuits for d-level systems', *Phys. Rev. Lett.* **94**(23), 230502. 42, 55

Byrnes, T., Wen, K. and Yamamoto, Y. (2012), 'Macroscopic quantum computation using bose-einstein condensates', *Phys. Rev. A* **85**(4), 040306. 23, 130

Calkins, B., Mennea, P. L., Lita, A. E., Metcalf, B. J., Kolthammer, W. S., Lamas-Linares, A., Spring, J. B., Humphreys, P. C., Mirin, R. P., Gates, J. C. et al. (2013), 'High quantum-efficiency photon-number-resolving detector for photonic on-chip information processing', *Opt. Express* **21**(19), 22657–22670. 18, 99, 154, 162

Campbell, E. T. (2014), 'Enhanced fault-tolerant quantum computing in d-level systems', *Phys. Rev. Lett.* **113**(23), 230501. 16, 26, 50, 72, 152, 191

Campbell, E. T., Anwar, H. and Browne, D. E. (2012), 'Magic-state distillation in all prime dimensions using quantum reed-muller codes', *Phys. Rev. X* **2**(4), 041021. 16, 49, 72, 150, 177

Cao, Y., Peng, S.-G., Zheng, C. and Long, G.-L. (2011), 'Quantum Fourier transform and phase estimation in qudit system', *Communications in Theoretical Physics* **55**, 790–794. xvii, 111, 112

Carter, S. G., Sweeney, T. M., Kim, M., Kim, C. S., Solenov, D., Economou, S. E., Reinecke, T. L., Yang, L., Bracker, A. S. and Gammon, D. (2013), 'Quantum control of a spin qubit coupled to a photonic crystal cavity', *Nature Photonics* **7**(4), 329–334. 22, 104, 187

Chen, K., Li, C.-M., Zhang, Q., Chen, Y.-A., Goebel, A., Chen, S., Mair, A. and Pan, J.-W. (2007), 'Experimental realization of one-way quantum computing with two-photon four-qubit cluster states', *Phys. Rev. Lett.* **99**(12), 120503. 21, 72, 98, 192

Chen, M., Menicucci, N. C. and Pfister, O. (2014), 'Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb', *Phys. Rev. Lett.* **112**(12), 120505. 18, 21, 72, 99, 191, 192

Chen, X., Zeng, B., Gu, Z.-C., Yoshida, B. and Chuang, I. L. (2009), 'Gapped two-body hamiltonian whose unique ground state is universal for one-way quantum computation', *Phys. Rev. Lett.* **102**(22), 220501. 98

Chien, A. A. and Karamcheti, V. (2013), 'Moore's law: The first ending and a new beginning', *Computer* (12), 48–53. 5

Childs, A. M. (2009), 'Universal computation by quantum walk', *Phys. Rev. Lett.* **102**(18), 180501. 26

Childs, A. M., Gosset, D. and Webb, Z. (2013), 'Universal computation by multi-particle quantum walk', *Science* **339**(6121), 791–794. 26

Childs, A. M., Leung, D., Mancinska, L. and Ozols, M. (2011), 'Characterization of universal two-qubit hamiltonians', *Quant. Info. Comput.* **11**(1), 19–39. 165, 240

Christensen, S. L., Béguin, J.-B., Bookjans, E., Sørensen, H. L., Müller, J. H., Appel, J. and Polzik, E. S. (2014), 'Quantum interference of a single spin excitation with a macroscopic atomic ensemble', *Phys. Rev. A* **89**, 033801. 130

Church, A. (1936), 'An unsolvable problem of elementary number theory', *American journal of mathematics* pp. 345–363. 5

Ciccarello, F., Paternostro, M., Kim, M. S. and Palma, G. M. (2008), 'Extraction of singlet states from noninteracting high-dimensional spins', *Phys. Rev. Lett.* **100**(15), 150501. 189

Cirac, J. I. and Zoller, P. (1995), 'Quantum computations with cold trapped ions', *Phys. Rev. Lett.* **74**, 4091. 22

Coppersmith, D. (1994), An approximate fourier transform useful in quantum computing, Technical report, Technical report, IBM Research Division. 112

Dada, A. C., Leach, J., Buller, G. S., Padgett, M. J. and Andersson, E. (2011), 'Experimental high-dimensional two-photon entanglement and violations of generalized bell inequalities', *Nature Phys.* **7**(9), 677–680. 17, 99, 130

Danos, V., Kashefi, E. and Panangaden, P. (2007), 'The measurement calculus', *Journal of the ACM (JACM)* **54**(2), 8. 21, 71, 72, 73, 76, 81, 100, 192, 194

Danos, V., Kashefi, E., Panangaden, P. and Perdrix, S. (2009), 'Extended measurement calculus', *Semantic techniques in quantum computation* pp. 235–310. 21, 72, 192

Das, A. and Chakrabarti, B. K. (2008), 'Colloquium: Quantum annealing and analog quantum computation', *Rev. Mod. Phys.* **80**(3), 1061. 26

Dawson, C. M. and Nielsen, M. A. (2006), 'The solovay-kitaev algorithm', *Quant. Info. Comput.* **6**(1), 81–95. 44, 237

De Beaudrap, N. (2013), 'A linearized stabilizer formalism for systems of finite dimension', *Quant. Info. Comput.* **13**(1-2), 73–115. 47

De la Madrid, R. (2005), 'The role of the rigged hilbert space in quantum mechanics', *Eur. J. Phys.* **26**(2), 287. 32

Deppe, F., Mariantoni, M., Menzel, E. P., Marx, A., Saito, S., Kakuyanagi, K., Tanaka, H., Meno, T., Semba, K., Takayanagi, H. et al. (2008), 'Two-photon probe of the Jaynes-Cummings model and controlled symmetry breaking in circuit qed', *Nature Physics* **4**(9), 686–691. 128

Deutsch, D. (1985), Quantum theory, the church-turing principle and the universal quantum computer, *in* 'Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences', Vol. 400, The Royal Society, pp. 97–117. 7, 26

Deutsch, D. (1989), 'Quantum computational networks', *Proc. Roy. Soc.* **425**(1868), 73–90. 19, 165

Deutsch, D., Barenco, A. and Ekert, A. (1995), 'Universality in quantum computation', *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* **449**(1937), 669–677. 165, 239, 240

Devitt, S. J., Schirmer, S. G., Oi, D. K. L., Cole, J. H. and Hollenberg, L. C. L. (2007), 'Subspace confinement: how good is your qubit?', *New J. Phys.* **9**(10), 384. 16

Dicke, R. H. (1954), 'Coherence in spontaneous radiation processes', *Phys. Rev.* **93**(1), 99. 131, 250

DiVincenzo, D. P. (1995), 'Two-bit gates are universal for quantum computation', *Phys. Rev. A* **51**(2), 1015. 11

Doherty, A. C. and Wardrop, M. P. (2013), 'Two-qubit gates for resonant exchange qubits', *Phys. Rev. Lett.* **111**(5), 050503. 187

Dooley, S., Joo, J., Proctor, T. and Spiller, T. P. (2015), 'Generating non-classical states from spin coherent states via interaction with ancillary spins', *Optics Communications* **337**, 71–78. 130

Dooley, S., McCrossan, F., Harland, D., Everitt, M. J. and Spiller, T. P. (2013), 'Collapse and revival and cat states with an n-spin system', *Phys. Rev. A* **87**(5), 052323. 130, 255, 256

Duclos-Cianci, G. and Poulin, D. (2013), ‘Kitaev’s $\mathbb{Z}_d$-code threshold estimates’, *Phys. Rev. A* **87**(6), 062338. 16, 72

Duncan, R. and Perdrix, S. (2010), Rewriting measurement-based quantum computations with generalised flow, *in* ‘Automata, Languages and Programming’, Springer, pp. 285–296. 21, 101, 192

Durt, T., Englert, B.-G., Bengtsson, I. and Życzkowski, K. (2010), ‘On mutually unbiased bases’, *Int. J. Quant. Inf.* **8**(04), 535–640. 37

Eberle, T., Steinlechner, S., Bauchrowitz, J., Händchen, V., Vahlbruch, H., Mehmet, M., Müller-Ebhardt, H. and Schnabel, R. (2010), ‘Quantum enhancement of the zero-area sagnac interferometer topology for gravitational wave detection’, *Phys. Rev. Lett.* **104**(25), 251102. 154

Einstein, A., Podolsky, B. and Rosen, N. (1935), ‘Can quantum-mechanical description of physical reality be considered complete?’, *Phys. Rev.* **47**(10), 777. 38

Epstein, C. (2012), ‘Adiabatic quantum computing: An overview’, *Quantum Complexity Theory* **6**, 845. 26

Erdélyi (ed.), A. (1954), ‘Tables of integral transforms’, *New York: McGraw-Hill* **1**. 231

Fang, M., Fenner, S., Green, F., Homer, S. and Zhang, Y. (2006), ‘Quantum lower bounds for fanout’, *Quant. Info. Comput.* **6**(1), 46–57. 21, 52, 57

Farinholt, J. (2014), ‘An ideal characterization of the clifford operators’, *Journal of Physics A: Mathematical and Theoretical* **47**(30), 305303. 45, 46, 87, 153

Fedorov, A., Steffen, L., Baur, M., Da Silva, M. P. and Wallraff, A. (2011), ‘Implementation of a toffoli gate with superconducting circuits’, *Nature* **481**(7380), 170–172. 118

Feynman, R. P. (1982), ‘Simulating physics with computers’, *Int. J. Th. Phys.* **21**(6/7), 467–488. 7, 8

Fowler, A. G. (2013), ‘Analytic asymptotic performance of topological codes’, *Phys. Rev. A* **87**(4), 040301. 14

Fowler, A. G., Hill, C. D. and Hollenberg, L. C. (2004), ‘Quantum-error correction on linear-nearest-neighbor qubit arrays’, *Physical Review A* **69**(4), 042314. 69

Furst, M., Saxe, J. B. and Sipser, M. (1984), ‘Parity, circuits, and the polynomial-time hierarchy’, *Mathematical Systems Theory* **17**(1), 13–27. 52

Gao, W.-B., Yao, X.-C., Cai, J.-M., Lu, H., Xu, P., Yang, T., Lu, C.-Y., Chen, Y.-A., Chen, Z.-B. and Pan, J.-W. (2011), 'Experimental measurement-based quantum computing beyond the cluster-state model', *Nature Photon.* **5**(2), 117–123. 150

Gazeau, J.-P. (2009), *Coherent states in quantum physics*, Wiley. 230, 250, 251, 255, 256

Gerry, C. and Knight, P. (2005), *Introductory quantum optics*, Cambridge university press. 36, 127, 128, 229

Ghosh, J., Fowler, A. G., Martinis, J. M. and Geller, M. R. (2013), 'Understanding the effects of leakage in superconducting quantum-error-detection circuits', *Phys. Rev. A* **88**(6), 062329. 16

Gibbons, K. S., Hoffman, M. J. and Wootters, W. K. (2004), 'Discrete phase space based on finite fields', *Phys. Rev. A* **70**(6), 062101. 29, 33

Gilchrist, A., Langford, N. K. and Nielsen, M. A. (2005), 'Distance measures to compare real and ideal quantum processes', *Phys. Rev. A* **71**(6), 062310. 42

Glauber, R. J. (1963), 'Coherent and incoherent states of the radiation field', *Phys. Rev.* **131**(6), 2766. 230

Goldreich, O. (2008), *Computational Complexity: A Conceptual Perspective*, Cambridge University Press. 52, 91

Gottesman, D. (1997), 'Stabilizer codes and quantum error correction', *arXiv preprint quant-ph/9705052* . 118

Gottesman, D. (1999*a*), Fault-tolerant quantum computation with higher-dimensional systems, *in* 'Quantum Computing and Quantum Communications', Springer, pp. 302–313. 45, 46, 47

Gottesman, D. (1999*b*), The heisenberg representation of quantum computers, *in* S. P. Corney, R. Delbourgo and P. D. Jarvis, eds, 'Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics', International Press arXiv preprint quant-ph/9807006, p. 32. 45, 47

Gottesman, D. (2010), 'An introduction to quantum error correction and fault-tolerant quantum computation', *ArXiv:0904.2557* **68**, 13–60. 14, 44

Gottesman, D., Kitaev, A. and Preskill, J. (2001), 'Encoding a qubit in an oscillator', *Phys. Rev. A* **64**(1), 012310. 99, 100, 125, 151, 152, 154

Gröblacher, S., Hammerer, K., Vanner, M. R. and Aspelmeyer, M. (2009), 'Observation of strong coupling between a micromechanical resonator and an optical cavity field', *Nature* **460**(7256), 724–727. 128

Gross, C., Strobel, H., Nicklas, E., Zibold, T., Bar-Gill, N., Kurizki, G. and Oberthaler, M. K. (2011), 'Atomic homodyne detection of continuous-variable entangled twin-atom states', *Nature* **480**(7376), 219–223. 18, 151

Gross, D. (2006), 'Hudson's theorem for finite-dimensional quantum systems', *J. Math. Phys.* **47**(12), 122107. 96

Grover, L. K. (1996), A fast quantum mechanical algorithm for database search, *in* 'Proceedings of the twenty-eighth annual ACM symposium on Theory of computing', ACM, pp. 212–219. 8, 26, 191

Gu, M., Weedbrook, C., Menicucci, N. C., Ralph, T. C. and van Loock, P. (2009), 'Quantum computing with continuous-variable clusters', *Phys. Rev. A* **79**(6), 062318. 50, 72, 99, 152, 153, 154

Halil-Shah, K. and Oi, D. K. L. (2013), Ancilla driven quantum computation with arbitrary entangling strength, *in* 'Theory of Quantum Computation, Communication, and Cryptography, 8th Conference, TQC 2013, LIPIcs-Leibniz International Proceedings in Informatics, Vol. 23.'. 25, 178, 180, 181, 189

Halil-Shah, K. and Oi, D. K. L. (2014), 'A minimum control ancilla driven quantum computation scheme with repeat-until-success style gate generation', *arXiv preprint arXiv:1401.8004* . 25, 104, 178, 180, 181, 189

Hall, W. (2007), 'Cluster state quantum computation for many-level systems', *Quant. Info. Comput.* **7**, 184–208. 46, 72

Harrow, A. W., Recht, B. and Chuang, I. L. (2002), 'Efficient discrete approximations of quantum gates', *J. Math. Phys.* **43**(9), 4445–4451. 44, 237

Hemaspaandra, L. A. (2012), 'Sigact news complexity theory column 74.', *SIGACT News* **43**(2), 51–52. 51

Hollenberg, L. C. L., Greentree, A. D., Fowler, A. G. and Wellard, C. J. (2006), 'Two-dimensional architectures for donor-based quantum computing', *Phys. Rev. B* **74**(4). 69

Holstein, T. and Primakoff, H. (1940), 'Field dependence of the intrinsic domain magnetization of a ferromagnet', *Phys. Rev.* **58**(12), 1098. 255

Horsman, C., Brown, K. L., Munro, W. J. and Kendon, V. M. (2011), 'Reduce, reuse, recycle for robust cluster-state generation', *Phys. Rev. A* **83**(4), 042327. 108, 109, 133, 197

