Experiments with Generalized Quantum Measurements and Entangled Photon Pairs

by

Devon N. Biggerstaff

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science
in
Physics

Waterloo, Ontario, Canada, 2009

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

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

D. N. Biggerstaff

Abstract

This thesis describes a linear-optical device for performing generalized quantum measurements on quantum bits (qubits) encoded in photon polarization, the implementation of said device, and its use in two different but related experiments. The device works by coupling the polarization degree of freedom of a single photon to a 'mode' or 'path' degree of freedom, and performing a projective measurement in this enlarged state space in order to implement a tunable four-outcome positive operator-valued measure (POVM) on the initial quantum bit. In both experiments, this POVM is performed on one photon from a two-photon entangled state created through spontaneous parametric down-conversion.

In the first experiment, this entangled state is viewed as a two-qubit photonic cluster state, and the POVM as a means of increasing the computational power of a given resource state in the cluster-state model of quantum computing. This model traditionally achieves deterministic outputs to quantum computations via successive projective measurements, along with classical feedforward to choose measurement bases, on qubits in a highly-entangled resource called a cluster state; we show that 'virtual qubits' can be appended to a given cluster by replacing some projective measurements with POVMs. Our experimental demonstration fully realizes an arbitrary three-qubit cluster computation by implementing the POVM, as well as fast active feed-forward, on our two-qubit photonic cluster state. Over 206 different computations, the average output fidelity is 0.9832 ± 0.0002; furthermore the error contribution from our POVM device and feedforward is only of order 10^{-3}, less than some recent thresholds for fault-tolerant cluster computing.

In the second experiment, the POVM device is used to implement a deterministic protocol for remote state preparation (RSP) of arbitrary photon polarization qubits. RSP is the act of preparing a quantum state at a remote location without actually transmitting the state itself. We are able to remotely prepare 178 different pure and mixed qubit states with an average fidelity of 0.995. Furthermore, we study the the fidelity achievable by RSP protocols permitting only classical communication, without shared entanglement, and compare the resulting benchmarks for average fidelity against our experimental results. Our experimentally-achieved average fidelities surpass the classical thresholds whenever classical communication alone does not trivially allow for perfect RSP.

Acknowledgements

Several people deserve thanks for helping to make my Masters degree successful.

First, thank you to my supervisor Kevin Resch, who had great ideas for experiments and an open-door policy when I had questions. Kevin expected much from me, and taught me much about the intricacies of academic physics.

Particular thanks go to Rainer Kaltenbaek, whose help and advice proved invaluable whenever I encountered problems in the lab or in calculations. Rainer taught me everything from useful little tricks to broad strategies for attacking certain problems. Finally, without his programming skills in LabView, Matlab, and Mathematica, my research would have taken much longer and been far more tedious.

A significant part of my enjoyment of experimental physics stems from the camaraderie of the lab environment. In fact the company of other nerds is one of the few factors protecting against mental instability when one spends countless long hours in a dark windowless room otherwise filled primarily with computers, lasers, and Rube-Goldberg-esque optical contraptions. So thank you to Rainer (again) and to Jonathan Lavoie, Kurt Schrieter, and Deny Hamel for their good humor and helpful attitudes.

Thanks are also due to those collaborators outside my research group who contributed their time, effort, and most importantly their ideas towards the research presented in this thesis and towards related publications. Nathan Killoran not only did great work on the theory of thresholds for remote state preparation without entanglement, but also as my friend and housemate made an invaluable sounding-board, as I would discuss the progress and problems in the experiment with him, and he those in the theory with me. Thank you also to Terry Rudolph whose ideas helped inspire the experiments in this thesis, and who made our writing and editing quick and productive and yet maintained his patience throughout careful explanations to me of several concepts. Thank you also to Norbert Lütkenhaus and Gregor Weihs for their ideas, contributions, and guidance.

Heartfelt and sincere thanks go to Mike and Ophelia Lazaridis for their financial largess in support of science in Waterloo, including the Institute for Quantum Computing, and in particular for generously supporting me during two years of my tenure here as a Masters student through the Mike and Ophelia Lazaridis Fellowship for international graduate students at IQC.

During my degree I benefited greatly from the consistently high level of administrative and technical support for students' research at the University of Waterloo physics depart-

ment and particularly at IQC. Many thanks to Zhenwen Wang in the Science Technical Services electronics shop for his amazing ability to understand what I needed a new piece of electronic logic to do, even when I did not, and then to design, manufacture and deliver it working perfectly within weeks or even days. Thanks also to all the administrative staff in the physics department and at IQC for their adept support and unfailing good humor.

Without the lessons, encouragement, and sage advice imparted to me by previous supervisors I would never have reached this point in my physics career. Special thanks go to Alan Thorndike at the University of Puget Sound who supervised me and collaborated on my first serious experimental research project, and along the way introduced me both to quantum mechanics and to experimental optics, and taught me much of what I know about how to think like a physicist. I am also very grateful to Mike Raymer and Andrew White for enthusiastically taking me on in their laboratories, for teaching me my way around an academic optics lab, and for their good counsel regarding my future.

Finally, many thanks and much love to all the family and friends whose emotional support helped keep me going during my masters. In particular to my girlfriend Katrina, my brother Tyson, and my parents Dennis and Rae Lynn—thank you so much, I love you all, and I'll see you again very soon!

Dedication

This is dedicated to the world's most ridiculous excuse for a dog, who passed away at the venerable age of 15 while I was writing this thesis, and to my family and everyone else who misses him. Rest in peace, Sumo. 1994–2009.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

"What happens when we perform this kind of measurement on that entangled system?" Since first posed by Erwin Schrödinger in 1935 [1], this seemingly simple question has inspired much progress in understanding quantum theory, and many of the most useful protocols in quantum information, quantum communication, quantum metrology, and quantum computing.

That same year, Einstein, Podolsky and Rosen famously elucidated the way in which perfect correlations would be obtained when performing the same measurement on the subsystems of a bipartite entangled system, even for measurements of non-commuting observables [2]. Almost 30 years later, John S. Bell achieved a crucial insight by considering the correlations between the outcomes of measurements on the two subsystems which were neither the same nor canonically conjugate, and famously showed that these correlations were sufficiently strong that one cannot consider each measurement to have been simply revealing pre-existing properties of the subsystems, at least not if one accepts the seemingly common-sense notion that neither the choice of measurement on a system nor its outcome can affect the outcome of a simultaneous measurement on a distant system [3].

Among the most famous protocols in quantum information, quantum dense coding enables the transmission of two classical bits of information in a single quantum bit[4], and quantum teleportation enables an unknown quantum state held at one location to be prepared at a distant location via the transmission of only two classical bits [5]. Both protocols work based on properly performing measurements on subsystems of an entangled system. Quantum cryptography, the most well-known result from the study of quantum communication and perhaps the first to have real-world applications, allows the uncondi-

tionally secure distribution of a cryptographic key through the use of measurements on distributed entangled systems [6]. In quantum metrology, entanglement is employed to allow increased precision in some measurements. For instance, measurements of optical phase using four-photon entangled states can achieve better precision than the standard quantum limit [7]. In quantum computing, the "one-way" or cluster-state model allows universal quantum computation using only measurements and classical feedforward on a large, ordered, multi-partite entangled resource called a cluster-state [8, 9, 10].

Most of these protocols involve performing projective measurements, the standard determination of the value of an observable that most physicists probably have in mind when they think of quantum measurement. However, the theory of generalized quantum measurements allows significantly more freedom in the choice of a set of measurement operators, and such measurements, sometimes called Positive Operator-Valued Measures or POVMs, have been shown to be optimal for some quantum information tasks, in particular discrimination between non-orthogonal states [11]. Also, beginning with the tests of Bell's theorem [12, 13, 14], entangled photons have been among the earliest systems used to test many of these protocols (see e.g. [15, 16, 17, 18]). This is due to the relative ease of preparing, distributing and measuring entangled photons.

In this thesis I present results derived from inquiring once again as to the utility of measurements on entangled systems, but this time considering generalized measurements. I present and explain a tunable linear-optical apparatus for performing a range of four-outcome POVMs on the polarization degree-of-freedom of a single photon. I then detail two experiments enabled by this measurement apparatus, both performed using polarization-entangled photon pairs. The first experiment concerns cluster-state quantum computing. After explaining how POVMs can be used to extend the computational power of a given cluster resource, I present the results of an experiment showing that by performing a POVM one subsystem from a system of two entangled binary quantum systems, or qubits, and employing classical feedforward of the measurement result, one can implement a cluster computation which would normally require three qubits.

The second experiment concerns remote state preparation, a protocol related to quantum teleportation but where the state to be remotely prepared is known to the transmitting party. By implementing a tunable POVM on one photon from an entangled pair and transmitting the result as a two-bit classical string, the other photon can be deterministically prepared in an arbitrary pure or mixed polarization state. Furthermore bounds are derived on remote state preparation *without* entanglement, i.e. limited to only classical commu-

nication, and our experimental protocol clearly surpasses these bounds in every instance where classical communication is not sufficient for perfect remote state preparation.

1.1 Overview of the Thesis

The results concerning cluster-state quantum computation and remote state preparation were first prepared, along with my experimental and theoretical collaborators, as papers to be submitted for publication. These papers, with the addition of notes concerning the contributions of the several co-authors, constitute Chapters 4 and 5. In Chapter 2, I present a review of concepts from the theory of quantum information and quantum computing which will be relevant to the experiments, including quantum states and qubits, quantum measurement theory, quantum state tomography, teleportation, and cluster-state quantum computation. Chapter 3 provides an overview of using polarization-entangled photonic qubits for quantum information tasks, including their production, manipulation, and measurement, and specifically addresses the realization of the apparatuses used in the cluster-state and remote state preparation experiments, including the source of entangled photon pairs, the apparatus for performing the POVM, and the use of feedforward to implement correction operations on the other photon.

I have endeavored to present sufficient background information in the earlier chapters such that any physicist could have a complete understanding of Chapters 4 and 5, and also to include most everything that could be useful as a reference for someone using significant portions of my experimental apparatus in the future. Because of this, to physicists knowledgeable in quantum information, much of the material in Ch. 2 may already be familiar. Such a reader might wish to skip this chapter, with the possible exceptions of sections 2.1.3.3, 2.1.5, 2.2.2, and 2.2.3 (especially 2.2.3.2). Furthermore, there is some unavoidable repetition between Chapters 2 and 3, where many concepts and experimental apparatuses and procedures are explained in detail, and Chapters 4 and 5 which concern the experiments and results. Most of Ch. 3 could therefore also be skipped by a reader who is somewhat familiar with single-photon experiments and is uninterested in the details of the experimental implementation.

In Chapter 6 I review the main results of the thesis and suggest some future directions for related investigations.

Chapter 2

Background: Quantum Information and Computation

2.1 Quantum Information

2.1.1 Quantum States

In quantum theory the state of an isolated physical system can be represented as a unit vector $|\psi\rangle$ in an abstract Hilbert space $\mathcal{H}$, where the inner product $\langle\psi|\,\psi\rangle = 1$ (the normalization condition). If $\{|\psi_i\rangle\}$ are all physically valid states then any superposition $|\phi\rangle = \sum_i c_i\,|\psi_i\rangle$, $c_i \in \mathbb{C}$ will also be a physically valid state, as long as $\langle\phi|\,\phi\rangle$ is still equal to unity, or equivalently $\sum_i |c_i|^2 = 1$. This is known as the *superposition principle.*

If $\mathcal{H}$ is of finite dimension d[1], then $|\psi\rangle$ can be represented as a d-vector in a particular orthonormal basis $\{|\chi_j\rangle\}$ with $j = \{1, \ldots, d\}$ and $\langle\chi_i|\,\chi_k\rangle = \delta_{ik}$. The normalization condition implies the following restriction on the d elements of the vector c_i: $\sum_i |c_i|^2 = 1$. A d-dimensional system is sometimes called a *qudit.*

However it may be that the physical system in question is *not* isolated, meaning that through previous interactions it has become somehow correlated with the environment. In fact in experiment this is nearly always unavoidable[2]. In this case we must resort to the

[1] For the remainder of this thesis we are concerned only with finite-dimensional Hilbert spaces.

[2] Of course, we could just expand the definition of "system" at the expense of "environment" in order to include those (previously external) physical systems with which our original system has become correlated. This is often cumbersome in theory, impossible in experimental practice, and undesirable in both.

density operator formalism: a state is represented by an $d \times d$ nonnegative operator ρ acting on $\mathcal{H}_d$ which is Hermitian (self-adjoint; $\rho^\dagger = \rho$) and has trace one ($\mathrm{Tr}\rho \equiv \sum_{i=1}^{d} |\rho_{ii}|^2 = 1$). Any density matrix can be written as $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ for at least one choice of $\{|\psi_i\rangle\}$, and if the set $\{|\psi_i\rangle\}$ are orthonormal then the p_i will be nonnegative probabilities that sum to unity. If the system could be considered isolated then all p_i but one (say, $i = \alpha$) will be zero, $\mathrm{Tr}\rho^2$ will equal one, and we say the system is in a *pure state* $\rho = |\psi_\alpha\rangle\langle\psi_\alpha|$. Otherwise if more than one $p_i > 0$ we say the state is *mixed*, and $P = \mathrm{Tr}\rho^2$ is a measure of the degree of mixedness called the *purity*. For a qudit $\frac{1}{d} \leq P \leq 1$[3].

Although d linearly independent vectors suffice to span the space of *pure* states in $\mathcal{H}_d$, due to the greater complexity allowed by mixed states d^2 matrices are required to span the space of possible density operators. Note that these basis matrices need not necessarily be density operators themselves; for instance the basis $e_{jk} = |j\rangle\langle k|$ may suffice but for $j \neq k$ do not represent physical states. An orthonormal operator basis can be defined under the *Hilbert-Schmidt inner product* ([19],p.76), defined for matrices A and B as $(A, B) = \mathrm{Tr}(A^\dagger B)$.

The state space of a composite system consisting of subsystems $\{\mathcal{H}^j\}$, $j = \{0, 1, \ldots\}$, each with respective dimension d_j, is given by the tensor product $\bigotimes_j \mathcal{H}^j = \mathcal{H}^0 \otimes \mathcal{H}^1 \otimes \mathcal{H}^2 \otimes \ldots$, and will have dimension $\prod_j d_j$.

2.1.1.1 Qubits

The simplest type of quantum system, and the one with which we will be mostly concerned in this thesis, is two-dimensional i.e. has state space $\mathcal{H}_2$. This is often called a *two-level* system or a quantum bit or *qubit*. This is a direct quantum analogue of the (classical) bit (or cbit), the simplest unit of classical information, which is a binary system with states **0** and **1**. A qubit has two logical basis states,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.1}$$

However, unlike the cbit, a qubit can also occupy any superposition $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$ with $|c_0|^2 + |c_1|^2 = 1$. The set $\{|0\rangle, |1\rangle\}$ is called the logical or computational basis for $\mathcal{H}_2$.

[3] Alternately the purity is sometimes defined as $P = \frac{d+1}{d}\left[\mathrm{Tr}(\rho^2) - \frac{1}{d}\right]$ so that $0 \leq P \leq 1$.

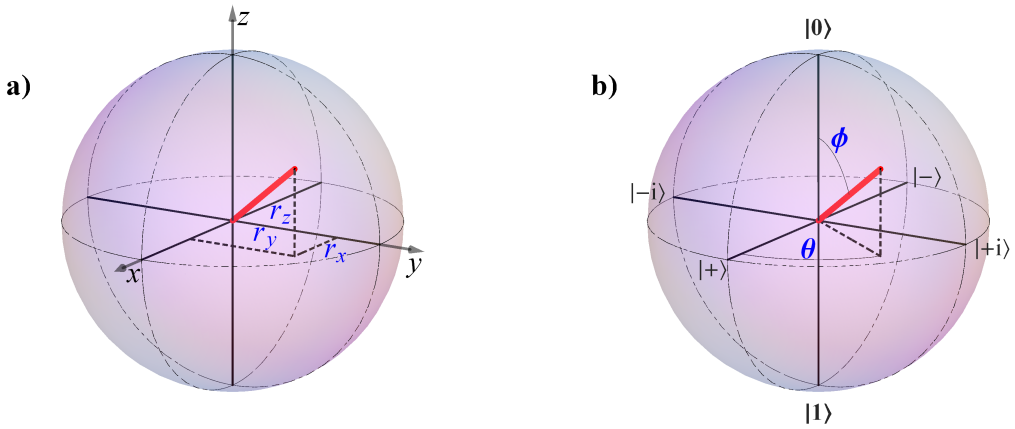


Figure 2.1: The Bloch sphere. a) shows a qubit state represented as a Bloch vector with Cartesian coordinates (r_x, r_y, r_z). b) shows the same qubit state represented as a Bloch vector with spherical polar coordinates ϕ and θ. In both cases $r = \sqrt{\sum_i r_i^2} = 1$, so the state shown is pure, but Bloch vectors with length $r < 1$ are also possible and represent mixed states.

A particularly useful operator basis for representing the state of a qubit in density matrix form consists of the three 2×2 *Pauli matrices* and the identity matrix:

$$\sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$
$$\sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \sigma_0 = \mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.2}$$

In this basis any arbitrary qubit state ρ can be written as[4]

$$\rho = \frac{\mathbb{1} + \vec{r} \cdot \vec{\sigma}}{2}, \tag{2.3}$$

where $\vec{\sigma} = (X, Y, Z)$, $|\vec{r}| \leq 1$, and $\vec{r}$ is a vector whose components (r_x, r_y, r_z) are respectively given by the Hilbert-Schmidt inner product of the state with the respective Pauli operator,

[4] This equation can be simplified to $\rho = \frac{1}{2}\vec{r'} \cdot \vec{\sigma'}$ where $\vec{\sigma'}$ is the ordered set *including* σ_0. However $\mathrm{Tr}(\sigma_0 \rho) = \frac{1}{2}$ for *any* valid quantum state and thus the 'r'_0-component' of a state is neither useful nor necessary for orienting the state e.g. in the Bloch sphere representation.

i.e. $r_i = \mathrm{Tr}(\sigma_i \rho)$. The $x-$, $y-$, and $z-$axes are often called the *Bloch axes* as they serve to orient the *Bloch sphere*, a useful representation of the state space of a qubit as a three-dimensional unit sphere, shown in Fig. 2.1. Points on the surface of the Bloch sphere represent possible pure qubit states, and points inside the sphere represent mixed states.

The points at ± 1 on the three orthogonal axes of the Bloch sphere represent eigenstates of the respective Pauli operators:

$$\begin{aligned}
&\text{The eigenstates of } X: \quad |\pm\rangle && \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) && \mapsto \frac{1}{2}(\sigma_0 \pm \sigma_1) \\
&\text{The eigenstates of } Y: \quad |\pm i\rangle && \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle) && \mapsto \frac{1}{2}(\sigma_0 \pm \sigma_2) \\
&\text{The eigenstates of } Z: \quad |0,1\rangle && && \mapsto \frac{1}{2}(\sigma_0 \pm \sigma_3)
\end{aligned} \tag{2.4}$$

Note that the last column represents the states in density operator form whereas the others are in state vector form. These three eigenbases of the Pauli operators are sometimes called the *standard* bases, and the six states themselves the *standard* states.

Alternately, an arbitrary qubit state can be written as

$$\rho(\phi, \theta, r) = r\,|\psi(\phi,\theta)\rangle\langle\psi(\phi,\theta)| + (1-r)(\mathbb{1}/2), \tag{2.5}$$

where

$$|\psi(\phi,\theta)\rangle = \cos(\phi/2)\,|0\rangle + e^{i\theta}\sin(\phi/2)\,|1\rangle\,. \tag{2.6}$$

Here $\phi \in [0, \pi)$ and $\theta \in [0, 2\pi)$ are the polar and azimuthal angles of ρ in the Bloch sphere representation, respectively, and $r = |\vec{r}| = \sqrt{2\left(\mathrm{Tr}\rho^2 - \frac{1}{2}\right)} \in [0,1]$ is the radius of the state's Bloch vector. Note the straightforward relation between the Bloch radius and the purity $P = \mathrm{Tr}\rho^2$. In the remainder of this thesis I may sometimes refer to a qubit's state vector, density operator, or Bloch vector as the *state* of the qubit; my meaning should be clear from the context.

Note finally that a qubit, like a (c)bit, is a unit of information, not a physical system, but in any experimental application must be *represented* by the state of a physical system, or (more likely) by a particular, defined subspace of states of a physical system. For instance, cbits are often represented in solid-state computer memory by a charge across a tiny capacitor, with some threshold separating the *high*-charge state **1** from the *low*-charge state **0**. Similarly, qubits can be represented by the charge (or flux or phase) in a superconducting Josephson junction circuit, the spins of electrons or nuclei, the ground and first excited energy levels of quantum dot, or the polarization of a single photon.

2.1.2 State Evolution

In quantum theory the evolution of any closed system must be described by a *unitary transformation*, represented by the action of a unitary operator. If the system is a qudit this operator can be represented by a $d \times d$ unitary matrix U; U is unitary if and only if $U^\dagger U = \mathbb{1}$. In quantum theory, an operator $\hat{O}$ acts on a state vector $|\psi\rangle$ as $\hat{O}|\psi\rangle$, and on other operators, including a density operator ρ, as $\hat{O}\rho\hat{O}^\dagger$. Unitary operators are trace-preserving and therefore purity-preserving, and also preserve inner products [19].

Some important unitary operators on qubits have already been encountered: the Pauli operators in Eq. 2.2, which each act on a qubit state by rotating it by π about the respective Bloch axis. In fact, all unitary transformations on a qubit correspond to geometric rotations of the state in the qubit sphere. Other important examples include rotations about the three Bloch axes by an *arbitrary* angle ξ:

$$X_{(\xi)} \equiv e^{-i\xi X/2}, \qquad Y_{(\xi)} \equiv e^{-i\xi Y/2}, \qquad Z_{(\xi)} \equiv e^{-i\xi Z/2}. \tag{2.7}$$

Any rotation in 3-space can be written in the Euler representation as a product of three rotations by arbitrary angles around two non-parallel axes, e.g. $U_{\text{rot}} = \hat{n}_{(\alpha)}\hat{m}_{(\beta)}\hat{n}_{(\gamma)}$. Thus, any unitary on a qubit can, for instance, be decomposed into three successive rotations about two different Bloch axes (see [19], pp.175-6.)

Another important unitary operation on qubits is the *Hadamard* operation H, which maps Z to X and vice-versa:

$$\begin{aligned} H &= \frac{1}{\sqrt{2}}(Z+X) & &= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ HZH &= X, & HXH &= Z, \\ H|0,1\rangle &= |\pm\rangle\,, & H|\pm\rangle &= |0,1\rangle\,. \end{aligned} \tag{2.8}$$

The most general evolution of a quantum system is not necessarily unitary, because the system may not be closed—it may interact with the environment. Analogously to the way density operators are needed to represent mixed states of non-isolated systems, more general quantum operations $\mathcal{E}$ are needed to describe the evolution of non-closed systems. There are several ways of representing general quantum operations, but all have roughly the same physical interpretation: A system S, which includes as subsystems both the system in question ρ and the (relevant part of) the environment, undergoes some combination of

unitary evolution and quantum measurement (discussed in sec. 2.1.3). This process can be represented by the action of some combination of unitary operators and measurement operators on S; when one neglects the environment and considers only ρ, the output will appear to be the result of a general quantum operation.

In this thesis there will be little need to resort to the formalism of general quantum operations, but they would be necessary, for instance, to *fully* describe the action of our optical POVM apparatus or our unitary correction apparatus on a single photon (see Chs. 3, 4, 5.)

2.1.3 Quantum Measurement

2.1.3.1 Projective Measurements

In addition to density operators and unitary operators, another important type of operator in quantum theory is the *projection operator*, or *projector*. A projector P acting on a qudit in $\mathcal{H}_d$ is used to find the *projection* of the qudit into an n-dimensional subspace W^n (where $n < d$.) In fact if $n = 1$ then P looks just like a pure state density operator $|\phi\rangle\langle\phi|$, where $|\phi\rangle$ is the state onto which one is projecting; if $1 < n \leq d$ then the projector is given by

$$P \equiv \sum_{j \in W^n} |\phi_j\rangle\langle\phi_j| \,, \tag{2.9}$$

where the entire set $\{|\phi_j\rangle\}$ forms a basis for $\mathcal{H}_d$. n is called the *rank* of the projector. The action of a projector P on a state ρ is to 'filter out' only that part of ρ which lives in W^n (i.e. those components of ρ parallel to some $|\phi\rangle \in W^n$). Projectors are *hermitian*, meaning $P^\dagger = P$, and also satisfy $P^2 = P$.

A projective measurement on a qudit is defined by an *observable* O, a hermitian operator acting on $\mathcal{H}_d$ which can be written as[5]:

$$O = \sum_m \lambda_m P_m, \tag{2.10}$$

where $\{P_m\}$ are orthogonal projectors ($P_{m'} P_m = \delta_{m,m'} P_m$) that sum to unity ($\sum_m P_m = \mathbb{1}$), and P_m projects onto the eigenspace of O with eigenvalue λ_m ([19], pp. 70 and 87-88).

[5] This is called a spectral decomposition.

When one performs a projective measurement on a system ρ, outcome m is obtained with probability $p(m) = \mathrm{Tr}(P_m\rho)$, and the state ρ' of the system after measurement is

$$\rho' = \frac{P_m \rho P_m}{p(m)}. \tag{2.11}$$

Clearly the number n of possible outcomes of a projective measurement on a qudit must be at most as large as the dimension d of the system being measured, or else the corresponding projectors could not all be orthogonal. The special case where $n = d$, or equivalently each P_m is a rank-one projector $P_m = |\phi_m\rangle\langle\phi_m|$ for some orthonormal basis $\{|\phi_m\rangle\}$, is often called a Von Neumann measurement, a *complete* projective measurement, or to be specific a 'measurement in the basis $\{|\phi_m\rangle\}$'. The simplest example is a measurement in the computational basis $\{|k\rangle\}$, $k = \{0, 1, \ldots, d-1\}$. Note finally that any complete projective measurement on a qudit specified by observable $\Omega = \sum_j \lambda_j |\lambda_j\rangle\langle\lambda_j|$ can be implemented as a unitary U on the system, followed by a projective measurement in the computational basis, where $U_{jk} = \langle\lambda_j| k\rangle$[6]. For instance a measurement of X on a qubit can be accomplished by a Hadamard operation before a computational-basis measurement (see (2.8).)

Projective measurements have the nice property that it is straightforward to calculate their *average value*, also called *expectation value*, which is the expected average of the outcome over many measurements on the same state. The average value $\langle O\rangle$ of an observable O for a state ρ, given by $\sum_m \lambda_m p(m)$, simplifies to $\mathrm{Tr}(O\rho)$.

To measure an average value $\langle O\rangle$ in the lab, it is sufficient to repeat the projective measurement on a large number n of identically prepared systems, recording the outcome $m_i, i \in \{1, \ldots, n\}$, and then take the mean $(\sum_i \lambda_{m_i})/n$. However it is often the case (in particular when working with photons) that a measurement apparatus only records a single outcome, while the others are discarded. In this case, it is often more convenient to calculate the average value of the observable from the average values of the projectors. The average value of a projector P_m for a state ρ is just the probability $p(m)$ that ρ is found in the subspace W_m associated with P_m. Each $p(m) = \mathrm{Tr}(P_m\rho)$ can usually be calculated from easily-measurable quantities such as a count rate, given by the number ν of identically-prepared systems in state ρ that are projected into W_m in some time interval, divided by the interval, and a normalization rate, given by the total rate at which systems

[6] Alternately, the columns of $U^\dagger$ are the eigenvectors of Ω. All of this is a consequence of the spectral theorem.

are generated. The average value of the observable is then given by the weighted average of the average values of the projectors: $\langle O \rangle = \sum_m \lambda_m \langle P_m \rangle = \sum_m \lambda_m p(m)$. Because ν is finite and due to the Poissonian distribution of counting statistics, which is well-approximated as Gaussian for large numbers, ν will have an error of approximately $\sqrt{\nu}$. The counts used to determine the normalization rate will likely also have approximately square-root errors, and the total error in the average values of projectors or observables can then be obtained via standard error propagation techniques.

In addition to being unitary operators and forming a Hilbert-Schmidt-orthogonal operator basis for qubits, the Pauli matrices $\{\sigma_j\}$ are all also important qubit observables, especially in the context of quantum state tomography (section 2.1.5). A measurement of Z is a measurement in the computational basis of a qubit.

2.1.3.2 Fidelity of states

In quantum information it is often desirable to quantify the 'closeness' of two quantum states ρ_1 and ρ_2. One oft-used measure is the *fidelity*, which, if at least one of the two states is pure e.g. $\rho_1 = |\phi\rangle\langle\phi|$, is given by

$$F(|\phi\rangle\langle\phi|, \rho_2) = \langle\phi| \rho |\phi\rangle . \tag{2.12}$$

This has a nice interpretation: it is equivalent to $F(P, \rho_2) = \mathrm{Tr}(P\rho_2)$ where P is the projector $|\phi\rangle\langle\phi|$, and this is just the probability that ρ_2 will be projected onto $|\phi\rangle$. Like any probability, F varies between 0, meaning ρ_2 is orthogonal to ρ_1, and 1 meaning $\rho_2 = P = \rho_1$. For two pure qubit states in the Bloch sphere representation, the fidelity can be calculated via a convenient geometrical relation: if the states are separated by a central angle ζ, then

$$F = \cos^2\left(\frac{\zeta}{2}\right). \tag{2.13}$$

A generalization of the fidelity to mixed states should:

- reduce to Eq: 2.12 if one of the states is pure,
- yield $F = 1$ if $\rho_1 = \rho_2$, and
- yield $F = 0$ if ρ_1 is orthogonal to ρ_2.