Hostens, E., Dehaene, J. and De Moor, B. (2005), 'Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic', *Phys. Rev. A* **71**(4), 042315. 45, 46, 47, 87

Howard, M. and Vala, J. (2012), 'Qudit versions of the qubit $\pi/8$ gate', *Phys. Rev. A* **86**(2), 022316. 50, 152

Høyer, P. and Špalek, R. (2003), Quantum circuits with unbounded fan-out, *in* 'STACS 2003', Springer, pp. 234–246. 21, 52, 69, 88, 91, 193

Høyer, P. and Špalek, R. (2005), 'Quantum fan-out is powerful', *Theory of computing* **1**(5), 83–101. 21, 52, 69, 70, 88, 193

Hu, Y., Zhou, Z.-W. and Guo, G.-C. (2007), 'Always on non-nearest-neighbour coupling in scalable quantum computing', *New J. Phys.* **9**(2), 27. 26

Hucul, D., Inlek, I. V., Vittorini, G., Crocker, C., Debnath, S., Clark, S. M. and Monroe, C. (2015), 'Modular entanglement of atomic qubits using photons and phonons', *Nature Phys.* **11**, 37. 25, 197

Humphreys, J. E. (1972), *Introduction to Lie algebras and representation theory*, Vol. 9, Springer Science & Business Media. 43

Humphreys, P. C., Metcalf, B. J., Gerrits, T., Hiemstra, T., Lita, A. E., Nunn, J., Nam, S. W., Datta, A., Kolthammer, W. S. and Walmsley, I. A. (2015), 'Tomography of photon-number resolving continuous-output detectors', *arXiv preprint arXiv:1502.07649* . 18, 99, 154, 162

Ionicioiu, R., Popescu, A. E., Munro, W. J. and Spiller, T. P. (2008), 'Generalized parity measurements', *Phys. Rev. A* **78**(5), 052326. 104

Ionicioiu, R., Spiller, T. P. and Munro, W. J. (2009), 'Generalized toffoli gates using qudit catalysis', *Phys. Rev. A* **80**(1), 012312. xvii, 120, 121, 126, 130

Jaynes, E. T. and Cummings, F. W. (1963), 'Comparison of quantum and semiclassical radiation theories with application to the beam maser', *Proceedings of the IEEE* **51**(1), 89–109. 128

Jensen, K., Wasilewski, W., Krauter, H., Fernholz, T., Nielsen, B. M., Owari, M., Plenio, M. B., Serafini, A., Wolf, M. M. and Polzik, E. S. (2011), 'Quantum memory for entangled continuous-variable states', *Nature Phys.* **7**(1), 13–16. 18

Joo, J., Knight, P. L., O'Brien, J. L. and Rudolph, T. (2007), 'One-way quantum computation with four-dimensional photonic qudits', *Phys. Rev. A* **76**(5), 052326. 99

Jouguet, P., Elkouss, D. and Kunz-Jacques, S. (2014), 'High-bit-rate continuous-variable quantum key distribution', *Phys. Rev. A* **90**(4), 042329. 15

Kashefi, E., Oi, D. K. L., Browne, D., Anders, J. and Andersson, E. (2009), 'Twisted graph states for ancilla-driven universal quantum computation', *Electronic Notes in Theoretical Computer Science* **249**, 307–331. 137, 138, 139, 140, 142, 149, 158, 162

Katajainen, J., Van Leeuwen, J. and Penttonen, M. (1988), 'Fast simulation of turing machines by random access machines', *SIAM Journal on Computing* **17**(1), 77–88. 7

Khosla, K., Vanner, M., Bowen, W. and Milburn, G. (2013), 'Quantum state preparation of a mechanical resonator using an optomechanical geometric phase', *New J. Phys.* **15**(4), 043025. 108

Kitaev, A. Y. (1997), 'Quantum computations: algorithms and error correction', *Russ. Math. Surv.* **52**(6), 1191–1249. 44, 185, 237

Klesse, R. and Frank, S. (2005), 'Quantum error correction in spatially correlated quantum noise', *Phys. Rev. Lett.* **95**(23), 230503. 14

Klimov, A. B., Muñoz, C. and Sánchez-Soto, L. L. (2009), 'Discrete coherent and squeezed states of many-qudit systems', *Phys. Rev. A* **80**(4), 043836. 29, 229, 230

Klimov, A. B., Sánchez-Soto, L. L. and de Guise, H. (2005), 'Multicomplementary operators via finite Fourier transform', *J. Phys. A: Math. Gen.* **38**(12), 2747. 29

Knill, E., Laflamme, R. and Zurek, W. H. (1998), 'Resilient quantum computation', *Science* **279**(5349), 342–345. 13, 14

Knuth, D. E. (1980), *The Art of Computer Programming*, Vol. 2: Seminumerical Algorithms (see page 190), 2nd edition edn, MA: Addison-Wesley. 14

Krauter, H., Salart, D., Muschik, C. A., Petersen, J. M., Shen, H., Fernholz, T. and Polzik, E. S. (2013), 'Deterministic quantum teleportation between distant atomic objects', *Nature Phys.* **9**(7), 400–404. 18

Ladd, T. D., Goldman, J., Yamaguchi, F., Yamamoto, Y., Abe, E. and Itoh, K. (2002), 'All-silicon quantum computer', *Physical Review Letters* **89**(1), 017901. 69

Laflamme, R., Miquel, C., Paz, J. P. and Zurek, W. H. (1996), 'Perfect quantum error correcting code', *Phys. Rev. Lett.* **77**(1), 198. 14

Lamata, L., León, J., Pérez-García, D., Salgado, D. and Solano, E. (2008), 'Sequential implementation of global quantum operations', *Phys. Rev. Lett.* **101**(18), 180506. 161, 177, 181, 189

Lanyon, B. P., Barbieri, M., Almeida, M. P., Jennewein, T., Ralph, T. C., Resch, K. J., Pryde, G. J., O'Brien, J. L., Gilchrist, A. and White, A. G. (2009), 'Simplifying quantum logic using higher-dimensional Hilbert spaces', *Nature Phys.* **5**(2), 134–140. 16

Lanyon, B. P., Jurcevic, P., Zwerger, M., Hempel, C., Martinez, E. A., Dür, W., Briegel, H. J., Blatt, R. and Roos, C. F. (2013), 'Measurement-based quantum computation with trapped ions', *Phys. Rev. Lett.* **111**(21), 210501. 21, 72, 98, 150, 192

Lawrie, I. D. (2012), *A unified grand tour of theoretical physics*, CRC Press. 223

Li, X., Voss, P. L., Sharping, J. E. and Kumar, P. (2005), 'Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band', *Phys. Rev. Lett.* **94**(5), 053601. 129

Lim, Y. L., Beige, A. and Kwek, L. C. (2005), 'Repeat-until-success linear optics distributed quantum computing', *Phys. Rev. Lett.* **95**(3), 030505. 158, 180

Lima, G., Neves, L., Guzmán, R., Gómez, E. S., Nogueira, W. A. T., Delgado, A., Vargas, A. and Saavedra, C. (2011), 'Experimental quantum tomography of photonic qudits via mutually unbiased basis', *Opt. Express* **19**(4), 3542–3552. 17, 99, 130

Lloyd, S. (1993), 'A potentially realizable quantum computer', *Science* **261**(5128), 1569–1571. 26

Lloyd, S. (1995), 'Almost any quantum logic gate is universal', *Phys. Rev. Lett.* **75**(2), 346. 43, 49, 55, 123, 165, 166, 176, 185, 239, 240

Lloyd, S. (2003), 'Hybrid quantum computing', *arXiv:quant-ph/0008057* . 16, 123

Lloyd, S. and Braunstein, S. L. (1999), 'Quantum computation over continuous variables', *Phys. Rev. Lett.* **82**(8), 1784–1787. 31, 39, 42, 43, 44, 49, 153

Lloyd, S. and Slotine, J.-J. E. (1998), 'Analog quantum error correction', *Phys. Rev. Lett.* **80**(18), 4088. 16

Louis, S. G. R., Munro, W. J., Spiller, T. P. and Nemoto, K. (2008), 'Loss in hybrid qubit-bus couplings and gates', *Phys. Rev. A* **78**(2), 022326. 108, 132, 133, 197

Louis, S. G. R., Nemoto, K., Munro, W. J. and Spiller, T. P. (2007), 'The efficiencies of generating cluster states with weak nonlinearities', *New J. Phys.* **9**(6), 193. 24, 104, 108, 109, 129, 133

Lü, X.-Y., Xiang, Z.-L., Cui, W., You, J. Q. and Nori, F. (2013), 'Quantum memory using a hybrid circuit with flux qubits and nitrogen-vacancy centers', *Phys. Rev. A* **88**(1), 012329. 130, 131

Lukin, M. D. (2003), 'Colloquium: Trapping and manipulating photon states in atomic ensembles', *Rev. Mod. Phys.* **75**(2), 457. 130

Luxmoore, I., Wasley, N., Ramsay, A., Thijssen, A., Oulton, R., Hugues, M., Kasture, S., Achanta, V., Fox, A. and Skolnick, M. (2013), 'Interfacing spins in an ingaas quantum dot to a semiconductor waveguide circuit using emitted photons', *Phys. Rev. Lett.* **110**(3), 037402. 22, 104, 187

Lvovsky, A. I. (2014), 'Squeezed light', *arXiv preprint arXiv:1401.4118* . 154

Ma, S., Li, Z., Li, P., Fang, A., Gao, S. and Li, F. (2015), 'Two-mode squeezing generation in hybrid chains of superconducting resonators and nitrogen-vacancy-center ensembles', *J. Phys. B: At. Mol. Opt. Phys.* **48**(3), 035504. 130

Majer, J., Chow, J. M., Gambetta, J. M., Koch, J., Johnson, B. R., Schreier, J. A., Frunzio, L., Schuster, D. I., Houck, A. A., Wallraff, A., Blais, A., Devoret, M. H., Girvin, S. M. and Schoelkopf, R. J. (2007), 'Coupling superconducting qubits via a cavity bus', *Nature* **449**(7161), 443–447. 104

Marchiolli, M. A., Ruzzi, M. and Galetti, D. (2007), 'Discrete squeezed states for finite-dimensional spaces', *Phys. Rev. A* **76**(3), 032102. 229

Marcos, D., Wubs, M., Taylor, J. M., Aguado, R., Lukin, M. D. and Sørensen, A. S. (2010), 'Coupling nitrogen-vacancy centers in diamond to superconducting flux qubits', *Phys. Rev. Lett.* **105**(21), 210501. 130, 131

Markov, I. L. (2014), 'Limits on fundamental limits to computation', *Nature* **512**(7513), 147–154. 5

Maslov, D., Dueck, G. W., Miller, D. M. and Negrevergne, C. (2008), 'Quantum circuit simplification and level compaction', *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on* **27**(3), 436–444. 119

Matsuda, N., Shimizu, R., Mitsumori, Y., Kosaka, H. and Edamatsu, K. (2009), 'Observation of optical-fibre kerr nonlinearity at the single-photon level', *Nature photonics* **3**(2), 95–98. 129

Mehmet, M., Ast, S., Eberle, T., Steinlechner, S., Vahlbruch, H. and Schnabel, R. (2011), 'Squeezed light at 1550 nm with a quantum noise reduction of 12.3 db', *Opt. Express* **19**(25), 25763–25772. 154

Menicucci, N. C. (2014), 'Fault-tolerant measurement-based quantum computing with continuous-variable cluster states', *Phys. Rev. Lett.* **112**(12), 120504. 100, 154, 163

Menicucci, N. C., van Loock, P., Gu, M., Weedbrook, C., Ralph, T. C. and Nielsen, M. A. (2006), 'Universal quantum computation with continuous-variable cluster states', *Phys. Rev. Lett.* **97**(11), 110501. 20, 21, 71, 76, 79, 99, 100, 192, 194

Menzel, E. P., Di Candia, R., Deppe, F., Eder, P., Zhong, L., Ihmig, M., Haeberlein, M., Baust, A., Hoffmann, E., Ballester, D., Inomata, K., Yamamoto, T., Nakamura, Y. andSolano, E., Marx, A. and Gross, R. (2012), 'Path entanglement of continuous-variable quantum microwaves', *Phys. Rev. Lett.* **109**(25), 250502. 17

Metropolis, N. (1987), 'The beginning of the monte carlo method', *Los Alamos Science* **15**(584), 125–130. 14

Milburn, G. J. (1999), 'Simulating nonlinear spin models in an ion trap', *arXiv:quant-ph/9908037* . 104, 108, 132, 196

Milburn, G., Schneider, S. and James, D. (2000), 'Ion trap quantum computing with warm ions', *Fortschritte der Physik* **48**(9-11), 801–810. 108

Mischuck, B. and Mølmer, K. (2013), 'Qudit quantum computation in the jaynes-cummings model', *Phys. Rev. A* **87**(2), 022341. 129

Monroe, C., Raussendorf, R., Ruthven, A., Brown, K. R., Maunz, P., Duan, L.-M. and Kim, J. (2014), 'Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects', *Phys. Rev. A* **89**(2), 022317. xiv, 25

Moore, C. (1999), 'Quantum circuits: Fanout, parity and counting', *Electronic Colloquium on Computational Complexity* . 21, 52, 61

Moore, C. and Nilsson, M. (1998), 'Some notes on parallel quantum computation', *arXiv preprint quant-ph/9804034* . 21, 52

Moore, C. and Nilsson, M. (2001), 'Parallel quantum computation and quantum codes', *SIAM Journal on Computing* **31**(3), 799–815. 21, 52, 59, 64, 70, 88, 91, 193

Moore, G. E. (1998), 'Cramming more components onto integrated circuits', *Proceedings of the IEEE* **86**(1), 82–85. 5

Morimae, T. (2010), 'Strong entanglement causes low gate fidelity in inaccurate one-way quantum computation', *Phys. Rev. A* **81**(6), 060307. 163

Morimae, T. and Kahn, J. (2010), 'Entanglement-fidelity relations for inaccurate ancilla-driven quantum computation', *Phys. Rev. A* **82**(5), 052314. 163

Mücke, M., Figueroa, E., Bochmann, J., Hahn, C., Murr, K., Ritter, S., Villas-Boas, C. J. and Rempe, G. (2010), 'Electromagnetically induced transparency with single atoms in a cavity', *Nature* **465**(7299), 755–758. 129

Munro, W. J., Nemoto, K. and Spiller, T. P. (2005), 'Weak nonlinearities: a new route to optical quantum computation', *New J. Phys.* **7**(1), 137. 108, 132

Munro, W. J., Nemoto, K., Spiller, T. P., Barrett, S. D., Kok, P. and Beausoleil, R. G. (2005), 'Efficient optical quantum information processing', *J. Opt. B: Quantum Semiclass. Opt.* **7**(7), S135. 129

Muthukrishnan, A. and Stroud Jr, C. R. (2000), 'Multivalued logic gates for quantum computation', *Phys. Rev. A* **62**(5), 052309. 16

Nebe, G., Rains, E. M. and Sloane, N. J. (2001), 'The invariants of the clifford groups', *Des. Codes Cryptogr.* **24**(1), 99–122. 49, 150, 177

Nebe, G., Rains, E. M. and Sloane, N. J. A. (2006), *Self-dual codes and invariant theory*, Vol. 17, Springer. 49, 150, 177