The function which accomplishes this is given by [20]:

$$F(\sigma,\tau) = \left[\mathrm{Tr}\left(\sqrt{\sqrt{\sigma}\,\tau\sqrt{\sigma}}\right)\right]^2. \tag{2.14}$$

Unfortunately, this definition of the fidelity does not have a physical interpretation which this author finds to be as intuitive or enlightening when both states are mixed as when at least one is pure.

2.1.3.3 Generalized Measurements and POVMs

Many physicists may only be familiar with pure states, unitary evolution processes, and projective measurements. Indeed, if one includes a sufficient part of the 'environment' in one's definition of the 'system', then all of quantum theory can in principle be reduced to pure states, unitary evolution, and projective measurements. However the formalisms of mixed states and general quantum processes serve both to greatly simplify some calculations and to provide a mathematical representation which may bring different physical features to light, in some cases enabling different insights. The formalism of generalized measurements or POVMs can serve the same purposes with respect to quantum measurement theory.

A general quantum measurement on a qudit can be represented by any set of operators $\{M_m\}$ acting on $\mathcal{H}_d$ such that $\sum_m M_m^\dagger M_m = \mathbb{1}$. In particular, $\{M_m\}$ need not be projectors, nor need they be orthogonal, and the number n of possible measurement outcomes may be greater than d. After a measurement $\{M_m\}$ is performed on a system in state ρ yielding outcome m, the resulting state will be

$$\rho' = \frac{M_m \rho M_{m'}}{p(m)}, \tag{2.15}$$

where $p(m) = \mathrm{Tr}(M_m^\dagger M_m \rho)$ is the probability that outcome m is obtained. We can define $M_m^\dagger M_m = E_m$, and $\{E_m\}$ will then be a set of positive operators such that $\sum_m E_m = \mathbb{1}$ and $p(m) = \mathrm{Tr}(E_m\rho)$. $\{E_m\}$ is sometimes called a POVM for *Positive Operator-Valued Measure*, and in fact, though it properly applies only to $\{E_m\}$ according to Ref. [19], p.90, the term *POVM* is sometimes also used to refer to the generalized measurement $\{M_m\}$ as well. The operators E_m are called the *elements* of the POVM.

Unlike projective measurements, where the number of possible outcomes is upper-bounded by the dimension d of the Hilbert space $\mathcal{H}_d$ of the measured system, the number

n of operators in a POVM $\{E_m\}$ may be greater than d. However, any n-outcome POVM can be implemented by performing a projective measurement on some $\mathcal{H}_n$, of which $\mathcal{H}_d$ is a subspace. This is sometimes called Neumark's or Naimark's theorem, and in practice it means that any POVM on a physical system S with associated Hilbert space $\mathcal{H}_d^S$ can be implemented by coupling the system to some ancillary system A (which may itself be a composite system), and performing a projective measurement in the combined Hilbert space $\mathcal{H}_d^S \otimes \mathcal{H}^A$ (see [21], pp. 283-289).

2.1.4 Quantum Correlations and Entanglement

Valid quantum states in a composite Hilbert space $\bigotimes_i \mathcal{H}^i$ can be simple tensor products of states in the subsystems $\bigotimes_i |\psi\rangle_i$, where $|\psi\rangle_i \in \mathcal{H}_i$. For instance, for a composite system of two qubits $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$, such product states include $|0\rangle^A \otimes |0\rangle^B$, $|0\rangle^A \otimes |1\rangle^B$, $|1\rangle^A \otimes |0\rangle^B$, $|1\rangle^A \otimes |1\rangle^B$, or any $|\phi\rangle^A \otimes |\chi\rangle^B$. We often omit the tensor product, the labels, and even the separate kets, writing e.g. $|00\rangle$, understood to mean $|0\rangle^A \otimes |0\rangle^B$. Such a state is called separable, and a mixed state is said to be separable if it can be written as a convex sum of separable states: $\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B$ where $\{p_i\}$ are nonnegative and sum to one.

However, due to the superposition principle (p. 4) any normalized sum of valid states is *also* a valid state, including those that cannot be written as a product state. Important examples include the *Bell states*, named after J.S. Bell's seminal work on entanglement and its consequences [3]:

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{2}(|00\rangle \pm |11\rangle) \qquad \left|\Psi^{\pm}\right\rangle = \frac{1}{2}(|01\rangle \pm |10\rangle). \tag{2.16}$$

The Bell states form an often-convenient orthonormal basis for $\mathcal{H}_2 \otimes \mathcal{H}_2$, hereafter called the *Bell basis*. Another example of an entangled state is the so-called n-*GZH* states [22], $|GHZ\rangle_n = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$.

These states have several interesting and (some might say) counter-intuitive properties which have incited much research and debate in the history of quantum theory, its interpretation or foundations, and quantum information. Consider performing a measurement in the computational basis (a measurement of Z) on one qubit (say A) from a Bell state, without measuring qubit B: both outcomes are equally probable. In fact, if particle B is discarded or ignored, the outcomes will be equiprobable for *any* binary observable on A: in other words, qubit A appears to be maximally-mixed. However, consider measuring *both* qubits in the computational basis: although the specific outcome of the measurement on

the first qubit is completely random, it completely determines the outcome of the measurement on the second qubit. For the $|\Phi\rangle$ states the outcomes will be perfectly correlated; for the $|\Psi\rangle$ states they will be anticorrelated. Einstein, Podolsky, and Rosen famously noted these correlations in 1935 and used them to argue against the completeness of quantum theory [2].

Remarkably, these correlations persist regardless of the measurement basis. For instance the 'singlet' state $|\Psi^-\rangle$ can be written as $\frac{1}{\sqrt{2}}(|\psi\rangle\,|\psi_\perp\rangle - |\psi_\perp\rangle\,|\psi\rangle)$ for *any* orthonormal basis $\{|\psi\rangle, |\psi_\perp\rangle\}$. Thus the measurement outcomes in such a basis will always be perfectly anticorrelated, and the outcomes of measuring A and B respectively in two different bases will be imperfectly correlated in a straightforward way[7]. Furthermore, the correlations persist even if qubits A and B are spacelike-separated at the time of measurement so that neither measurement can properly be said to have occurred 'first.' Bell's famous theorem shows that these correlations are stronger than would be possible for classical systems, which always inhabit defined states rather than superpositions [3], and experimental tests confirm that the correlations observed for some systems in nature obey the predictions of quantum theory, rather than conforming to classically intuitive notions [23, 24, 25, 26].

Viewed as a resource, entanglement enables many of the most famous and useful experiments and applications in quantum information and quantum computing, including Bell inequality violations, quantum teleportation (see Sec. 2.1.6,) quantum key distribution [27, 6, 28, 29, 30, 31, 32, 33], and the experiments in this thesis concerning cluster-state quantum computation and remote quantum state preparation.

2.1.4.1 Quantifying Entanglement

The Bell and GHZ states are said to be maximally-entangled because, when measured in the same bases, the subsystems exhibit perfect correlations. Equivalently, if the other subsystems are ignored or discarded, any one subsystem appears maximally-mixed. Various measures have been developed to quantify the amount of entanglement present in a state of a composite system (see [34] for a detailed review).

The amount of entanglement in one maximally-entangled qubit pair (e.g. a Bell state) is commonly called an ebit. One way to quantify the entanglement in a system is through its

[7] In particular if observable $\vec{r_A}\cdot\vec{\sigma}$ is measured on qubit A and $\vec{r_B}\cdot\vec{\sigma}$ is measured on qubit B, where $\vec{r_{A(B)}}$ are two different pure-state Bloch vectors, then the expectation value of the product of the two observables $\langle\vec{r_A}\cdot\vec{\sigma}\otimes\vec{r_B}\cdot\vec{\sigma}\rangle$ is given by $-\vec{r_A}\cdot\vec{r_B}$ [3].

fidelity with some target state, e.g. for a two-qubit system with one of the Bell states. Other more general measures of the entanglement in a two-qubit system are the *concurrence* and *tangle*, both of which are related to the *entanglement of formation* $E_F(\rho)$, which is perhaps the canonical measure of pure state entanglement and represents the minimum number of ebits required to construct ρ through local operations ([35], p.29). The concurrence is given by $C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$, where the λ_i are the eigenvalues, in decreasing order, of the matrix $R \equiv \sqrt{\sqrt{\rho}\rho_{sf}\sqrt{\rho}}$, and ρ_{sf} is the 'spin-flipped' density operator given by $(Y \otimes Y)\rho^*(Y \otimes Y)$. The tangle $T(\rho) \equiv C^2(\rho)$. Both measures range from 0 for unentangled states to 1 for maximally entangled qubit pairs, and are easier to compute than other measures such as the entanglement of formation or entropy of entanglement. The tangle is used to quantify entanglement in this thesis.

2.1.5 Quantum State Tomography

In quantum theory no single measurement can completely determine the state ρ of a quantum system. This is because, after an observable is measured on a system, the subsequent state of that system will be an eigenstate of that observable, nullifying the chance to obtain information about the original state with respect to other observables. However, it is possible to estimate ρ for a large number of *identically- prepared* systems via a finite number of measurements of different observables. This task is called *quantum state tomography* and is a valuable tool for assessing the outcomes of experiments and the success of quantum information, computation, and communication protocols.

Recall from equation 2.3 that the state ρ of a single qubit can be expanded in terms of the Pauli matrices as $\frac{\mathbb{1}}{2} + \frac{1}{2}\sum_j \mathrm{Tr}(\sigma_j\rho)\sigma_j$. Any set of d^2 linearly independent operators acting on $\mathcal{H}_d$ is said to be *tomographically complete*; the Pauli matrices for a qubit have the added benefit of being orthogonal under the Hilbert-Schmidt inner product. Recall that $\mathrm{Tr}(\sigma_j\rho)$ is the average value of an *observable*, and as such can be measured in the lab as described on p. 10. Measuring the average value of each σ_j amounts to determining the three (Cartesian) coordinates of the state's Bloch vector, which uniquely determine the state.

One need not even measure all six projectors corresponding to the six standard states (the eigenstates of $\{\sigma_j\}$;) projections onto one eigenstate of each σ_j are sufficient to determine ρ (the $2^2 = 4$ parameters of a qubit are constrained by normalization so that there are really only three *free* parameters.) However in practice the normalization rate usually

need also be determined, which necessitates a fourth projection; a standard tomographic set is then to measure the average values of the projectors $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |+i\rangle\langle +i|\}$. However in practice a more accurate reconstruction can be obtained by measuring the projections onto all six standard states [35]. Such a set is an example of an *overcomplete* tomographic set, so-called because they contain more than the 2^d projectors required to span the qudit Hilbert space. Overcomplete tomography using all six standard projectors is used throughout this thesis.

The state of a composite system of n qubits can be tomographically reconstructed using measurements of observables which are tensor products of Pauli operators, e.g. $\bigotimes_{i=1}^{n} \sigma_j^i, j \in \{x, y, z\}$. James *et. al.* showed that measurements of 4^n projections are sufficient [36]. However, again overcomplete tomography with 6^n projections leads to more accurate reconstructions and is used herein. Furthermore they found a solution to the problem that, due to measurement noise (e.g., in the case of counting photons, the aforementioned Poissonian fluctuations) sometimes the density matrix ρ_r reconstructed via standard techniques (linear tomography) is not *physical* in that it may have negative eigenvalues. The details of their solution will not be addressed here but the basic idea involves parameterizing the distance of ρ_r from physically valid density matrices, and then finding the nearest physically valid ρ, the one most likely to have produced the obtained measurement results. This technique is called *maximum-likelihood tomography* and is used throughout this thesis.

2.1.5.1 Error Determination and Monte Carlo Methods

Calculating the error in a tomographically-reconstructed density operator (or in quantities one might wish to calculate from that operator i.e. fidelity, purity, and tangle) is laborious using standard error-propagation techniques, and difficult or impossible when using non-linear reconstruction methods such as maximum-likelihood tomography. Another method to obtain error estimates for such quantities is via performing stochastic numerical simulations of the errors. This is often called the *Monte Carlo method* and can be summarized as follows:

1. From the data set $\mathcal{N} = \{n_i\}$ obtained when measuring each projection used in the tomographic reconstruction, generate a large number of random sample data sets $\{\mathcal{N}^S\}$ using appropriate estimates of the probability distribution for the data. For instance for the aforementioned case of counting photons, the individual n_i will be

counts recorded in some time interval, and *assuming that the primary source of error is Poissonian counting fluctuations*, one can generate the corresponding set of sample counts $\{n^s\}_i$ by selecting at random from a Poissonian distribution with standard deviation $\sigma_i = \sqrt{n_i}$.

2. For each sample data set $\mathcal{N}_j^S$ perform the numerical tomography and generate a density matrix ρ_j^S.

3. The uncertainty in any desired quantity determined from the (original) reconstructed density matrix ρ_r, such as the purity or tangle or fidelity with some target state ρ^{tar}, is then given by the standard deviation of the same quantity, calculated for each ρ_j^S. For instance the estimate of the error in the purity of the reconstructed density matrix, $\Delta P(\rho_r)$, will be the standard deviation $\sigma(\{P(\rho^S)\})$.

The utility of the Monte Carlo method requires the validity of several assumptions. First the statistical data fluctuations must be the dominant source of error in the reconstructed density matrix, as opposed to systematic errors. e.g. in the measurement settings, or problems with the tomographic reconstruction process. Furthermore the number k of sample data sets $\mathcal{N}^S$ must be sufficient for the sample standard deviation to be a good estimate of the population standard deviation. This in turn may require significant computing power and/or time, dependent on the mathematical details of the tomographic reconstruction method used.

While these assumptions are important and deserve careful consideration, they have been investigated thoroughly in e.g. [35] where it has been shown that for tomography of photonic qubits using measurement methods very similar to those employed herein, and based on $k = 200$ simulations (which is the number we used to provide error estimates on the two-photon density matrices in Figs. 4.3 and 5.5), Monte Carlo methods yield quite good error estimates.

There are also several occasions in this thesis where I estimate the error in (single-qubit) tomographic reconstructions of our experimental output without the aid of Monte Carlo techniques. Particularly in Ch. 5, where I wish to estimate the error in the averege fidelity with which we can prepare ensembles of qubit states, each specified by a set $\{r, \phi, \theta\}$ of the radius and polar and azimuthal angles of the desired output state in the Bloch sphere. In this case I do so by taking the standard error of the mean of the fidelities for each of

the states in the ensemble[8]. Ideally, this number yields a range within which the average fidelity for the ensemble would be likely to fall if tomographic reconstructions of all the states in the ensemble were performed again, with the experimental apparatus identically aligned.

However, in order for this to be the case, one must assume that the fidelities are drawn from the same distribution, regardless of the settings $\{r, \phi, \theta\}$ of each particular state. This assumption would be completely valid if and only if the error in the fidelity value for every state was determined entirely by Poissonian counting statistics, and not by systematic errors which could vary in their effects depending on r, ϕ and θ. This assumption is undoubtably untrue, due both to the vagaries of the imperfect 2-photon entangled states (see for instance Figs. 4.4 and 4.3), and due to the functioning of our apparatus for performing POVMS, especially vis-a-vis fluctuations in the ambient laboratory temperature (see sec. 3.5.1). However, for the source used for the experiments in Chs. 4 and 5, and for data taken during a sufficiently short time period when the lab temperature was not fluctuating too much, the systematic errors due to these factors should be small compared to the error due to Poissonian counting fluctuations. In fact, Monte Carlo simulations based on the counts for tomography of just one output qubit state, when compared with the expected variance in output states accross the Bloch sphere due to the imperfect tomographically-reconstructed 2-photon entangled state, suggest that error in the output fidelity due to the former is approximately 2 or 3 times as large as the variation over the space of all possible settings $\{r, \phi, \theta\}$ expected due to the latter. In this case, the standard error in the mean will yield a reasonable estimate of the expected variance in potential future measurements of the average output fidelity for ensembles of states at different locations on the Bloch sphere, if anything yielding a slight overestimate.

2.1.6 Teleportation

As an example of a useful quantum information protocol illustrating or utilizing many of the concepts presented in previous sections, I will briefly describe the *quantum teleportation* of a qubit state. This protocol will be contrasted with that for remote state preparation in chapter 5. My treatment of teleportation largely follows Ref. [37], pp. 80-81.

Imagine two separated parties Alice and Bob share an entangled state $|\Phi^+\rangle$, i.e. they

[8]The standard error of the mean of a quantity F over an ensemble s is given by the sample standard deviation divided by the square root of sample size, or $\sigma_F/\sqrt{n_s}$.

each have one qubit from the state, and that Alice also has a qubit in state $|\psi\rangle$ which she would like to transmit to Bob. Using only classical communication, this would normally require a double-infinity of cbits to fully specify the real numbers θ and ϕ (see Eq. 2.5); however by exploiting the shared entangled state Alice can accomplish this task by communicating only two cbits!

The protocol can be explained as follows: the initial state of the three qubits is $|\psi\rangle|\Phi^+\rangle$. However, the state of the two qubits in Alice's possession can be rewritten in the Bell basis:

$$|\psi\rangle\left|\phi^+\right\rangle = \frac{1}{2}\left[\left|\Phi^+\right\rangle|\psi\rangle + \left|\Psi^+\right\rangle(X|\psi\rangle) + \left|\Phi^-\right\rangle(Z|\psi\rangle) + \left|\Psi^-\right\rangle(XZ|\psi\rangle)\right]. \tag{2.17}$$

Alice measures her two qubits in the Bell basis and transmit the result to Bob, encoded in two cbits as follows:

$$\left|\Phi^+\right\rangle \mapsto \mathbf{00} \qquad \left|\Psi^+\right\rangle \mapsto \mathbf{01} \tag{2.18}$$

$$\left|\Phi^-\right\rangle \mapsto \mathbf{10} \qquad \left|\Psi^-\right\rangle \mapsto \mathbf{11} \tag{2.19}$$

To complete the protocol, Bob performs Z on his qubit if the first cbit of his received message is $\mathbf{1}$ and X on his qubit if the second cbit is $\mathbf{1}$ (otherwise performing the identity $\mathbb{1}$.) Bob's resulting output state will be $|\psi\rangle$.

The teleportation protocol is shown in the form of a *quantum circuit diagram* in Fig. 2.2. Note that Alice's measurement of her two qubits in the Bell basis, or *Bell state measurement* (BSM) is shown as a unitary—specifically a c-NOT operation (see section 2.2.1) and a Hadamard—followed by a measurement in the computational basis. However this is not the only possible means of performing a BSM, and the teleportation protocol succeeds regardless of the method used.

2.2 Quantum Computing

Quantum computers promise great speedups in solving certain classes of problems and in simulating physical systems [19]. The most common model of quantum computation is the quantum circuit or network model $\mathrm{QC}_{\mathcal{N}}$, which is an analogue of the circuit model of classical computation based on boolean operators such as NOT, AND and NAND. In $\mathrm{QC}_{\mathcal{N}}$, quantum bits (qubits) are prepared in some initial state, usually some fiduciary

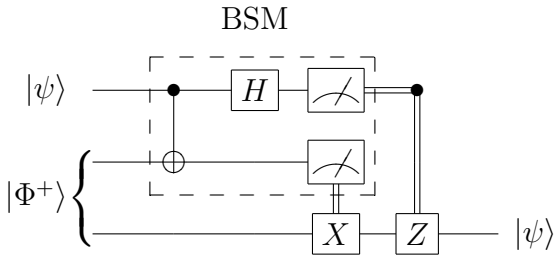


Figure 2.2: Teleportation circuit. The top two rails represent Alice's qubits whereas the bottom represents Bob's. Alice possesses a qubit in the (possibly unknown) state $|\psi\rangle$ as well as one qubit from a $|\Phi^+\rangle$ Bell pair; Bob has the other. Alice measures the combined state of her two qubits in the Bell basis (Bell State Measurement, BSM) and encodes the measurement result in two cbits sent to Bob. The cbits control which Pauli operation(s) Bob performs on his qubit, which will then be left in state $|\psi\rangle$.

state such as $|0\rangle^{\otimes n}$, and then propagated through a succession of *gates*, which represent unitary operators acting on one, two, or more qubits. The final state of the qubits after these operations constitutes the output of the quantum computation.

The cluster state model of quantum computation $\mathrm{QC}_{\mathcal{C}}$ is a different model for how a quantum computation would proceed. In $\mathrm{QC}_{\mathcal{C}}$, a specific entangled, ordered and (usually) large state of several qubits, called a *cluster state*, is first prepared, and then the processing of the quantum information occurs via a series of successive single-qubit projective measurements on the qubits in the cluster. Classical feed-forward must sometimes be used to choose the bases for measurements, based on the outcomes of previous measurements in the computation.

The initial cluster can be prepared via various procedures, some of which it is convenient to describe via quantum gates, but once it has been prepared, no quantum gates are necessary in order to enact the computation. This may prove to be a great advantage for some potential physical implementations of quantum computing, where one- and (in particular) two-qubit gates have proven difficult to realize. In particular, for photonic quantum computing as considered in this thesis, two-qubit gates are quite difficult to implement in practice, and thus cluster computation presents itself as an attractive option.

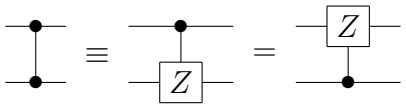
$\mathrm{QC}_{\mathcal{C}}$ can be used to fully efficiently simulate $\mathrm{QC}_{\mathcal{N}}$: they are computationally equivalent.

This section 2.2 is structured as follows: I first briefly review the $\mathrm{QC}_{\mathcal{N}}$ model, including common notation, several important gates, and results concerning sufficient operations for *universal* quantum computing, meaning the ability to implement arbitrary quantum computations. I then more thoroughly introduce $\mathrm{QC}_{\mathcal{C}}$: I define a cluster state, describe how one might be created, and outline how a cluster state quantum computation proceeds. The chapter ends with an outline of a proof that $\mathrm{QC}_{\mathcal{C}}$ is universal, in that cluster-state quantum computations can efficiently simulate a universal set of gate operations from $\mathrm{QC}_{\mathcal{N}}$.

2.2.1 Circuit Quantum Computing: A Brief Review

The diagram shown for quantum teleportation, Fig. 2.2, represents a quantum circuit, which processes quantum information in $\mathrm{QC}_{\mathcal{N}}$: In this diagram the horizontal lines are called *quantum wires*, and each represents the progression through time of a qubit. Boxes on quantum wires represent single-qubit gates, which act on the qubit with the unitary operation denoted by the content of the box. Vertical lines with boxes or other markers at the endpoints (on quantum wires) represent two-qubit gates, unitary operations involving the qubits on those quantum wires. Meters represent measurements, usually taken to be Von Neumann measurements in the computational basis. Double-lines represent classical information (in this case the outcome of the computational basis measurements).

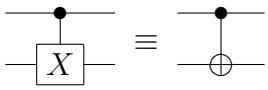
The processing of quantum information in $\mathrm{QC}_{\mathcal{N}}$ proceeds by enacting the operations represented by the gates in the circuit diagram, in left-to-right order, on some input state of qubits. Several operations represented by important single qubit gates have already been encountered (see e.g. Eqs. (2.7,2.8)). The following represents an important two-qubit gate, the controlled-Z or controlled-PHASE or CZ gate.



$$\equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \tag{2.20}$$

Here the small bullet indicates that the bulleted qubit *controls* the action of the connected gate: the connected operation occurs if the control is in state $|1\rangle$, but not if the control is in state $|0\rangle$. The action of the CZ gate is such that it can equivalently be described as a

Z operation on the second qubit, controlled by the first, or as a Z on the first, controlled by the second. Another important two-qubit gate is the controlled-X (c-NOT or CX).



$$\equiv \quad \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.21}$$

Either of these is said to be an *entangling gate* because for some input state $|\psi\rangle\,|\chi\rangle$, the output will be maximally entangled. As an example, if the input state to the c-NOT is $|+0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$, meaning the control qubit is in $|+\rangle$ and the target qubit in $|0\rangle$, the output will be $\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,X\,|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the $|\Phi^+\rangle$ Bell state. Note also that, just as the X and Z gates are related by the Hadamard operation by Eq. (2.8), the CX and CZ gates are related by a Hadamard on the target qubit:

$$\begin{aligned} (\mathbb{1} \otimes H) \times CX \times (\mathbb{1} \otimes H) &= CZ, \text{ and} \\ (\mathbb{1} \otimes H) \times CZ \times (\mathbb{1} \otimes H) &= CX. \end{aligned} \tag{2.22}$$

An important result which will not be proven here concerns *universal gate sets*: it can be proven that from a subset of one- and two-qubit gates, all possible unitary quantum operations on any finite number of qubits can be constructed. In other words, such a set is *universal* for arbitrary quantum computations. In particular, the set of all single-qubit unitary operations along with any one entangling two-qubit gate (such as the CZ) constitutes a universal set ([37], Theorem 4.3.3, p.69). In section 2.2.2 we will outline a proof that $\mathrm{QC}_{\mathcal{C}}$ can efficiently simulate arbitrary single-qubit unitaries as well as the CZ gate, thus effectively showing $\mathrm{QC}_{\mathcal{C}}$ to be capable of effecting arbitrary quantum computations.

2.2.2 The Cluster-State Model of Quantum Computation

The idea of cluster state quantum computing is due to R. Raussendorf, H. J. Briegel, and collaborators [9, 8, 10]. $\mathrm{QC}_{\mathcal{C}}$ has also been called "one-way quantum computing" because the computation proceeds via irreversible 'one-way' projective measurements, in contrast to $\mathrm{QC}_{\mathcal{N}}$ wherein all the processing of quantum information is done via unitary operations which are necessarily reversible.

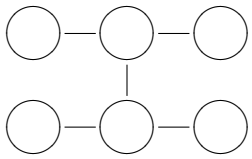


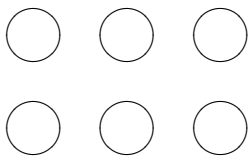
Figure 2.3: Example cluster state. A cluster state is an entangled state defined by a graph with qubits at the vertices and edges representing an entangling operation.

Cluster states can be defined mathematically via eigenvalue equations, and those definitions will be given in section 2.2.2.2. However, the author has not found such a means of definition to be particularly enlightening. In this section we attempt to give a useful intuition for what a cluster state is via enumerating a particularly simple procedure for creating one.

2.2.2.1 Preparation Procedure

Fig. 2.3 represents a cluster state and will be useful for explaining many of their salient features. Each open circle represents a qubit. Technically, these qubits can be at the vertices of any graph[9]. The edges in the graph then represent entanglement of a specific type which will be explained shortly. A 'cluster state' originally referred to the case where the graph in question was a a regular two- or three-dimensional lattice, usually with a boundary, and the term 'graph state' was used to refer to the case wherein the qubits are arranged on some more general graph, but this usage has blurred over time and it is now common to refer to all graph states as cluster states.

An n-qubit cluster state can be created via the following procedure: One begins with a collection of n qubits, perhaps but not necessarily in some fiduciary state such as $|0\rangle^{\otimes n}$, represented pictorially (for n=6) as follows:



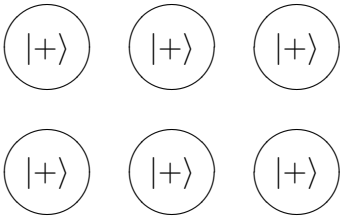
(2.23)

[9]In the usual mathematical definition of an ordered set of vertices and edges

One then prepares all the qubits in the state $|+\rangle$; this can be done, for instance, by applying the Hadamard operation to all qubits in $|0\rangle^{\otimes n}$. Mathematically we have:

$$|+\rangle_{\mathcal{C}} = |+\rangle^{\otimes n} = H^{\otimes n} |0\rangle^{\otimes n} = \bigotimes_{a \in \mathcal{C}} |+\rangle_a \,, \tag{2.24}$$

where n qubits constitute the cluster $\mathcal{C}$. Pictorially this results in the following:



(2.25)

The final step in creating the cluster state is to perform a CZ operation between each pair of qubits connected by an edge on the underlying graph. This is equivalent to acting with the following operator

$$S^{(\mathcal{C})} = \prod_{b \in N(a)} S^{ab}, \tag{2.26}$$

where

$$S^{ab} = |0\rangle^a \langle 0| \otimes \mathbb{1}^b + |1\rangle^a \langle 1| \otimes Z^b, \tag{2.27}$$

and $b \in N(a)$ if and only if a, b are connected by an edge of the underlying graph defining $\mathcal{C}$. This operator defines the CZ operations; it is notable that all the individual CZ operations between pairs of neighboring qubits commute, so these operations can be done in any temporal order, or all at once. Then the final cluster state is:

$$|\psi\rangle_{\mathcal{C}} = S^{(\mathcal{C})} |+\rangle_{\mathcal{C}} \tag{2.28}$$

Pictorially, we represent the final cluster state as in Fig. 2.3.

2.2.2.2 Eigenvalue Equations

The preparation procedure outlined previously leads to a final state which satisfies the eigenvalue equation:

$$K_a |\psi\rangle_{\mathcal{C}} = \pm |\psi\rangle_{\mathcal{C}} \,, \quad \forall \ a \in \mathcal{C}, \tag{2.29}$$

where K_a is an operator that is a product of Pauli matrices on the qubit a and its neighbors, defined as

$$K_a = X_a \bigotimes_{b \in N(a)} Z_b. \tag{2.30}$$

Any state satisfying this eigenvalue equation will be a cluster state useful for $\mathrm{QC}_{\mathcal{C}}$[10]. Such a state could result from the preparation procedure defined in section 2.2.2.1, or from other preparation procedures. The salient point is that, once created, such a cluster state will be universal for quantum computation.

2.2.3 Computation Procedure

Once the cluster is prepared $\mathrm{QC}_{\mathcal{C}}$ proceeds by performing projective measurements on the qubits in the cluster in appropriate bases. Classical feed-forward based on measurement results, including classical logical processing of the outcomes, [10] may be used to choose the bases for subsequent measurements.

Note that any cluster $\mathcal{C}$ can be subdivided into input qubits $\mathcal{C}_I$ (taken to be the leftmost qubits in a pictorial representation such as Fig. 2.3), output qubits $\mathcal{C}_O$ (taken to be the rightmost qubits) which, after the cluster computation is complete, will encode the output state of the processed computational qubits, and body qubits $\mathcal{C}_B$, taken to be all the qubits not in the other two sets. It is often convenient to take the input qubits to be in some arbitrary state $|\psi_{\mathrm{in}}\rangle$ (instead of $\bigotimes_{a \in \mathcal{C}_I} |+\rangle_a$) before the entangling operation $S^{(\mathcal{C})}$. We can make this generalization without loss of generality, because the qubits in $\mathcal{C}_I$ could be the output qubits $\mathcal{C}_O$ of a previous step in the computation, such as a preprocessing cluster which could prepare the state $|\psi_{\mathrm{in}}\rangle$ solely via measurement.

Different measurement bases serve different purposes in $\mathrm{QC}_{\mathcal{C}}$:

- Measurements in the computational basis do not effect the overall computation and can be used to remove qubits from the cluster, leaving (up to an unimportant global phase) an identical cluster with the qubit in question removed.
- Measurements in $|\pm\rangle$ are used to propagate or teleport computational qubits along the physical qubits in the cluster.

[10] Obviously, any classical processing must be polynomial in required resources in order for the overall cluster computation to be efficient.

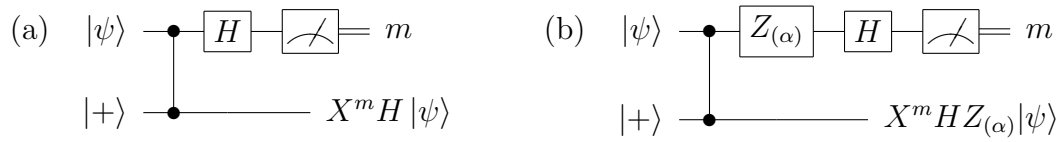


Figure 2.4: One-bit teleportation. a) This circuit shows how an arbitrary input state $|\psi\rangle$ can be transferred between two qubits, up to known single-qubit unitaries, using a single CZ gate and measurement. b) This extension of the previous circuit shows how some unitaries (specifically rotations about the z-axis) can also be 'teleported' to the second qubit, even if the unitary acts on the first qubit *after* their initial CZ interaction. This circuit identity underlies $\mathrm{QC}_{\mathcal{C}}$.

- Measurements in the following bases are used to perform rotations on computational qubits, as will be explained in the following section:

$$|\alpha_{\pm}\rangle = Z_{(\alpha)} H |0,1\rangle = \frac{|0\rangle \pm e^{i\alpha}|1\rangle}{\sqrt{2}} \tag{2.31}$$

2.2.3.1 One-Bit Teleportation and Arbitrary Rotations

My explanation of how measurements in these bases effect their purposes, and our subsequent demonstration of the universality of $\mathrm{QC}_{\mathcal{C}}$, owes much to the exposition of Michael Nielsen [38], although I have added some details and simplified in some instances. First, note the straightforward identity from the circuit model shown in Fig. 2.4a), sometimes called one-bit teleportation. In this circuit m is the outcome (0 or 1) of the measurement on the first qubit. This identity can be proven as follows: without loss of generality, let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The state after the CZ gate is then $\alpha|0\rangle|+\rangle + \beta|1\rangle|-\rangle$, which becomes $\alpha|+\rangle|+\rangle + \beta|-\rangle|-\rangle$ after the Hadamard operation. This state can be re-written as $(|0\rangle \otimes H|\psi\rangle + |1\rangle \otimes XH|\psi\rangle)/\sqrt{2}$, which completes the demonstration of the identity.

The identity can be further generalized as shown in Fig. 2.4b). The proof follows simply from noting that all rotations of the form $Z_{(\alpha)}$ commute with the CZ gate, and thus this circuit is equivalent to a), but with the state $Z_{(\alpha)}|\psi\rangle$ input for the first qubit.

This simple identity can be used to demonstrate several example circuits in $\mathrm{QC}_{\mathcal{C}}$, and in fact to suggest a proof of the universality of $\mathrm{QC}_{\mathcal{C}}$.

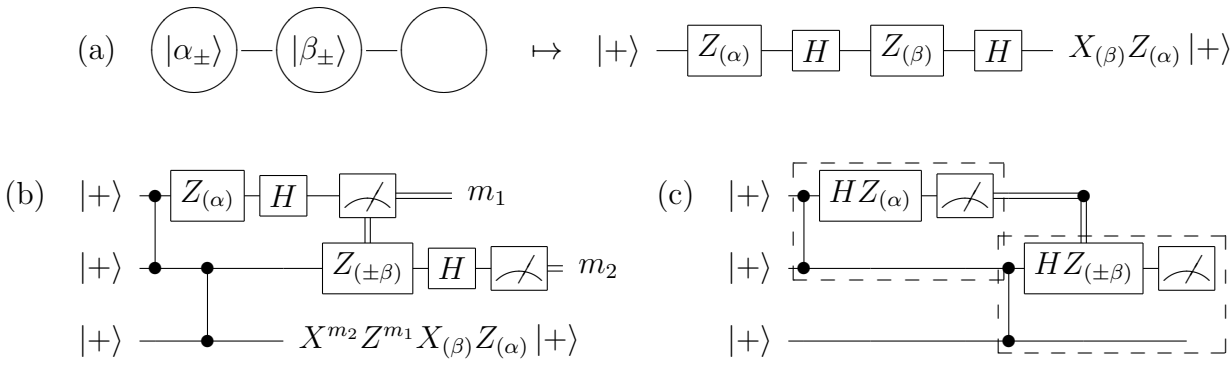


Figure 2.5: State preparation in the cluster model. a) The simple linear three-qubit cluster on the left simulates the circuit on the right and can thereby effect the preparation of an arbitrary pure qubit state via successive rotations of $|+\rangle$ around the z and x axes. The cluster computation in a) is by definition equivalent to the circuit computation in b), which if temporally re-ordered as in c) can be seen as two chained instances of the generalized one-bit teleportation protocol from Fig. 2.4b).

2.2.3.2 Single-Qubit Unitaries in the Cluster Model

The circuit in Fig. 2.4b) is effected by the following cluster computation:

(2.32)

Here the label in the first qubit refers to the basis in which that cluster is measured, and the second qubit yields the output $X^m HZ_{(\alpha)}|\psi\rangle$. The correspondence between this cluster and circuit Fig. 2.4b) can be seen by considering the process to create and measure the cluster: first a qubit is prepared in state $|\psi\rangle$ and another in $|+\rangle$, and then these are entangled via a CZ gate. Then the first qubit is measured in the basis $|\alpha_\pm\rangle$, which is equivalent to successive rotations by the operators $Z_{(\alpha)}$ and H, followed by measurement in the computational basis. So this cluster computation effects a single-qubit rotation of the form $HZ_{(\alpha)}$.

By concatenating rotations of this form, one can effect more general single-qubit rotations. For instance, the cluster computation in Fig. 2.5a) can effect the preparation of an arbitrary pure qubit state from the input $|+\rangle$ state. We explain this example in some

detail because, up to an unimportant re-definition of the rotation angles and local unitaries on the inputs, this is the computation we implement experimentally in Chapter 4. Note that the operator $HZ_{(\beta)}HZ_{(\alpha)}$ is equal to $X_{(\beta)}Z_{(\alpha)}$ by Eq. (2.8), and that by rotating the state $|+\rangle$ first around the z-axis and then around the x-axis by arbitrary angles, one can reach any other point on the surface of the Bloch sphere, i.e. any pure qubit state. To see that this cluster computation effects the stated circuit computation, note that it is by definition equal to that of the circuit shown in Fig. 2.5b). However, due to the fact that the CZ gate on the second and third qubits in (b) commutes with the operations on the first qubit, it can be delayed until after the measurement on the first circuit, re-ordering the time orientation of the circuit as in (a). Note that the boxed sections of this circuit are both of the form of Fig. 2.4, and thus the output is equal to $X^{m_2}HZ_{(\pm\beta)}X^{m_1}HZ_{(\alpha)}|+\rangle$, where m_1 and m_2 are the outputs of the measurements on the first and second qubits, respectively.

The enacted unitary differs from the desired unitary $HZ_{(\beta)}HZ_{(\alpha)}$ due to the factors X^{m_2} and X^{m_1}. However, the sign of $\pm\beta$ can be chosen based on m_1 such that $Z_{(\pm\beta)}X^{m_1} = X^{m_1}Z_{(\beta)}$. Therefore the enacted unitary is equal to $X^{m_2}Z^{m_1}HZ_{(\beta)}HZ_{(\alpha)}$, which, up to the known Pauli matrix $X^{m_2}Z^{m_1}$, is identical to the desired unitary rotation.

In Chapter 4, we show that this same computation can be performed using only two qubits if the measurement on the first qubit is a particular POVM, instead of a simple Von Neumann measurement.

This example illustrates two important points:

1. For any cluster computation designed to enact a desired unitary rotation U_g, (where g refers to the desired gate), the signs of measurement bases need to be appropriately chosen based on earlier outcomes in order to enact the desired computation. This necessitates a certain time-ordering of the measurements, generally from left to right in a cluster diagram.[11]

2. Even if measurement bases are correctly chosen using feedforward, the enacted unitary may differ by a correction unitary called a *byproduct operator*, and denoted U_Σ. This operator is due only to the randomness of the measurement results and

[11] When $g \in \mathcal{G}_C$, the Clifford group, which includes common unitaries such as the Paulis, Hadamard, and c-NOT, no feedforward is necessary to choose measurement bases, and the necessary Pauli corrections can all be delayed until the end of the computation. Thus all such gates can, if desired, be performed in a single time-step or with any temporal ordering [39].

will always be a product of Pauli operators. For instance, in the above example $U_\Sigma = X^{m_2} Z^{m_1}$.

The output of the cluster computation can then always be written as:

$$|\psi_{\text{out}}\rangle = U_\Sigma U_g |\psi_{\text{in}}\rangle \tag{2.33}$$

One must then perform a final correction $U_\Sigma^\dagger = U_\Sigma$, or, equivalently, change the final measurement basis in order to achieve the desired outcome. During the remainder of this chapter we will omit the byproduct operators, which is equivalent to assuming that all processing measurements yield the positive-eigenvalue outcome.

The step from preparing an arbitrary state in the cluster model to performing an arbitrary qubit unitary is not difficult. I have shown how to perform unitaries of the form $HZ_{(\alpha)}$ in $\text{QC}_\mathcal{C}$. Because $HZ_{(\alpha)}H = X_{(\alpha)}$, we can use these operators to perform unitary rotations around two perpendicular axes in the Bloch sphere. Therefore using the Euler decomposition of an arbitrary rotation (p. 8), an arbitrary single-qubit unitary can be performed using a 4-qubit linear cluster.

2.2.3.3 Two-Qubit Unitaries in the Cluster Model

Along with arbitrary single-qubit unitaries, the demonstration that $\text{QC}_\mathcal{C}$ can simulate a single two-qubit entangling gate shows that it can simulate a *universal gate set* from $\text{QC}_\mathcal{N}$, and thus perform arbitrary quantum computations.

Unsurprisingly perhaps given the preparation procedure outline in Sec. 2.2.2.1, the CZ gate acting on two arbitrary input qubits is particularly simple to demonstrate in $\text{QC}_\mathcal{C}$; it can be enacted by the cluster computation shown in Fig. 2.6a). This cluster computation is by definition equal to the circuit model computation in part b), and can therefore be viewed as a CZ gate on the middle two qubits, followed by four copies of the one-bit teleportation circuit in Fig. 2.4a). The output at the top and bottom qubits will be:

$$\begin{aligned} |\psi_{\text{out}}\rangle &= \alpha \left(X^{m_2} H X^{m_3} H |0\rangle \otimes X^{m_5} H X^{m_4} H |\chi\rangle\right) \\ &+ \beta \left(X^{m_2} H X^{m_3} H |1\rangle \otimes X^{m_5} H X^{m_4} H Z |\chi\rangle\right) \end{aligned} \tag{2.34}$$

Up to a byproduct operator on each qubit, this is equal to $\alpha |0\rangle \otimes |\chi\rangle + \beta |1\rangle \otimes Z |\chi\rangle$, which is the output of a CZ gate on $|\phi\rangle$ and $|\chi\rangle$.

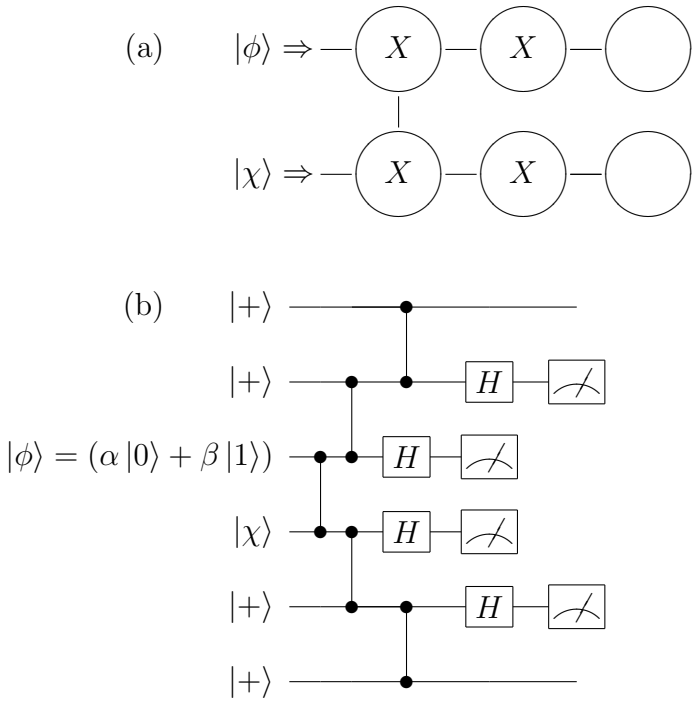


Figure 2.6: A CZ operation in the cluster model. The cluster in a) is by definition equivalent to the circuit in b), but both simply simulate a CZ gate on the input qubits $|\phi\rangle$ and $|\chi\rangle$. Note that, without loss of generality, $|\phi\rangle$ and $|\chi\rangle$ could have been the output of an earlier portion of the cluster computation.

Other examples of cluster computations can be seen in Ch. 4, Fig. 4.1.

I note finally that experiments with clusters have been carried out using various physical implementations including neutral atoms in optical lattices [40], as well as linear optics [41, 18, 42, 43, 44, 45, 46]. Furthermore, quantum error correction has been shown to be possible in the $QC_{\mathcal{C}}$ model, and thresholds for fault-tolerance have been found in e.g. [47, 48].

Chapter 3

Experimental Implementation

This chapter concerns the details of the implementation of the experiments described in this thesis. I first describe the protocols implemented in the experiments in Chs. 4 and 5 via quantum circuit diagrams in Sec. 3.1. These protocols are implemented with polarization-encoded photonic qubits. They require the integration of experimental apparatus which can be divided into three primary pieces: a source of polarization-entangled photon pairs, a linear-optical device for performing a tunable POVM on a polarization-encoded photonic qubit, and a setup for performing fast correction unitaries with Pockels cells and for performing tomography on the output. In the remaining sections of the chapter I detail the experimental implementation of these protocols in three sections themed around the creation, unitary manipulation, and measurement of polarization-entangled photons. In each section I move from a general overview to the specific implementations used in this thesis. In sec. 3.2, I discuss the process of spontaneous parametric downconversion conventionally used to create isolated optical photons for quantum information experiments before describing the specific source of polarization-entangled photon pairs utilized in herein. In sec. 3.3 I discuss birefringence before describing the implementation of unitary rotations on polarization-encoded photons with waveplates, and the implementation of fast-switchable unitaries with Pockels cells. In sec. 2.1.3 I describe the implementation of Von-Neumann measurements on polarization-entangled photons and the apparatus used to implement the POVM measurement in the experiments. This included a discussion of photon detectors and of the classical logical processing of the POVM apparatus outcome. Finally in sec. 3.5 I discuss the integration of all these components to perform the protocols, and some problems encountered while implementing the experiments.

3.1 Experimental Protocols

This thesis concerns two different experiments, both involving the implementation of a specific POVM (see secs. 2.1.3.3) on one qubit from an entangled pair. Circuits for these experiments are shown in Fig. 3.1.

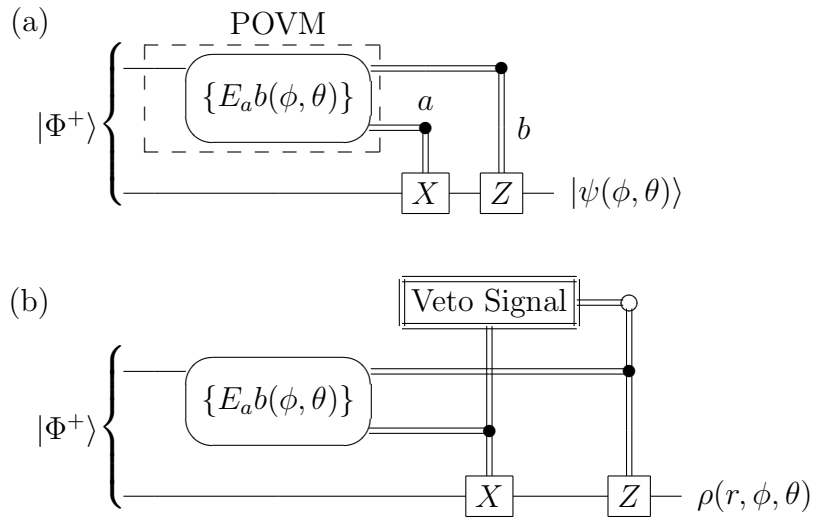


Figure 3.1: Circuits depicting the experiments detailed in Chs. 4 and 5. a) A POVM $\{E_{ab}(\phi,\theta)\}$ is performed on one qubit from an entangled $|\Phi^+\rangle$ pair (see Eq. (3.1)). The measurement has four outcomes which can be encoded in two classical binary signals, which in turn respectively (classically) control an X and Z operation on the other qubit, resulting in an arbitrary pure output state $|\psi(\phi,\theta)\rangle$ as in Eq. (2.6). b) A slight modification of the circuit, via the introduction of a Veto Signal which also classically controls the X and Z operations with probabilistic operation, can result in arbitrary *mixed* state outputs. The mechanism will be further explained in secs. 5.3.1 and 5.5.1.

The experiments begin with an entangled pair in the Bell state $|\Phi^+\rangle_{12}$ with subsystems 1 and 2. A POVM $\{E_{ab}\}$ consisting of four measurement operators, each equal to a rank-one projector up to normalization and labeled by a two-bit classical string ab, is performed

on subsystem 1:

$$\begin{aligned} E_{00}(\phi,\theta) &= \frac{\rho^*(\phi,\theta)}{2} \\ E_{01}(\phi,\theta) &= \frac{Z\rho^*(\phi,\theta)Z}{2} \\ E_{10}(\phi,\theta) &= \frac{X\rho^*(\phi,\theta)X}{2} \\ E_{11}(\phi,\theta) &= \frac{XZ\rho^*(\phi,\theta)ZX}{2}. \end{aligned} \tag{3.1}$$

Here $\rho(\phi,\theta) = |\psi(\phi,\theta)\rangle\langle\psi(\phi,\theta)|$, with $|\psi(\phi,\theta)\rangle$ as in Eq. (2.6), and $\rho^*(\phi,\theta)$ is the complex conjugate of ρ in the computational basis. The X and Z operations are then performed on qubit 2, controlled respectively by the bit values of a and b, resulting in an output state $|\psi(\phi,\theta)\rangle$. In Chs. 4 and 5, this POVM is called $\{\mathcal{E}_n\}$ and $\{E_m\}$, respectively.

For any arbitrary pure qubit state $|\psi\rangle$, the Bell state $|\Phi^+\rangle$ can be written as follows:

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|\psi^*\rangle\,|\psi\rangle + |\psi_\perp\rangle\,|\psi_\perp^*\rangle) \\ &= \frac{1}{2}(|\psi^*\rangle\otimes|\psi\rangle + Z\,|\psi^*\rangle\otimes Z\,|\psi\rangle + X\,|\psi^*\rangle\otimes X\,|\psi\rangle + XZ\,|\psi^*\rangle\otimes XZ\,|\psi\rangle) \end{aligned} \tag{3.2}$$

In order to facilitate subsequent data analysis, the output of the computation (qubit 2) should be $|\psi(\phi,\theta)\rangle$, where ϕ and θ are the polar and azimuthal Bloch angles, therefore our POVM elements are all related by Pauli operators to the projector of $|\psi^*\rangle$. This explains the appearance of the complex conjugation operation in the definition of the POVM elements.

Note the similarities between the circuit in Fig. 3.1 and the teleportation protocol in Fig. 2.2, as well as the preparation of an arbitrary state in the cluster model shown in in Fig. 2.5. Like the teleportation circuit, the circuit in 3.1a) results in an arbitrary quantum state using a $|\Phi^+\rangle$ state and two transmitted cbits controlling 'correction' Pauli operations. However, the state must be *known*, as in the cluster preparation circuit where the desired rotation angles are chosen by the experimenter (here ϕ and θ are parameters of the measurement chosen by the experimenter.) Unlike teleportation or standard cluster preparation, the circuit depicted here requires only *two* qubits, and, also unlike teleportation, requires no Bell-state measurement.

3.1.1 Photonic Qubits

These experiments were realized using single photons as qubits, primarily encoded in polarization (although the implementation of the POVM requires entangling the polarization with a 'path' degree of freedom to create the expanded Hilbert space $\mathcal{H}_4$ for the generalized measurement.) Single optical photons are in several respects ideal candidates for physical implementation of qubits: they travel at the speed of light for quick communication, they generally interact quite weakly with each other and with many types of matter leading to low environment-induced decoherence, and they are relatively easy to manipulate and measure. The latter point is especially true of photonic qubits encoded in the polarization degree of freedom, which is what I used for the experiments in this thesis. However photonic qubits pose some problems as well: due to their weak interaction, multi-qubit gates are experimentally difficult to implement. Furthermore, both reliable, deterministic sources of isolated single photons and highly efficient detectors have proven difficult to achieve, the latter especially if *non-demolition* detection is desired, meaning detecting the photon without destroying it i.e. through absorbtion in the detector.

Before proceeding to discuss the creation, manipulation, and measurement of polarization-encoded photonic qubits in some detail, I pause to briefly mention other possible ways to encode quantum information in single photons. Besides polarization, the other degrees of freedom of a single photon are its *time-frequency* and *spatial-momentum* distributions. Photons have been entangled in the former (time-bin entanglement [49] and frequency entanglement [50, 51]) and in the latter (spatial-mode entanglement [52] and path entanglement [53]). Of these, path encoding is one of the most promising techniques for application in large-scale quantum computing. In this scheme, a qubit is represented by a photon which can be in a superposition of two different paths or rails, such as two arms of an interferometer. Single-qubit unitaries can be implemented by controlling the phase at an interferometric junction of the two paths, and multi-qubit unitaries by interfering the rails corresponding to different qubits. The difficulties with such an implementation stem from the requirement for precise phase-stabilization and control over many coupled interferometers, although this may be mitigated in the future with advancing integrated-optics technology. Path encoding will be employed to extend the Hilbert space of our polarization qubit for the POVM (see sec. 3.4.2).

When encoded in polarization,[1] the convention is to represent the logical basis states

[1] By definition the polarization is the direction of the electric field vector.

$|0\rangle$ and $|1\rangle$ by the orthogonal horizontal and vertical polarization components $|H\rangle$ and $|V\rangle$, respectively. The eigenstates of the X and Y operators are then respectively represented by the (Anti-)Diagonal and Right/Left circular polarization components as follows:

$$\begin{aligned} |0\rangle &\mapsto |H\rangle & |1\rangle &\mapsto |V\rangle \\ |+\rangle &\mapsto |D\rangle & |-\rangle &\mapsto |A\rangle \\ |+i\rangle &\mapsto |L\rangle & |-i\rangle &\mapsto |R\rangle\,. \end{aligned} \tag{3.3}$$

It is also possible to create photon pairs entangled in multiple degrees of freedom, e.g. $(|HH\rangle + |VV\rangle) \otimes (|P_A P_A\rangle + |P_B P_B\rangle)/2$, where A and B refer to two different paths, but all the encoding is done on the same two photons (i.e. the first position in each ket refers to the same photon). This is called hyperentanglement, and will be referenced in Ch. 4 but not directly employed in this thesis.

The experimental apparatuses used to create polarization-entangled photon pairs, perform the requisite POVM, encode and transmit the outcome, implement the requisite 'correction' unitaries, and measure the final output is shown in Fig. 3.2.

3.2 Creating Photons through Spontaneous Parametric Downconversion

While several methods exist for producing photons for use in quantum information tasks, the most successful and widely-applied has doubtless been *spontaneous parametric downconversion* (SPDC) in nonlinear crystals [56]. Because the apparatus for creating the photons used in these experiments was built by my colleague Deny Hamel and was not a focus of my research, and also because the SPDC process and its implementation in photon sources has been extensively treated in many other papers, books, and theses, I will not detail it here, but will nonetheless address it briefly for the sake of completeness. In writing this material I draw on Refs. [35, 57] and the appendices to [58].

SPDC is a non-linear optical process relying on the second-order coefficient $\chi^{(2)}$ of the polarization response of some media to an applied propagating electromagnetic field. In SPDC a high-energy "pump" field is mixed with two lower-energy vacuum fields, known for historical reasons as the *signal* and *idler*, in such a nonlinear medium. This three-wave

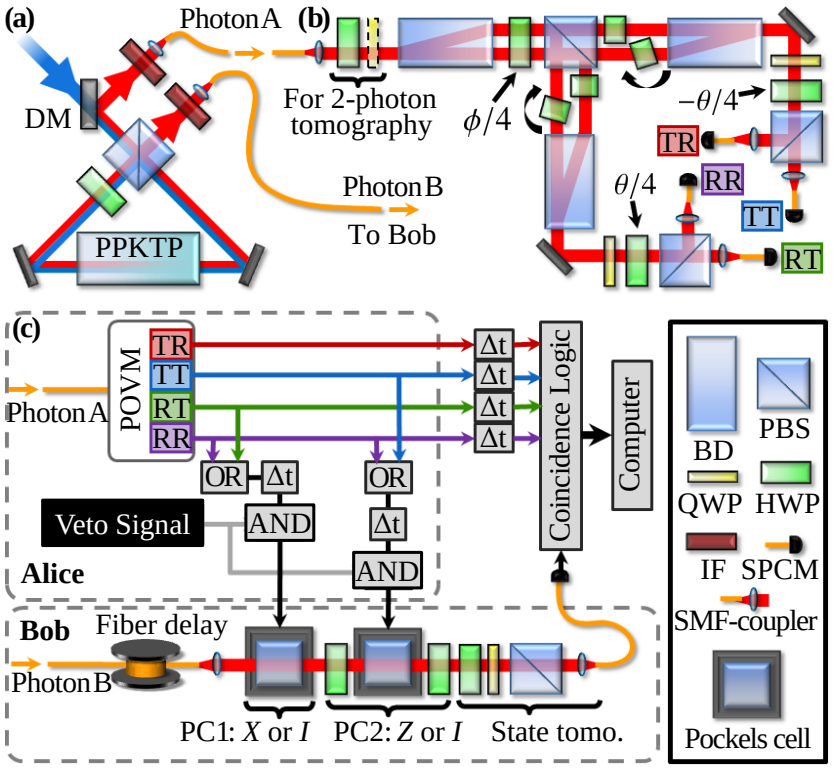


Figure 3.2: Diagram of the experimental apparatus. (Note that this is identical to Fig. 5.4, but is included in both places for the reader's convenience.) (a) Entangled photon pairs are produced via parametric downconversion in a polarization-based Sagnac interferometer [54, 55] (see text for details) and distributed via single-mode fibers (SMFs). (b) A POVM is performed on photon A. The apparatus consists of a double-interferometer based on calcite beam displacers (BDs) which couple the polarization qubit to a 'path' qubit for the generalized measurement. See sec. 3.4.2 for details. (c) Schematic of the entire experimental protocol. The POVM $\{E_{a,b}\}$ is performed on Photon A. Based on the outcome m a message is encoded in two classical electronic signals, and then sent to Bob with probability r which is controlled by a Veto Signal. Dependent on the message, up to two Pockels cells (PCs) fire to perform the necessary unitary correction on Photon B, which has been delayed in a 50 m fiber to allow time to trigger the PCs. Bob's output is analyzed using quantum state tomography. Note: DM: dichroic mirror; IF: blocking and interference filter; PBS: polarizing beamsplitter; H(Q)WP: half (quarter) wave-plate; SPCM: fiber-coupled single-photon counting module.

mixing process is described by an interaction Hamiltonian of the form

$$\mathcal{H} = \gamma(\chi^{(2)})a_s^\dagger a_i^\dagger a_p + \gamma(\chi^{(2)})a_s a_i a_p^\dagger, \tag{3.4}$$

where the a_j and $a_j^\dagger$ are respectively annihilation and creation operators for a photon in the j^{th} mode. The first term in this Hamiltonian describes SPDC while the second describes the reverse process *sum-frequency generation* (SFG). While SFG is a classical effect describable via Maxwell's equations, SPDC admits no such classical description due to the mixing of pump light with previously-unpopulated vacuum fields and is thus a distinctly quantum-mechanical effect.