Neeley, M., Ansmann, M., Bialczak, R. C., Hofheinz, M., Lucero, E., O'Connell, A. D., Sank, D., Wang, H., Wenner, J., Cleland, A. N., Michael, R. G. and Martinis, J. M. (2009), 'Emulation of a quantum spin with a superconducting phase qudit', *Science* **325**(5941), 722–725. 17, 130, 150

Neumann, P., Beck, J., Steiner, M., Rempp, F., Fedder, H., Hemmer, P. R., Wrachtrup, J. and Jelezko, F. (2010), 'Single-shot readout of a single nuclear spin', *Science* **329**(5991), 542–544. 187

Neumann, P., Mizuochi, N., Rempp, F., Hemmer, P., Watanabe, H., Yamasaki, S., Jacques, V., Gaebel, T., Jelezko, F. and Wrachtrup, J. (2008), 'Multipartite entanglement among single spins in diamond', *science* **320**(5881), 1326–1329. 187

Nickerson, N. H., Fitzsimons, J. F. and Benjamin, S. C. (2014), 'Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links', *Phys. Rev. X* **4**, 041041. xiv, 25, 197

Nielsen, M. A. and Chuang, I. L. (2010), *Quantum computation and quantum information*, Cambridge university press. 42, 49, 89, 111, 112, 118, 176, 244

O'Leary, D. P., Brennen, G. K. and Bullock, S. S. (2006), 'Parallelism for quantum computation with qudits', *Phys. Rev. A* **74**(3), 032334. 127

Pachos, J. K. (2012), *Introduction to topological quantum computation*, Cambridge University Press. 26

Paetznick, A. and Svore, K. M. (2014), 'Repeat-until-success: Non-deterministic decomposition of single-qubit unitaries', *Quant. Info. Comput.* **14**(15-16), 1277–1301. 158, 180

Parasa, V. and Perkowski, M. (2011), Quantum phase estimation using multivalued logic, *in* 'Multiple-Valued Logic (ISMVL), 2011 41st IEEE International Symposium on', IEEE, pp. 224–229. 16, 70, 72, 111, 193

Parasa, V. and Perkowski, M. (2012), Quantum pseudo-fractional Fourier transform using multiple-valued logic, *in* 'Multiple-Valued Logic (ISMVL), 2012 42nd IEEE International Symposium on', IEEE, pp. 311–314. 16, 26, 70, 72, 193

Pelletier, F. J. and Martin, N. M. (1990), 'Post's functional completeness theorem', *Notre Dame Journal of Formal Logic* **31**(3), 462–475. 95, 96

Petrosyan, D., Bensky, G., Kurizki, G., Mazets, I., Majer, J. and Schmiedmayer, J. (2009), 'Reversible state transfer between superconducting qubits and atomic ensembles', *Phys. Rev. A* **79**(4), 040304. 130, 131

Poot, M. and van der Zant, H. S. J. (2012), 'Mechanical systems in the quantum regime', *Physics Reports* **511**(5), 273–335. 36, 127

Proctor, T. J. (2015), 'Low depth measurement-based quantum computation beyond two-level systems', *arXiv:1510.06472* . 1, 51, 71

Proctor, T. J., Andersson, E. and Kendon, V. (2013), 'Universal quantum computation by the unitary control of ancilla qubits and using a fixed ancilla-register interaction', *Phys. Rev. A* **88**(4), 042330. 2, 137, 162

Proctor, T. J., Dooley, S. and Kendon, V. (2015), 'Quantum computation mediated by ancillary qudits and spin coherent states', *Phys. Rev. A* **91**, 012308. 2, 103, 105, 132

Proctor, T. J. and Kendon, V. (2014), 'Minimal ancilla mediated quantum computation', *EPJ Quantum Technology, 1:13* . 2, 165

Proctor, T. J. and Kendon, V. (2015), 'Higher-dimensional ancilla-driven quantum computation', *arXiv:1510.06462* . 2, 137, 165

Proctor, T. J. and Kendon, V. (2016), 'Hybrid quantum computing with ancillas', *Contemporary Physics* pp. 1–18. 2

Proctor, T. J. and Spiller, T. P. (2012), 'Low-error measurement-free phase gates for qubus computation', *Phys. Rev. A* **86**(6), 062304. 24, 108, 129

Rabl, P., DeMille, D., Doyle, J. M., Lukin, M. D., Schoelkopf, R. J. and Zoller, P. (2006), 'Hybrid quantum processors: molecular ensembles as quantum memory for solid state circuits', *Phys. Rev. Lett.* **97**(3), 033003. 130, 131

Radcliffe, J. M. (1971), 'Some properties of coherent spin states', *J. Phys. A: Gen. Phys.* **4**(3), 313. 250, 255, 256

Radmore, P. M. and Barnett, S. M. (1997), *Methods in theoretical quantum optics*, Oxford University Press Oxford,, UK. 36, 127, 153, 227, 229

Ralph, T. C. (2011), 'Quantum error correction of continuous-variable states against gaussian noise', *Phys. Rev. A* **84**(2), 022339. 16

Ralph, T. C., Resch, K. J. and Gilchrist, A. (2007), 'Efficient toffoli gates using qudits', *Phys. Rev. A* **75**(2), 022313. 16

Raussendorf, R. and Briegel, H. J. (2001), 'A one-way quantum computer', *Phys. Rev. Lett.* **86**(22), 5188–5191. xiii, 20, 21, 27, 71, 79, 192

Raussendorf, R., Browne, D. E. and Briegel, H. J. (2003), 'Measurement-based quantum computation on cluster states', *Phys. Rev. A* **68**(2), 022312. 21, 72, 192

Raussendorf, R. and Harrington, J. (2007), 'Fault-tolerant quantum computation with high threshold in two dimensions', *Phys. Rev. Lett.* **98**(19), 190504. 14

Raussendorf, R., Harrington, J. and Goyal, K. (2007), 'Topological fault-tolerance in cluster state quantum computation', *New J. Phys.* **9**(6), 199. 26

Reiserer, A., Kalb, N., Rempe, G. and Ritter, S. (2014), 'A quantum gate between a flying optical photon and a single trapped atom', *Nature* **508**(7495), 237–240. 22, 187

Rivest, R. L., Shamir, A. and Adleman, L. (1978), 'A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM* **21**(2), 120–126. 7

Robledo, L., Childress, L., Bernien, H., Hensen, B., Alkemade, P. F. A. and Hanson, R. (2011), 'High-fidelity projective read-out of a solid-state spin quantum register', *Nature* **477**(7366), 574–578. 187

Rossi, A., Vallone, G., Chiuri, A., De Martini, F. and Mataloni, P. (2009), 'Multipath entanglement of two photons', *Phys. Rev. Lett.* **102**(15), 153902. 17, 99, 130

Rozenberg, G., Bck, T. and Kok, J. N. (2011), *Handbook of natural computing*, Springer. 6

Saeedi, M. and Pedram, M. (2013), 'Linear-depth quantum circuits for n-qubit toffoli gates with no ancilla', *Phys. Rev. A* **87**(6), 062318. 119, 120

Saeedi, M., Wille, R. and Drechsler, R. (2011), 'Synthesis of quantum circuits for linear nearest neighbor architectures', *Quantum Information Processing* **10**(3), 355–377. 69

Sakurai, J. J. (1985), *Modern quantum mechanics*, Addison-Wesley Reading, Massachusetts. 32

Saraceno, M. (1990), 'Classical structures in the quantized baker transformation', *Ann. Phys.* **199**(1), 37–60. 229

Satoh, T., Matsuzaki, Y., Kakuyanagi, K., Munro, W. J., Semba, K., Yamaguchi, H. and Saito, S. (2015), 'Scalable quantum computation architecture using always-on ising interactions via quantum feedforward', *arXiv:1501.07712* . 26

Schrödinger, E. (1935), 'The present status of quantum mechanics', *Die Naturwissenschaften* **23**(48), 1–26. 12

Schuld, M., Sinayskiy, I. and Petruccione, F. (2015), 'An introduction to quantum machine learning', *Contemporary Physics* **56**(2), 172–185. 8, 26, 191

Schuster, D. I., Houck, A. A., Schreier, J. A., Wallraff, A., Gambetta, J. M., Blais, A., Frunzio, L., Majer, J., Johnson, B., Devoret, M. H. et al. (2007), 'Resolving photon number states in a superconducting circuit', *Nature* **445**(7127), 515–518. 128

Shannon, C. E. (1941), 'Mathematical theory of the differential analyzer', *J. Math. Phys. MIT* **20**, 337–354. 14

Sheridan, L. and Scarani, V. (2010), 'Security proof for quantum key distribution using qudit systems', *Phys. Rev. A* **82**(3), 030301. 15

Shi, Y. (2002), 'Both toffoli and controlled-not need little help to do universal quantum computation', *arXiv preprint quant-ph/0205115* . 118

Shor, P. W. (1994), Algorithms for quantum computation: Discrete logarithms and factoring, *in* 'Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on', IEEE, pp. 124–134. 8, 11, 26, 35, 191

Shor, P. W. (1995), 'Scheme for reducing decoherence in quantum computer memory', *Phys. Rev. A* **52**(4), R2493. 13, 14

Shor, P. W. (1997), 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM journal on computing* **26**(5), 1484–1509. 8, 11, 26, 35, 111, 191

Shore, B. W. and Knight, P. L. (1993), 'The Jaynes-Cummings model', *Journal of Modern Optics* **40**(7), 1195–1238. 128

Silberhorn, C. (2007), 'Detecting quantum light', *Contemporary Physics* **48**(3), 143–156. 37

Smith, A., Anderson, B. E., Sosa-Martinez, H., Riofrío, C. A., Deutsch, I. H. and Jessen, P. S. (2013), 'Quantum control in the cs 6 s 1/2 ground manifold using radio-frequency and microwave magnetic fields', *Phys. Rev. Lett.* **111**(17), 170502. 17, 100, 128, 130, 191

Spiller, T. P., Nemoto, K., Braunstein, S. L., Munro, W. J., van Loock, P. and Milburn, G. J. (2006), 'Quantum computation by communication', *New J. Phys.* **8**(2), 30. 24, 103, 104, 108, 129, 132, 196

Stanwix, P. L., Pham, L. M., Maze, J. R., Le Sage, D., Yeung, T. K., Cappellaro, P., Hemmer, P. R., Yacoby, A., Lukin, M. D. and Walsworth, R. L. (2010), 'Coherence of nitrogen-vacancy electronic spin ensembles in diamond', *Phys. Rev. B* **82**(20), 201201. 130

Steane, A. M. (1996), 'Error correcting codes in quantum theory', *Phys. Rev. Lett.* **77**(5), 793. 13, 14

Stern, M., Catelani, G., Kubo, Y., Grezes, C., Bienfait, A., Vion, D., Esteve, D. and Bertet, P. (2014), 'Flux qubits with long coherence times for hybrid quantum circuits', *Phys. Rev. Lett.* **113**(12), 123601. 22, 104

Stroud, A. and Muthukrishnan, C. R. (2002), 'Quantum fast Fourier transform using multilevel atoms', *J. Mod. Opt.* **49**(13), 2115–2127. 16, 127

Su, X., Hao, S., Deng, X., Ma, L., Wang, M., Jia, X., Xie, C. and Peng, K. (2013), 'Gate sequence for continuous variable one-way quantum computation', *Nat. Commun.* **4**. 18, 21, 72, 99, 151, 162, 192

Su, X., Tan, A., Jia, X., Zhang, J., Xie, C. and Peng, K. (2007), 'Experimental preparation of quadripartite cluster and greenberger-horne-zeilinger entangled states for continuous variables', *Phys. Rev. Lett.* **98**(7), 070502. 17

Sun, H., Niu, Y., Jin, S. and Gong, S. (2008), 'Phase control of the kerr nonlinearity in electromagnetically induced transparency media', *J. Phys. B: At. Mol. Opt. Phys.* **41**(6), 065504. 129

Sylvester, J. J. (1882), 'On a geometrical treatment of a theorem in numbers', *Johns Hopkins University Circulars* **I**, 209. 31

Sylvester, J. J. and Baker, H. F. (2012), *The collected mathematical papers of James Joseph Sylvester*, Vol. 3, Cambridge University Press. 31

Takahashi, Y. and Tani, S. (2013), Collapse of the hierarchy of constant-depth exact quantum circuits, *in* 'Computational Complexity (CCC), 2013 IEEE Conference on', IEEE, pp. 168–178. 70, 88, 193

Takahashi, Y., Tani, S. and Kunihiro, N. (2010), 'Quantum addition circuits and unbounded fan-out', *Quant. Info. Comput.* **10**(9), 872–890. 21, 52, 70, 88, 193

Tame, M. S., Bell, B. A., Di Franco, C., Wadsworth, W. J. and Rarity, J. G. (2014), 'Experimental realization of a one-way quantum computer algorithm solving simon's problem', *Phys. Rev. Lett.* **113**(20), 200501. 21, 72, 98, 192

Taminiau, T. H., Cramer, J., van der Sar, T., Dobrovitski, V. V. and Hanson, R. (2014), 'Universal control and error correction in multi-qubit spin registers in diamond', *Nat. Nanotechnol.* . 104, 187

Taminiau, T. H., Wagenaar, J. J. T., Van der Sar, T., Jelezko, F., Dobrovitski, V. V. and Hanson, R. (2012), 'Detection and control of individual nuclear spins using a weakly coupled electron spin', *Phys. Rev. Lett.* **109**(13), 137602. 104

Terhal, B. M. (2015), 'Quantum error correction for quantum memories', *Rev. Mod. Phys.* **87**(2), 307. 14, 133, 197

Thomson, W. (1875), 'Mechanical integration of the general linear differential equation of any order with variable coefficients', *Proc. Roy. Soc.* **24**(164-170), 271–275. 14

Tiecke, T., Thompson, J., de Leon, N., Liu, L., Vuletić, V. and Lukin, M. (2014), 'Nanophotonic quantum phase switch with a single atom', *Nature* **508**(7495), 241–244. 22, 187

Toffoli, T. (1980), *Reversible computing*, Springer. 118

Travaglione, B. C. and Milburn, G. J. (2001), 'Generation of eigenstates using the phase-estimation algorithm', *Phys. Rev. A* **63**(3), 032301. 16

Trummer, I. and Koch, C. (2015), 'Multiple query optimization on the D-Wave 2X adiabatic quantum computer', *arXiv preprint arXiv:1510.06437* . 26

Turing, A. M. (1936), 'On computable numbers, with an application to the entscheidungsproblem', *Proc. London Math. Soc., 42:2* pp. 230–265. 5

Tyc, T. and Sanders, B. C. (2004), 'Operational formulation of homodyne detection', *J. Phys. A: Math. Gen.* **37**(29), 7341. 151

Ukai, R., Iwata, N., Shimokawa, Y., Armstrong, S. C., Politi, A., Yoshikawa, J.-i., van Loock, P. and Furusawa, A. (2011), 'Demonstration of unconditional one-way quantum computations for continuous variables', *Phys. Rev. Lett.* **106**(24), 240504. 18, 21, 72, 99, 151, 162, 191, 192