Although SPDC can lead to higher order photon-number states in the signal and idler fields (i.e. multiple photons in the same mode at the same time instead of one photon each in the signal and idler modes), the coupling constant γ is small enough in most media that even with bright coherent pump fields the vacuum and single-photon terms vastly exceed the multi-photon terms. This is especially true with low-power continuous-wave pump beams, as used in this thesis, and thus the output can be well-approximated as a spontaneous source of pairs of single photons in the signal and idler modes ([35], ch.6.)

3.2.1 (Quasi-)Phase Matching Conditions

In the downconversion process energy must be conserved, and usually for any significant efficiency momentum must be nearly conserved among the three photons as well[2]. Usually this requires that the signal and idler frequencies sum to the pump frequency, and their wavevectors sum to the pump wavevector. These conditions require the three interacting fields to be in phase along their direction of propagation and are thus often called the *phase-matching conditions*. This is often accomplished via manipulating the geometry of the interaction such that the indices of refraction of the pump, signal and idler fields are matched for certain propagation directions (with respect to the crystallographic axes) and polarization directions of each field; these are respectively called angle phase-matching and birefringent phase-matching.

A more recently-developed technique takes advantage of *periodically-poled* crystal structures, where the nonlinear material is specially grown such that its effective nonlinearity is

[2]It is possible that momentum is not *exactly* conserved due to the finite crystal length which allows for some absorbtion or contribution of momentum by the crystal phonon field.

flipped with a period equal to the coherence length of the pump and signal/idler phases. This allows for *quasi-phase-matching*, where the effective wavevector of the structure contributes to the momentum conservation condition, allowing greater experimental freedom for the pump and downconversion directions, wavelengths, and polarizations [57]. In particular, the poling period and operating temperature can be tuned such that the signal and idler are orthogonally polarized and all three propagation directions are collinear along one of the crystallographic axes. This rids the interaction of the birefringent walkoff problems that plague angle- and birefringent-phase-matched downconversion setups, and thereby allows for much longer crystals, and thus longer interaction times and higher SPDC rates.

3.2.1.1 The Sagnac Source of Entangled Photon Pairs

In this thesis we are specifically interested in the production of polarization-entangled photon pairs. The source used for the experiments described herein was built by Deny Hamel based on a design first implemented by Kim *et. al.* [54] and later refined by Fedrizzi *et. al.* [55, 57]. It is shown schematically in Fig. 3.2a), and as an annotated photograph in Fig. 3.3. Note that in Fig. 3.2a) the signal and idler outputs are respectively labeled Photon A and Photon B. The source produces entangled photon pairs via embedding a periodically-poled potassium titanyl phosphate $KTiOPO_4$ (PPKTP) nonlinear crystal in a polarization Sagnac interferometer.

A Sagnac interferometer is one in which two counter-propagating beams follow the same path, but propagating in opposite directions, before recombining interferometrically. Due to the fact that both beams traverse the same optical path, the Sagnac configuration is insensitive to mechanical displacements except rotations, and is therefore quite stable without the need for active stabilization or phase-locking. In a polarization Sagnac interferometer, the input/output beamsplitter is a *polarizing* beamsplitter (PBS), so that one beam (the one traveling clockwise in Fig. 3.2a) is initially H-polarized, while the other (traveling counter-clockwise in the figure) is initially V-polarized. The PPKTP crystal is oriented, cut, and temperature-tuned for collinear, degenerate type-II SPDC. Here collinear means the pump, signal, and idler beams all propagate in the same direction, degenerate means the signal and idler output wavelengths are the same ($\lambda_s = \lambda_i$), and type-II refers to the orthogonal polarization of the output signal and idler beams: $|H\rangle_p \mapsto |H\rangle_s |V\rangle_i$, and any V-component of the pump does not satisfy the phase-matching conditions for downconversion.

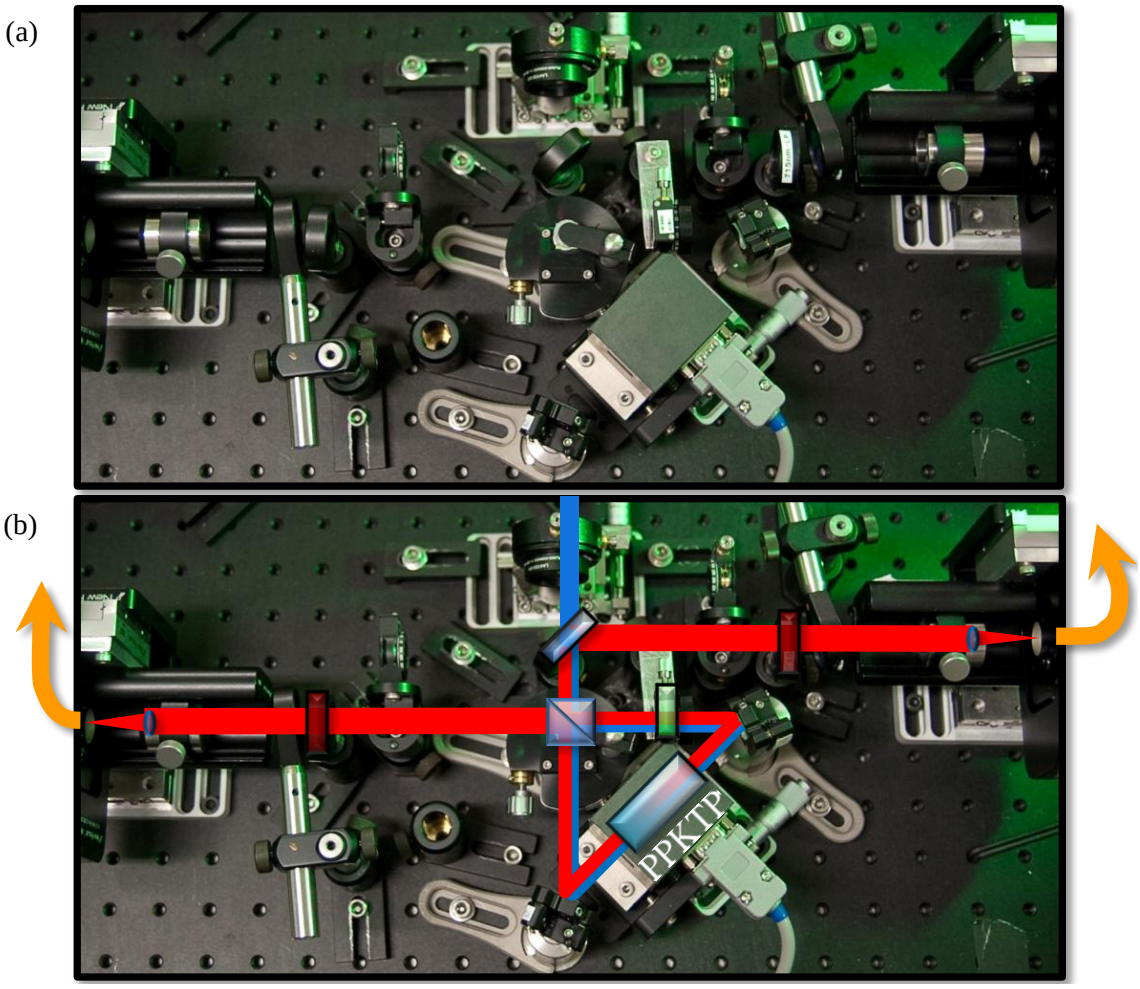


Figure 3.3: Photographs of the Sagnac source of polarization-entangled photon pairs used for the experiments in this thesis. a) A photograph of the source. b) A photograph with superimposed depictions of the beam path, important optical elements, and output fibers.

To produce entangled photon pairs from this source, the PBS is ensured to operate at both the pump and signal/idler wavelengths, and a similarly dual-wavelength half-wave plate (HWP, see sec. 3.3.2) at 22.5° is inserted before the PPKTP for the V-polarized pump beam (and thus after the PPKTP for the H-polarized pump), so that the type-II phase-matching conditions are met for *both* counter-propagating pump beams. This leads to counter-clockwise-propagating SPDC pairs of the form $|H\rangle_s |V\rangle_i$, while the clockwise-propagating pairs are rotated by the HWP: $|H\rangle_s |V\rangle_i \xmapsto{HWP} |V\rangle_s |H\rangle_i$. The clockwise- and counter-clockwise propagating pairs are then coherently combined at the input/output PBS, which for a pump beam with equal H and V components yields an output state of the form:[3]

$$\frac{1}{\sqrt{2}} \left(|H\rangle_s |V\rangle_i + e^{i\phi} |V\rangle_s |H\rangle_i \right). \tag{3.5}$$

Note that the signal photon always exits the interferometer back along the path of the incoming pump beam, but is separated from the exiting pump by a dichroic mirror (DM), while the idler exits through the other PBS output port.

The phase ϕ in this maximally-entangled output state can be adjusted by changing the phase between the H- and V-polarized components of the pump beam, usually by tilting a waveplate with its optic axis in the H- or V-plane about its vertical axis. In particular the output can be adjusted to the Bell states $|\Psi^{\pm}\rangle$ (see sec. 2.1.4. A notable feature of the polarizing Sagnac interferometer SPDC configuration is that longitudinal walk-off in the nonlinear crystal, which in other schemes for entangled-pair generation might lead to timing information and therefore distinguishability and loss of entanglement, is automatically compensated due to the bi-directional pumping and the fact that signal photons always end up in one output mode, and idlers in the other.

In the particular implementation of this source used in the experiment, a 25 mm long PPKTP crystal is embedded in the polarization Sagnac interferometer and pumped by a grating-stabilized UV diode laser outputting < 1 mW at 404.5 nm, leading to degenerate downconversion at $\lambda_{s,i} = 809$ nm. The resulting entangled photon pairs are coupled into single-mode fibers (SMFs). Long-pass filters and 5 nm FWHM interference filters before the fiber-couplers rid the transmitted light of any stray UV pump photons. These fibers are used to transport the photons to the other portions of the experimental apparatus. Fiber polarization-conrollers, called "bat-ears" by experimentalists due to their appearance, are used to rotate the output state to $|\Phi^-\rangle$, as will be further described in sec. 3.5.

[3] Note that the 'i' in the exponential is the imaginary number whereas that in subscripts refers to 'idler.'

The quality of sources of entangled photons is measured by at least two general features: the rate of pair production and the quality of entanglement, both suitably quantified. The former is often quantified simply as [pairs s^{-1}], or as the pair rate normalized by the pump power [pairs s^{-1} mW^{-1}], or even as the *spectral brightness* given in pairs per second per mW of pump power per nm of output photon bandwidth [pairs s^{-1} mW^{-1} nm^{-1}]. The entanglement can be quantified by performing state tomography on the source output and calculating some measure like the tangle, or even the fidelity with a desired output like one of the Bell states. A third feature often but not always desired is a high *efficiency*, meaning that a high proportion of the photons detected at the source outputs are from an entangled pair. At the pump power used in these experiments of about 0.86 mW, the rates detected out of the fibers were typically 150 kHz single detection events at each output ("singles") and 30 kHz coincident pairs (within a suitable window; photon detection will be discussed further in sec. 3.4). This yields a brightness of about 3.5×10^4 pairs $s^{-}1$ $mW^{-}1$ and an efficiency of 20%, both comparable to the state-of-the-art (see e.g. [57]). Typical tomographically-reconstructed density matrices of the source output state are shown in Figs. 4.3 and 5.5. The figures of merit varied slightly from day to day but with careful alignment we generally achieved a tangle of about 0.93 and a fidelity with the intended Bell state of about 0.980 (more precise numbers are given in the respective chapters 4 and 5, and in the figure captions.)

3.3 Manipulating Polarization-Encoded Photons

The evolution of polarized beams or photons through optical circuits is often found using *Jones calculus*. In this method, the polarization of a beam is represented through a vector

$$\vec{J} = \begin{bmatrix} A_H \\ A_V \end{bmatrix}, \tag{3.6}$$

where A_i is the complex amplitude of the i^{th} component of the electric field. The Jones vector is often normalized such that $\sum_i A_i = 1$. Notice that a normalized Jones vector is the same vector used to represent a polarization qubit. In fact, the techniques from Jones calculus can be used to calculate the propagation of a single polarization-encoded photonic qubit through an optical circuit of polarizing elements. The difference is that for a photon, the squares of the vector components yield the probability of finding the photon to have the respective polarization, whereas the components of the classical vector represent the

square-root of the normalized *intensity* in the respective polarization mode. Note that care must be taken and classical techniques can not always be so readily employed when considering the propagation through an optical circuit of *more than one* photon, where non-classical interference effects can happen, leading for example to the famous Hong-Ou-Mandel effect [59] in which two photons with identical transverse spatial modes, time-frequency distributions, and polarizations will 'bunch' when impinging on a beamsplitter from different input ports. In such cases it is often better to perform the circuit analysis in terms of the creation and annihilation operators a_k and $a_k^\dagger$ for the different modes $\{k\}$.[4]

The action of optical elements or circuit components are represented by Jones matrices, and in fact the Jones matrices for ideal elements are often unitaries or projectors. I will physically motivate several Jones matrices for polarizing elements used in the experiments in this thesis, and show how they can be used to manipulate and measure photonic polarization qubits and in particular to construct our POVM apparatus.

3.3.1 Birefringence and Polarizing Beamsplitters

A common way of manipulating the polarization of light is through the use of *birefringent* materials. These are materials for which the light will experience a different index of refraction and therefore travel at a different speed depending on its polarization with respect to the crystallographic axes of the material. Of course, the index of refraction also depends on the frequency; the following best applies to monochromatic plane waves. My discussion of birefringence and optical components employing this effect is drawn from [35] Ch. 4, [61] pp.336-358, and [62] Ch. 6. Regardless of the direction of propagation and angle of incidence, any birefringent medium will split the incoming light into two *normal modes*, orthogonal polarization states which are unchanged by propagation through the medium (they're eigenstates of the transformation it induces on the polarization state). Generally light in one of these modes will travel faster through the medium than light in the other, and thus the normal modes define a 'fast axis' and 'slow axis', both perpendicular to the direction of propagation. The simplest birefringent materials are *uniaxial* meaning

[4] The details of the quantization of classical electromagnetic field are outside the scope of this thesis. However, in such a quantization, the complex-valued amplitudes associated with classical electromagnetic field modes α_k, and their complex conjugates α_k^*, are replaced respectively by annihilation operators a_k and their *Hermitian* conjugates, creation operators $a_k^\dagger$. Single photons behave in some sense 'like classical beams' because they are linear functions of creation operators acting on the vacuum field $|0\rangle$: a single photon in a superposition among modes k can be written as $\left(\sum_k A_k a_k^\dagger\right)|0\rangle$. See [35] ch. 2 or [60].

they have a single crystallographic axis of symmetry, the *optic axis* $\hat{a_o}$. Light polarized parallel to this axis is said to have *extraordinary* polarization and will experience an index of refraction n_e, while light polarized perpendicular to $\hat{a_o}$ is said to be *ordinary* and will experience an index n_o.

Consider a beam propagating through a uniaxial material, without loss of generality along the axis z. If $z = \hat{a_o}$ then all polarizations of the beam are ordinary. Otherwise z and $\hat{a_o}$ define a *principal plane*; any component of the beam polarized perpendicular to this plane will be ordinary and experience index of refraction n_o, while the component in the plane is called the e-ray and will experience an index

$$n(\theta) = \sqrt{\frac{n_o^2}{\cos^2\theta} + \frac{n_e^2}{\sin^2\theta}}, \tag{3.7}$$

where θ is the angle between z and $\hat{a_o}$.

When the optic axis is neither parallel nor perpendicular to the direction of propagation of the beam as it enters the crystal, birefringent media can lead to the effect of *double refraction* or *walkoff*,[5] where the ordinary-polarized component of the input ray and the extraordinary-polarized component refract at different angles. For an angle of incidence θ_i, the angles of refraction θ_o and θ_e of the o- and e-rays are given by a modified Snell's law:

$$\begin{aligned} \sin\theta_i &= n_o \sin\theta_o \\ \sin\theta_i &= n(\theta_e)\sin(\theta_e), \end{aligned} \tag{3.8}$$

where $n(\theta_e)$ is given by Eq. (3.7). A thorough treatment of this and related birefringent phenomena can be found in Ref. [62], pp. 210-222.

This effect can be used to construct several types of *polarizing beamsplitters*, devices which separate an input beam into two orthogonally-polarized and spatially-separated output modes. If one looks only at one output mode of a polarizing beamsplitter, i.e. by blocking or simply failing to detect the other mode, then their action is to project onto a single polarization, and their Jones matrix is given by e.g. $|H\rangle\langle H|$ or $|V\rangle\langle V|$, depending on the output mode considered. A particular type of polarizing beamsplitter made with the uniaxial birefringent crystal calcite is shown in Fig. 3.4. This element, called a *calcite beam*

[5] sometimes called spatial walkoff, as it involves differing propagation directions in the crystal for e- and o-rays, to distinguish it from temporal walkoff which results from a difference in the *phase velocities* of e and o polarizations.

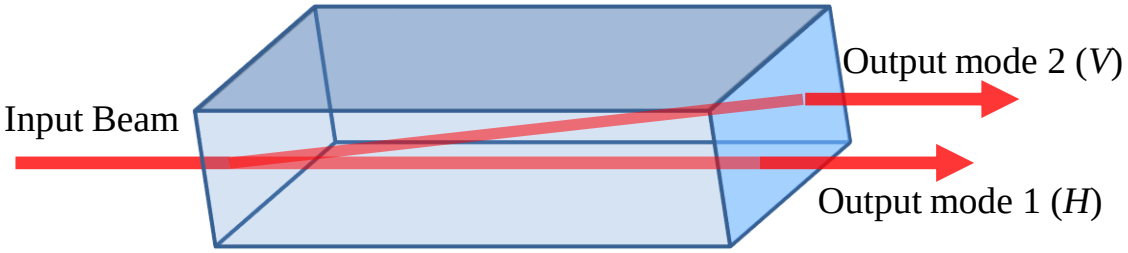


Figure 3.4: (Color online) Calcite Beam Displacer. This type of polarizing beamsplitter, made from a single block of calcite, cut for the maximum walkoff angle between orthogonal polarizations of a normally-incident beam, separates the beam into two spatially separated but parallel output beams in output modes 1 and 2. Note that if both output beams are in the horizontal plane, as shown here, then it is the vertical output which is deviated.

displacer (BD) is unique in that the orthogonally-polarized output beams are parallel, and forms a key component in the construction of the POVM apparatus.

Some birefringent polarizers, in particular Glan-type prisms, only yield one very-highly polarized output beam (usually the transmitted beam, which for normal orientations of these polarizers is H-polarized) while the other output is either broken into multiple beams or not fully polarized, and thus these can only be used to project (perhaps with some loss) onto one polarization mode. Another important type of polarizing beamsplitter, which I will refer to as a PBS-cube or simply a PBS, actually operates not based on birefringent effects but rather using a stack of many layers of polarizing dielectric films at the interface between two triangular glass prisms, joined to form a cube with the dielectric across the inner diagonal. These will also be used in the POVM apparatus, and are useful for making a projective measurement of polarization because they separate the input beam into two output modes with orthogonal polarizations and perpendicular propagation directions.

3.3.2 Waveplates

An important optical component constructed from birefringent materials, in particular quartz, is the phase retarder or waveplate, which I have already mentioned in discussing the Sagnac source of polarization-entangled photons. These are birefringent uniaxial crystals

cut and mounted such that the optic axis is parallel to the entrance face, and therefore one component of the incoming beam always experiences n_e and the perpendicular component n_o. The difference in refractive index means that the e-component will have experienced a phase shift $\Delta\phi$ relative to the o-component when they exit the waveplate, given by $\Delta\phi = k_0 d|n_o - n_e|$, where d is the thickness of the plate and k_0 the magnitude of the wavevector of the incident light in free space.

The action of a waveplate with the optic axis oriented horizontally is described (up to an unimportant global phase) by the Jones matrix:

$$U_{wp}(\phi) = \begin{bmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{bmatrix}. \tag{3.9}$$

Notice that this is the same operator as for a rotation about the *Bloch* z-axis by ϕ.

The action in the H,V-basis of any polarizing optical component when rotated by an angle θ from the horizontal around the direction of propagation can be found by applying the two-dimensional rotation operator[6] $R(-\theta)$ to the corresponding Jones matrix, where

$$R(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}. \tag{3.10}$$

For instance the action of a ϕ-waveplate, rotated around the direction of propagation by θ is

$$U_{rwp}(\phi,\theta) \equiv R(-\theta)U_{wp}(\phi)R^\dagger(-\theta) = R(-\theta)U_{wp}(\phi)R(\theta). \tag{3.11}$$

This is a fairly general unitary, describing a rotation by ϕ about the *real* superposition of the computational basis states (i.e. the linear polarization) making an angle *in the Bloch sphere* of θ with $|H\rangle$.

Fortunately, most applications do not require control over the retardance ϕ of a waveplate, but rather use combinations of just two: the *half-waveplate* (HWP)

$$\begin{aligned} HWP(\theta) &= -iU_{rwp}(\pi,\theta) \\ &= \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}, \end{aligned} \tag{3.12}$$

[6]The basis in which the component operates is related by a rotation of *positive* θ to the H,V-basis, therefore the transformation to find its action in the H,V-basis is a rotation by *negative* θ.

and the *quarter-waveplate* (QWP), which I define for my calculations as

$$\begin{aligned} QWP(\theta) &= iU_{rwp}\left(\frac{-\pi}{2}, \theta\right) \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix} i+\cos 2\theta & \sin 2\theta \\ \sin 2\theta & i-\cos 2\theta \end{bmatrix}. \end{aligned} \tag{3.13}$$

These are called as such because they retard one polarization by a half (quarter) wavelength with respect to the other. Note that the global phases ($-i$ and i respectively) are added only for convenience, and also that $HWP(0) = Z$, $HWP(\pi/4) = X$, and $HWP(\pi/8) = H$. Finally, notice that the HWP and QWP operators are both unitary and Hermitian: they are their own inverse and their own conjugate-transpose.

In practice, waveplates which only retard light along the 'slow' axis by half or a quarter wavelength are quite thin and therefore fragile and difficult to manufacture and use. However, waveplates with $\phi/k_0 = n + \frac{1}{2}\lambda_0$ or $n + \frac{1}{4}\lambda_0$, where n is an integer, accomplish the same purpose for monochromatic light of vacuum wavelength λ_0. However if the n is large and so is the bandwidth of the incident light, such a *multi-order* waveplate imparts different retardances and thus different phases to the various frequency components of the input. A more precise solution is to use two multi-order waveplates, differing in retardance by π ($\pi/2$ for a QWP), mounted back-to-back with the fast axis of one aligned with the slow axis of the other to yield a *compound zero-order waveplate*. The waveplates used in the POVM apparatus, implementation of fast unitary corrections, and tomography in this thesis were exclusively air-spaced compound zero-order waveplates designed for a central operating wavelength of 810 nm.[7].

QWPs can transform linear polarizations to elliptical, and vice-versa, while HWPs can rotate any linear polarization to any other, or rotate the axes of the ellipse of an elliptically polarized beam. An arbitrary unitary rotation can be achieved by concatenating three waveplate rotations at arbitrary angles, specifically in the order $QWP(\alpha)HWP(\beta)QWP(\gamma)$ or QHQ [35]. It is interesting to contrast this decomposition of an arbitrary unitary—into rotations about three arbitrary linear-polarization axes by two fixed amounts (π and $\frac{\pi}{2}$)—with the Euler decomposition (p. 8) of an arbitrary unitary into rotations by three arbitrary angles about two different fixed non-parallel axes.

[7] Casix WPZ1315-λ/4-810 and WPZ1315-λ/2-810

3.3.3 Fast Unitaries with Pockels Cells

Waveplates serve perfectly well to perform slow unitaries on polarization-encoded photonic qubits. By *slow*, I refer not to the speed of the actual unitary transformation, which takes only on the order of 10 ps for the actual transit time of the photon through the waveplate(s), but rather to the speed at which the unitary is switchable, which depends on the speed at which the experimenter is able to precisely mechanically *rotate* the waveplates. These times are generally much too slow for the fast switching required to implement the correction unitaries (the classically-controlled X and Z operations) in e.g. Fig. 3.1. The speed at which these need to be switched depends on the source rate and detector characteristics but might typically be from a few to a few hundred nanoseconds, too fast for cheap reliable mechanical rotations.

Such fast-switchable unitaries can be implemented on polarization photonic qubits using e.g. acousto-optic modulators (AOMs) or Pockels cells. I will describe the latter, as they were employed in the experiments in this thesis, drawing on Ref. [62], pp. 696-701.

In some materials the index of refraction will change in proportion to an applied electric field; this is known as the Pockels effect after its discoverer Friedrich Pockels. An arrangement of such a material with electrodes to control the Pockels effect is called a Pockels cell (PC). In a birefringent material exhibiting the Pockels effect, the two orthogonally-polarized normal modes of an incident beam will experience a total relative phase shift

$$\phi_{\text{total}} = \phi_0(d, n_f, n_s) + \pi \frac{V}{V_\pi}, \tag{3.14}$$

where ϕ_0 is the phase shift induced with no applied electric field and takes the form of Eq. (3.9), only the fast and slow axes might not correspond to n_e and n_o if the crystal is not uniaxial or the propagation direction is not perpendicular to the optic axis. V is the voltage applied across the medium, and V_π is an important property of the physical system called the *half-wave voltage*, which depends on the crystal material, size, and geometry, the frequency of light considered, and the geometry of the electrodes across which the voltage is applied. The half-wave voltage is that for which the retardance changes by π. Often the PC system is arranged such that $\phi_0 = 0$ and there is no (spatial) walk-off; in this case the PC performs the identity on an incident polarization state when no voltage is applied, and acts as a HWP if V_π is applied.

The Pockels cells used to perform the correction unitaries in the experiments in this

thesis were constructed of rubidium titanyl phosphate $RbTiOPO_4$ (RTP) [8]. They are *transverse*-operating, meaning that the voltage is applied perpendicular to the direction of propagation. Because RTP actually exhibits some temporal walkoff along the direction of propagation, these PCs are constructed from two crystals of equal optical thickness, the one oriented with its fast axis parallel to the slow axis of the other (similar to the compound zero-order waveplates discussed above, only here the net retardance is $\phi = 0$ when no external voltage is applied). They have a 4 mm aperture and a 20 mm length. For more info see Ref. [63] and [64].

[8] Leysop RTP4-20-AR800

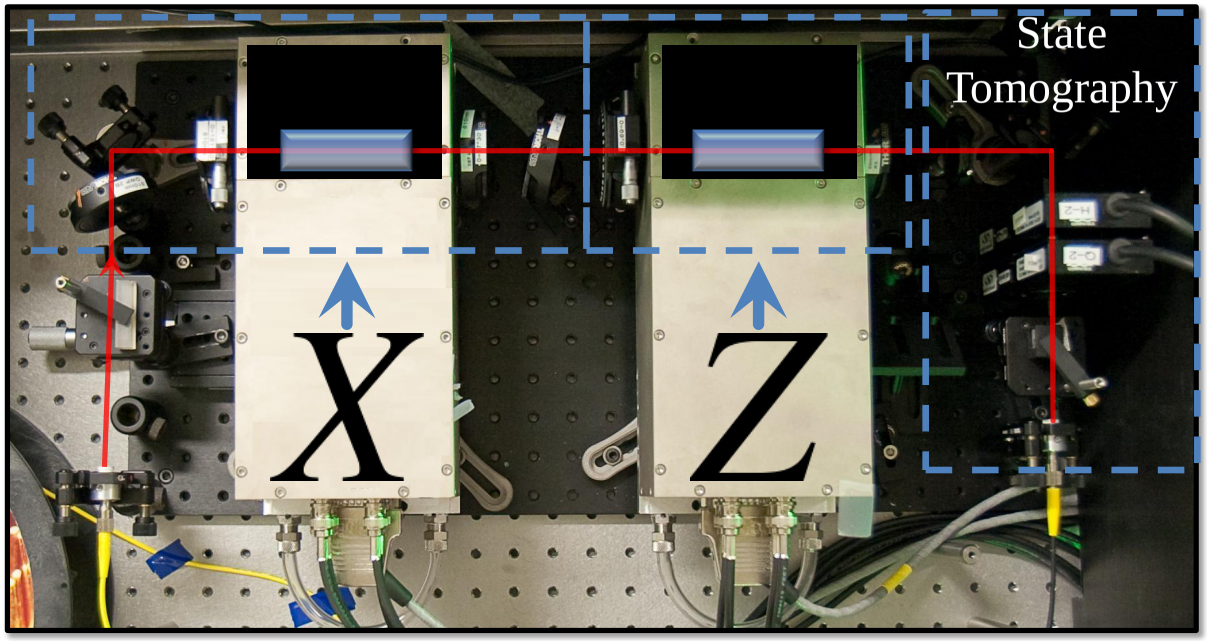


Figure 3.5: Annotated photograph of the Pockels cell setup for performing correction unitaries and the polarization analyzer for tomography of the output state. Light is coupled in through the input fiber collimator at the far left. A Calcite BD polarizer on a translation stage can be used for alignment purposes but is removed for normal operation. The beam then reflects off two mirrors and passes through multiple waveplates and the two Pockels cells (PCs). The first PC, along with the two 'compensation' WPs before it and two more following, enacts the X operation when triggered; the second PC along with one HWP before and after enacts Z. The final two (motorized) WPs and beamsplitter form a polarization analyzer, used for state tomography of the output. They project onto an arbitrary polarization state, which is then coupled into fiber and detected. Note that the crystals shown inside the PCs are merely a cartoon representation, as metal lids were in fact on each PC housing at the time of the photograph.