Van den Nest, M. (2013), 'Efficient classical simulations of quantum Fourier transforms and normalizer circuits over abelian groups', *Quant. Info. Comput.* **13**(11-12), 1007–1037. 47

Van Loock, P. (2010), 'A note on quantum error correction with continuous variables', *J. Mod. Opt.* **57**(19), 1965–1971. 16

Van Loock, P., Munro, W. J., Nemoto, K., Spiller, T. P., Ladd, T. D., Braunstein, S. L. and Milburn, G. J. (2008), 'Hybrid quantum computation in quantum optics', *Phys. Rev. A* **78**(2), 022303. 108, 129

Vourdas, A. (2003), 'Factorization in finite quantum systems', *J. Phys. A: Math. Gen.* **36**(20), 5645. 29

Vourdas, A. (2004), 'Quantum systems with finite Hilbert space', *Rep. Prog. Phys.* **67**(3), 267. 29, 33

Walborn, S. P., Lemelle, D. S., Almeida, M. P. and Souto Ribeiro, P. H. (2006), 'Quantum key distribution with higher-order alphabets using spatially encoded qudits', *Phys. Rev. Lett.* **96**(9), 090501. 17, 99

Waldherr, G., Wang, Y., Zaiser, S., Jamali, M., Schulte-Herbrüggen, T., Abe, H., Ohshima, T., Isoya, J., Du, J. F., Neumann, P. and Wrachtrup, J. (2014), 'Quantum error correction in a solid-state hybrid spin register', *Nature* **506**(7487), 204–207. 187

Wallquist, M., Hammerer, K., Rabl, P., Lukin, M. and Zoller, P. (2009), 'Hybrid quantum devices and quantum engineering', *Physica Scripta* **2009**(T137), 014001. 128

Wallraff, A., Schuster, D. I., Blais, A., Frunzio, L., Huang, R.-S., Majer, J., Kumar, S., Girvin, S. M. and Schoelkopf, R. J. (2004), 'Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics', *Nature* **431**(7005), 162–167. 128

Wang, X. and Zanardi, P. (2002), 'Simulation of many-body interactions by conditional geometric phases', *Phys. Rev. A* **65**(3), 032327. 108, 129, 196

Wang, Y.-D., Kemp, A. and Semba, K. (2009), 'Coupling superconducting flux qubits at optimal point via dynamic decoupling with the quantum bus', *Phys. Rev. B* **79**(2), 024502. 22, 104, 129

Watson, F. H. E., Campbell, E. T., Anwar, H. and Browne, D. E. (2015), 'Qudit color codes and gauge color codes in all spatial dimensions', *Phys. Rev. A* **92**(2), 022312. 16, 72, 191

Watson, G. N. (1928), 'Theorems stated by ramanujan (iv): Theorems on approximate integration and summation of series', *Journal of the London Mathematical Society* **1**(4), 282–289. 242

Weigert, S. and Wilkinson, M. (2008), 'Mutually unbiased bases for continuous variables', *Phys. Rev. A* **78**(2), 020303. 37

Weisstein, E. W. (2004), Gaussian integral, *in* 'MathWorld-A Wolfram Web Resource', Wolfram Research, Inc. 242

Weyl, H. (1950), *The theory of groups and quantum mechanics*, Courier Dover Publications. 29

Wootters, W. K. (1987), 'A wigner-function formulation of finite-state quantum mechanics', *Ann. Phys.* **176**(1), 1–21. 29, 33, 37

Wootters, W. K. and Zurek, W. H. (1982), 'A single quantum cannot be cloned', *Nature* **299**(5886), 802–803. 13

Xue, Z.-Y. (2012), 'Fast geometric gate operation of superconducting charge qubits in circuit qed', *Quantum Inf. Process.* **11**(6), 1381–1388. 22, 104, 129

Yamamoto, Y., Ladd, T. D., Press, D., Clark, S., Sanaka, K., Santori, C., Fattal, D., Fu, K. M., Höfling, S., Reitzenstein, S. and Forchel, A. (2009), 'Optically controlled semiconductor spin qubits for quantum information processing', *Phys. Scr.* **T137**, 014010. 104

Yang, X., Li, S., Zhang, C. and Wang, H. (2009), 'Enhanced cross-kerr nonlinearity via electromagnetically induced transparency in a four-level tripod atomic system', *J. Opt. Soc. Am. B* **26**(7), 1423–1434. 129

Yokoyama, S., Ukai, R., Armstrong, S. C., Sornphiphatphong, C., Kaji, T., Suzuki, S., Yoshikawa, J.-i., Yonezawa, H., Menicucci, N. C. and Furusawa, A. (2013), 'Ultra-large-scale continuous-variable cluster states multiplexed in the time domain', *Nature Photon.* **7**(12), 982–986. 18, 21, 72, 98, 191, 192

Yoshihara, F., Fuse, T., Ashhab, S., Kakuyanagi, K., Saito, S. and Semba, K. (2016), 'Superconducting qubit-oscillator circuit beyond the ultrastrong-coupling regime', *arXiv preprint arXiv:1602.00415* . 129

Yukawa, M., Ukai, R., van Loock, P. and Furusawa, A. (2008), 'Experimental generation of four-mode continuous-variable cluster states', *Phys. Rev. A* **78**(1), 012301. 18

Zhang, W.-M., Gilmore, R. et al. (1990), 'Coherent states: theory and some applications', *Rev. Mod. Phys.* **62**(4), 867. 250

Zhong, M., Hedges, M. P., Ahlefeldt, R. L., Bartholomew, J. G., Beavan, S. E., Wittig, S. M., Longdell, J. J. and Sellars, M. J. (2015), 'Optically addressable nuclear spins in a solid with a six-hour coherence time', *Nature* **517**(7533), 177–180. 22, 194

Zhou, D. L., Zeng, B., Xu, Z. and Sun, C. P. (2003), 'Quantum computation based on d-level cluster state', *Phys. Rev. A* **68**(6), 062303. 20, 21, 49, 71, 76, 79, 99, 100, 192, 194, 239

Zhu, X., Saito, S., Kemp, A., Kakuyanagi, K., Karimoto, S.-i., Nakano, H., Munro, W. J., Tokura, Y., Everitt, M. S., Nemoto, K. et al. (2011), 'Coherent coupling of a superconducting flux qubit to an electron spin ensemble in diamond', *Nature* **478**(7368), 221–224. 130, 131, 254

Zhu, Y. (2010), 'Large kerr nonlinearities on cavity-atom polaritons', *Opt. Lett.* **35**(3), 303–305. 129

Zilic, Z. and Radecka, K. (2007), 'Scaling and better approximating quantum fourier transform by higher radices', *IEEE Transactions on computers* **56**(2), 202–207. xvii, 16, 72, 111, 112

Appendix A

The quantum harmonic oscillator

A quantum harmonic oscillator (QHO) is a system governed by the Hamiltonian

$$\hat{H}_{\text{QHO}} = \frac{1}{2}(\hat{x}^2 + \hat{p}^2). \tag{A.1}$$

The QHO Hamiltonian obtained directly from quantisation of a particular classical harmonic oscillator will contain physical constants, such as mass or a spring constant, and these have been been set to unity here (or absorbed into the operators via a rescaling of position and momentum). The *vacuum* state - which by definition is the lowest energy eigenstate of $\hat{H}_{\text{QHO}}$ - is required sporadically in this thesis, and hence a derivation of the spectrum of the QHO Hamiltonian is included here for completeness. This is covered in many text-books, e.g., see the elegant derivation of Lawrie (2012), which is similar to that given here and on which this is based.

It is useful (and conventional) to express the QHO Hamiltonian using the 'ladder' *creation* and *annihilation* operators defined respectively by

$$\hat{a}^\dagger := \frac{1}{\sqrt{2}}(\hat{x} - i\hat{p}), \qquad \hat{a} := \frac{1}{\sqrt{2}}(\hat{x} + i\hat{p}). \tag{A.2}$$

Via the canonical commutation relation $[\hat{x}, \hat{p}] = i$, it is easily confirmed that they obey the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$. In terms of these operators, the QHO Hamiltonian may be re-expressed as

$$\hat{H}_{\text{QHO}} = \hat{a}^\dagger \hat{a} + \frac{1}{2}. \tag{A.3}$$

From $[\hat{a}, \hat{a}^\dagger] = 1$, it follows that

$$[\hat{H}_{\text{QHO}}, \hat{a}] = -\hat{a}, \qquad [\hat{H}_{\text{QHO}}, \hat{a}^\dagger] = \hat{a}^\dagger. \tag{A.4}$$

As $\hat{H}_{\text{QHO}}$ is Hermitian all of its eigenvalues are real numbers and hence the set of eigenvalues is some (not necessarily strict) subset of $\mathbb{R}$. Let E denote an arbitrary eigenvalue and $|E\rangle$ an associated normalised eigenvector, i.e.,

$$\hat{H}_{\text{QHO}}|E\rangle = E|E\rangle. \tag{A.5}$$

For convenience, the same notation is being used for these eigenvectors as is used herein for the computational basis states but these are *not* computational basis states. The question is 'what values can E take?'. For any vector $|v\rangle$ then $\langle v|v\rangle \geq 0$, as this is one of the defining properties of an inner product. Let $|v\rangle = \hat{a}|E\rangle$. Then for any eigenvalue E,

$$E - 1/2 = \langle E| \left(\hat{H}_{\text{QHO}} - 1/2\right) |E\rangle = \langle E|\hat{a}^\dagger \hat{a}|E\rangle = \langle v|v\rangle \geq 0. \tag{A.6}$$

This implies that all $E \geq 1/2$, and hence the spectrum is bounded below by 1/2. Now consider $\hat{a}^\dagger|E\rangle$. Then, using Equation A.4, it follows that

$$\hat{H}_{\text{QHO}} \left(\hat{a}^\dagger|E\rangle\right) = \hat{a}^\dagger(\hat{H}_{\text{QHO}} + 1)|E\rangle = (E+1)\left(\hat{a}^\dagger|E\rangle\right). \tag{A.7}$$

Similarly, using Equation A.4, it can also be shown that

$$\hat{H}_{\text{QHO}} \left(\hat{a}|E\rangle\right) = (E-1)\left(\hat{a}|E\rangle\right). \tag{A.8}$$

Hence, the creation and annihilation operators have the action of raising and lowering an energy eigenstate by a unit of energy, that is

$$\hat{a}^\dagger|E\rangle \propto |E+1\rangle \qquad \hat{a}|E\rangle \propto |E-1\rangle. \tag{A.9}$$

These relations are not equalities as they are not necessarily the normalised eigenstates (they are not).

It is now shown that the lowest energy is 1/2. Denote the lowest energy (which we have shown exists) by E_0, then

$$\hat{H}_{\text{QHO}} \left(\hat{a}|E_0\rangle\right) = (E_0-1)\left(\hat{a}|E_0\rangle\right). \tag{A.10}$$

There is no eigenvalue lower than E_0, and hence this equation can only hold if $\hat{a}|E_0\rangle = 0$. It then follows that

$$E_0 = \langle E_0|\hat{H}_{\text{QHO}}|E_0\rangle = \langle E_0|(\hat{a}^\dagger\hat{a} + 1/2)|E_0\rangle = 1/2. \tag{A.11}$$

Therefore, using $E_0 = 1/2$ in combination with Equation A.7, we have shown that any $n + 1/2$, for $n = 0, 1, 2, \ldots$, is an eigenvalue of the QHO Hamiltonian.

It only remains to show that there are no other eigenvalues. Assume that $E+\lambda$ is an eigenvalue with $E \in \mathbb{N}$ and $\lambda \in [0,1)$, which covers all remaining possible values. Then $\hat{a}^E|E+\lambda\rangle = |\lambda\rangle$. But $\hat{a}|\lambda\rangle = 0$, as otherwise $\hat{a}|\lambda\rangle$ would be an eigenvector with a negative eigenvalue, and this condition implies that $\lambda = 1/2$ as already shown in Equation A.11. Hence, there are no further eigenvalues. The lowest energy eigenstate of the QHO, $|E_0\rangle = |1/2\rangle$, is called the vacuum state and elsewhere in this thesis it is denoted $|\text{vac}\rangle$ (rather than the conventional $|0\rangle$) to clearly distinguish it from a computational basis state. Finally, it is explicitly noted that we have seen that the vacuum state has the property

$$\hat{a}|\text{vac}\rangle = \frac{1}{\sqrt{2}}(\hat{x}+i\hat{p})|\text{vac}\rangle = 0, \tag{A.12}$$

as this equality is required in Appendix B.

Appendix B

Squeezed states

In this appendix it is shown that the computational basis states of a QCV can be approximated using squeezed vacuum states, with the correspondence exact in the limit of infinite squeezing. Similar derivations can be found in a variety of sources, for example, see Braunstein and van Loock (2005). The unitary *squeezing operator* is defined here by[1]

$$S(z) := e^{-i\ln(z)(\hat{x}\hat{p}+\hat{p}\hat{x})/2}, \tag{B.1}$$

where $z \in \mathbb{R}_{\geq 0}$. This operator describes a variety of non-linear optical processes [Radmore and Barnett (1997)]. Using the relation

$$e^{\hat{A}}\hat{B}e^{-\hat{A}} = \hat{B} + [\hat{A},\hat{B}] + \frac{1}{2!}[\hat{A},[\hat{A},\hat{B}]] + \dots, \tag{B.2}$$

it may be shown that

$$S(z)^{\dagger}\hat{x}S(z) = z\hat{x}, \qquad S(z)^{\dagger}\hat{p}S(z) = \frac{1}{z}\hat{p}, \tag{B.3}$$

and hence the squeezing operator stretches position and squeezes momentum if $z > 1$, and vice-versa for $0 < z < 1$. The state of interest here is the *squeezed vacuum* defined by

$$|z\rangle := S(z)|\text{vac}\rangle, \tag{B.4}$$

where $|\text{vac}\rangle$ is the grounded state of the QHO Hamiltonian $\hat{H}_{\text{QHO}} = \frac{1}{2}(\hat{x}^2 + \hat{p}^2)$, as introduced in Appendix A. The above relations (along with $S(z)S(z)^{\dagger} = \mathbb{I}$) may be

[1] It may also be defined to take a complex parameter, which is not needed here. Furthermore, note that this is the same operator as the squeezing gate that is introduced in Section 2.4.4, where here we are considering the particular case of QCVs and the operator has instead been written in terms of its generating Hamiltonian, rather than simply defined in terms of its action on the computational basis.

used to show that

$$(\hat{x}/z + iz\hat{p})S(z)|\text{vac}\rangle = S(z)(\hat{x} + i\hat{p})|\text{vac}\rangle = 0, \tag{B.5}$$

where this last relation holds because $(\hat{x} + i\hat{p})|\text{vac}\rangle = 0$, as seen in Equation A.12. Therefore, it has been shown that

$$(\hat{x}/z + iz\hat{p})|z\rangle = 0. \tag{B.6}$$

For $0 < z \ll 1$, then $\hat{x}/z + iz\hat{p} \approx \hat{x}/z$ and hence $|z\rangle$ is approximately the eigenstate of $\hat{x}$ with eigenvalue zero, which is the zero computational basis state $|0\rangle$. The correspondence is exact in the limit of $z \to 0$, i.e.,

$$\lim_{z \to 0} |z\rangle = |0\rangle. \tag{B.7}$$

Other computational basis states can be obtained by applying the Pauli $X(q)$ gate (as defined in Equation 2.13) to these states, and the conjugate basis states (see Equation 2.27), which are the eigenstates of $\hat{p}$, can be obtained via the Fourier gate. Alternatively, the eigenstate of $\hat{p}$ with eigenvalue zero is obtained in the limit $z \to \infty$ of the state $|z\rangle$. Infinite squeezing (associated with $z = 0$ or $z = \infty$) is not physical. However, when the squeezing is finite the states given here approximate the eigenstates of $\hat{x}$ and $\hat{p}$.