3.3.3.1 Testing and Aligning the Pockels Cells

The Pockels cells were purchased along with mounts, driving electronics, and power supplies as a package (model BME PC_dpp) from Bergmann Messgeraete Entwicklung KG (BME). Each is mounted with its optic axis at 45° such that it performs an X operation when V_π is applied, switching horizontal and vertical polarization. However, HWPs at 22.5°, which perform the Hadamard operation, were placed before and after the second Pockels cell. This changes the net action of the HWP-PC-HWP to Z when the high voltage (HV) is on, and yet it still acts as the identity when the HV is off: $HXH = Z$ and $H\mathbb{1}H = \mathbb{1}$ (see Eq. (2.8)). Each PC is driven by a double push-pull driver which controls the application of the high voltage. The triggering pulses for the push-pull driver are from a specially designed pulse splitter box BME_sp02, also included in the package from BME. The pulses which switch the HV on and off can be triggered independently, or the experimenter can set the splitter box such that the 'off' pulse always follows the 'on' pulse after a specified amount of time. I set the HV to turn off approximately 20 ns after each 'on' pulse (which came from the classical logic and ultimately from the photon detectors; see sec. 3.4.3).

The optical circuit for using the Pockels cells to perform correction unitaries, and then performing tomography on the output, is shown schematically in Fig. 3.2c), but a more detailed version in the form of an annotated photograph is shown in Fig. 3.5. When setting up the Pockels cells, they must first be aligned such that the beam is retro-reflected (i.e. normally incident to the entrance face) and passes approximately through the center of the aperture. Several steps are then required to properly align the PCs and assure that the entire setup was performing the correct transformations on incident photons when both, neither, or either PC was triggered. The half-wave voltage must be found, the correct delay must be determined such that each PC, if triggered by a signal photon detection, will be fully on when the idler photon passes through, and finally waveplates must be used to compensate for slight misalignments in each PCs orientation.

The half-wave voltage V_π can initially be roughly found by sending an H-polarized beam of approximately the desired wavelength[9] through the Pockels cell with the polarization analyzer set to project onto H, and examining the the output signal from a fast photodiode with an oscilloscope as the Pockells cell is triggered periodically and the HV is adjusted. When the output signal is minimized during the time that the HV is 'on', then the PC is sending H-polarized light nearly to V, and thus operating close to V_π. A

[9]Source: Thorlabs CPS808 808 nm collimated laser diode module.

more precise determination of V_π was effected using photon pairs from SPDC. This was accomplished by triggering the PC on the detection of a signal photon, sending H-polarized idler photons into the PC, projecting the output onto $|H\rangle$, and counting the number of coincident detections in a certain time interval as a function of the HV value.

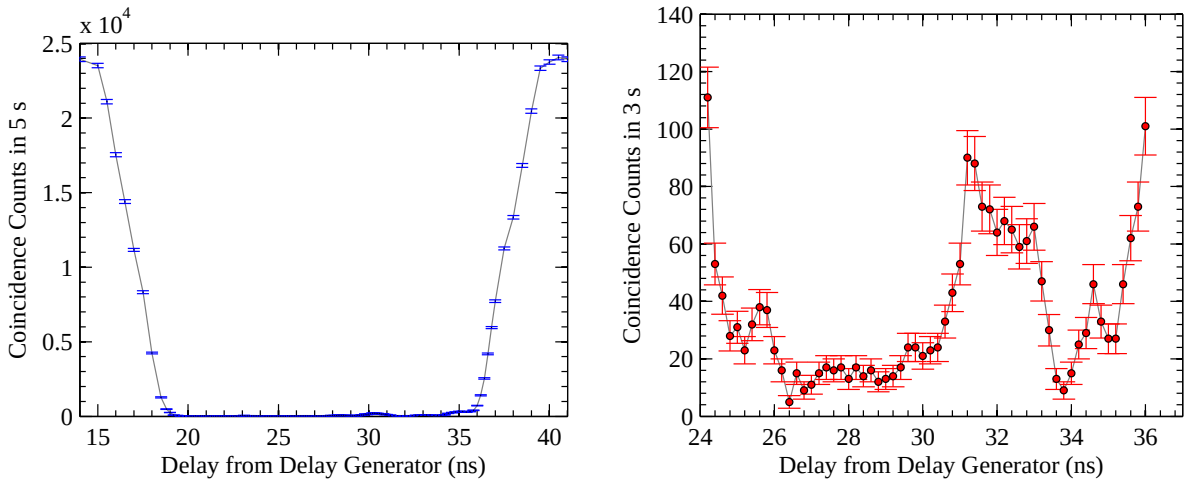


Figure 3.6: Scanning for optimal Pockels cell delay. The Pockels cells were both set such that the high voltage would be on for approximately 20 ns after being triggered. However, due probably to some ringing in the electronics, the retardance imparted by the PCs appeared to vary during this interval. To find the optimal delay for triggering each PC after a detection event in one of Alice's POVM outcomes, I placed the PC between anti-crossed polarizers and counted coincidences between the output of the PC setup and Alice's detectors as I scanned the triggering delay. This figure shows two such scans, of coincidence counts versus the delay imparted by the Stanford Research Systems delay generator before triggering the second PC (Z), at a voltage setting of 467 on the voltage dial or ≈ 1.027 kV. The other PC was off during this scan. The error bars are given by the square root of the number of photons counted, and the grey line is meant only to guide the eye. The data in the left graph shows the full triggering period of the Pockels cell, and was taken on April 21, 2009, while the right graph shows a different scan intended to zoom in and isolate the ringing effect, and was taken on April 27. Based on the results of the right scan and another more detailed scan I set the delay to 28.1 ns.

Determining the correct delay should have been a simple matter, in the same configura-

tion just described, of scanning the delay[10] between the detection of a signal photon and the triggering of the PC, and searching for the minimum coincidence rate as a function of delay. According to my chosen settings for the splitter box triggering the push-pull circuit, the HV should ideally have been applied across the PCs for a window of approximately 20 ns after being triggered, thus yielding some freedom in the delay setting. However, in practice I found that the coincidence rate varied significantly during this window. I attribute this to some ringing effect in the electronics. Finding the best delay then required carefully scanning the delay in e.g. 0.5 ns steps and counting coincidences for several seconds at each setting in order to determine a delay value for which the HV would consistently be closest to V_π as the idler photon passed through the PC. Two examples of such scans are shown in Fig. 3.6. Using this technique I was able to achieve a contrast ratio through each Pockels cell of nearly 3000:1, measured using coincidence counts.

Because each PC was not mounted with its fast and slow axes perfectly aligned along the $\pm 45°$ directions from the horizontal, and no fine adjustment of this mounting angle was possible, extra waveplates were required to assure that the net operation still corresponded to X (or Z), while still leaving the polarization unchanged when the PC was not triggered. For instance if the fast axis of the first PC were aligned at $45° + 2\delta$, this could be corrected with HWPs at angle δ before and after the PC: $HWP(\delta) \times HWP(45° + 2\delta) \times HWP(\delta) = X$ and $HWP(\delta) \times \mathbb{1} \times HWP(\delta) = \mathbb{1}$, at least up to a global phase on the operation. For the PC meant to perform Z, the same two waveplates could be used to compensate this angular misalignment as were used to perform the Hadamard operations transforming X to Z: $HWP(22.5° + \delta) \times HWP(45° + 2\delta) \times HWP(22.5° + \delta) = Z$.

Solving all three of these problems required multiple iterations, switching between searching for the optimal high voltage setting, delay, and δ for each Pockels cell, in each case by searching for the setting that most effectively minimized coincidence counts when the expected photon polarization after the respective PC was orthogonal to the analyzer setting. However, this iterative search procedure was further complicated by an unanticipated experimental difficulty, which I only understood in retrospect after already having fixed it. Ideally the Jones matrix of a mirror would be the identity: the mirror, while changing the direction of propagation, would do nothing to the polarization state of an incident beam. I knew when building the PC-setup that *dielectric* mirrors often impart a phase between the component of the incident polarization in the plane of reflection and that component perpendicular to said plane. However, I purposefully used silver-surfaced

[10] using a scanning delay generator, Stanford Research Systems model DG535

mirrors in order to avoid this problem, and was under the impression they would impart no such relative phase.

For the first PC, intended to implement X, I found myself unable to attain a combination of δ-correction waveplate angles and HV setting such that the correct unitary was implemented. I tested the PC by inputting the six standard states and performing tomography on the output, and found that when δ and the HV were set such that $|H\rangle$ was rotated to $|V\rangle$ and vice-versa, the setup would impart some rotation to $|D\rangle$ and $|A\rangle$, which should be eigenstates of the X operation. Conversely, if I adjusted the HV such that no net transformation was enacted on $|D\rangle$ and $|A\rangle$, then the setup would not fully rotate $|H\rangle$ to $|V\rangle$ and vice-versa, leaving instead some elliptically-polarized output. Eventually I solved this problem through the introduction of two auxiliary QWPs, one placed before the first mirror and the other after the δ-correction HWP for the X-PC. These auxiliary QWPs, set with their fast axes at 0°, were tilted about their vertical axes such as to introduce equal and opposite relative phase shifts between H- and V-polarizations. These introduced no net transformation of the polarization state when the HV was off, while compensating for what I thought at the time to be an incomplete rotation when the PC was triggered. It was only later that I surmised that these waveplates were actually compensating for relative phase shifts introduced by the reflections from the silver mirrors, and not for a problem with the Pockels cell.

With all the waveplates properly oriented, I found the half-wave voltage V_π for both PCs to correspond to a setting of 467 on the voltage dial on the respective HV power supplies. As this dial is supposed to represent a range of 0 to 2.2 kV, this would imply $V_\pi = 1.027$ kV. However, I never confirmed this value independently.

I finally tested the PCs by inputting all six standard states and performing tomography on the output state for all combinations of neither, either, or both PCs being triggered. For all of these 24 combinations of input states and PC settings, the fidelity of the tomographically reconstructed density matrix with the ideal output state was 0.998 or better, suggesting near perfect operation of the unitary correction apparatus.

3.4 Measuring Polarization-Encoded Photonic Qubits

3.4.1 Von Neumann Measurements

Von Neumann measurements of photon polarization are fairly easy to implement. A PBS cube serves to measure a photon's polarization in the computational basis: photons in the transmitted ports are projected onto $|H\rangle$, whereas those in the reflected port are projected onto $|V\rangle$. A Von Neumann measurement in an arbitrary basis can be accomplished with suitable waveplates before the PBS. While three waveplates in the QHQ formation are necessary to perform an arbitrary unitary, a single HWP and QWP suffice to rotate an arbitrary basis into the computational basis, and therefore a HWP, QWP, and PBS form an arbitrary *polarization analyzer*. Such an analyzer is used to perform the various projections of our photons needed for tomography throughout this thesis.

3.4.2 The POVM Apparatus

Controllable generalized measurements are generally more difficult to implement on photonic qubits. For examples of how some types of generalized measurements have been or could be implemented, see Refs. [65, 66, 67, 68, 69, 70].

The POVM used in my experiments (Eq. (3.1)) was implemented as shown in Fig. 3.2b), and is also shown in more detail as an annotated photograph in Fig. 3.7. It is an interferometer, or rather two interlocking interferometers with one input and four outputs corresponding to the four POVM elements. The optical elements used to separate and recombine the interferometer paths are calcite beam displacers as in Fig. 3.4. Because the two paths exit the first BD parallel, and all the reflecting optics (as well as some of the waveplates) are common to both paths before the recombine in subsequent BDs, such a configuration is inherently phase-stable; in fact, like the Sagnac configuration of the entangled photon source, it is insensitive to all mechanical displacements except rotations [71]. This negates the need for active stabilization, thus reducing experimental complexity and/or increasing operation fidelity for longer measurement periods compared to many other implementations of generalized measurements e.g. Refs. [68, 70].

The operation of the POVM apparatus can be explained as follows. The reader may find it helpful to follow Fig. 3.2b), beginning at the first BD. Consider an arbitrary pure input qubit state, expressed without loss of generality as $\alpha|H\rangle + \beta|V\rangle$. The first BD

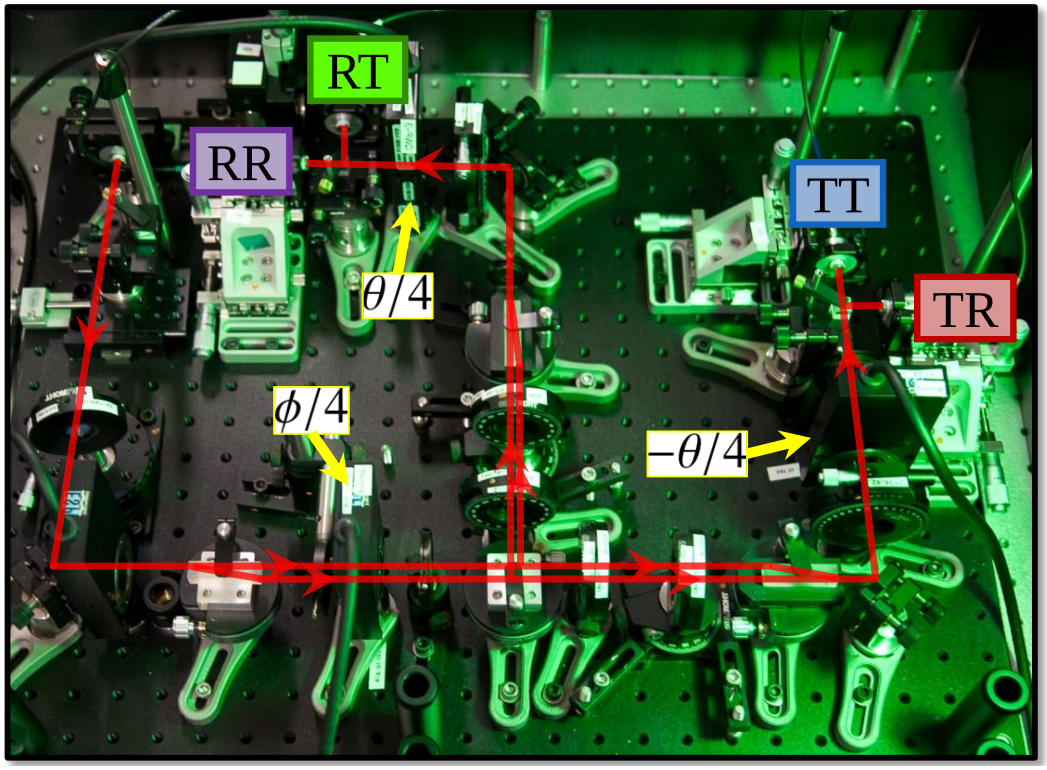


Figure 3.7: Annotated photograph of the POVM apparatus. The annotations label the four outputs (discussed in the text) and the waveplates used to set the angles ϕ and θ defining the POVM.

separates the polarization components of this state into two different paths, which I'll refer to as U for the upper path in the figure and L for the lower path. The resulting state is then entangled:

$$\alpha\,|H\rangle + \beta\,|V\rangle \xrightarrow{BD} \alpha(|H\rangle \otimes |U\rangle) + \beta(|V\rangle \otimes |L\rangle). \tag{3.15}$$

The two paths then pass through a HWP at angle $\phi/4$ and a PBS cube; the result is to project the polarization state of the light transmitted through the PBS cube (in both paths) onto $\cos(\phi/2)\,|H\rangle + \sin(\phi/2)\,|V\rangle$, and the reflected light onto the orthogonal state $\sin(\phi/2)\,|H\rangle - \cos(\phi/2)\,|V\rangle$. This can be viewed as a projective measurement on the polarization subspace of the combined polarization-path Hilbert space.

The next waveplates to be encountered, along with the the recombination BDs in each arm, serve to transfer the 'path' qubit back into polarization encoding such that it might also be measured. In the transmitted (reflected) arm, a HWP at 45° in the U (L) path serves to rotate the polarization from H to V (V to H). The waveplate in the other path is a HWP at 0° which serves to equalize the optical path lengths of the U and L paths, and can be tilted around its vertical axis to implement an arbitrary waveplate unitary (see Eq. (3.9)), and thereby adjust the relative phase of the U and L paths. The phase introduced between the U and L paths, in each arm, should be $e^{i\pi/2}$ (mod 2π of course).

The two paths, now with orthogonal polarizations and the proper relative phase, are then coherently recombined in BDs. The net result is to map $|U\rangle \mapsto |V\rangle$ and $|L\rangle \mapsto i\,|H\rangle$ in the transmitted arm, and $|U\rangle \mapsto |H\rangle$ and $|L\rangle \mapsto i\,|V\rangle$ in the reflected arm. The path qubit, now mapped into polarization, then passes through a QWP at 45°, a HWP at angle $-\theta/4$ ($+\theta/4$ in the reflected arm), and another PBS cube. This projects the state in the transmitted arm onto $\frac{1}{\sqrt{2}}\left(|H\rangle \pm ie^{i\theta}\,|V\rangle\right)$, and that in the reflected arm onto $\frac{1}{\sqrt{2}}\left(|H\rangle \pm ie^{-i\theta}\,|V\rangle\right)$, where in both cases the '+' outcome is transmitted, and the '−' outcome reflected. Each of these four outcomes is then collected into single-mode fibers to be transported to detectors.

The net result of the entire apparatus described above is that the light which is (T)ransmitted at the first PBS and (R)eflected at the second has been projected onto the state $\rho^*(\phi,\theta)$, where $\rho = |\psi\rangle\langle\psi|$ and $|\psi(\phi,\theta)\rangle = \cos(\phi/2)\,|H\rangle + e^{i\theta}\sin(\phi/2)\,|V\rangle$ describes an arbitrary pure state with spherical angles ϕ and θ in the Bloch sphere representation (see sec. 2.1.1.1). I refer to this outcome as TR. This is the element E_{00} of the POVM $\{E_{ab}\}$ which the apparatus was intended to implement, and furthermore outcomes TT, RT, and RR correspond respectively to E_{01}, E_{10}, and E_{11}, as desired.

3.4.2.1 Aligning the POVM apparatus

This short section is intended primarily for the benefit of anyone who may wish to use the POVM apparatus for further experiments in the future. The POVM apparatus described above can be aligned using a fiber-coupled 808 nm diode laser, an 'input PBS' which is set on a translation stage near the input fiber-collimator so as to be removable (shown in Fig. 3.7 but not Fig. 3.2), the 'input HWP' which is shown before the first BD in Fig. 3.2c), and a photodiode. For the latter I used the NewFocus model 2107 photodiode, along with the LabView program "observe_interference_live.vi", written by Rainer Kaltenbaek, which shows the output signal on a computer and calculates the visibility of interference fringes in real time. A fiber-coupled source of broadband near-infrared light is also helpful, e.g. from a sufficiently-attenuated mode-locked titanium-sapphire laser emitting 10 to 15 nm of bandwidth centered at 790 or 800 nm.

To align the apparatus, first all the optics must be properly placed, the waveplates set to the correct angles, and the input and output fiber-couplers properly aligned. In my usual procedure, I then input the light from the Ti:sapphire laser if available, or if not then the light from the diode laser. With the H-polarizing input PBS in place, and the 'input HWP' and the 'ϕ-HWP' both set to 22.5°, one should in theory be able to detect interference fringes of 100% visibility in any of the four output ports as the 'tilting' HWP in the respective arm is turned, thereby changing the relative phase upon path recombination in the second BD. The angle of the θ-HWP should not affect this visibility, but in fact it is a good idea to check the interference visibility both when this waveplate is set to 0° and when it is set to 22.5°. The interference visibility can then be adjusted by rotating of the recombination BD, primarily about the vertical axis, so as to equalize the interferometric path lengths; this should be done with the 'tilting' HWPs near normal incidence. This task is much easier with the broader-bandwith Ti:sapphire light, as the interference visibility falls off more quickly for unequal path lengths with this higher input bandwidth. Using this technique I was able to obtain interference visibilities of 99.8% or better in both arms, as measured using the photodiode and LabView program mentioned above.

The final task is to set the correct recombination phase using the 'tilting' HWPs. For the transmitted arm, this is done by minimizing the optical power in the TT output with the input HWP, ϕ-HWP, and θ-HWP respectively set to 22.5°, 22.5°, and 0°. For the reflected arm, the RT output should be minimized with the input HWP, ϕ-HWP, and θ-HWP respectively set to -22.5°, 22.5°, and 0°. I prefer to minimize the outcomes transmitted at the final PBSs, instead of reflected, because there is some small leakage

of H-polarized light into the reflected output ports in these PBS cubes. For both these mimizations, it is best to turn up the gain on the photodiode to its highest setting.

3.4.3 Detection and Logic

Once projected onto the desired output state, either by the POVM apparatus or by the polarization analyzer after the Pockels cells, the photons must then be detected. In the experiments in this thesis, this is accomplished by first collecting the photons into single-mode fibers, which in turn transport the photons to single photon detectors, specifically PerkinElmer four-channel SPCM-AQ4C modules. Each of these contains four separate fiber-coupled silicon avalanche photodiodes; when a photon is absorbed in the diode a 25 ns electronic TTL pulse is produced which can in turn be manipulated with further electronics or detected by e.g. an oscilloscope or computer.

These detectors are each specified to have a quantum efficiency between 45% and 50% at 810 nm and a maximum dead time of 50 ns after a detection event, during which further incident photons will not generate an output pulse [72]. The detectors used in these experiments were measured to have dark count rates ranging from 100 to 500 counts per second, defined as the rate at which they output signals when on, but with their optical inputs blocked.

For the experiments in this thesis and in fact most quantum information experiments with single photons as qubits, it is important to identify those detection events corresponding to pairs from SPDC, as opposed to those from dark counts or ambient light. Furthermore, in order for our experimental protocols to have succeeded, the photons from a shared entangled pair must have been measured both in the POVM and in the analyzer following the Pockels cells. These purposes are accomplished by including in the final data analysis only those detection events which form coincidence counts. By a coincidence count, I mean an incidence where two detection events, one in a POVM output detector and one in the detector for the analyzer following the Pockels cells, occur simultaneously to within a narrow time window. The coincidence window used in this thesis is approximately 5 ns. Our coincidence-logic box, like most of the other classical TTL logic used in these experiments, was custom-built by Zhenwen Wang of the University of Waterloo Science Technical Services.

Before being directed to the coincidence-logic box, the outputs from the four POVM-outcome detectors are first copied so that their individual rates can be recorded, and so

that they can be used to trigger the Pockels cells. A logical OR operation is then applied between the pulses stemming from the RT and RR outcomes, and the resulting signal is used to trigger the X-implementing Pockels cell. A logical OR operation between the TT and RR outcomes generates the signal which triggers the Z-performing Pockels cell. As described in sec. 3.3.3.1, the correct delay must be applied to each signal before it triggers the PCs.

The idler photons are stored in a 50 m fiber loop before entering the unitary correction apparatus in order to allow time for the POVM, logical processing of the outcome, and triggering of the Pockels cells. Of course, this means that photons from the same SPDC pair do not actually produce simultaneous detection events. Instead, the signals from the POVM detectors must be electronically delayed such that they arrive at the coincidence-logic box simultaneously with the detector signal from the idler photon, which has experienced a much longer optical path prior to detection.

3.5 Integration of Experimental Components, Data Acquisition, and Analysis

Once the source of entangled photon pairs, the setup for unitary corrections and output analysis, and the POVM apparatus had all been individually aligned, it was necessary to connect the output fibers from the source to the inputs of the other two apparatuses, and ensure that the proper entangled state was being transmitted for the experimental protocols. This was accomplished via a set of fiber polarization controllers, known to optics experimentalists as 'bat-ears,' in each of the fibers leading from the source to the other two apparatuses. These were used to ensure a joint input state into the POVM apparatus and unitary correction setup of $\frac{1}{\sqrt{2}}(|H_s H_i\rangle + e^{i\zeta}|V_s V_i\rangle)$. A phase-plate, consisting of a QWP at 0° capable of tilting around the vertical axis, is placed following the input fiber-coupler to the POVM apparatus and was used to adjust the phase ζ to π. The resulting $|\Phi^-\rangle$ state was then analyzed via two-photon tomography, as discussed in sec. 3.2.1.1, using the polarization analyzer after the Pockels cells for the idler photon (with the Pockels cells switched off) and the 'input' HWP and QWP shown before the first BD in the POVM apparatus in Fig. 3.2b). When not in use for tomography, the 'input' QWP was removed and the HWP set to 0°, thereby performing a Z operation on the signal photon and transforming the $|\Phi^-\rangle$ state to $|\Phi^+\rangle$, as required for the protocols illustrated in Fig. 3.1.

LabView software written by Rainer Kaltenbaek was used to control the settings of the ϕ- and θ-waveplates in the POVM apparatus, as well as the analyzer HWP and QWP following the unitary correction setup. For each desired POVM setting $\{\phi, \theta\}$, this software set those waveplates to the required angles, then projected the output of the unitary correction apparatus onto all six standard states sequentially, recorded the coincidence events between this detector and any of the four POVM detectors, and automatically performed maximum-likelihood tomographic analysis on the resulting dataset. The counts and the the tomographically-reconstructed density matrices were recorded in a text file where they could be used for further data analysis.

3.5.1 Problems due to Temperature Variation

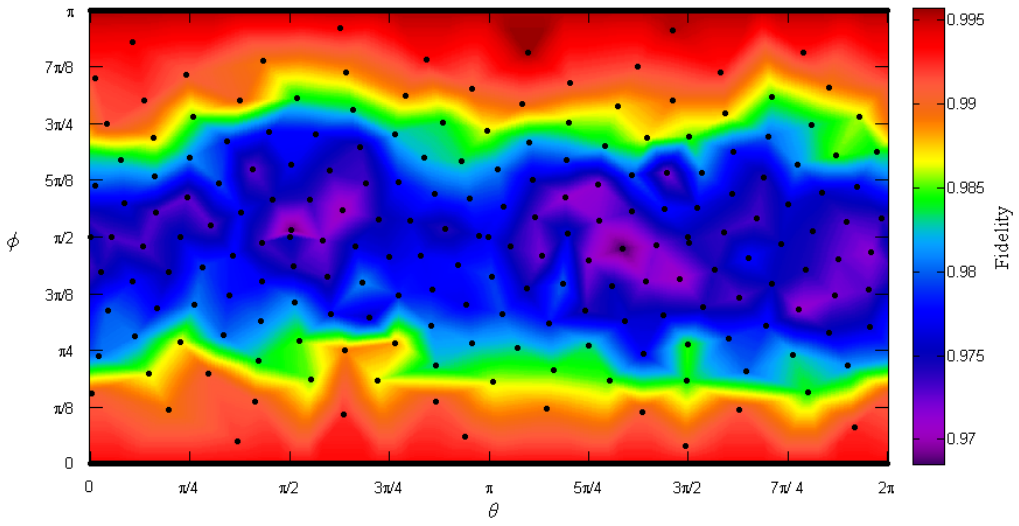


Figure 3.8: Fidelity of the experimental protocol as a function of the settings ϕ and θ of the POVM apparatus. These should ideally be the polar and azimuthal angle of the output state. Note that this data was not taken with the Sagnac source described above, but rather with a different source constructed by Kurt Schreiter and Aron Pasieka and modeled after Ref. [73]. The entire top and bottom lines of the graph correspond respectively to the same ideal output state, the 'South pole' and 'North pole' of the Bloch sphere respectively. The black dots represent the settings for which data was taken. The coloring of the rest of the plane was achieved via numerical interpolation between the results at these 206 points.

An example of some results obtained using the POVM apparatus and unitary correction setup is shown in Fig. 3.8. Note that this data was in fact taken with a different source of entangled photons than the one described in sec. 3.2.1.1, built by Kurt Schreiter and Aron Pasieka and modeled after Ref. [73]. However, this source was used with the POVM apparatus and unitary correction setup in exactly the manner described above.

The data shows the fidelity between the tomographically reconstructed output state and the output of the ideal protocol as a function of the polar angle ϕ and the azimuthal angle θ of the ideal output in the Bloch sphere representation. Note that the top and bottom of the graph respectively correspond to the 'South pole' and 'North pole' of Bloch sphere, and thus each represent only one distinct state. The coloring of the plane, representing fidelity, was obtained by interpolating between the fidelity values obtained for 206 different measured output states, represented in the figure as black circles. Note that these are the same 206 sets of settings $\{\phi, \theta\}$ as measured to produce Fig. 4.4, and the interpolation was accomplished using the same methods as well.

Notice that the fidelity is noticeably better near the 'poles' of the Bloch sphere than near the 'equator', which contains the states with equal superpositions of $|H\rangle$ and $|V\rangle$. This is due in part to the characteristics of this source, which exhibited significantly better correlations in the $|H, V\rangle$ basis than the $|D, A\rangle$ basis. However it is also due in part to variations in the ambient laboratory temperature, which can slightly shift the relative phase of the U and L paths in the POVM apparatus before recombination in the respective beam displacer. For the preparation of states near the 'poles' of the Bloch sphere, i.e. $\phi \approx 0$ or π, this has little effect on the output state, as the measured photon is nearly localized in either the U or L path. However, for states near the 'equator', the measured photon is in a near-equal superposition of these two paths, and the recombination phase significantly affects the output state.