Appendix C

Displacement operators

In this appendix the relationship between Pauli operators, the $\mathbb{C}$-number parameterised displacement operators and coherent states is given. Displacement operators are ubiquitous in the theory of quantum optics [Gerry and Knight (2005); Radmore and Barnett (1997)] (i.e., displacement operators for QCVs) and for discrete systems these are less common but are used by a variety of authors, see e.g., the work of Klimov et al. (2009); Marchiolli et al. (2007); Saraceno (1990).

The *displacement operator*, parameterised by two numbers $q, q' \in \mathbb{S}_d$, may be defined in terms of the Pauli operators by[1]

$$\mathcal{D}(q, q') := \omega^{-2^{-1}qq'} Z(q') X(q). \tag{C.1}$$

Obviously, this may alternatively be parameterised by a single complex number α (with suitable restrictions on the values it may take in the discrete case). To obtain the normal definition of the $\mathbb{C}$-number parameterised displacement operator take

$$\mathcal{D}(\alpha) \equiv \mathcal{D}\left(\sqrt{2}\Re(\alpha), \sqrt{2}\Im(\alpha)\right). \tag{C.2}$$

For a QCV (e.g., optics) it is conventional to express the displacement operator in the 'entangled' form

$$\mathcal{D}(q, q') = \exp(i(q'\hat{x} - q\hat{p})), \tag{C.3}$$

which may be derived from the relations $Z(q) = \exp(iq\hat{q})$ and $X(q) = \exp(-iq\hat{p})$ along with the canonical commutation relation and the Weyl formula

$$e^A e^B = e^{\frac{1}{2}[A,B]} e^{A+B}, \tag{C.4}$$

[1] In this definition, 2^{-1} is the multiplicative inverse of 2 in $\mathbb{S}_d$. For QCVs this is obviously $1/2$. For odd dimension qudits this always exists (d and 2 are co-prime) and is $(d + 1)/2$. For even dimensions this phase factor could be omitted, or 2^{-1} could be replaced with $1/2$.

which holds when $[A,[A,B]] = [B,[A,B]] = 0$, and is a special case of the Baker-Campbell-Hausdorff formula [Gazeau (2009)]. The other common form for the QCV displacement operator is written in terms of the *creation* and *annihilation* operators

$$\hat{a}^\dagger := \frac{1}{\sqrt{2}}(\hat{x} - i\hat{p}), \qquad \hat{a} := \frac{1}{\sqrt{2}}(\hat{x} + i\hat{p}), \tag{C.5}$$

which obey the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$, and are also introduced in Appendix A in the context of the quantum harmonic oscillator. It is easily shown that

$$\mathcal{D}(\alpha) = \exp(\alpha a^\dagger - \alpha^* a), \tag{C.6}$$

with $\alpha \in \mathbb{C}$. This form is the most common in quantum optics. From this equation, which is often used to *define* the displacement operator, it is certainly not obvious (at least to me) that this operator is analogous to the qubit Pauli operators.

Displacement operators may be used to define the $\mathbb{C}$-number parameterised coherent states by

$$|\alpha\rangle := \mathcal{D}(\alpha)|\psi_0\rangle, \tag{C.7}$$

where $|\psi_0\rangle$ is some reference state. The well-known Glauber (or standard) coherent states [Glauber (1963)] are obtained for a QCV with the reference state as the vacuum, $|\text{vac}\rangle$, which is the lowest energy eigenstate of the quantum Harmonic oscillator. This state and the quantum harmonic oscillator are introduced in Appendix A. For qudits, coherent states are less often considered but one choice of reference state to define them is an eigenstate of the Fourier transform F [Klimov et al. (2009)[2]].

[2] This choice can be motivated by analogy to the QCV case - the eigenstates of the quantum harmonic oscillator are eigenstates of the QCV Fourier transform. This follows from results in Appendix D.

Appendix D

The Fourier gate

This appendix provides derivations for the properties of the Fourier gate, F, that are stated in Section 2.2.1 of the main text. For convenience, the definition of the Fourier gate for a general QV is repeated here. It is defined by,

$$F|q\rangle = \frac{1}{\sqrt{d}} \sum_{q' \in \mathbb{S}_d} \omega^{qq'} |q'\rangle, \tag{D.1}$$

with $q \in \mathbb{S}_d$. The reader is referred back to the start of Section 2.2 for an explanation of the QV-type independent notation used in this appendix. The following relation will be useful:

$$\frac{1}{d} \sum_{r \in \mathbb{S}_d} \omega^{r(q-q')} = \delta(q-q'), \tag{D.2}$$

where $q - q'$ is taken modulo d for qudits. For qudits this is straightforward to prove directly[1], and for QCVs it holds because the Fourier transform of a complex exponential function $e^{-iq'r}$ is a delta function, with the exact relation given by [Erdélyi (ed.)]

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}r e^{-q'r} e^{+iqr} = \sqrt{2\pi}\delta(q-q'). \tag{D.3}$$

It is first confirmed that F is indeed a unitary operator. Using Equation D.2

[1] This can be shown using the formula for a geometric series, which is the relation that $\sum_{r=0}^{d-1} a^r = \frac{1-a^d}{1-a}$ for any $a \in \mathbb{C}$ except $a = 1$. For $q \neq q'$ this gives $\frac{1}{d}\sum_{r=0}^{d-1} \omega^{(q-q')r} = \frac{1}{d}\frac{1-\omega^{d(q-q')}}{1-\omega^{q-q'}} = \frac{1}{d}\frac{1-1}{1-\omega^{q-q'}} = 0$. For $q = q'$ the sum is obviously equal to unity, giving the required result.

and the orthogonality relation $\langle q|q'\rangle = \delta(q-q')$, it follows that

$$FF^\dagger = \frac{1}{d}\sum_{q,q',r,r'\in\mathbb{S}_d} \omega^{qq'-rr'}|q\rangle\,\langle q'|r\rangle\,\langle r'|, \tag{D.4}$$

$$= \frac{1}{d}\sum_{q,r,r'\in\mathbb{S}_d} \omega^{r(q-r')}|q\rangle\langle r'|, \tag{D.5}$$

$$= \sum_{q,r'\in\mathbb{S}_d} \delta(q-r')|q\rangle\langle r'|, \tag{D.6}$$

$$= \sum_{q\in\mathbb{S}_d} |q\rangle\langle q|, \tag{D.7}$$

$$= \mathbb{I}. \tag{D.8}$$

The same derivation holds to show that $F^\dagger F = \mathbb{I}$, confirming that F is unitary. A simple adaption of this derivation shows that

$$F^2 = \sum_{q\in\mathbb{S}_d} |-q\rangle\langle q|, \tag{D.9}$$

which is a useful relation in itself and which implies that $F^4 = \mathbb{I}$, as stated in the main text.

In Equation 2.26 it was claimed that, under conjugation by F, the Pauli $X(q)$ and $Z(q)$ gates are transformed via the cyclic relation

$$\begin{tikzcd}
X(q) \arrow[r] & Z(q) \arrow[d] \\
Z(-q) \arrow[u] & X(-q) \arrow[l]
\end{tikzcd} \tag{D.10}$$

Again using Equation D.2 and the orthogonality relation $\langle q|q'\rangle = \delta(q-q')$, it follows that

$$FZ(p)F^\dagger = \frac{1}{d}\sum_{p',q,q',r,r'\in\mathbb{S}_d} \omega^{pp'+qq'-rr'}|q\rangle\left\langle q'|p'\right\rangle\left\langle p'|r\right\rangle\left\langle r'\right|, \tag{D.11}$$

$$= \frac{1}{d}\sum_{p',q,q',r,r'\in\mathbb{S}_d} \delta(q'-p')\delta(p'-r)\omega^{pp'+qq'-rr'}|q\rangle\langle r'|, \tag{D.12}$$

$$= \frac{1}{d}\sum_{p',q,r'\in\mathbb{S}_d} \omega^{p'(p+q-r')}|q\rangle\langle r'|, \tag{D.13}$$

$$= \sum_{q,r'\in\mathbb{S}_d} \delta(q-r'+p)|q\rangle\langle r'|, \tag{D.14}$$

$$= \sum_{r'\in\mathbb{S}_d} |r'-p\rangle\langle r'|, \tag{D.15}$$

$$= X(-p). \tag{D.16}$$

Note that, as always, $r'-p$ is to be taken modulo d for a d-dimensional qudit. A very similar derivation shows that $FX(p)F^\dagger = Z(p)$. Specifically,

$$FX(p)F^\dagger = \frac{1}{d}\sum_{p',q,q',r,r'\in\mathbb{S}_d} \omega^{qq'-rr'}|q\rangle\left\langle q'|p'+p\right\rangle\left\langle p'|r\right\rangle\left\langle r'\right|, \tag{D.17}$$

$$= \frac{1}{d}\sum_{p',q,q',r,r'\in\mathbb{S}_d} \delta(q'-p'-p)\delta(p'-r)\omega^{qq'-rr'}|q\rangle\langle r'|, \tag{D.18}$$

$$= \frac{1}{d}\sum_{p',q,r'\in\mathbb{S}_d} \omega^{qp+p'(q-r')}|q\rangle\langle r'|, \tag{D.19}$$

$$= \sum_{q,r'\in\mathbb{S}_d} \delta(q-r')\omega^{qp}|q\rangle\langle r'|, \tag{D.20}$$

$$= \sum_{q\in\mathbb{S}_d} \omega^{qp}|q\rangle\langle q|, \tag{D.21}$$

$$= Z(p). \tag{D.22}$$

Together, these prove the required cyclic relation given in this appendix and in Equation 2.26.

Finally, it is confirmed that applying the quantum harmonic oscillator Hamiltonian, $\hat{H}_{\text{QHO}} = \frac{1}{2}(\hat{x}^2+\hat{p}^2)$, for a time $t = 3\pi/2$ generates the QCV Fourier gate, as claimed in the main text. This means showing that, for a QCV

$$F = e^{-i\frac{3\pi}{4}(\hat{x}^2+\hat{p}^2)}. \tag{D.23}$$

More generally, using the notation $U(\hat{H},t) := e^{-it\hat{H}}$, consider the operator

$$U(\hat{H}_{\text{QHO}},t) = e^{-i\frac{t}{2}(\hat{x}^2+\hat{p}^2)}, \tag{D.24}$$

which is generated by the QHO Hamiltonian applied for a time t and may be termed a *phase-space rotation*. Using the relation

$$e^{A}Be^{-A} = B + [A,B] + \frac{1}{2!}[A,[A,B]] + \frac{1}{3!}[A,[A,[A,B]]] + \dots, \tag{D.25}$$

it is simple to derive that the conjugation action of $U(\hat{H}_{\text{QHO}},t)$ on $\hat{x}$ and $\hat{p}$ is

$$\hat{x} \xrightarrow{U(\hat{H}_{\text{QHO}},t)} \hat{x}\cos t - \hat{p}\sin t, \qquad \hat{p} \xrightarrow{U(\hat{H}_{\text{QHO}},t)} \hat{p}\cos t + \hat{x}\sin t. \tag{D.26}$$

These equalities are the reason for the name given to this operator. It is clear that for $t = 3\pi/2$ this has the action $\hat{x} \to \hat{p}$ and $\hat{p} \to -\hat{x}$. This action on the position and momentum operators implies that this is the Fourier transform - as stated above and in the main text. One way to see this is that the cyclic conjugation relation in Equation D.10 may be derived by using these equalities, the relations $X(q) = e^{-iq\hat{p}}$ and $Z(q) = e^{iq\hat{x}}$ given in Equation 2.14, and the general equality that for any unitary U then

$$Ue^{\hat{A}}U^{\dagger} = e^{U\hat{A}U^{\dagger}}. \tag{D.27}$$

The conjugation action of an operator on $X(q)$ and $Z(q)$ entirely defines an operator (up to global phase) and hence $U(\hat{H}_{\text{QHO}},3\pi/2)$ is the Fourier gate.

Appendix E

Clifford conjugation relations

In this appendix the conjugation relations of the Fourier, phase and CZ gates on Pauli operators are derived. It will be shown that

$$p_{\xi,q,q'} \xrightarrow{Z(p)} p_{\xi+2pq,q,q'}, \tag{E.1}$$

$$p_{\xi,q,q'} \xrightarrow{F} p_{\xi-2qq',-q',q}, \tag{E.2}$$

$$p_{\xi,q,q'} \xrightarrow{P(p)} p_{\xi+pq(q+\varrho_d),q,q'+pq}, \tag{E.3}$$

$$p_{\xi,(q_1,q_2,q_1',q_2')} \xrightarrow{\text{CZ}} p_{\xi+2q_1q_2,(q_1,q_2,q_1'+q_2,q_2'+q_1)}. \tag{E.4}$$

as was stated in Equation 2.51 to 2.53 of the main text. The first relation follows directly from the Weyl commutation relation of Equation 2.44 and hence does not require a derivation.

Consider the Fourier gate, F. The conjugation relations of this gate on $X(q)$ and $Z(q)$ have already been derived in Appendix D and are

$$X(q) \xrightarrow{F} Z(q), \qquad Z(q) \xrightarrow{F} X(-q). \tag{E.5}$$

Then, using the Weyl commutation relation, it follows that

$$\begin{aligned} p_{\xi,q,q'} \xrightarrow{F} \omega^{\xi/2} Z(q)X(-q') &= \omega^{\xi/2}\omega^{-qq'}X(-q')Z(q), && \text{(E.6)}\\ &= \omega^{(\xi-2qq')/2}X(-q')Z(q), && \text{(E.7)}\\ &= p_{\xi-2qq',-q',q}. && \text{(E.8)} \end{aligned}$$

This confirms the relation claimed in Equation E.2 of this appendix and in the main text.

Consider now the phase gate, $P(p)$. The conjugation action of the phase gate on

$X(q)$ is

$$\begin{aligned}
P(p)X(q)P(p)^\dagger &= \sum_{r,s,r\in\mathbb{S}_d} \omega^{\frac{p}{2}(r(r+\varrho_d)-t(t+\varrho_d))}|r\rangle\langle r|s+q\rangle\langle s|t\rangle\langle t|, && \text{(E.9)}\\
&= \sum_{r,s,t\in\mathbb{S}_d} \omega^{\frac{p}{2}(r(r+\varrho_d)-t(t+\varrho_d))}\delta(s+q-r)\delta(t-s)|r\rangle\langle t|, && \text{(E.10)}\\
&= \sum_{r,t\in\mathbb{S}_d} \omega^{\frac{p}{2}(r(r+\varrho_d)-t(t+\varrho_d))}\delta(t+q-r)|r\rangle\langle t|, && \text{(E.11)}\\
&= \sum_{t\in\mathbb{S}_d} \omega^{\frac{p}{2}((t+q)(t+q+\varrho_d)-t(t+\varrho_d))}|t+q\rangle\langle t|, && \text{(E.12)}\\
&= X(q)\sum_{t\in\mathbb{S}_d} \omega^{pq(q+\varrho_d)/2}\omega^{ptq}|t\rangle\langle t|, && \text{(E.13)}\\
&= \omega^{pq(q+\varrho_d)/2}X(q)Z(pq). && \text{(E.14)}
\end{aligned}$$

To get from E.12 to E.13 the brackets have been expanded which for QCVs, and when $t+q<d$ for qudits, follows directly as there is no modulo arithmetic to consider. For qudits, in the parts of the sum where $t+q\geq d$, then $t+q$ represents $t+q-d$ and such a replacement is in general necessary to obtain the correct answer. However, in this case, the calculation with or without this replacement gives the same result.[1] The phase gate commutes with $Z(q)$. Hence it follows that

$$p_{\xi,q,q'} \xrightarrow{P(p)} \omega^{(\xi+pq(q+\varrho_d))/2}X(q)Z(pq+q') = p_{\xi+pq(q+\varrho_d),q,q'+pq}, \tag{E.15}$$

which is the result stated in Equation E.3 and in the main text.

Finally, consider the CZ gate. From the Weyl commutation relation, the relation that $(\mathbb{I}\otimes v^\dagger)\cdot \mathrm{C}u\cdot(\mathbb{I}\otimes v) = \mathrm{C}(v^\dagger u v)$ and the equality $\mathrm{C}(\omega^q\mathbb{I}) = Z(q)\otimes\mathbb{I}$, it may be shown that

$$X(q_1)\otimes X(q_2) \xrightarrow{\text{CZ}} \omega^{q_1q_2}X(q_1)Z(q_2)\otimes X(q_1)Z(q_2). \tag{E.16}$$

The CZ commutes with $Z(q)$ and hence this implies that

$$p_{\xi,(q_1,q_2,q_1',q_2')} \xrightarrow{\text{CZ}} p_{\xi+2q_1q_2,(q_1,q_2,q_1'+q_2,q_2'+q_1)}, \tag{E.17}$$

as stated in Equation E.4 and in the main text. This concludes the derivation of the Clifford group generator conjugation relations.

[1] This is because ω is d periodic.

Appendix F

The Solovay-Kitaev theorem

Let $\mathcal{G}$ denote any finite set of fixed gates containing gates that act on a constant number of qudits which is approximately universal for computation over qudits such that if $g \in \mathcal{G}$ then $g^\dagger$ may be exactly generated by a finite sequence of gates from $\mathcal{G}$. Then the following, known as the *Solovay-Kitaev theorem*, holds:

Theorem F.1 (Kitaev (1997))**.** *For any gate $U \in U(d^n)$ and for any $\epsilon > 0$ there exists a finite sequence of gates from $\mathcal{G}$ of length no more than $\exp(O(n))O(\log^c(1/\epsilon))$ that is an ϵ-approximation to U where c is some constant. Furthermore, this sequence may be found by a classical algorithm with the same order runtime.*

The value of c depends on the particular proof, for example an explicit efficient algorithm with $c = 3.97$ is provided in the review paper of Dawson and Nielsen (2006). However c cannot be less than 1, as proven by Harrow et al. (2002) who have shown that in some circumstance the optimal value of 1 can be obtained but with no constructive method for finding these gate sequences. One important consequence of this theorem that is used herein is that one set of approximately universal single-qudit gates is essentially as good as any other set of approximately universal single-qudit gates, in the sense that they require a very small overhead to simulate one another to high precision.

Appendix G

Generic rotation gates

Consider the single-qudit gate set

$$\mathcal{G}_{\text{gen}} = \{R(\varphi), F\}, \tag{G.1}$$

where $\varphi : \mathbb{Z}(d) \to \mathbb{R}$ is a generic function, where the term 'generic' is used to mean that $\vartheta(q)$ is randomly sampled from $\mathbb{R}$ for each $q \in \mathbb{Z}(d)$.[1] By appealing to a standard argument used by Lloyd (1995) and Deutsch et al. (1995), in this appendix it is shown that this gate set can approximately generate any single-qudit gate. Hence, along with any entangling gate, this gate provides an approximately universal gate set for qudit-based quantum computation, via the results of Brylinski and Brylinski (2002) (see Proposition 2.2).

Proof: If an $R(\vartheta)$ unitary for any $\vartheta : \mathbb{Z}(d) \to \mathbb{R}$ may be approximated to arbitrary accuracy using F and $R(\varphi)$, then these two gates may approximate any single-qudit gate. This is because Zhou et al. (2003) have shown that any single-qudit can be decomposed into $R(\vartheta)$ and F gates. For a generic function $\varphi : \mathbb{Z}(d) \to \mathbb{R}$ it follows that $\varphi(q)$ and $\varphi(q')$ will be irrational multiples of π and each other for every $q, q' \in \mathbb{Z}(d)$ with $q \neq q'$.[2] For convenience, write these d different phase angles as a vector $\vec{\phi} = (\varphi(0), \dots, \varphi(d-1))$. Obviously, it is only necessary to be able to generate a rotation gate with any vector of phase angles, $\vec{\theta}$, with the restriction to $\vec{\theta} \in [0, 2\pi)^d$, as trivially $e^{i(x+2\pi)} = e^{ix}$. For $N \in \mathbb{N}$, consider

$$\vec{\phi}_N \equiv N\vec{\phi} \mod 2\pi = (N\varphi(0), N\varphi(1), \dots, N\varphi(d-1)) \mod 2\pi. \tag{G.2}$$

It is known that, for any vector $\vec{\phi}$ with elements that are irrational multiples of π and each other, the vectors $\vec{\phi}_1$, $\vec{\phi}_2$, $\vec{\phi}_3$, ... fill up the interval $[0, 2\pi)^d$, or stated

[1] Equivalently, we could consider the gate $R(\varphi)$ to be randomly selected from the set of all rotation gates.

[2] The intuition behind this is that there are only countably many functions that are not of this sort (the rational numbers are countable), but there are uncountably many functions $\vartheta : \mathbb{Z}(d) \to \mathbb{R}$.

another way, the set $\{\vec{\phi}_N \mid N \in \mathbb{N}\}$ is a dense subset of $[0, 2\pi)^d$. For example, this argument or closely related arguments are made in Lloyd (1995), Deutsch et al. (1995), and Childs et al. (2011). As such, for a $R(\vartheta)$ gate with any $\vartheta : \mathbb{Z}(d) \to \mathbb{R}$ and given any $\epsilon > 0$ there is some $N(\epsilon) \in \mathbb{N}$ such that $R(\varphi)^{N(\epsilon)}$ is an ϵ-approximation to $R(\vartheta)$. A more rigorous proof than that given here could be obtained by adapting the arguments of Childs et al. (2011), which are concerned with the universality of two-qubit Hamiltonians and unitaries.

Appendix H

The phase basis

In this appendix the action of the Pauli operators on the phase basis and the overlap between the states in the computational, conjugate and phase bases is derived. This will show that these bases are a set of three mutually unbiased bases for any type of QV. The phase basis is defined to be

$$\mathcal{B}_{\times} := \{|\times_q\rangle := PF|q\rangle \mid q \in \mathbb{S}_d\}, \tag{H.1}$$

where the reader is reminded that the phase gate P (the gate $P(p)$ with $p = 1$) is given by the action

$$P|q\rangle = \omega^{q(q+\varrho_d)/2}|q\rangle, \tag{H.2}$$

as first defined in Equation 2.49. Using the definition of the phase basis, the Pauli conjugation relation for the phase gate given in Equation 2.52, and the action of the Pauli operators on the conjugate basis given in Equation 2.29, it follows that

$$\begin{aligned} \omega^{\xi/2}X(a)Z(b)|\times_q\rangle &= \omega^{\xi/2}X(a)Z(b)P|+_q\rangle, && \text{(H.3)} \\ &= P\omega^{(\xi-a(a+\varrho_d))/2}X(a)Z(b-a)|+_q\rangle, && \text{(H.4)} \\ &= \omega^{(\xi-a(a+\varrho_d))/2+a(a-b-q)}|\times_{q+b-a}\rangle, && \text{(H.5)} \\ &= \omega^{(\xi+a(a-\varrho_d))/2-a(b+q)}|\times_{q+b-a}\rangle, && \text{(H.6)} \end{aligned}$$

as stated in Equation 7.28 of the main text.

Consider the overlap between arbitrary phase and computational basis states. Using the action of the phase gate on the computational basis and the overlap $\langle q|+_{q'}\rangle = \omega^{qq'}/\sqrt{d}$, it follows that for all $q, q' \in \mathbb{S}_d$ then

$$\begin{aligned} \langle q|\times_{q'}\rangle &= \langle q|P|+_{q'}\rangle, && \text{(H.7)} \\ &= \omega^{-q(q+\varrho_d)/2}\langle q|+_{q'}\rangle, && \text{(H.8)} \\ &= \omega^{q(q'-(q+\varrho_d)/2)}/\sqrt{d}, && \text{(H.9)} \end{aligned}$$

as stated in Equation 7.30 of the main text. Now, consider the overlap of arbitrary conjugate and phase basis states. Again, using the action of the phase gate on the computational basis and the overlap of the conjugate and computational bases, it follows that for all $q, q' \in \mathbb{S}_d$ then

$$\left\langle +_q \middle| \times_{q'} \right\rangle = \left\langle +_q \middle| P \middle| +_{q'} \right\rangle, \tag{H.10}$$

$$= \sum_{k \in \mathbb{S}_d} \omega^{\frac{k}{2}(k+\varrho_d)} \left\langle +_q \middle| k \right\rangle \left\langle k \middle| +_{q'} \right\rangle, \tag{H.11}$$

$$= \frac{1}{d} \sum_{k \in \mathbb{S}_d} e^{i\pi(k^2+k(2(q'-q)+\varrho_d))/d}. \tag{H.12}$$

This is a generalised quadratic Gauss sum when the QV is a qudit, and a Gaussian integral when the QV is a QCV. It can be evaluated using the following two results: For any $a, b \in \mathbb{N}$ such that $a > 0$ and $a + b$ is even then [Berndt and Evans (1981)]

$$\frac{1}{a} \sum_{k=0}^{a-1} e^{i\pi(k^2+bk)/a} = e^{i\frac{\pi}{4}} e^{-i\pi\frac{b^2}{4a}} / \sqrt{a}. \tag{H.13}$$

As $d \neq 0$ and $d + 2(q - q') + \varrho_d$ is even ($\varrho_d = 0$ and $\varrho_d = 1$ for even and odd d respectively), this can be applied to Equation H.12 for the case of qudits. For QCVs, the following integral relation can be used [Watson (1928); Weisstein (2004)]:

$$\frac{1}{a} \int_{-\infty}^{\infty} \mathrm{d}k \, e^{i\pi(k^2+bk)/a} = e^{i\frac{\pi}{4}} e^{-i\pi\frac{b^2}{4a}} / \sqrt{a}, \tag{H.14}$$

which has an exactly equivalent form to the discrete case. Hence, using these two relations it follows that in all cases

$$\left\langle +_q \middle| \times_{q'} \right\rangle = e^{i\frac{\pi}{4}} e^{-i\pi\frac{(2(q'-q)+\varrho_d)^2}{4d}} / \sqrt{d}, \tag{H.15}$$

$$= \omega^{qq'} \omega^{-\frac{q}{2}(q-\varrho_d)} \omega^{-\frac{q'}{2}(q'+\varrho_d)} \omega^{\frac{d-\varrho_d}{8}} / \sqrt{d}, \tag{H.16}$$

as stated in Equation 7.31 of the main text. This concludes this appendix on the phase basis.

Appendix I

The Hadamard and π-by-8 gates

Here it is proven that $v_0 = H$ and $v_1 = THT$ form a universal set of single qubit gates. This in turn provides a proof for the universality of the commonly used gate set $\mathcal{G}_{HT} = \{H, T\}$ due to Boykin et al. (2000). denote the n^{th} roots of the X and Z operators by $X^{\frac{1}{n}}$ and $Z^{\frac{1}{n}}$. Any $u \in SU(2)$ can be written as

$$u = \exp\left(i\varphi\hat{n}\cdot\vec{\sigma}\right), \tag{I.1}$$

where $\varphi \in \mathbb{R}$ is some rotation angle and $\vec{\sigma} = (X, Y, Z)$ is the vector of Pauli operators, $\hat{n} = (n_x, n_y, n_z)$ is some unit vector in $\mathbb{R}^3$. Hence, $\hat{n}\cdot\vec{\sigma} = n_x X + n_y Y + n_z Z$. Via a direct expansion it is simple to show that

$$\exp\left(i\varphi\hat{n}\cdot\vec{\sigma}\right) = \cos\varphi\mathbb{I} + i\sin\varphi(\hat{n}\cdot\vec{\sigma}). \tag{I.2}$$

Hence it follows that $Z = i\exp\left(-i\frac{\pi}{2}Z\right)$ and $X = i\exp\left(-i\frac{\pi}{2}X\right)$ where the phase factor i is need as the Pauli operators are not in $SU(2)$. Therefore

$$Z^{\frac{1}{n}} \cong \exp\left(-i\frac{\pi}{2n}Z\right), \qquad X^{\frac{1}{n}} \cong \exp\left(-i\frac{\pi}{2n}X\right), \tag{I.3}$$

where '$\cong$' is used to denote equality up to a phase and $X^{\frac{1}{n}} = HZ^{\frac{1}{n}}H$ as $HZH = X$. It is straightforward to confirm that $T \cong Z^{\frac{1}{4}}$ and so $v_+ := v_0v_1 \cong X^{\frac{1}{4}}Z^{\frac{1}{4}}$ and $v_- := v_1v_0 \cong Z^{\frac{1}{4}}X^{\frac{1}{4}}$. From a simple explicit calculation it can be shown that

$$v_\pm \cong \cos^2\frac{\pi}{8} - i\sin^2\frac{\pi}{8}\left(\cot\frac{\pi}{8}(Z+X) \mp Y\right). \tag{I.4}$$

If v_+ or v_- is written in the form of Equation I.2, this implies that $\cos\varphi_\pm = \cos^2\frac{\pi}{8}$ and hence φ is an irrational multiple of π [Boykin et al. (2000)]. Furthermore,

$\hat{n}_\pm = n_\pm/\|n_\pm\|$ where $n_\pm = -(\cot\frac{\pi}{8}, \mp 1, \cot\frac{\pi}{8})$. As φ is an irrational multiple of π then it is possible to approximate to arbitrary accuracy any rotation around the $n_\pm$ axis by m applications of $v_\pm$, with m a finite integer. As these axes of rotation are not parallel then any arbitrary rotation can be decomposed into rotations around these axes [Nielsen and Chuang (2010)[1]]. This then proves that v_+ and v_- and hence v_0 and v_1 are a universal set of single qubit gates. Essentially the same proof can be used to show that the single-qubit gate set $\{H, R(\theta)HR(\theta)\}$ for generic θ is a universal set.

[1] See exercise 4.11.