As the lab temperature varied away from the temperature at which the POVM apparatus phases were aligned, this caused a corresponding decrease in the output fidelity of the protocols. This is illustrated in Fig. 3.9, which shows the output fidelity for expected states $\{|\psi(\phi, \theta)\rangle\}$ near the Bloch equator, the output fidelity for states near the Bloch poles, and the ambient laboratory temperature as a function of time. This data was obtained from the results of tomographies on the output for 2060 sets of POVM settings $\{\phi, \theta\}$, taken over a period of nearly two days. Note that not all 2060 output fidelities are included in this figure, but rather only those that fall within $\pi/10$ radians of either the Bloch 'equator' or one of the 'poles.'

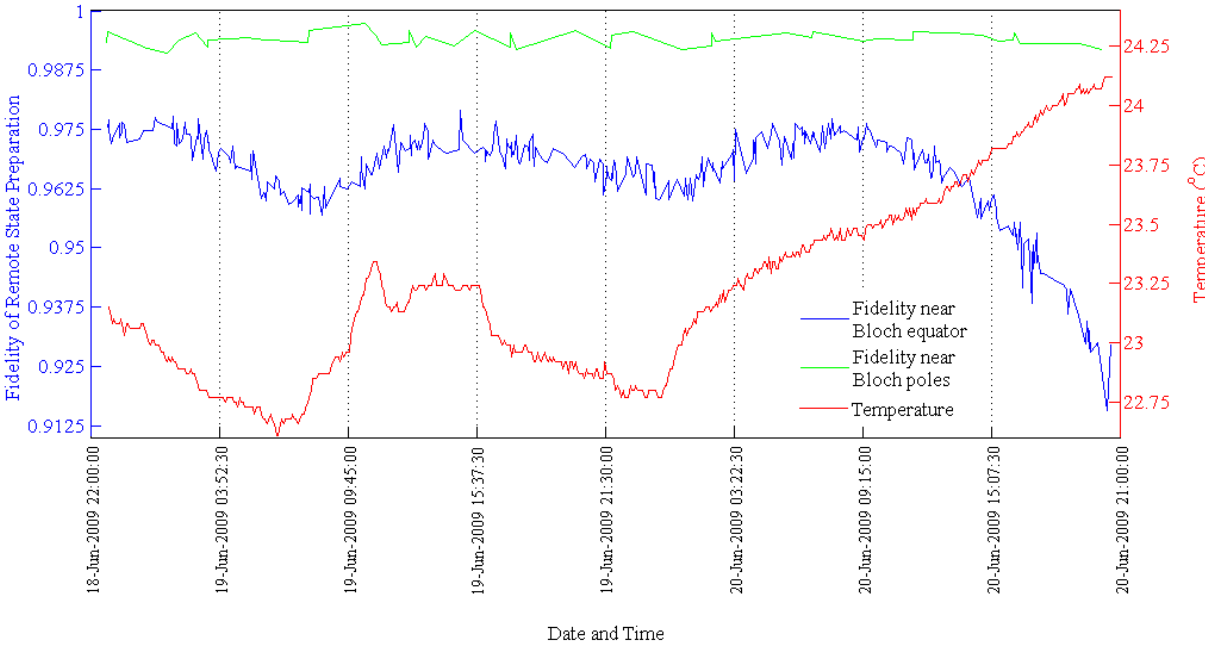


Figure 3.9: Fidelity of the experimental protocol for those settings near the Bloch 'equator' and those near the Bloch 'poles', and ambient laboratory temperature, as a function of time. The green line represents the protocol fidelity for those POVM settings for which the ideal output should have been within $\pi/10$ radians of either the North or South 'pole' of the Bloch sphere. The blue line represents the protocol fidelity for settings with ideal outputs within $\pi/10$ radians of the Bloch 'equator', consisting of states which are near-equal superpositions of $|H\rangle$ and $|V\rangle$. The red line shows the temperature in the laboratory.

The correlations between temperature change and fidelity for states near the 'equator' are illustrated even more starkly in Fig. 3.10, which again shows the output fidelities for states near the Bloch 'equator', but this time also shows the *absolute temperature difference* $|T - T_0|$, where T_0 was the temperature at which the POVM apparatus was aligned. In this case the correlations are clearly visible. In practice, these results meant that, given the usual degree of temperature fluctuations in our laboratory, data could only be taken for approximately four or five hours without the need to re-align the POVM apparatus. However, this window still allows time to perform the protocol and tomographically reconstruct

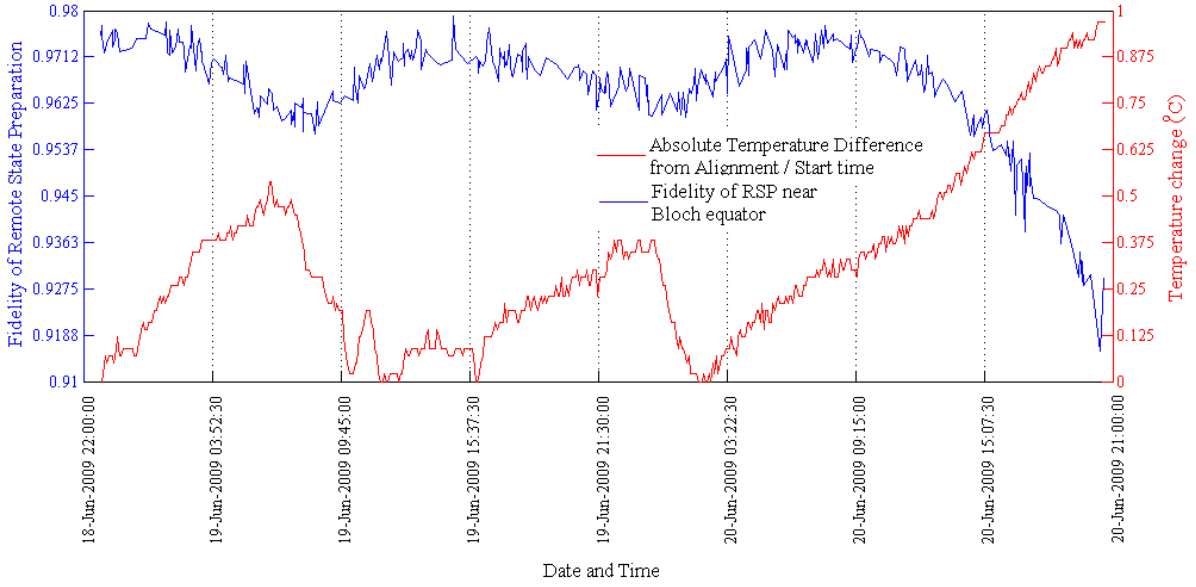


Figure 3.10: Fidelity of the experimental protocol for those settings near the Bloch 'equator', and the absolute difference $|T - T_0|$ between the ambient lab temperature T and the temperature T_0 at the time of POVM alignment, as a function of time. Notice the strong anticorrelations between the absolute temperature difference and the fidelity: the further the temperature deviates from its initial value, the worse the protocol fidelity becomes.

the output for several hundred different sets of settings $\{\phi, \theta\}$.

Chapter 4

Cluster-State Quantum Computing Enhanced by High-Fidelity Generalized Measurements

4.1 Notes and Acknowledgements

The remaining sections of this chapter consist of the following paper, which is currently available on the physics e-print repository the arXiv, and at the time of writing this thesis is in submission for publication:

Devon N. Biggerstaff, Terry Rudolph, Rainer Kaltenbaek, Deny Hamel, Gregor Weihs, and Kevin J. Resch. Cluster-state quantum computation enhanced by high-fidelity generalized measurements. e-print arXiv:quant-ph/0909.2843v1, 2009.

Abstract

We introduce and implement a technique to extend the quantum computational power of cluster states by replacing some projective measurements with generalized quantum measurements (POVMs). As an experimental demonstration we fully realize an arbitrary three-qubit cluster computation by implementing a tunable linear-optical POVM, as well as fast active feedforward, on a two-qubit photonic cluster state. Over 206 different computations, the average output fidelity is 0.9832 ± 0.0002; furthermore the error contribution

from our POVM device and feedforward is only of $O(10^{-3})$, less than some recent thresholds for fault-tolerant cluster computing.

Changes for this Thesis

In order to maintain consistency to the best extent possible with the e-print version and with any eventual published version of this material, the material has not been changed from the version posted online and submitted for publication, with the following exceptions:

- Equations and figures have been re-numbered in line with the remainder of the thesis.
- Figures have been re-sized.
- The references of this chapter have been merged into one bibliography with those of the rest of the thesis, including changes to the numbering and reference style.
- Titles have been given to sections and subsections for clarity of organization and consistency with the remainder of the thesis.
- For the benefit of the reader, references to background material presented earlier in the thesis have been added where appropriate.

Acknowledgement of Contributions by Co-Authors

The material presented in this chapter stems from joint work with collaborators who form the co-authors on the e-print version and that submitted for publication. I take this opportunity to thank each of my co-authors for their work, their help, and their patience with me. The major contributions of each author, including myself, were as follows:

- **I, Devon N. Biggerstaff** constructed the experimental apparatus with the exception of the Sagnac source of polarization-entangled photon pairs (built by Deny Hamel) and the individual (classical) TTL logic components. Furthermore I tested and aligned the apparatus and calculated its expected output as detailed in Ch. 3, analyzed the experimental data, created the figures, wrote the first draft of all the text except for sec. 4.3, and had primary responsibility for the editing process.

- **Terry Rudolph** initially developed the theory for the use of POVM measurements to extend the power of cluster-state quantum computing, wrote the primary draft of the material in sec. 4.3, and provided invaluable help and suggestions with the remainder of the writing and editing process.
- **Rainer Kaltenbaek** wrote all the software for controlling the measurement apparatuses and performing tomographic analysis of the results. In addition he performed initial testing of the Pockels cells, numerically calculated the settings for the set of 200 maximally-spread pure states which we computed (see p. 74), and was an invaluable resource in helping me understand and address experimental problems. Finally he also played a large part in the editing process.
- **Deny Hamel** built the Sagnac source of polarization-entangled photon pairs (see Fig. 4.2a) and helped me to align it and integrate it with the rest of the experiment.
- **Gregor Weihs** helped procure the experimental equipment for the Sagnac source.
- **Kevin J. Resch** Developed the initial design for the POVM apparatus as well as the theory for this specific experimental implementation of Terry's ideas concerning cluster computing and generalized measurements, and supervised all my experimental work, data analysis, and the entire writing and editing process.

4.2 Introduction

Measurement-based (cluster) computation [8, 9, 10] is an attractive alternative to standard circuit-based quantum computing (see sec2.2.2). Instead of requiring multi-qubit gates, which are hard to implement experimentally, cluster computing requires only simple, single-qubit projective measurements (see Sec. 2.2.2-2.2.3). However, the prerequisite is a highly-entangled, multi-qubit cluster state. Thus far, laboratory cluster states [18, 42, 74, 43, 44, 45, 46] have proven difficult to generate and limited in size. In order to make the most of these resources it is thus desirable to find means to extend the computational power of available clusters. Here we introduce one such technique, based on performing Positive Operator-Valued Measures (POVMs, see Sec. 2.1.3.3)[21, 65, 67] on cluster-state qubits instead of standard projective measurements. As an experimental demonstration, we implement this technique to perform a three-qubit cluster computation for state preparation using linear optics and two entangled photons. Our results show the

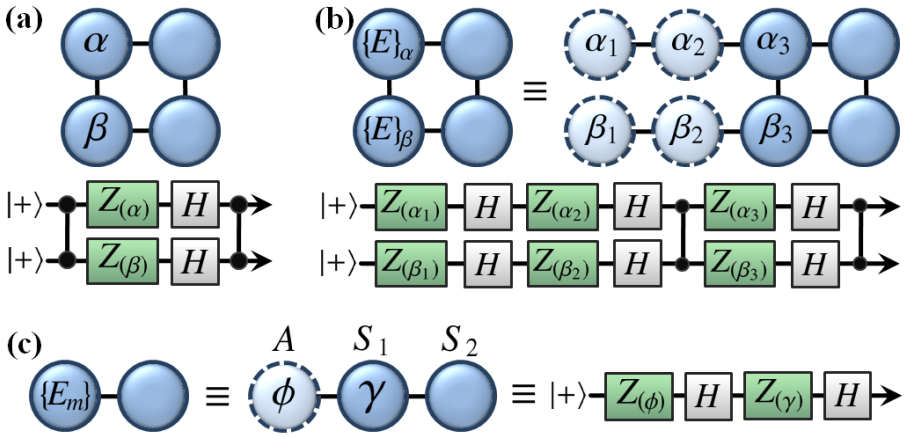


Figure 4.1: Cluster computing with POVMs. (a) A four-qubit 'box' cluster, one of the largest clusters achievable experimentally with optical qubits [18, 42, 74, 43, 44, 45, 46]. By measuring the input cluster qubits and implementing the correct Pauli error correction, one achieves output equivalent to the circuit shown. Note: $\{X, Y, Z\}$: standard Pauli operators; H: Hadamard operator $(X+Z)/\sqrt{2}$; $Z_{(\beta)}$: $\exp(iZ\beta/2)$; α (on a cluster qubit): measurement in $|\alpha_\pm\rangle = |0\rangle \pm \exp(i\alpha)\,|1\rangle$. (b) A larger computation, and equivalent circuit, achievable via implementing POVMs on each input qubit of the same 'box' cluster. Cluster qubits with dashed outlines represent 'virtual' qubits simulated by performing POVMs $\{E\}_\alpha$ and $\{E\}_\beta$. (c) The computation we perform experimentally. By performing the POVM $\{E_m\}$ on the input qubit to our two-qubit cluster, we realize a three-qubit linear cluster computation, which in turn corresponds to a circuit for arbitrary pure state preparation via successive rotations of $|+\rangle$ around the z and x axes.

error introduced by the POVM apparatus and subsequent feedforward to be of $O(10^{-3})$, suggesting operation within recent thresholds for fault-tolerant cluster quantum computing [48].

4.3 Theory

Every POVM can be implemented by interacting an ancilla with the system to be measured, and performing projective measurement(s) on the combined Hilbert space [21] (see p. 13). Consider using the controlled-Z (CZ) operation (the interaction) to attach a new

small cluster (the ancilla) to a qubit S (the system) in a cluster to be used for computation. By then performing single-qubit projective measurements on the ancillary cluster and S, we implement a POVM on S. For cluster computation, it matters only that the correct POVM is implemented; the manner in which this is accomplished is immaterial. In particular it may not be necessary to perform the (often technically challenging) task of interacting S with ancillary physical systems; the same POVM can be implemented using additional degrees of freedom of the qubit itself [75, 76], which are readily available in many architectures. For the photonic polarization qubits considered herein, one can employ an additional spatial-mode degree of freedom to implement an arbitrary 4-outcome POVM, and all single-qubit POVMs can be obtained by suitable (classical) processing of such a POVM [75].

As a specific example, consider the 4-qubit box cluster [18], and equivalent circuit, shown in Fig. 4.1a). By performing POVMs on each of the first two qubits, one can effectively add 'virtual' qubits, thereby simulating a larger circuit, as shown in Fig. 4.1b).

Our approach differs fundamentally from recent experiments employing hyperentangled photon pairs for cluster computing [46, 44]. In contrast to those works, our method can replace arbitrarily large pieces of cluster, and avoids the complications of sources producing particles entangled in multiple degrees of freedom. Furthermore our technique incorporates perfect automatic feedforward in the 'virtual' qubits, and is sufficiently versatile to serve as a useful primitive for large-scale cluster computers: POVMs (including those performed herein) can be applied, without modification, towards enhancing the computational power of *any* given cluster.

Before addressing the specifics of implementing an optical POVM to simplify cluster computations, let us mention some other closely related quantum information processing tasks. The ability to perform an arbitrary POVM on one qubit from a (not necessarily maximally) entangled pair constitutes the basic primitive of quantum steering [1, 77], which underlies the optimal cheating attacks [27, 78] on generalizations of the BB84 two-party bit commitment protocol. It also underlies the procedure for achieving maximum disturbance-free control [79], a basic primitive of quantum cryptography.

As a demonstration of our technique, consider the computation in Fig. 4.1c). We employ the smallest non-trivial cluster of two qubits; as depicted, a POVM on the first qubit allows a three-qubit computation. We label the ancillary qubit A and the system qubits S_1 and S_2. In the manner of a standard cluster computation, we imagine A is initially in the state $|+\rangle_A$, is bonded to S_1 via a CZ gate CZ_{S_1A}, and is then projected into the basis

$|\phi_\pm\rangle = |0\rangle \pm e^{i\phi}|1\rangle$. Depending on the sign of the outcome (+ or −), qubit S_1 must subsequently be projected into either $|\gamma_\pm\rangle$ or $X|\gamma_\pm\rangle$, respectively. These measurements are equivalent to the 4 projectors $\Pi_{ab}^{S_1A} = Z^a|\phi_+\rangle_A\langle\phi_+|Z^a \otimes X^aZ^b|\gamma_+\rangle_{S_1}\langle\gamma_+|Z^bX^a$, where $a, b \in \{0, 1\}$. We can represent this process as a POVM on S_1 as:

$$E_{ab}^{S_1} = \langle +_A|CZ_{S_1A}\Pi_{ab}^{S_1A}CZ_{S_1A}|+_A\rangle. \tag{4.1}$$

As can be readily verified, the POVM elements are $\{E_m\} = \frac{1}{2}\left\{\sigma_m|\chi\rangle\langle\chi|\sigma_m^\dagger\right\}$, where we use the index $m = 1, ..4$, $|\chi(\phi,\gamma)\rangle = \cos(\phi/2)|0\rangle - ie^{i\gamma}\sin(\phi/2)|1\rangle$, and $\sigma_m \in \{\mathbb{1}, X, XZ, Z\}$.

The cluster model requires active feedforward in order to drive deterministic quantum computations despite inherently random measurement outcomes [80, 74]. When using POVMs on cluster qubits, the required feedforward depends on the measurement outcome: after performing POVM $\{E_m\}$ on S_1 and obtaining outcome m, the operator σ_m must be applied to the output qubit S_2 in order to recover the outcome of the circuit in Fig. 4.1c).

4.4 Experimental Implementation

In our experiment we begin with photons in the Bell state $|\Phi^+\rangle_{S_1S_2}$, where $|\Phi^\pm\rangle = |HH\rangle \pm |VV\rangle$, and H and V indicate horizontal and vertical polarization, our $|0\rangle$ and $|1\rangle$, respectively. $|\Phi^+\rangle$ differs from a 2-qubit cluster by a Hadamard on one photon. We make a convenient adjustment of our second measurement angle so as to implement the POVM:

$$\{\mathcal{E}_n(\phi,\,\theta)\} = \frac{1}{2}\{Z\rho^*Z,\,\rho^*,\,X\rho^*X,\,XZ\rho^*ZX\}, \tag{4.2}$$

where $\rho = |\psi\rangle\langle\psi|$, and $|\psi(\phi,\,\theta)\rangle = \cos(\phi/2)|H\rangle + e^{i\theta}\sin(\phi/2)|V\rangle$. After performing $\{\mathcal{E}_n\}$ on photon S_1 from our actual two-photon state $|\Phi^+\rangle_{S_1S_2}$, obtaining outcome n, and implementing $\sigma_n \in \{Z, \mathbb{1}, X, XZ\}$ on S_2, the output will be state $|\psi(\phi,\theta)\rangle$, where ϕ and θ are adjustable experimental parameters which respectively correspond to the polar and azimuthal angle of the output in the Bloch sphere representation (see Sec. 2.1.1.1).

We generate entangled photons as shown in Fig. 4.2a) [54, 55] (see sec. 3.2.1.1). A grating-stabilized diode laser outputs 0.86 mW at 404.5 nm to bi-directionally pump a 25 mm periodically-poled $KTiOPO_4$ (PPKTP) crystal in a polarization-dependent Sagnac interferometer, yielding 809 nm entangled photons via type-II parametric downconversion. At this power, the SMFs typically output singles (coincidence) rates of 150 (30) kHz. Polarization controllers (bat-ears) in the SMFs ensure the output is $|\Phi^+\rangle$.

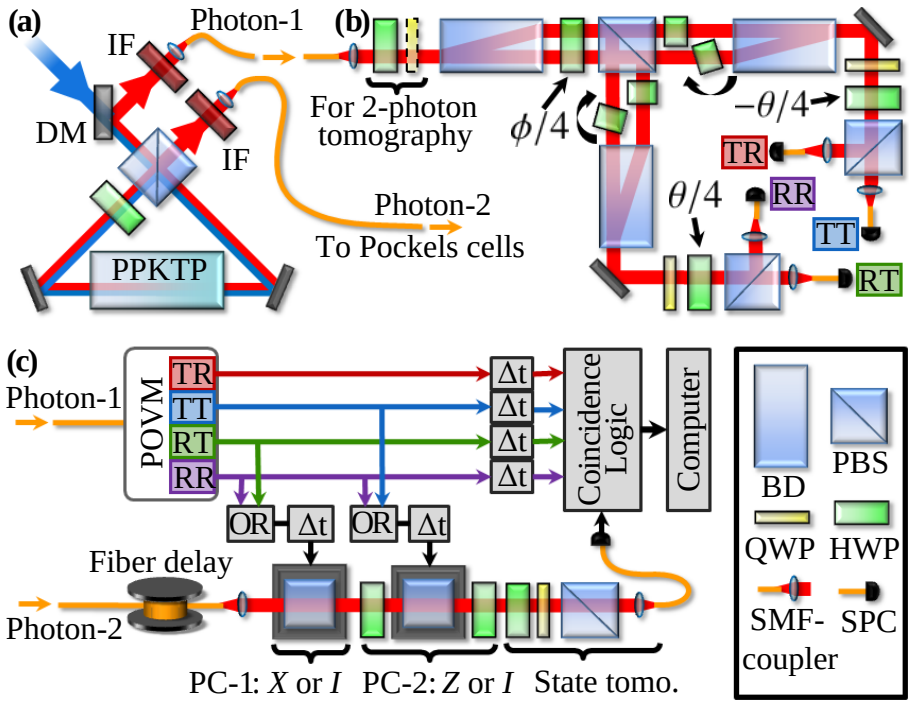


Figure 4.2: Experimental implementation of cluster-state computing with a POVM. a) A source [54, 55] produces maximally-entangled photon pairs coupled into single-mode fiber (SMF). b) The POVM is based on an optical interferometer constructed using calcite beam-displacers (BDs), which couple the polarization of the photon to the path, thereby enlarging the state space for the generalized measurement. Details are given in the text. c) Schematic of the cluster-state quantum computer. Photon-1 is measured in the POVM. Two Pockels cells (PCs), each fired dependent on the measurement outcome, actively perform the required correction of Pauli errors. A 50 m SMF serves to delay Photon-2, allowing time to trigger the PCs. The computational output is analyzed using quantum state tomography. Note: DM: dichroic mirror; IF: blocking and interference filter; PBS: polarizing beamsplitter; H(Q)WP: half (quarter) wave-plate; SPCM: fiber-coupled single-photon counting module.

The apparatus for performing the POVM $\{\mathcal{E}_n\}$ is depicted schematically in Fig. 4.2b) (see sec. 3.4.2). It is a polarization-based double interferometer employing calcite beam displacers (BDs). Due to transverse walk-off, these couple polarization with optical path, enlarging the state space from dimension two to four. The settings $\{\phi, \theta\}$ of the POVM are determined by half-wave plates (HWPs) in the interferometer. Polarization measurements are implemented using polarizing beamsplitters (PBSs). The four output modes are coupled into SMF and detected using single-photon counting modules (SPCMs). The BD construction is inherently phase-stable because the interfering paths propagate through common optics [71]. Furthermore, we align the setup using an 809 nm diode laser injected through the input SMF and a removable polarizing optic, and typically measure classical interference visibilities $> 99.8\%$; thus the setup is promising for high-fidelity, stable operation.

The action of this apparatus can be understood as follows. An arbitrary input qubit is in state $a\,|H\rangle + b\,|V\rangle$. The first BD displaces the H- relative to the V-component, introducing a 'path qubit' with basis states upper $|U\rangle$ and lower $|L\rangle$, and thereby creating the entangled state $a\,|HU\rangle + b\,|VL\rangle$. The polarization qubit is then measured using a HWP at angle $\phi/4$ and a PBS. HWPs at 45° then flip the polarization in path U (L) in the transmitted (reflected) arm. HWPs at 0° are included in the other path to balance path-lengths, and allow the phase to be adjusted via tilting about their vertical axes. Recombining the paths at subsequent BDs converts the 'path' qubit back to polarization; this qubit is then measured via a QWP at 45°, a HWP at $-\theta/4$ ($+\theta/4$), and a PBS in the transmitted (reflected) arm. This yields the POVM elements $\{\mathcal{E}_n\}$ as follows: The outcome TR which stems from (T)ransmission at the first PBS and (R)eflection at the second then corresponds to $\rho^*(\phi, \theta)/2$, and the TT, RT and RR outcomes to $Z\rho^*Z/2$, $X\rho^*X/2$, and $XZ\rho^*ZX/2$, respectively.

We implement the necessary feedforward using two fast $RbTiOPO_4$ (RTP) Pockels cells (PCs) (Leysop RTP4-20-AR800), able to switch to their half-wave voltage of 1.027 kV in < 5 ns, both oriented such as to enact an X operation (i.e. a HWP at 45°) when triggered. The first PC will be triggered by POVM outcomes RT or RR; the second is surrounded by HWPs which rotate its action to Z, and is triggered by outcomes TT or RR. Photon-2 is stored in a 50m SMF for 250 ns of delay to allow ample time for detection, logic, and triggering the PCs. Note that one stage of feedforward is incorporated directly into the design of the POVM since the angle of the last HWP is dependent on the outcome of the polarization measurement. This reduces experimental cost and complexity, as we require

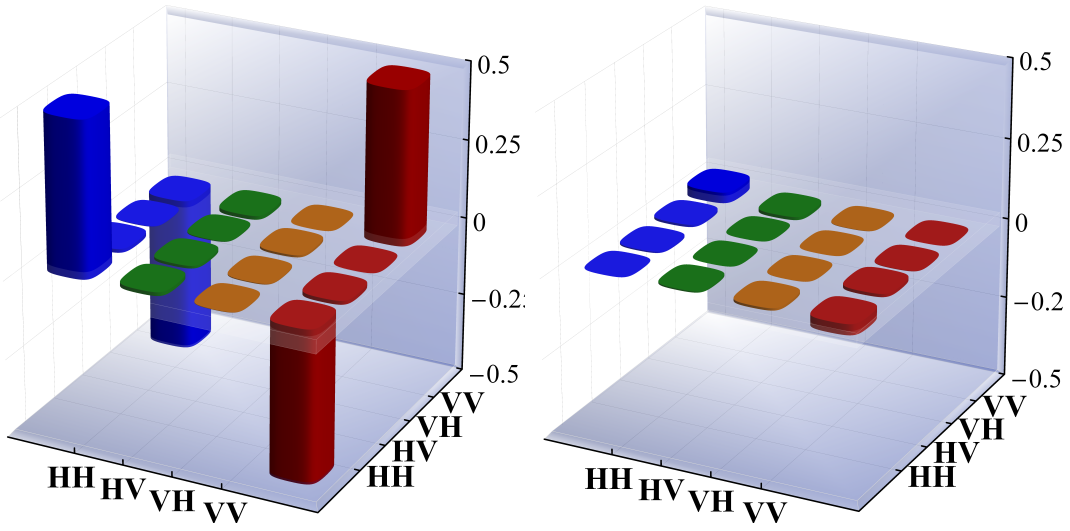


Figure 4.3: Experimentally reconstructed density matrix $\rho_{S_1S_2}$of our two-photon cluster state: real part (left) and imaginary part (right). The fidelity with the ideal state $|\Phi^-\rangle$ is $F = 0.980 \pm 0.001$; the tangle is $T = 0.926 \pm 0.002$ and the purity, $\mathrm{Tr}(\rho^2)$, is $P = 0.963 \pm 0.002$ [20, 81].

one less PC over a direct implementation [74]. It also improves computational speed, as each additional PC requires delaying the relevant photon by $O(100)$ns to allow time for detection, logic, and triggering; in our POVM this feedforward requires a mere couple ns of optical path. After correction, we perform state tomography on Photon-2 using a HWP, QWP, PBS, and SPCM. Our raw data consists of coincidence counts between this output and any one of the four POVM outcomes.

4.5 Results and Conclusions

We characterized the entangled state generated in fibers 1 and 2 (see Fig 4.2a) via over-complete state tomography (see sec. 2.1.5). To analyze Photon-1, we employed the first two waveplates in the POVM and the H output of the first BD; the V output was blocked, and the other waveplates set so as to direct all photons to output TT. We then counted coincidences between this output and that of the polarization analyzer following the (switched off) PCs. The density matrix is reconstructed via a maximum-likelihood technique [36], and shown in Fig. 4.3. Our measured state $\rho_{S_1S_2}$ has fidelity $F = 0.980$ with $|\Phi^-\rangle$. When

not in use for tomography, the QWP at the beginning of the POVM is removed and the HWP set to 0°, which maps the $|\Phi^-\rangle$ source state to $|\Phi^+\rangle$.

We tested this cluster computer by performing computations with 206 different measurement settings $\{\theta, \phi\}$ over a period of four hours. The target output states $\{|\psi(\phi, \theta)\rangle\}$ include the six eigenstates of X, Y and Z, and 200 numerically-generated settings designed to be spread evenly over the surface of the Bloch sphere. For each computation, the output density matrix ρ_m is tomographically reconstructed based on coincidence measurements integrated over 8 s for each of six analyzer settings (the eigenstates of X, Y and Z.) We record maximum coincidence rates of about 3 kHz, summed over the four outputs.