Appendix J

Stochastic gate implementation

This appendix includes derivations of equalities that were stated without proof in Section 7.4, which is concerned with what might be termed a 'stochastic minimal control model' of ancilla-based quantum computation. The gate which will be needed in this appendix is

$$\bar{E}_{ar}(v,w,\vartheta) := F_a^{\dagger} \cdot \mathrm{C}_r^a[\nu_{v,w,\vartheta}], \tag{J.1}$$

where $\nu : \mathbb{S}_{d_a} \to U(d)$ is the function defined by $\nu_{v,w,\vartheta}(q) = vR(2\pi q\vartheta/d_a)w$, for some $v,w \in U(d)$ and some phase-function ϑ with the restriction that $\vartheta : \mathbb{S}_d \to \mathbb{S}_{d_a}$. Equation 7.18 will be useful in this appendix, which states that

$$\bar{E}_{ar}(v,w,\vartheta) = F_a^{\dagger} v_r \cdot \mathrm{C}_a^r[Z(\vartheta)] \cdot w_r, \tag{J.2}$$

which can be easily confirmed directly by considering the action of this operator on computational basis states.

To begin, the relation stated in Equation 7.32 of the main text is derived. This is equivalent to the statement that

$$\frac{\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle}{\|\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle\|} = v_r'(m)v_s''(m) \cdot \left(v_r v_s \cdot D(\phi_\vartheta) \cdot w_r w_s\right), \tag{J.3}$$

where $|\psi_0\rangle = F|\times_0\rangle$ with $|\times_0\rangle$ the zero phase-basis state, ϕ_ϑ is the two-parameter function given by $\phi_\vartheta(q,p) = 2\pi\vartheta(q)\vartheta(p)/d_a$, and the ($m$-dependent) local gates are given by

$$v'(m) = vR(-2m\pi\vartheta/d_a)v^{\dagger}, \tag{J.4}$$

$$v''(m) = vR(2m\pi\vartheta/d_a)R(-\pi\vartheta(\vartheta+\varrho_{d_a})/d_a)v^{\dagger}. \tag{J.5}$$

It is easily confirmed that

$$\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle = v_r v_s \hat{O}(m) w_r w_s, \tag{J.6}$$

where $\hat{O}(m)$ is diagonal in the computational basis (as generalised control gates do not change the computational basis states of the control QV) and is given by

$$\hat{O}(m) = \sum_{q,p \in \mathbb{S}_d} C_m(q,p) |q\rangle\langle q|_r \otimes |p\rangle\langle p|_s, \tag{J.7}$$

with the coefficients found from the equality

$$C_m(q,p) = \langle m| F^\dagger Z(\vartheta(p)) F^\dagger Z(\vartheta(q)) F |\times_0\rangle. \tag{J.8}$$

Using the action of the Pauli operators on the phase basis state given in Equation 7.28, then

$$\begin{aligned} C_m(q,p) &= \langle m| F^\dagger Z(\vartheta(p)) F^\dagger Z(\vartheta(q)) F |\times_0\rangle, && \text{(J.9)} \\ &= \langle +_m | Z(\vartheta(p)) X(\vartheta(q)) |\times_0\rangle, && \text{(J.10)} \\ &= \langle +_m | \omega_a^{\vartheta(q)(\vartheta(q)-\varrho_d)/2} \big| \times_{\vartheta(p)-\vartheta(q)} \big\rangle, && \text{(J.11)} \\ &= \omega_a^{\vartheta(q)(\vartheta(q)-\varrho_{d_a})/2} \omega_a^{m(\vartheta(p)-\vartheta(q))} \omega_a^{-(\vartheta(p)-\vartheta(q))(\vartheta(p)-\vartheta(q)+\varrho_{d_a})/2} / \sqrt{d_a}, && \text{(J.12)} \end{aligned}$$

where deriving this last equality has used Equation 7.31 and holds only up to a (m-dependent) phase, which has been omitted for simplicity as it contributes only a global phase to the operator. Expanding this into phases dependent on $\vartheta(q)$, $\vartheta(p)$ and $\vartheta(q)\vartheta(p)$ gives

$$C_m(q,p) = \omega_a^{\vartheta(q)\vartheta(p)} \omega_a^{-\vartheta(q)m} \omega_a^{\vartheta(p)m} \omega_a^{-\frac{\vartheta(p)}{2}(\vartheta(p)+\varrho_{d_a})} / \sqrt{d_a}. \tag{J.13}$$

Note that $|C_m(q,p)| = 1/\sqrt{d_a}$ for all values of m, and so $\|\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle\| = 1/\sqrt{d_a}$. Therefore, the gate implemented on the r and s QVs is unitary and has the form

$$\frac{\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle}{\|\langle m|\bar{E}_{as}\bar{E}_{ar}|\psi_0\rangle\|} = v'_r(m) v''_s(m) \cdot \left(v_r v_s \cdot D(\phi_\vartheta) \cdot w_r w_s \right), \tag{J.14}$$

where ϕ_ϑ is given by $\phi_\vartheta(q,p) = 2\pi\vartheta(q)\vartheta(p)/d_a$ and the (m-dependent) local gates are given by

$$\begin{aligned} v'(m) &= v R(-2m\pi\vartheta/d_a) v^\dagger, && \text{(J.15)} \\ v''(m) &= v R(2m\pi\vartheta/d_a) R(-\pi\vartheta(\vartheta+\varrho_{d_a})/d_a) v^\dagger, && \text{(J.16)} \end{aligned}$$

which confirms Equation 7.32 of the main text.

The $D(\phi_\vartheta)$ gate is an entangling-gate for any phase-function ϑ such that there is some q and p for which $(\vartheta(q)-\vartheta(p))^2 \bmod d \neq 0$. This is because the action of $D(\phi_\vartheta)$ on an arbitrary pair of computational basis states is $|q,p\rangle \to \omega_a^{\vartheta(q)\vartheta(p)}|q,p\rangle$

and hence for the separable input

$$|\psi_{\text{in}}\rangle = \frac{1}{2}(|q,q\rangle + |q,p\rangle + |p,q\rangle + |p,p\rangle), \tag{J.17}$$

the $D(\phi_\vartheta)$ gate outputs

$$|\psi_{\text{out}}\rangle = \frac{1}{2}\left(\omega_a^{\vartheta(q)^2}|q,q\rangle + \omega_a^{\vartheta(q)\vartheta(p)}(|q,p\rangle + |p,q\rangle) + \omega_a^{\vartheta(p)^2}|p,p\rangle\right). \tag{J.18}$$

This is a separable state if and only if

$$\omega_a^{\vartheta(q)^2}\omega_a^{\vartheta(p)^2} = \omega_a^{2\vartheta(q)\vartheta(p)}, \tag{J.19}$$

and hence it is entangled if $\vartheta(q)^2 + \vartheta(p)^2 - 2\vartheta(q)\vartheta(p) \bmod d \neq 0$, that is, if

$$(\vartheta(q) - \vartheta(p))^2 \bmod d \neq 0. \tag{J.20}$$

Therefore given that there is some q and p such that this is true, then the gate creates an entangled state for some separable inputs which is the definition of a gate being entangling.

The relation of Equation J.21 is now derived, which states that

$$\frac{\langle m|\bar{E}_{ar}|\psi_0\rangle}{\|\langle m|\bar{E}_{ar}|\psi_0\rangle\|} = \tilde{v}R\left(-2m\pi\vartheta/d_a\right)w =: \mu(m), \tag{J.21}$$

where $\tilde{v} = vR(\pi\vartheta\left(\vartheta - \varrho_{d_a}\right)/d_a)$. It is clear that

$$\langle m|\bar{E}_{ar}|\psi_0\rangle = v_r\hat{o}(m)w_r, \tag{J.22}$$

where $\hat{o}(m) = \sum_{q\in\mathbb{S}_d} c_m(q)|q\rangle\langle q|$ with the coefficients, $c_m(q)$, given by

$$\begin{aligned} c_m(q) &= \langle m|F^\dagger Z(\vartheta(q))F|\times_0\rangle, \\ &= \langle m|X(\vartheta(q))|\times_0\rangle, \\ &= \omega_a^{\vartheta(q)(\vartheta(q)-\varrho_{d_a})/2}\left\langle m|\times_{-\vartheta(q)}\right\rangle, \\ &= \omega_a^{\vartheta(q)(\vartheta(q)-\varrho_{d_a})/2}\omega_a^{-m\vartheta(q)}/\sqrt{d_a}, \end{aligned}$$

with the last equality derived via Equation 7.30, and again holds only up to (m-dependent) irrelevant global phase. It may be easily confirmed that this implies the relation stated above. This concludes the appendix.

Appendix K

Ancillary spin ensembles

In this appendix a brief outline is given of a method for implementing an entangling gate on a pair of qubits via interactions with an ancillary qubit ensemble. This gate method can be understood in terms of a controlled geometric phase and hence is related to the ancilla-based gate techniques of Chapter 5. The method for implementing the gate is very straightforward - the majority of this appendix is dedicated to presenting the necessary introduction to collective spin operators for a qubit ensemble and showing how a geometric phase can be accessed via a closed path of phase-space $SU(2)$ displacements. The initial parts of the following section have been partially covered in the main text, but are included here for clarity.

K.1 The collective spin operators

Consider an ensemble of N qubits. Define the collective x, y, z, and total spin operators, respectively, by

$$J_x := \sum_{j=1}^{N} X_j = X_1 + X_2 + ...X_N, \tag{K.1}$$

$$J_y := \sum_{j=1}^{N} Y_j = Y_1 + Y_2 + ...Y_N, \tag{K.2}$$

$$J_z := \sum_{j=1}^{N} Z_j = Z_1 + Z_2 + ...Z_N, \tag{K.3}$$

$$J^2 := J_x^2 + J_y^2 + J_z^2. \tag{K.4}$$

Note that the Y Pauli operator may be defined in terms of X and Z by $Y := iXZ$. As Pauli operators acting on different qubits commute, it immediately follows from the commutation relation for the qubit Pauli operators, $[X, Y] = 2iZ$, that

$$[J_x, J_y] = 2iJ_z, \tag{K.5}$$

with cyclic permutations giving the remaining relations between J_x, J_y and J_z. It is straightforward to show that

$$[J^2, J_k] = 0, \tag{K.6}$$

for $k = x, y, z$. As J^2 and J_z commute, an orthonormal basis for the total Hilbert space on the spin ensemble can be found that consists of the joint eigenstates of J^2 and J_z and these are known as the *Dicke states* [Dicke (1954)]. The Dicke states may be denoted by $|j, m, d\rangle$, where

$$J^2|j, m, d\rangle = j(j + 2)|j, n, d\rangle, \qquad J_z|j, m, d\rangle = (2n - j)|j, n, d\rangle, \tag{K.7}$$

with $j \in \{0, 1, ..., N\}$, $n \in \{0, 1, ..., j\}$ and $d \in \{1, ..., d(j, n)\}$, where $d(j, n)$ is the degeneracy of the J^2 and J_z eigenvalue pair.[1] In what follows, only the $j = N$ subspace will be of interest and in this subspace the eigenvalues of J_z are *not* degenerate, implying that the subspace has dimension $N + 1$. The states in this subspace are symmetric with respect to the exchange of qubits in the ensemble [Arecchi et al. (1972)]. Using the shorthand $|n_D\rangle \equiv |N, n, 1\rangle$, it may be shown that in terms of the state of each individual qubit

$$|n_D\rangle = \binom{N}{n}^{-1/2} \sum_{\text{perm}} \left|1^{\otimes(N-n)}0^{\otimes n}\right\rangle, \tag{K.8}$$

where the sum is over all possible arrangements of the n excitations and $\binom{N}{n} = N!/n!(N - n)!$ is the binomial coefficient, required to normalise the state.

The $SU(2)$ *displacement operator* for the spin ensemble, which is also sometimes referred to as a ‘rotation operator’ [Arecchi et al. (1972); Gazeau (2009)], may be defined by

$$\mathcal{D}_N(\theta, \varphi) := \exp\left(i\left(\frac{\theta}{2}\sin\varphi J_x - \frac{\theta}{2}\cos\varphi J_y\right)\right), \tag{K.9}$$

where $\theta, \varphi \in \mathbb{R}$ [Zhang et al. (1990)]. A spin coherent states (or $SU(2)$, atomic or Bloch states) of the $N + 1$ dimensional symmetric subspace of a qubit ensemble [Arecchi et al. (1972); Gazeau (2009); Radcliffe (1971)] is then defined by

$$|\theta, \varphi\rangle_N := \mathcal{D}_N(\theta, \varphi)|0, 0\rangle_N, \tag{K.10}$$

[1] It is clear that the eigenvalues must be degenerate as there are N^2 different (j, n) labelling pairs but 2^N states are required to span a Hilbert space of dimension 2^N.

where the reference state is taken to be

$$|0,0\rangle_N = |0_D\rangle = |1\rangle^{\otimes N}. \tag{K.11}$$

Hence, a spin coherent state is a separable state of N qubits in the same pure state, which may be written as

$$|\theta,\varphi\rangle_N = \left(\cos\frac{\theta}{2}|1\rangle - e^{-i\varphi}\sin\frac{\theta}{2}|0\rangle\right)^{\otimes N}, \tag{K.12}$$

and as such, a spin coherent state can be represented on a Bloch sphere and the displacement operator can be interpreted as a rotation around some vector in the xy-plane.

An alternative parameterisation for the spin coherent states may be introduced, which will be useful in the following and which is analogous to writing a QCV (i.e., a field-mode) coherent state in terms of a complex number α. Take

$$\zeta = -e^{-i\varphi}\tan\frac{\theta}{2}, \tag{K.13}$$

which is a stereographic projection of the sphere onto the complex plane [Gazeau (2009)] and with which the spin coherent states can be expressed as

$$|\zeta\rangle_N = \left(\frac{|1\rangle + \zeta|0\rangle}{\sqrt{1+|\zeta|^2}}\right)^{\otimes N}. \tag{K.14}$$

This implies that the overlap between two spin coherent states is

$$\langle\zeta|\zeta'\rangle = \left(\frac{1+\zeta^*\zeta'}{\sqrt{(1+|\zeta|^2)(1+|\zeta'|^2)}}\right)^N. \tag{K.15}$$

In this parameterisation, the displacement operator may be written as

$$\mathcal{D}_N(\zeta) = \left(\frac{I_2 + \zeta\sigma_+ - \zeta^*\sigma_-}{\sqrt{1+|\zeta|^2}}\right)^{\otimes N}, \tag{K.16}$$

where $\sigma_\pm := \frac{1}{2}(X \pm iY)$. By definition $|\zeta\rangle_N = \mathcal{D}_N(\zeta)|0\rangle_N$, and it is simple to confirm that

$$\mathcal{D}_N(\zeta_2)\mathcal{D}_N(\zeta_1)|0\rangle_N = e^{iN\phi(\zeta_1,\zeta_2)}\left|\frac{\zeta_1+\zeta_2}{1-\zeta_1\zeta_2^*}\right\rangle_N, \tag{K.17}$$

where the phase factor is given by

$$e^{i\phi(\zeta_1,\zeta_2)} = \frac{1-\zeta_1\zeta_2^*}{|1-\zeta_1\zeta_2^*|}. \tag{K.18}$$

K.2 Geometric phases via $SU(2)$ displacements

It is now shown how a closed path of displacements, acting on the 'vacuum' state, $|0\rangle_N$, can create a geometric phase. Displacements around the orthogonal x and y axes are given by taking $\cos\varphi = 0$ (which is equivalent to $\zeta \in \mathbb{R}$) and $\sin\varphi = 0$ (which is equivalent to $i\zeta \in \mathbb{R}$) respectively. Now, consider acting a sequence of these orthogonal displacements on the vacuum, $|0\rangle_N$. Specifically, consider

$$\mathcal{D}_N(-i\zeta_4)\mathcal{D}_N(-\zeta_3)\mathcal{D}_N(i\zeta_2)\mathcal{D}_N(\zeta_1)|0\rangle_N = e^{i\phi(\zeta_j,N)}|\zeta(\zeta_j)\rangle_N, \tag{K.19}$$

where $\zeta_j \in \mathbb{R}$ for $j = 1, 2, 3, 4$. Note that the LHS of this equation must be equal to the RHS for some $\zeta \in \mathbb{C}$ and $\phi \in \mathbb{R}$ because displacement operators transform coherent states to coherent states, up to a phase. Equation K.17 and simple algebraic manipulations can be used to shown that

$$\zeta(\zeta_j) = \frac{(\zeta_1 + i\zeta_2)(1 - i\zeta_3\zeta_4) - (1 + i\zeta_1\zeta_2)(\zeta_3 + i\zeta_4)}{(\zeta_1 + i\zeta_2)(\zeta_3 - i\zeta_4) + (1 + i\zeta_1\zeta_2)(1 + i\zeta_3\zeta_4)}, \tag{K.20}$$

with the phase factor given by $e^{i\phi(\zeta_j,N)} = (\beta/|\beta|)^N$ where β is

$$\beta(\zeta_j) = \frac{(1 + i\zeta_1\zeta_2)(1 + i\zeta_3\zeta_4) + (\zeta_1 + i\zeta_2)(\zeta_3 - i\zeta_4)}{(1 + i\zeta_1\zeta_2) + \zeta_3(\zeta_1 + i\zeta_2)}. \tag{K.21}$$

An area-dependent phase and no resultant displacement is created if $\zeta = 0$. If the 'phase space' in which the displacements act has a flat geometry (such as for a QCV, which has the phase space $\mathbb{R}^2$), it is required that $\zeta_1 = \zeta_3$ and $\zeta_2 = \zeta_4$, and the simplest case is given by taking $\zeta_1 = \zeta_2 = \zeta_3 = \zeta_4$. However, on the surface of a sphere (the relevant space here) this choice of displacements will not result in a closed loop. Via a geometric argument, as given in Figure K.1, it is possible to see that $\zeta = 0$ may be satisfied whilst restricting the displacement parameters such that $\zeta_4 = \zeta_1 = \eta$ and that such a restriction implies that $\zeta_2 = \zeta_3 = \tau(\eta)$ with $\tau \neq \eta$. It may then be shown, by setting Equation K.20 equal to zero, that such a choice for the displacement parameters implies that

$$\tau(\eta) = \frac{1 - \eta^2 - \sqrt{\eta^4 - 6\eta^2 + 1}}{2\eta}. \tag{K.22}$$

As $a + bi = |a + bi| \exp(i \tan^{-1}(b/a))$ when $a > 0$, the phase factor ϕ can be shown, using Equation K.21, to be given by

$$\phi(\eta, \tau, N) = N \tan^{-1}\left(\frac{2\eta\tau + \tau^2 - \eta^2}{1 + 2\eta\tau - \eta^2\tau^2}\right). \tag{K.23}$$

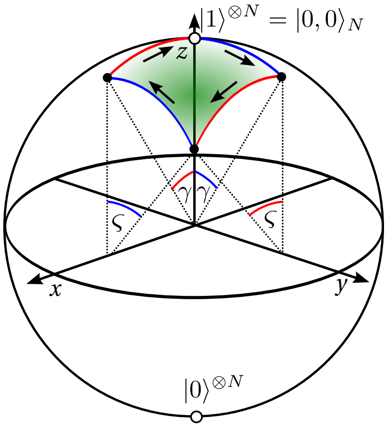


Figure K.1: A geometric phase is obtained by the displacement of a spin coherent state around a closed loop. If orthogonal displacements (rotations around the x and y axes) are considered it can be seen that the 1st and 4th rotations may be taken to be of an equal magnitude γ and that this implies that the 2nd and 3rd rotations are of an equal magnitude ς. The rotation angles γ and ς can be related to the complex variables η and τ from Equation K.22 via the stereographic projection.

This then implies that

$$\langle 0|_N \mathcal{D}_N(-i\eta)\mathcal{D}_N(-\tau)\mathcal{D}_N(i\tau(\eta))\mathcal{D}_N(\eta)|0\rangle_N = e^{i\phi(\eta,\tau,N)}. \tag{K.24}$$

As a side point, it is interesting to consider under what conditions $\tau \approx \eta$, which is when the curvature of the phase space can be ignored with the resultant phase space path still approximately closed. To consider this, τ and ϕ may be expanded around $\eta = 0$, giving

$$\tau(\eta) = \eta + O(\eta^3), \qquad \frac{\phi(\eta,\tau(\eta),N)}{N} = 2\eta^2 + O(\eta^4), \tag{K.25}$$

and hence, when $\eta \ll 1$ the higher order terms will be negligible. In this case, τ will be well approximated by η and the area-dependent phase created is approximately equal to that expected in a flat geometry.[2]

It is now shown how the geometric phase of Equation K.24 can be used to create a controlled phase gate on a pair of qubits, if they may interact with a spin ensemble via a type of controlled $SU(2)$ displacement. Consider the interaction between a computational qubit, labelled j, and a spin ensemble, of the form

$$\mathcal{D}^j_N(\zeta) := |0\rangle\langle 0|_j \otimes \mathcal{D}_N(\zeta) + |1\rangle\langle 1|_j \otimes \mathcal{D}_N(-\zeta). \tag{K.26}$$

[2] That the phase parameter here is $2\eta^2$ rather than η^2, when the displacement is around a 'square' of sides η, follows from the definition of the displacement operator, which implies that the geometric phase created is twice the area enclosed in phase space. This also appears in the phase accrued by displacements around a square of sides η with a QCV complex-number parameterised displacement operator, as can be seen by reference to Appendix C.

It then follows directly from Equation K.24 that

$$\langle 0|_N \mathcal{D}_N^t(-i\eta)\cdot\mathcal{D}_N^c(-\tau(\eta))\cdot\mathcal{D}_N^t(i\tau(\eta))\cdot\mathcal{D}_N^c(\eta)|0\rangle_N = \exp(i\phi(\eta,\tau,N)Z_c\otimes Z_t), \quad \text{(K.27)}$$

where $\tau(\eta)$ and $\phi(\eta,\tau,N)$ are given by Equation K.22 and Equation K.23 respectively. It is simple to confirm that this entangling gate is locally equivalent to $CR(4\phi)$, via local rotation gates. The value of ϕ can be fixed by changing the interaction parameters and may be chosen so that the implemented gate is CZ.

In order to implement this gate it is only necessary to be able to apply controlled displacements for $\zeta \in \mathbb{R}$, as for such ζ it is simple to confirm that

$$(HP^\dagger)^{\otimes N}\cdot\mathcal{D}_N^j(\zeta)\cdot(PH)^{\otimes N} = \mathcal{D}_N^j(i\zeta). \quad \text{(K.28)}$$

These local operations on the spin ensemble can be applied *without* single-qubit addressability of the constituent qubits in the ensemble and for this reason such control of the ensemble is physically plausible. The interaction between the computational qubits and the ensemble qubits used to implement this gate is simply

$$\hat{H}_{\text{SE}} = Z\otimes J_x, \quad \text{(K.29)}$$

and this interaction is physically realistic (e.g., it is not that dis-similar to the Hamiltonian in the experiment of Zhu et al. (2011), which couples a flux qubit to an NV-centre spin-ensemble in diamond). The discussions of Section 5.5, on encoding a qudit into a spin ensemble, are largely relevant again here and this can be referred back to for further details. An important source of errors for this gate method would be leakage out of the symmetric subspace, which could be caused by inhomogeneity in the ensemble, for example, if the coupling strength to the control computational qubit varies over the ensemble. If this gate method were to be further pursued, an important topic for future work would be to consider the effect on the computational model of such physically relevant errors within the realistic parameter regimes of a specific physical system.

To conclude this appendix, it is noted that there are two interesting formal links between this gate method and quantum computing on a register of qubits via a QCV ancilla, as covered by the geometric phase gate of Section 5.2. Firstly, in the limit of infinite constituent spins ($N\to\infty$) the spin ensemble mediated gate, introduced above, is formally equivalent to the 'qubus' geometric phase gate (up to some local rotation gates), whereby qubits are entangled via controlled Pauli operators acting on an ancillary QCV. This is because, as shown in Section K.3,

$$\lim_{N\to\infty}\mathcal{D}_N\left(\frac{\zeta}{\sqrt{N}}\right) = \exp\left(\zeta\hat{a}^\dagger - \zeta^*\hat{a}\right) = \mathcal{D}(\zeta), \quad \text{(K.30)}$$

where $\mathcal{D}(\zeta)$ is the $\mathbb{C}$-number parameterised displacement operator for a QCV, given in Equation C.6. This is itself equivalent to QCV Pauli operators, and in particular for $\alpha \in \mathbb{R}$, then $\mathcal{D}(\alpha/\sqrt{2}) = X(\alpha)$ and $\mathcal{D}(i\alpha/\sqrt{2}) = Z(\alpha)$, via Equation C.2 (see Appendix C more generally for further details). Another interesting relation between this spin ensemble based gate and QCV-based gates is that, instead of collective spin operators, all of the formalism of this appendix also applies to the angular momentum operators for a QCV in three dimensions (i.e., a quantum system with position and momentum in three spatial dimensions), as discussed briefly in Section K.4. Note that both of these connections are largely only of interest from a formal perspective.

K.3 The group contraction of $SU(2)$

The group contraction of $SU(2)$ demonstrates the $N \to \infty$ limit of the spin coherent states [Arecchi et al. (1972); Dooley et al. (2013); Gazeau (2009); Radcliffe (1971)] and shows that in this limit the displacement operator of Equation K.9 is equivalent to that for a bosonic mode, i.e., a QCV. By defining

$$J_{\pm} := \frac{1}{2}(J_x \pm iJ_y) = \sum_{j=1}^{N} \sigma_{\pm_j}, \tag{K.31}$$

the J spin operators can be represented by the creation and annihilation operators of a QCV by the Holstein-Primakoff transformation [Holstein and Primakoff (1940)]

$$\frac{J_+}{\sqrt{N}} = \hat{a}^\dagger \sqrt{1 - \frac{\hat{a}^\dagger \hat{a}}{2N}}, \qquad \frac{J_-}{\sqrt{N}} = \sqrt{1 - \frac{\hat{a}^\dagger \hat{a}}{2N}}\hat{a}, \qquad J_z = \hat{a}^\dagger \hat{a} - N. \tag{K.32}$$

It is straightforward to confirm that these operators obey the required $SU(2)$ commutation relations, given in terms of J_k with $k = x, y, z$ in Equation K.5. It then follows that

$$\lim_{N\to\infty} \frac{J_+}{\sqrt{N}} = \hat{a}^\dagger, \qquad \lim_{N\to\infty} \frac{J_-}{\sqrt{N}} = \hat{a}. \tag{K.33}$$

From the definition of $\mathcal{D}_N(\theta, \varphi)$ in Equation K.9, and the relation $\zeta = -e^{-i\varphi} \tan \frac{\theta}{2}$, it may be shown that

$$\mathcal{D}_N(\zeta) = \exp\left(\frac{\tan^{-1}|\zeta|}{|\zeta|}(\zeta J_+ + \zeta^* J_-)\right). \tag{K.34}$$

As $\tan^{-1}(x) = x + \mathcal{O}(x^3)$ via a Taylor expansion of $\tan^{-1}(x)$ around the $x = 0$, it is clear that

$$\lim_{N\to\infty} \frac{\tan^{-1}|\zeta/\sqrt{2N}|}{|\zeta/\sqrt{2N}|} = 1. \tag{K.35}$$

Combining these limits together results in the relationship between the $SU(2)$ and the Glauber displacement operators being given by

$$\lim_{N\to\infty} \mathcal{D}_N\left(\frac{\zeta}{\sqrt{N}}\right) = \exp\left(\zeta\hat{a}^\dagger - \zeta^*\hat{a}\right) = \mathcal{D}(\zeta), \tag{K.36}$$

where $\mathcal{D}(\zeta)$ is the $\mathbb{C}$-number parameterised displacement operator for a continuous variable given in Equation C.6. Furthermore, via this contraction process it may be shown that

$$\lim_{N\to\infty} \left|\frac{\zeta}{\sqrt{N}}\right\rangle_N = |\zeta\rangle, \tag{K.37}$$

where the RHS of this equation is a ($\mathbb{C}$-number parametrised) Glauber coherent state, as defined in Equation C.7 [Arecchi et al. (1972); Dooley et al. (2013); Gazeau (2009); Radcliffe (1971)]. This can be achieved by writing a spin coherent state in terms of the Dicke states $|n_D\rangle$ and then, in the limit of $N \to \infty$, associating the Dicke state $|n_D\rangle$ with the QHO energy eigenstate $|n\rangle$ (see Appendix A for details on the QHO) and noting that this has exactly the form of the QHO, or Glauber, coherent states written as an infinite sum of the QHO eigenstates.

K.4 Angular momentum operators

The collective spin operators obey exactly the same commutation relations as the (scaled[3]) angular momentum operators of elementary quantum mechanics

$$\hat{l}_x = 2(\hat{q}_y\hat{p}_z - \hat{q}_z\hat{p}_y), \tag{K.38}$$

$$\hat{l}_y = 2(\hat{q}_z\hat{p}_x - \hat{q}_x\hat{p}_z), \tag{K.39}$$

$$\hat{l}_z = 2(\hat{q}_x\hat{p}_y - \hat{q}_y\hat{p}_x), \tag{K.40}$$

$$\hat{l}^2 = \hat{l}_x^2 + \hat{l}_y^2 + \hat{l}_z^2, \tag{K.41}$$

where $[\hat{q}_j, \hat{p}_k] = i\delta_{jk}$, which are the position and momentum operators in orthogonal directions x, y and z. In this case, for any subspace of fixed total angular momentum l (i.e., an Eigen-space of $\hat{l}^2$), the $\hat{l}_z$ eigenvalues are non-degenerate and the spin coherent state formalism may be employed. In particular, the equivalent limit to $N \to \infty$ is given by taking $l \to \infty$ [Gazeau (2009)]. Therefore, the formalism and gate method presented above applies also to a system governed by such operators. As such, this provides a second link between gates mediated via spin ensembles and QCVs. However, it is likely that this is only interesting in an abstract sense, as I am unaware of any systems in which qubit-controlled angular displacements are a

[3] They have been scaled by a factor of 2 due to the definitions of the J operators. The spin operators could instead be scaled by a factor of 1/2.

physically relevant interaction.