Using the reconstructed density matrix $\rho_{S_1S_2}$ (Fig. 4.3), and assuming a perfect POVM and feedforward, we can estimate the output of the computation:

$$\rho_e(\phi, \theta) = \sum_{n=1}^{4} \sigma_n \mathrm{Tr}_1\left[(\mathcal{E}_n \otimes \mathbb{1})\rho_{S_1S_2}(\mathcal{E}_n \otimes \mathbb{1})^\dagger\right] \sigma_n^\dagger. \tag{4.3}$$

Fig. 4.4a) shows the fidelity between ρ_e and the target output $|\psi\rangle$.

Fig. 4.4b) shows the fidelity $F(\rho_m, |\psi\rangle)$ between our measured states and the target outputs. For these 206 computations the mean fidelity is 0.9832 ± 0.0002, where the uncertainty is the standard error in the mean. This compares favorably with the expected mean fidelity $F(\rho_e, |\psi\rangle) = 0.9865 \pm 0.0001$ for the same 206 states. The distribution of $F(\rho_m, |\psi\rangle)$ is largely explained by two factors: expected variance due to the imperfect entangled state, and fluctuations from Poissonian counting statistics, as determined by a Monte Carlo simulation.

We characterize the errors introduced by the POVM and feedforward using the quantity $(1 - F(\rho_e, \rho_m))$, shown in Fig. 4.4c), where F is the mixed-state fidelity [20] (see sec. 2.1.3.2. With a mean error of only $(1 - F) = (1.16 \pm 0.05) \times 10^{-3}$, our results demonstrate remarkable agreement with the model (Fig. 4.4a) based on $\rho_{S_1S_2}$. More importantly, this shows that our POVM and feedforward are very stable and exhibit a low error rate, comparable to some thresholds for fault-tolerant cluster computing [48].

We have shown how POVMs may be employed in cluster quantum computing to increase the computational power of any given cluster. Furthermore we have experimentally demonstrated this technique by fully realizing an arbitrary, high-fidelity three-qubit cluster computation using two photons. Some feedforward steps can be incorporated into the design of the POVM, significantly improving computational speed while reducing experi-

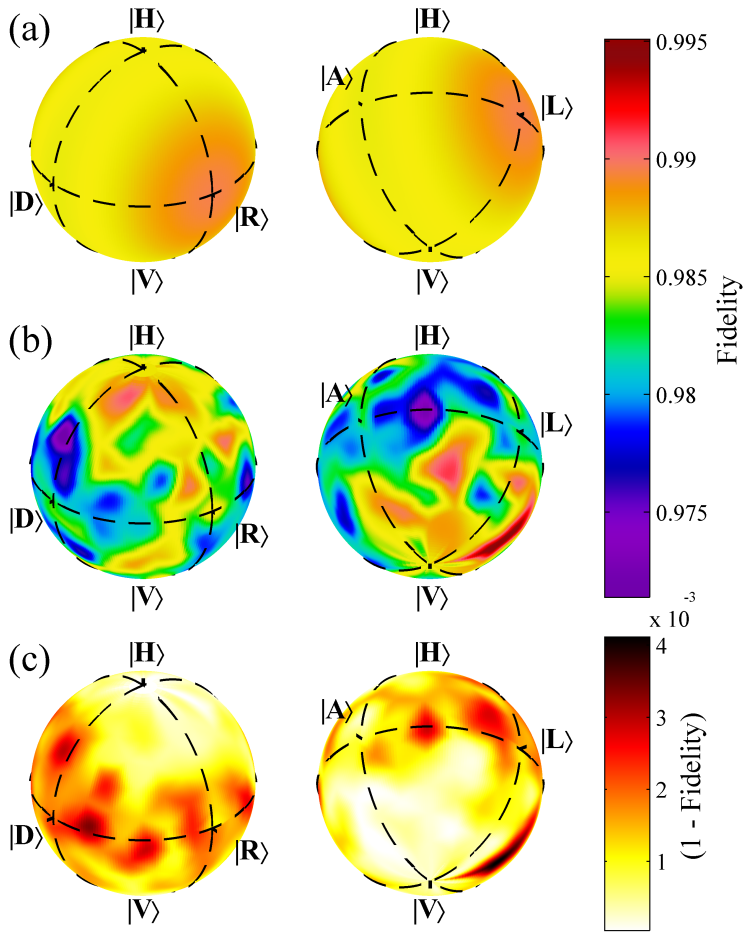


Figure 4.4: (Color) Expected and measured fidelity of computational output. a) The expected output fidelity based on the measured cluster state, $\rho_{S_1S_2}$, assuming perfect POVM operation and feedforward. b) The measured output fidelity with the target outputs; the mean is $F = 0.9832 \pm 0.0002$. c) The deviation from unity of the fidelity between the expected and measured states $1 - F(\rho_e, \rho_m)$; the mean is $(1 - F) = (1.16 \pm 0.05) \times 10^{-3}$. This shows our POVM and feedforward to be operating with very high fidelity.

mental complexity. This technique should be incorporated into future cluster computers to maximize the utility of available resources.

Acknowledgements We thank N. Killoran, N. Lütkenhaus, and K.M. Schreiter for valuable discussions, and Z. Wang for designing and building our TTL logic. D.B. acknowledges financial support from the Mike and Ophelia Lazaridis Fellowship. T.R. acknowledges support from EPSRC and the US Army Research Office. We are grateful for financial support from NSERC, OCE, and CFI.

Chapter 5

Derivation and Experimental Test of Fidelity Benchmarks for Remote Preparation of Arbitrary Quantum States

5.1 Notes and Acknowledgements

The remaining sections of this chapter consists of the following paper, which is currently available on the physics e-print repository the arXiv, and at the time of writing this thesis is in submission for publication:

Nathan Killoran, **Devon N. Biggerstaff**, Rainer Kaltenbaek, Kevin J. Resch, and Norbert Lütkenhaus. Derivation and experimental test of fidelity benchmarks for remote preparation of arbitrary quantum states. e-print arXiv:quant-ph/0909.5461, 2009.

Abstract

Remote state preparation (RSP) is the act of preparing a quantum state at a remote location without actually transmitting the state itself. Using at most two classical bits and a single shared maximally entangled state, one can in theory remotely prepare any qubit state with certainty and with perfect fidelity. However, in any experimental implementation

the average fidelity between the target and output states cannot be perfect. In order for an RSP experiment to demonstrate genuine quantum advantages, it must surpass the optimal threshold of a comparable classical protocol. Here we study the fidelity achievable by RSP protocols lacking shared entanglement, and determine the optimal value for the average fidelity in several different cases. We implement an experimental scheme for deterministic remote preparation of arbitrary photon polarization qubits, preparing 178 different pure and mixed qubit states with an average fidelity of 0.995. Our experimentally-achieved average fidelities surpass our derived classical thresholds whenever the classical protocol does not trivially allow for perfect RSP.

Changes for this Thesis

In order to maintain consistency to the best extent possible with the e-print version and with any eventual published version of this material, the material has not been changed from the version posted online and submitted for publication, with the following exceptions:

- Equations and figures have been re-numbered in line with the remainder of the thesis.
- Figures have been re-sized.
- The references of this chapter have been merged into one bibliography with those of the rest of the thesis, including changes to the numbering and reference style.
- The appendices to the paper have been moved to the end of the thesis, in Appendices A.1 and A.2.
- For the benefit of the reader, references to background material presented earlier in the thesis have been added where appropriate.

Acknowledgement of Contributions by Co-Authors

The material presented in this chapter stems from joint work with collaborators who form the co-authors on the e-print version and that submitted for publication. In particular, my colleague Nathan Killoran is primarily responsible for the theory content of this chapter and is first author on the associated paper, while I was primarily responsible for the experimental content. The material in this chapter will probably form a significant part of

Nathan's Ph.D. dissertation as well. I take this opportunity to thank each of my co-authors for their work, their help, and their patience with me. The major contributions of each author, including myself, were as follows:

- **Nathan Killoran** derived the thresholds for bounds on remote state preparation without shared entanglement, and worked with me to understand our experimental capabilities and try to produce bounds which could be tested and surpassed in the lab (*with* shared entanglement). Furthermore he created some of the figures, wrote the first draft of the paper except sections 5.3.1 and 5.5, and shared responsibility with me for the editing process.

- **I, Devon N. Biggerstaff** constructed the experimental apparatus with the exception of the Sagnac source of polarization-entangled photon pairs (built by Deny Hamel) and the individual (classical) TTL logic components. Furthermore I tested and aligned the apparatus and calculated its expected output as detailed in Ch. 3, analyzed the experimental data, created some of the figures, wrote the first drafts of sections 5.3.1 and 5.5, and shared responsibility with Nathan for the editing process.

- **Rainer Kaltenbaek** wrote all the software for controlling the measurement apparatuses and performing tomographic analysis of the results. In addition he performed initial testing of the Pockels cells and was an invaluable resource in helping me understand and address experimental problems. Finally he also played a large part in the editing process.

- **Kevin J. Resch** Developed the initial design for the POVM apparatus as well as the theory for its implementation in an RSP protocol, and supervised all my experimental work, data analysis, and the writing and editing process.

- **Norbert Lütkenhaus** supervised Nathan's theoretical investigations as well as the writing and editing process.

5.2 Introduction

The field of quantum information processing has revealed many communication and computational protocols which can theoretically outperform their classical counterparts [82, 19].

Among the most famous is quantum teleportation [5], wherein Alice uses pre-shared entanglement and limited forward classical communication to produce an arbitrary unknown quantum state at Bob's location (see sec. 2.1.6). Another example is *remote state preparation* [83, 84] (RSP), a variant of teleportation where Alice has full knowledge of the state she intends to prepare at Bob's location. RSP protocols have several practical applications including forming part of deterministic arbitrary single-photon sources [66] or efficient, high-fidelity quantum repeaters [68].

However, due to the practical limitations of imperfect devices, no RSP experiment can yield remotely-prepared output states which *exactly* match the intended states. Indeed, we should be satisfied when the output states have a high fidelity with the intended states. This raises the question: how high must this fidelity be, on average, for an experiment to demonstrate a genuine quantum advantage? In other words, if we restrict Alice and Bob to a comparable, fixed amount of classical communication—but no shared entanglement—what is the optimal average RSP fidelity they could achieve? It is only when an experiment surpasses such a classical threshold that we can be sure of having demonstrated verifiable advantages to quantum communication.

In several early publications on teleportation, thresholds are given to justify which results are genuinely in the non-classical regime [85, 53, 86, 87]. For example, for the teleportation of qubit states, average fidelities higher than $\frac{2}{3}$ are not possible with only classical resources [88]. To the best of our knowledge, such thresholds have neither been published nor tested for RSP. This paper then has two main objectives: First, we examine the limits on RSP with and without shared entanglement. Dependent on the target states and the allowed communication resources we derive several benchmarks separating genuinely quantum results from those which can be achieved with only classical communication. Second, we report and implement a new, fully-deterministic protocol for the remote preparation of arbitrary photon polarization states with high fidelity. Our protocol relies on generalized measurements (POVMs) and demonstrates several distinct advantages over previous experiments. In comparison with our derived benchmarks, our experimental data surpasses the limits of classical communication in all possible instances.

The remainder of this paper is organized as follows: In section 5.3, we outline the common framework for the RSP protocols examined in this work and flesh out the relevant theory in detail. We describe an entanglement-based protocol which theoretically achieves perfect fidelity between target and output qubit states using two classical bits of communication. We also analyze the optimal strategy in the "classical" case, where no

entanglement is allowed. In section 5.4 we evaluate the optimal classical thresholds and give benchmarks for several choices of pure target state ensembles, including finite, continuous, and mixed state ensembles. Section 5.5 describes our optical RSP experiment and compares our results to both pure and mixed state benchmarks. In section 5.6 we conclude the paper.

5.3 Theory

The goal of remote state preparation is to prepare a quantum state at a distant location, without sending the actual state. Alice, the sending party, knows exactly the target state ρ^{tar} that she wants Bob, the receiving party, to have. Several features are usually desired in an RSP protocol: Bob should need limited or zero knowledge of the state Alice is trying to prepare, and the required communication resources (classical and/or quantum) should be limited. Perhaps most importantly, the protocol should yield output states ρ^{out} at Bob's location which closely match the target states ρ^{tar} which Alice intended to prepare. There is no universally preferred measure for evaluating protocol performance, but in benchmarking situations where we want target and output states to match, the quantum fidelity [20] is a suitable choice, given by

$$F(\sigma,\tau) = \left[\text{Tr}\left(\sqrt{\sqrt{\sigma}\,\tau\sqrt{\sigma}}\right)\right]^2. \tag{5.1}$$

Ideally, the fidelity should be $F(\rho^{\text{tar}},\rho^{\text{out}}) = 1$ for any target state.

In order to make meaningful comparisons, we need a common framework to test the performance of RSP protocols and experiments. We imagine that Alice and Bob are challenged with the following task: Both parties are given full prior knowledge of some fixed ensemble of target states $\{\rho_\alpha^{\text{tar}}, p_\alpha\}$, and may coordinate beforehand on their strategy. To begin, Alice samples from the ensemble and, with probability p_{α_0}, she picks the index α_0. Unlike teleportation, Alice accesses the state *index*, not the state, though she has complete information about the state and may prepare herself a copy if desired. She communicates a message to Bob, sending a limited number c of classical bits (cbits). Bob then prepares an output state $\rho_{\alpha_0}^{\text{out}}$. Their goal is for the output states to match the target states with the highest possible quantum fidelity, on average, i.e. to maximize the quantity

$$\langle F\rangle = \sum_\alpha p_\alpha F(\rho_\alpha^{\text{tar}},\rho_\alpha^{\text{out}}). \tag{5.2}$$

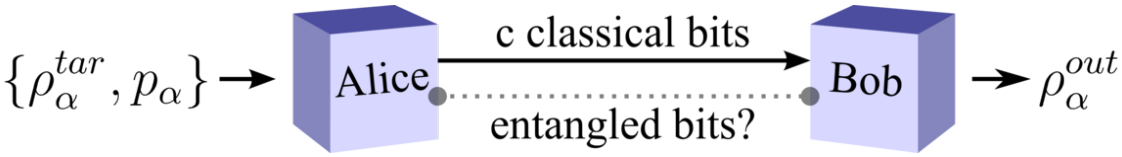


Figure 5.1: Evaluating remote state preparation protocols. Alice samples a state ρ^{tar} from a given distribution of target states and Bob aims to prepare a closely matching state. In classical RSP protocols, Alice may send only a limited number of classical bits to Bob. In quantum RSP protocols, the parties also share some pre-distributed entanglement. Their goal is to maximize $\langle F(\rho^{\text{tar}}, \rho^{\text{out}})\rangle$, the RSP fidelity averaged over the entire target distribution.

We will be considering the situation where the target ensemble consists of a finite number of states as well as that where the target ensemble forms a continuum. In the latter situation, the above sum and probabilities are generalized to an integral and probability densities, respectively.

We are concerned in this work with two types of remote state preparation, which we call the "quantum case" and the "classical case". These labels refer to the communication resources allowed, and not the state prepared, which is always quantum mechanical. In the quantum case, Alice and Bob share a pre-distributed entangled state to help with their task. In the classical case, no initial quantum correlations between Alice and Bob are allowed. In both cases, once a target state has been selected, only c cbits may be sent, and this classical communication is only permitted one way, from Alice to Bob. We will now investigate both of these cases separately.

5.3.1 Quantum RSP

In this section we discuss the abilities and limitations of several quantum RSP protocols and briefly survey previous experimental implementations. We confine the discussion to the remote preparation of qubit states, although some of the results generalize to higher dimensions. In all the protocols discussed, Alice must implement a measurement on her qubit from a shared entangled pair. We term a quantum RSP protocol *deterministic* if the protocol succeeds for every outcome of this measurement. Furthermore we differentiate between those quantum RSP protocols where Alice can prepare any *arbitrary* (pure or

mixed) qubit at Bob's location, and those protocols which require that Bob have some foreknowledge of the state (e.g. that it be from some particular ensemble which forms a proper subset of all possible qubit states). We then present the protocol employed in our experiment, which is deterministic and allows the preparation of arbitrary qubits.

An arbitrary qubit state ρ can be expressed in terms of the 2×2 Pauli matrices:

$$\rho = \frac{\mathbb{1} + \vec{r} \cdot \vec{\sigma}}{2}, \tag{5.3}$$

where $\vec{\sigma} = (X, Y, Z)$ and $\vec{r}$ is the Bloch vector which uniquely identifies the state according to its position in the Bloch sphere. Alternately, the same qubit can be written as

$$\rho(\phi, \theta, r) = r \left|\psi\right\rangle\!\left\langle\psi\right| + (1 - r)(\mathbb{1}/2), \tag{5.4}$$

where

$$\left|\psi(\phi, \theta)\right\rangle = \cos\left(\phi/2\right)\left|0\right\rangle + e^{i\theta} \sin\left(\phi/2\right)\left|1\right\rangle. \tag{5.5}$$

Here ϕ and θ are the polar and azimuthal angles of ρ in the Bloch sphere representation, respectively, and $r = |\vec{r}| = \sqrt{2\left(\mathrm{Tr}\rho^2 - \frac{1}{2}\right)} \in [0, 1]$ is the radius of the state's Bloch vector.

Most RSP (and teleportation) protocols begin with the assumption that Alice and Bob share an initial supply of maximally-entangled qubit pairs, usually one of the Bell states $|\Phi^{\pm}\rangle = \frac{1}{2}(|00\rangle \pm |11\rangle)$ and $|\Psi^{\pm}\rangle = \frac{1}{2}(|01\rangle \pm |10\rangle)$. Shared maximally-entangled pairs are sometimes called ebits (see sec. 2.1.4).

Lo first proved that in the asymptotic (large-N) limit, Alice can deterministically prepare N known pure qubit states from certain (restricted) ensembles at Bob's location using half the classical communication required for the teleportation protocol [83]; Pati [84] provided an explicit deterministic protocol whereby a single pure target qubit state $\rho^{\mathrm{tar}} = |\psi\rangle\langle\psi|$ from such an ensemble can be remotely prepared with only one cbit and one ebit. The basic idea is as follows: Alice and Bob decide beforehand on an ensemble of states consisting of a single great circle on the Bloch sphere, specified by a Bloch vector $\hat{n}$. For each remotely prepared qubit, they share a singlet state $|\Psi^-\rangle$. Alice projects her entangled qubit into the basis $\{|\psi\rangle, |\psi^{\perp}\rangle\}$. If the result is $|\psi^{\perp}\rangle$, Bob's qubit will be in state $|\psi\rangle$ as desired; if Alice's result is $|\psi\rangle$, Alice's transmitted cbit instructs Bob to perform the basis-specific NOT operation on his qubit via rotating by π about the $\hat{n}$ axis, thereby transforming his qubit $|\psi^{\perp}\rangle \mapsto |\psi\rangle$. However, if Alice wishes to remotely prepare an arbitrary pure qubit, not from a pre-specified great circle, Bob cannot reliably flip his qubit when he ends up with $|\psi^{\perp}\rangle$ due to the non-unitarity and thus non-physicality of

a universal-NOT operation [89], and therefore the protocol is non-deterministic with only 50% success probability.

Lo conjectured that two cbits transmitted from Alice to Bob would be necessary and sufficient for the deterministic remote preparation of an arbitrary qubit state with only one ebit [83]. This result was proven in Ref. [90] and, under more general conditions, in Ref. [91]. Many other papers have further investigated the trade-off between required cbits, ebits, and qubits for RSP (see e.g. Refs. [92, 93, 94, 95, 96, 97, 98]).

RSP protocols have been implemented to varying degrees in several experiments employing systems including nuclear magnetic spins [99], coherent superpositions of photonic Fock states [100], atom-photon entanglement [68], and polarization-entangled photon pairs [66, 101, 102, 103, 69, 70]. Among these, most of the employed protocols enabled the preparation of arbitrary pure states with 50% success probability–or alternately, the deterministic preparation of qubits from specific, restricted ensembles. Several also enabled preparation of some mixed states [66, 101, 103], and some allowed control of all three parameters $\{\phi, \theta, r\}$ required to prepare arbitrary pure or mixed states [102, 69]. Earlier, refs. [68, 69] and, while we were preparing this manuscript, [70] successfully implemented a generalized measurement on Alice's qubit which should allow Bob to perform a unitary correction and achieve the desired target state regardless of Alice's measurement outcome. However, in none of these papers is the required unitary actually implemented. To the best of our knowledge we present the first experimental implementation of a *fully deterministic* RSP protocol enabling the preparation of arbitrary (mixed and pure) qubit states.

Note however that in our actual experiment, Bob does not necessarily register a detection event every time that Alice detects a photon. This is due to coupling losses and detector inefficiency, which are unrelated to the efficiency of the RSP protocol itself. These experimental considerations necessitate postselection on coincident detection events between *any* of Alice's four measurement outcomes and Bob's detector. Only if a coincidence occurred can one infer that Alice and Bob shared an entangled pair (ebit), a prerequisite for quantum RSP. This differs from the protocol employed in e.g. Ref [102], which employs postselection to detect the ebit *and* for a specific measurement outcome. In our experiment the postselection is only used to verify a shared ebit, and the protocol then functions deterministically, succeeding for all of Alice's measurement outcomes [74].

Our protocol makes use of the Bell state $|\Phi^+\rangle$ and (at most) two cbits to remotely prepare an arbitrary state $\rho(\phi, \theta, r)$. For any pure state $|\psi\rangle$, the Bell state $|\Phi^+\rangle_{AB}$ can be written as $\frac{1}{2}\sum_{m=1}^{4} \sigma_m^A \sigma_m^B |\psi_A^*\rangle |\psi_B\rangle$, where $|\psi^*(\phi, \theta)\rangle$ is the complex conjugate of $|\psi(\phi, \theta)\rangle$ in

the computational basis, and $\sigma_m^{A(B)} \in \{\mathbb{1}, X, XZ, Z\}$ are Pauli operators acting on Alice's (Bob's) qubit.

First, consider the case where Alice would like to help Bob remotely prepare a pure state $\rho(\phi, \theta) = |\psi\rangle\langle\psi|$. She first performs a generalized measurement on her qubit, specifically a positive operator-valued measure or POVM [19, 65, 67], defined by the elements

$$\{E_m(\phi, \theta)\} = \frac{1}{2}\{\sigma_m |\psi^*\rangle\langle\psi^*| \sigma_m^\dagger\}. \tag{5.6}$$

Dependent on the outcome $m \in \{0, ..., 3\}$ obtained, Bob's qubit will be left in the state $\sigma_m \rho \sigma_m^\dagger$. Alice then encodes the outcome m in two cbits and transmits the resulting message to Bob. By implementing σ_m on his qubit, Bob will deterministically recover ρ.

The generalization of this scheme for preparing arbitrary mixed states is quite straightforward. If Alice sends the same message to Bob regardless of her measurement outcome, his qubit will be left in the maximally mixed state $\frac{1}{2}\mathbb{1}$. In order to remotely prepare an arbitrary state $\rho(\phi, \theta, r)$, Alice performs the same POVM $\{E_m(\phi, \theta)\}$ as she would to prepare the pure state $|\psi(\phi, \theta)\rangle\langle\psi(\phi, \theta)|$. However, she only transmits the correct message encoding the POVM outcome to Bob with probability r. Otherwise she sends a particular message, regardless of the outcome obtained. Thus with probability r Bob's qubit ends up in $|\psi\rangle\langle\psi|$, and with probability $(1 - r)$ he has $\frac{1}{2}\mathbb{1}$, as desired. Due to the unequal distribution of probabilities among the messages, the classical communication cost required to prepare mixed states, as measured by the Shannon entropy [104], will thus be less than for pure states. This cost will range from 0 cbits for preparation of the maximally mixed state to 2 cbits for pure states.[1]

5.3.2 Classical RSP

We now examine the classical case, where Alice and Bob share no entanglement. As our goal is to find the optimal achievable fidelity, we assume in this scenario that Alice and Bob are unencumbered by the imperfections of real-world devices. This assumption is in the spirit of security proofs for quantum key distribution, where any adversary Eve is assumed to be limited only by the laws of physics. It is only by surpassing the limits of this ideal scenario that an experiment can provably demonstrate genuine quantum advantages.

[1] In particular the Shannon entropy of the communication required for preparing a state of purity r will be $H(r) = 2 - \log_2(4 - 3r) + \frac{3r}{4}\log_2\left(\frac{4-3r}{r}\right)$.

Therefore, the one-way classical channel between Alice and Bob is assumed to be perfect, as is Bob's ability to prepare any desired output state.

Although the experiment detailed in Section 5.5 is for qubit states, some of the results in this section hold equally well for states in any finite dimensional Hilbert space. We begin with no assumptions about the dimension except that it is finite, and we will specialize to qubits (dimension 2) when appropriate. Furthermore, we are primarily interested in the case where the target states are pure, $\rho_\alpha^{\text{tar}} = |\psi_\alpha^{\text{tar}}\rangle\langle\psi_\alpha^{\text{tar}}|$, so that the quantum fidelity is equal to the matrix element

$$F(\rho_\alpha^{\text{tar}}, \rho_\alpha^{\text{out}}) = \left\langle \psi_\alpha^{\text{tar}} \right| \rho_\alpha^{\text{out}} \left| \psi_\alpha^{\text{tar}} \right\rangle . \tag{5.7}$$

Accordingly, we assume that the target ensemble consists of pure states $\{|\psi_\alpha^{\text{tar}}\rangle, p_\alpha\}$. In section 5.4 we give benchmarks based on specific choices for this target ensemble.

We now examine the question: what is the optimal RSP strategy when the parties share no quantum correlations, and Alice may only send c cbits to Bob? For every target state $|\psi_\alpha^{\text{tar}}\rangle$, Alice sends a string of c classical bits. We can label all messages of this type by a natural number $m(\alpha) = k \in \{0, 1, ..., 2^c - 1\}$. In general, the message assignment may be either deterministic (e.g. $m(\alpha) = 3$) or probabilistic, i.e. $m(\alpha) = k$ with probability $q_k(\alpha)$, where for each α, $\sum_k q_k(\alpha) = 1$. The probabilistic framework contains all deterministic strategies as special cases. Note that here we use 'deterministic' to refer to Alice's messaging strategy whereas elsewhere it is used to refer to the success probability of the protocol (Sec. 5.3.1); in general our meaning will be clear from the context.

Upon receiving the message k, Bob prepares some output state ρ_k^{out}. A probabilistic messaging strategy would necessarily lead Bob to prepare a *mixed* output state $\rho_{m(\alpha)}^{\text{out}} = \sum_k q_k(\alpha)\rho_k^{\text{out}}$ whenever state $|\psi_\alpha^{\text{tar}}\rangle$ is chosen. Similarly, for a given message k, Bob may change the output state probabilistically. This strategy is naturally incorporated into our framework, where we allow the output states ρ_k^{out} to be mixed.

To determine which choice of output states optimize the average fidelity, we rewrite it

in terms of the 2^c unique messages:

$$\begin{aligned}\langle F\rangle &= \sum_{\alpha} p_\alpha \left\langle \psi_\alpha^{\text{tar}} \right| \rho_{m(\alpha)}^{\text{out}} \left| \psi_\alpha^{\text{tar}} \right\rangle \\ &= \sum_{k=0}^{2^c-1} \sum_{\alpha} p_\alpha q_k(\alpha) \text{Tr}(\left|\psi_\alpha^{\text{tar}}\right\rangle\left\langle\psi_\alpha^{\text{tar}}\right| \rho_k^{\text{out}}) \\ &= \sum_{k=0}^{2^c-1} p_k \text{Tr}(\overline{\rho_k}\rho_k^{\text{out}}) \end{aligned} \tag{5.8}$$

where $p_k = \sum_\alpha p_\alpha q_k(\alpha)$ is the probability of Alice sending message k and

$$\overline{\rho_k} = \frac{1}{p_k} \sum_{\alpha} p_\alpha q_k(\alpha) \left|\psi_\alpha^{\text{tar}}\right\rangle\left\langle\psi_\alpha^{\text{tar}}\right| \tag{5.9}$$

is a weighted average of the states where message k might be sent. When the fidelity is written in this form, two notable features become apparent:

1. For each k, the quantity $\text{Tr}(\overline{\rho_k}\rho_k^{\text{out}})$ is upper bounded by the largest eigenvalue $\lambda_k^{\max}$ of the average state $\overline{\rho_k}$; this can be achieved if Bob outputs the corresponding eigenstate $\rho_k^{\text{out}} = |\lambda_k^{\max}\rangle\langle\lambda_k^{\max}|$. Thus, the optimal output states give

$$\langle F\rangle^{\max} = \sum_{k=0}^{2^c-1} p_k \lambda_k^{\max}. \tag{5.10}$$

2. Since the optimal output states are pure (by point 1), the optimal messaging strategy must, therefore, be deterministic, not probabilistic. In other words, a unique message is sent for each target state. This corresponds to only one $q_k(\alpha)$ being non-zero for each α.

Taking these two points into account greatly simplifies the structure of the fidelity optimization. Because the optimal message assignment is deterministic, the target ensemble is effectively split into 2^c disjoint partitions, depending only on the message $k \in \{0, 1, ..., 2^{c-1}\}$. For each partitioning of the target ensemble, we can also calculate the optimal output state and the resulting fidelity value using Eq. (5.10). All that remains is to determine *which partitioning* maximizes the value of Eq. (5.10). To clarify notation, we will henceforth use k to label both a message and the partition of the target ensemble

consisting of states for which that message is sent. Again, the meaning will be clear from the context.

In principle, for a finite number n of target states, the remaining optimization problem only requires checking the value of Eq. (5.10) for each of the finite number of possible partitionings, which can be done by computer. However the number of possible partitionings scales exponentially in n, rendering this calculation unreasonable for more than about $n = 10$ states. In section 5.4 we outline an algorithm which efficiently provides bounds to Eq. (5.10).

5.3.2.1 Qubits

If the states in question are qubits, we can put Eq. (5.10) into a simple geometric form. When expressed in its eigenbasis, a qubit state takes the form

$$\rho = \frac{1}{2}\begin{bmatrix} 1+r & 0 \\ 0 & 1-r \end{bmatrix} \tag{5.11}$$

where r is the radius of the state's Bloch vector. The largest eigenvector of a qubit is directly related to the radius: $\lambda^{\max} = \frac{1+r}{2}$. For any deterministic partitioning of the target ensemble, we denote the average Bloch vectors by $\vec{r_k} = \frac{1}{p_k}\sum_{\alpha\in k} p_\alpha \vec{r_\alpha}$ and their magnitudes by r_k. We find that the maximal average fidelity for qubits is given by

$$\langle F\rangle^{\max} = \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} p_k r_k\right). \tag{5.12}$$

Hence, for a given deterministic partitioning, the best average fidelity is determined by two sets of quantities: the probabilities p_k of sending each message and the length of the average Bloch vectors $\vec{r_k}$ within each of the 2^c partitions.

In section 5.4, we will outline how to determine which choice of messages, i.e. which partitioning of the target ensemble, maximizes Eq. (5.12).

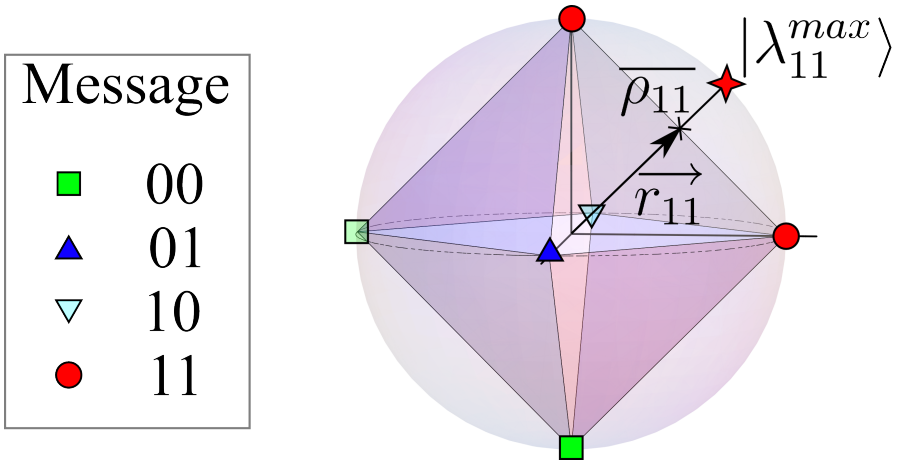


Figure 5.2: Example of a possible classical remote state preparation strategy. The target ensemble consists of the 6 pure states $\{|0\rangle, |1\rangle, \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}\}$ (represented here as the vertices of an octahedron inscribed within the Bloch sphere) with equal probabilities. A possible partitioning strategy is given for the case where two cbits of classical communication are allowed, and the optimal output state for partition 11 is detailed.

5.4 Threshold calculations

5.4.1 Finite ensembles

Assume now that we have fixed a *finite* ensemble of target states $\{\rho_\alpha^{\text{tar}}, p_\alpha\}_{\alpha=1}^n$. It is clear that whenever $n \leq 2^c$, the optimal classical protocol can achieve perfect fidelity since there is sufficient capacity in the message to uniquely label the state. The interesting cases have $n > 2^c$. Given the results of the previous section, the optimum average fidelity can be determined by checking the value of Eq. (5.10) for all partitionings of the n target states into 2^c disjoint subsets, but this can be inefficient even for modest values of n and c. Alternatively, we search for an upper bound on the threshold which is easier to calculate. If an experiment surpasses the upper bound, it has surpassed the actual threshold.

We will now outline an efficient algorithm for determining such upper bounds. For this algorithm, we make the additional assumption that each target state has equal probability to be chosen from the target ensemble. We note that each partition contains some number s of states and contributes one term to the sum in Eq. (5.10). Two different partitions with the same number of states may contribute differently to the average fidelity, depending on

the arrangement of the states. However, for each number $s \in \{0, 1, ..., 2^c - 1\}$, there is a set of s states which yields the maximal possible contribution $\langle F \rangle_s^{\max}$. By using these maximal values in Eq. (5.10) instead of the actual values, we obtain an upper bound on the threshold.

The first step in the algorithm involves checking all partitions of size s to find the maximal contribution $\langle F \rangle_s^{\max}$. Next, we list all the ways in which n elements can be divided into 2^c subsets. The order of the subsets does not matter, so for simplicity we can create our list in order of decreasing partition size. This list forms a table with 2^c columns. For each row i, we have a list of numbers $\{s_{ij}\}_{j=0}^{2^c-1}$ which sum to n. To determine the upper bound, we calculate the quantity

$$\langle F \rangle_i = \sum_{j=0}^{2^c-1} \frac{s_{ij}}{n} \langle F \rangle_{s_{ij}}^{\max}. \tag{5.13}$$

The highest $\langle F \rangle_i$ provides us with an upper bound on the optimal average fidelity.

It may even be the case that the threshold is equal to the upper bound found via the above algorithm, especially if the target ensemble exhibits a high degree of symmetry. To verify this, one would have to find a specific partitioning which leads to the same value as the upper bound. On the other hand, if we can show through other arguments that the highest $\langle F \rangle_i$ is unachievable, then the second highest $\langle F \rangle_i$ provides a new, smaller upper bound. We will make use of both of these points below.

Before proceeding, we pause to discuss the tradeoff between classical and quantum communication resources. The remote state preparation scheme outlined in sections 5.3.1 and 5.5 uses one entangled qubit (ebit) and two cbits sent from Alice to Bob to remotely prepare pure qubit states and less than two cbits for mixed states. A classical analog might limit Alice to sending two cbits to Bob each run. However, it may be argued that to distribute the entangled qubit between Alice and Bob requires at least one use of a quantum channel. A more fair comparison scenario might then allow Alice one use of this quantum channel per run, but only to send classical information. In this scenario, Alice sends three cbits in total. Arguably, this is unnecessary as one could consider the entanglement to be distributed by Bob or by a third party. However, the more cbits Alice is allowed to transmit, the higher the average fidelity the parties can achieve, rendering the benchmark that much harder to surpass in experiment. For completeness and comparison purposes we henceforth consider both the two and three cbit cases.

5.4.1.1 Benchmarks

Thus far no specific target ensemble has been chosen. We now examine several specific ensembles for comparison with experiment. We restrict ourselves to ensembles of pure qubit states with a uniform distribution: $p_i = \frac{1}{n}$. If our goal is to find benchmarks which are low enough to be experimentally surpassed, we should make the classical task as difficult as possible. Given the results above, this is accomplished by choosing ensembles of states which are maximally "spread apart", so that the average Bloch vector within any partition is as small as possible.

An effective choice is to use the vertices of the *Platonic solids* inscribed in the Bloch sphere as the target states. The Platonic solids are the tetrahedron, octahedron, cube, icosahedron, and dodecahedron, with 4, 6, 8, 12, and 20 vertices, respectively. Note that the orientation of these vertices with respect to a Cartesian reference frame does not matter in the classical case, but a specific choice must be made in an experiment. Also note that the tetrahedron states do not provide a surpassable benchmark for $c \geq 2$ because they can be prepared with perfect fidelity simply by assigning a unique message to each of the 4 states. Similarly, for three cbits, the benchmarks yielded by the tetrahedron, octahedron and cube ensembles are all trivially unity. For the other cases, however, we expect fidelity thresholds less than unity.

Indeed, using the algorithm above, we can calculate upper bounds on the remaining thresholds, all of which are less than unity. In fact, for every example studied except for one, the upper bounds were actually equal to the optimal classical thresholds. This was verified by finding explicit partitions such that Eq. (5.10) saturated the upper bounds. The one exception to this statement is the dodecahedron ensemble when $c = 2$. In this case, the upper bound returned by the algorithm would only be possible if we could partition the dodecahedron vertices into four disjoint pentagons. This is geometrically impossible, so we can omit this upper bound. The next highest bound, consisting of partitions of size 6, 5, 5, and 4, is indeed possible. The optimal thresholds and their corresponding partitions, along with experimental results, are given in Fig. 5.3.

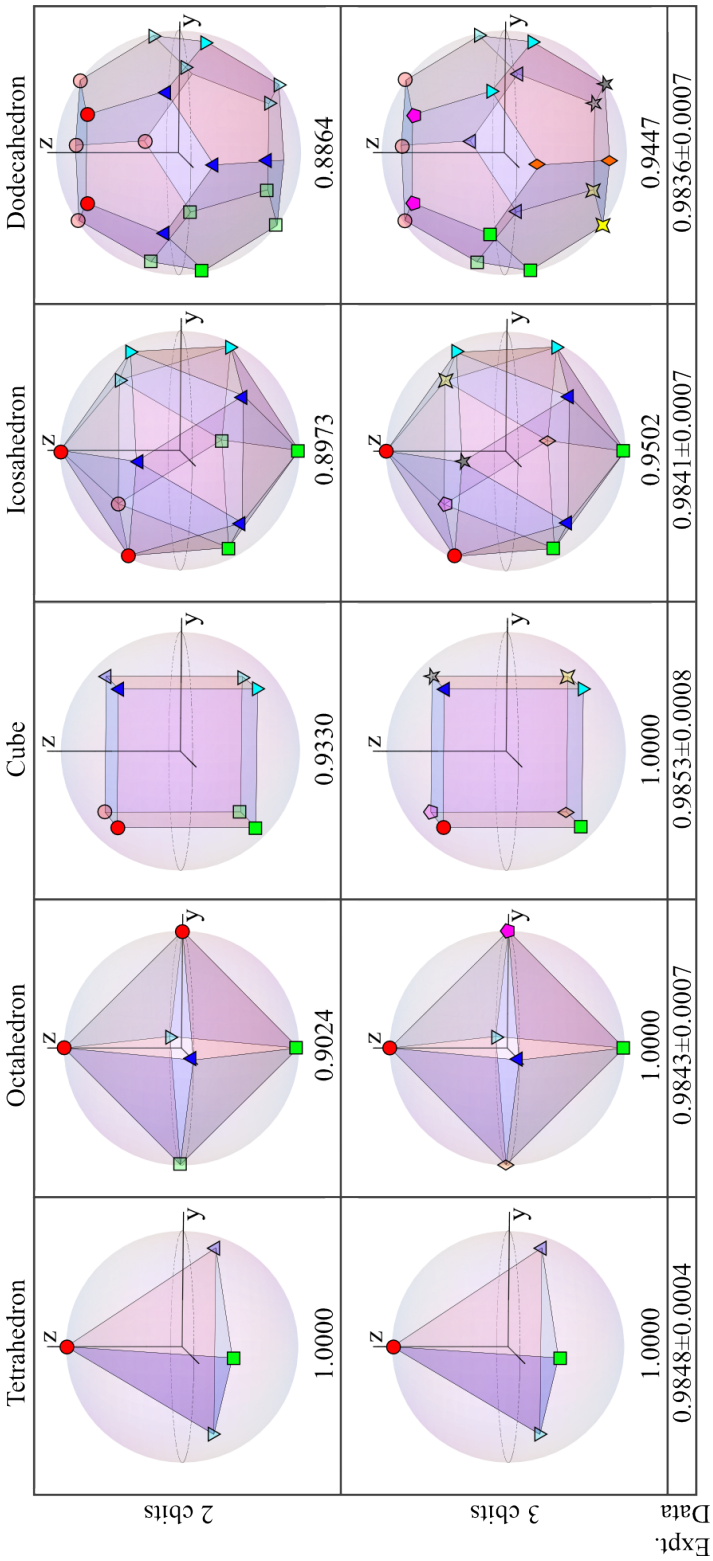


Figure 5.3: Five examples of pure state target ensembles, given by the vertices of the Platonic solids inscribed within the Bloch sphere, with uniform probability distributions. For both two and three cbits message capacity, optimal partitioning strategies are shown, along with the corresponding optimal average fidelity benchmarks. States labeled with the same symbol (e.g. red circles) are in the same partition. The tetrahedron (two or three cbits), octahedron (three cbits), and cube (three cbits) examples can in principle be remotely prepared with perfect fidelity using only classical communication, whereas the remaining ensembles cannot. Experimentally achieved mean fidelities for these ensembles are given in the bottom row; the reported uncertainty is the standard error of the mean. For all non-unity benchmarks, the experimental values surpass the benchmarks for two (three) transmitted cbits by at least 96 (46) times the standard error of the mean.

5.4.2 Continuous ensemble

Perhaps the most meaningful target ensemble is the uniform ensemble of all pure qubit states, i.e. the Bloch sphere itself. For the related problem of teleportation, the optimal classical strategy leads to an average fidelity of $\frac{2}{3}$ [88]. Remote state preparation should be easier than teleportation, since Alice has complete knowledge of the state. The fidelity threshold should therefore be higher, though the threshold will also depend on how many communicated cbits are allowed. Therefore, demonstrating genuine non-classical behaviour experimentally is more difficult for RSP than for teleportation.

We will now derive upper and lower bounds on the classical threshold for both two and three cbits. Many of the results for pure states from the previous section, suitably generalized, still hold here. Partitions will be denoted by Ω_k, with their union forming the surface of the Bloch sphere, $\cup_k \Omega_k = S^2$. The optimal average fidelity is still given by Eq. (5.12), but we make the modifications

$$\begin{aligned} p_k &\to \frac{1}{4\pi}\int_{\Omega_k} d\Omega = \frac{A_k}{4\pi}, \\ \vec{r_k} &\to \frac{1}{p_k}\frac{1}{4\pi}\int_{\Omega_k} \vec{r_\alpha} d\Omega = \frac{1}{A_k}\int_{\Omega_k} \vec{r_\alpha} d\Omega, \end{aligned} \tag{5.14}$$

where A_k is the surface area of partition k.

To obtain lower bounds on the threshold, we simply choose a particular partitioning. For two cbits, we imagine that a tetrahedron is inscribed in the Bloch sphere and connect the four vertices by segments of great circles (note: this is not to be confused with use of platonic solids in previous section). This leads to four disjoint regions on the surface of the Bloch sphere which form our partitions. To calculate the optimal average fidelity for this arrangement, we integrate Eq. (5.14) and make use of the following equation for great circles in spherical coordinates: $\cot(\phi) = a\sin(\theta + c)$ ([105], Lemma 28.1). Here, $\phi \in [0, \pi]$ and $\theta \in [0, 2\pi]$ are the polar and azimuthal angles, respectively, and a and c are constants determined by substituting two points which the great circle passes through. Using this relation, the bound can be worked out to be 0.8724. For three cbits, we use the eight octants as our partitions (equivalently, we connect the vertices of an inscribed octahedron). This straightforwardly gives a lower bound on the threshold of 0.9330. We conjecture that these two lower bounds are the optimal values, but we cannot prove at this time.

To obtain upper bounds, we use an idea similar to the algorithm detailed in section 5.4.1. If we can determine the maximal weighted average fidelity $\langle F\rangle_A^{\max}$ achievable for a given surface area A of the sphere, then we can calculate an upper bound using these values:

$$\langle F\rangle^{\max} \leq \sum_{k=0}^{2^c-1} \langle F\rangle_{A_k}^{\max} \; s.t. \; \sum_{k=0}^{2^c-1} A_k = 4\pi. \tag{5.15}$$

Out of all possible configurations of a given partition with area A_k, a circular cap on the Bloch sphere gives the longest average Bloch vector, and hence the largest average fidelity. Also, the optimal distribution occurs when all partition areas are equal, $A_k = \frac{4\pi}{2^c} \; \forall \; k$ (see Appendix A.1 for proofs of these statements). Of course, it is only possible to cover the Bloch sphere with 2^c disjoint circular caps when $c = 0$ or 1, so the upper bounds for $c \geq 2$ are not achievable.

Using the equations derived in Appendix A.1, the upper bounds for $c = 2$ and $c = 3$ work out to be 0.8750 and 0.9375, respectively. Even these simple ideas yield tight bounds on the continuum thresholds for two and three cbits. To summarize:

$$0.8724 \leq \langle F\rangle^{\max} < 0.8750 \text{ for } c = 2,$$
$$0.9330 \leq \langle F\rangle^{\max} < 0.9375 \text{ for } c = 3.$$

These numbers are significantly higher than the optimal classical teleportation fidelity of $\frac{2}{3}$. This confirms that, when restricted to classical communication only, the remote preparation of a known quantum state is indeed easier than the teleportation of an unknown quantum state. It is thus more difficult to demonstrate a genuine quantum advantage in an RSP experiment than in a teleportation experiment.

5.4.3 Mixed states

Here we consider the same type of qubit ensembles as in section 5.4.1, but with the modification that every state in an ensemble is a mixed state with Bloch vector length r. Unfortunately, if the target states are mixed states, finding classical thresholds is more complicated than in the pure state case. For instance, the optimal strategy is not necessarily one with deterministic messaging. Consider a target ensemble consisting of the three qubit states $\rho_{\alpha_1}^{\text{tar}} = |0\rangle\langle 0|$, $\rho_{\alpha_2}^{\text{tar}} = |1\rangle\langle 1|$, $\rho_{\alpha_3}^{\text{tar}} = \frac{1}{2}\mathbb{1}$ with equal probability $\frac{1}{3}$. Alice sends

messages according to the distribution

$$q_0(\alpha_1) = 1,\ q_1(\alpha_1) = 0$$
$$q_0(\alpha_2) = 0,\ q_1(\alpha_2) = 1$$
$$q_0(\alpha_3) = \frac{1}{2},\ q_1(\alpha_3) = \frac{1}{2},$$

and Bob prepares the two output states $\rho_0^{\text{out}} = |0\rangle\langle 0|$, $\rho_1^{\text{out}} = |1\rangle\langle 1|$. It is easy to see that this probabilistic messaging strategy, which uses only one cbit, allows Alice and Bob to remotely prepare any three of these states with arbitrarily high fidelity.

In fact, for any target ensemble which is contained in the convex hull of $N \leq 2^c$ suitably chosen points, Alice and Bob can achieve an arbitrarily high fidelity by using a probabilistic messaging strategy. For instance, if Alice has access to two cbits, she could specify four pure states which form the vertices of a tetrahedron and prepare any state within this tetrahedron with perfect fidelity. Similarly, with three cbits, she could perfectly prepare any state located within a cube whose vertices were pure states. For example, consider a uniform dodecahedron ensemble with each state having Bloch radius r. For two (three) cbits, if this radius is not larger than the radius of a sphere inscribed in the tetrahedron (cube), then the ensemble can be prepared with perfect fidelity. For two (three) cbits, the insphere radius is $\frac{1}{3}$ ($\sqrt{\frac{1}{3}}$). Similar statements can be made for any ensemble with states of constant radius.

The possibility that the optimal strategy could involve probabilistic messaging renders the optimization trickier, as we can no longer use a partitioning argument to find the optimal value. Another approach is to focus on finding the optimal strategy which involves only deterministic messages. This is the special case where, for each target state ρ_α^{tar}, only one of the $q_k(\alpha)$ is non-zero. The optimal value in this case, found by optimizing over output states, provides a lower bound to the true optimum. Unfortunately, this restriction does not fairly match with our experiment, where messages are probabilistically determined by measurement outcomes. However, surpassing this bound is at least a *necessary* condition, if not a sufficient one, for any remote state preparation experiment to demonstrate non-classical advantages.

Under this deterministic messaging assumption, the optimal choices of ρ_k^{out} (see proof in Appendix A.2) achieve a maximal average fidelity of

$$\langle F\rangle_{determ.}^{\max} = \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} p_k \sqrt{r_k^2 + 1 - r^2}\right), \tag{5.16}$$

where p_k and r_k are the same quantities as defined for pure qubit states. In general, this optimal value is achieved using mixed output states. The fidelity in Eq. (5.16) is modified from the pure state case, Eq. (5.12), by the additional term $1 - r^2$ under the square root. Since this term is fixed beforehand, it does not change which partitioning of the target ensemble is optimal. In other words, whichever partitioning maximizes Eq. (5.12) for an ensemble of pure states will also maximize Eq. (5.16), the fidelity bound for the corresponding ensemble with Bloch radius r. Experimental data is compared with these theoretical bounds in Fig. 5.7.

5.5 Experiment

We experimentally implemented the RSP protocol described in section 5.3.1 using optical photons as our qubits. The computational basis states are $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$, which respectively indicate indicate horizontal and vertical polarization.

5.5.1 Implementation

Our experimental setup comprises four parts:

1. The source for preparation of the Bell state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$.
2. The apparatus for performing Alice's POVM $\{E_m(\phi, \theta)\}$ on her qubit and subsequent logic to determine the message sent to Bob.
3. Bob's implementation (via Pockels cells) of the unitary correction σ_m on his qubit.
4. Tomographic analysis of the resulting remotely prepared qubits.

The source of entangled photon pairs is shown in Fig. 5.4a) [54, 55]. It relies on spontaneous parametric downconversion in a polarization-based Sagnac interferometer. A 25 mm long periodically-poled $KTiOPO_4$ (PPKTP) nonlinear optical crystal is embedded in the interferometer, and bi-directionally pumped by a grating-stabilized diode laser outputting < 1 mW at 404.5 nm. The crystal is temperature-tuned for collinear, degenerate type-II quasi-phase-matching. The resulting entangled photon pairs are coupled into single-mode fibers (SMFs) which, at this pump power, typically yield singles (coincidence) rates of

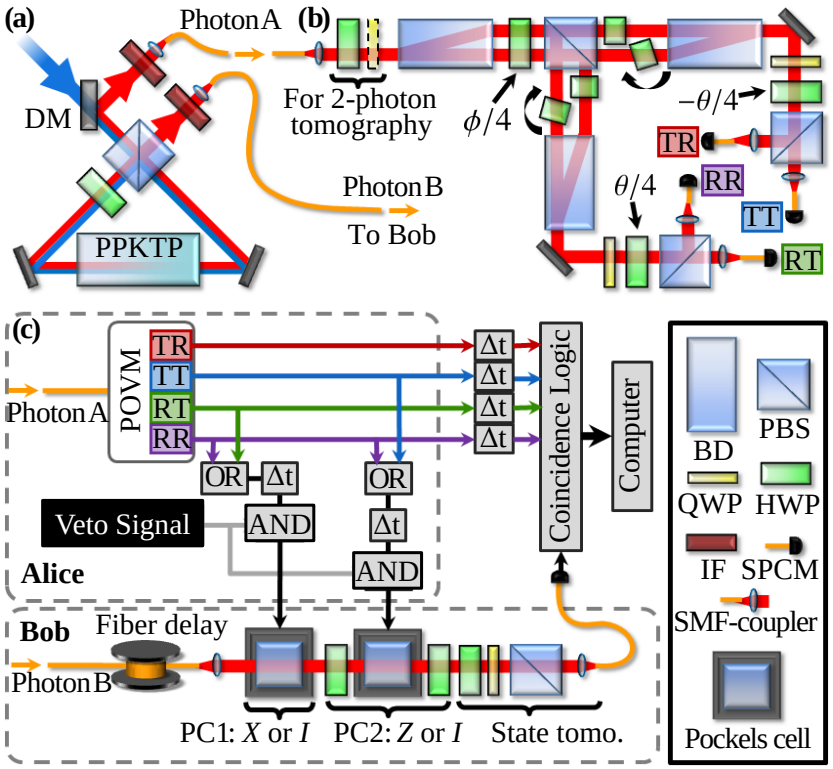


Figure 5.4: Remote state preparation experiment. (a) Entangled photon pairs are produced via parametric downconversion in a polarization-based Sagnac interferometer [54, 55] (see text for details) and distributed to Alice and Bob in single-mode fibers (SMFs). (b) The apparatus used by Alice to perform a POVM on her photon. It is a double-interferometer based on calcite beam displacers (BDs) which couple the polarization qubit to a 'path' qubit for the generalized measurement. Further details are in the text. (c) Schematic of the entire experimental RSP protocol. The POVM $\{E_m\}$ is performed on Photon A. Based on the outcome m a message is encoded in two classical electronic signals, and then sent to Bob with probability r which is controlled by a Veto Signal. Dependent on the message, up to two Pockels cells (PCs) fire to perform the necessary unitary correction on Photon B, which has been delayed in a 50 m fiber to allow time to trigger the PCs. Bob's output is analyzed using quantum state tomography. Note: DM: dichroic mirror; IF: blocking and interference filter; PBS: polarizing beamsplitter; H(Q)WP: half (quarter) wave-plate; SPCM: fiber-coupled single-photon counting module.

150 (30) kHz. Polarization controllers (bat ears, not shown) in the fibers rotate the output to the Bell state $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle)$. However, the first HWP in Alice's POVM apparatus, when not in use for tomographic characterization of the source output, flips this state to $|\Phi^+\rangle$ before her measurement.

The apparatus for performing Alice's POVM is shown in Fig. 5.4b), and has been described in detail in Ref. [106]. It is a polarization-based double interferometer employing waveplates, polarizing beamsplitter cubes (PBSs), and calcite beam-displacers. The latter serve to couple polarization with path, thereby enlarging the state space for the generalized measurement [107, 76]; half-wave plates (HWPs) are used to set the parameters $\{\phi, \theta\}$ of the POVM $\{E_m\}$. The four output modes are coupled into SMF and detected with single-photon counting modules (SPCMs). The outcome TR which stems from (T)ransmission at the first PBS and (R)eflection at the second corresponds to $\frac{1}{2}\rho(\phi, \theta)$, and the RT, RR, and TT outcomes to $\frac{1}{2}Z\rho Z$, $\frac{1}{2}X\rho X$, and $\frac{1}{2}XZ\rho ZX$, respectively.

Due to its the beam-displacer-based construction, the POVM apparatus is inherently phase-stable, without need for active stabilization [71]. To set the appropriate phase in each interferometer arm, we use an 809 nm diode laser injected through the input SMF and a removable polarizing optic; following careful tuning we typically measure classical interference visibilities $> 99.8\%$. The phase itself is set via tilting HWPs at 0°, shown with arrows in 5.4b), in one path of each interferometer arm about their vertical axes. This phase need only be set periodically, typically once per day, and can stay set for four hours or more, provided the ambient lab temperature remains stable, allowing time for the preparation and tomography of several hundred different states.

By means of fast electronic logic gates, the POVM outcome is encoded into the voltage state of two TTL signals. The POVM outcomes TR, TT, RT, and RR are encoded as binary strings "00", "01", "10", and "11", respectively. A value of "1" for the first (second) bit corresponds to a TTL pulse which will trigger Bob's X (Z) correction. For the preparation of pure states, these signals are always transmitted to Bob.

For the preparation of mixed states, a Veto Signal (see Fig. 5.4c)) is produced with probability $(1 - r)$, which is set by the fraction of time spent in the "0" state of a 2 MHz TTL square-wave from a function generator. If a veto signal is generated, it blocks the transmission of TTL pulses to Bob, which is equivalent to sending the message "00". As a result, the message "00" is sent with probability $(1-r)+r/4$, and the other three messages are each sent with probability $r/4$. Because the arrival times of photons in Alice's POVM apparatus are random, and the total rate much less than 2 MHz, the decision whether to

send each message is both random and independent.

Depending on the message received, Bob must implement the unitary correction σ_m on his qubit in order to achieve deterministic RSP. As shown in Fig. 5.4c), this is accomplished by means of two fast $RbTiOPO_4$ (RTP) Pockels cells (Leysop RTP4-20-AR800). At 809 nm these have a half-wave voltage of 1.027 kV and a switching time of < 5 ns. The first Pockels cell is oriented so that when triggered it implements an X operation, which flips $|H\rangle \mapsto |V\rangle$, and is fired if the first bit of the received messages is "1". The second Pockels cell, though similarly oriented, is preceded and followed by HWPs at 22.5° which rotate its action to Z, so that it flips $|D\rangle = |H\rangle + |V\rangle \mapsto |A\rangle = |H\rangle - |V\rangle$. This Pockels cell is fired if the second bit of the received message is "1". When not fired, each Pockels cell and associated waveplates have no net affect on the polarization of transmitted photons (they perform $\mathbb{1}$.) Bob's photon is stored in a 50 m loop of SMF to allow time for Alice's POVM and logic operations, and triggering of the Pockels cells based on the message.

After the correction stage, Bob's remotely prepared qubit is analyzed using a polarization analyzer consisting of a QWP, HWP, and PBS, fiber-coupled to a SPCM. Coincidence counts between this detector and Alice's detectors, summed over her four POVM outcomes, yields our raw data. Note that we do not subtract 'accidental' coincidence detections. For each remotely prepared state, the measured output density matrix ρ_m^{out} is tomographically reconstructed using a maximum-likelihood technique [36] based on coincidence measurements for each of six settings of Bob's analyzer (the eigenstates of X, Y, and Z).

5.5.2 Results

Our data was collected over two days: Day 1 for the remote preparation and tomography of all the pure states in Figs. 5.3 and 5.6, and Day 2 for the mixed states (those where the intended state has $r < 1$) in Fig. 5.7 and Table 5.1. Each day we characterized the entangled state ρ_{AB} via over-complete state tomography; the results are shown in Fig. 5.5. The polarization of Photon A is analyzed using the first two waveplates in the POVM apparatus and the H-polarized output of the first beam displacer; the other output is blocked and all subsequent waveplates are set so as to direct the resulting photons to the TT POVM outcome. Coincidences are recorded between this output and that of the polarization analyzer following Bob's (switched off) Pockels cells. We perform a tomographically overcomplete set of 36 different measurements, comprising all combinations of the six eigenstates of X, Y, and Z on Alice's and Bob's qubit, respectively. The results

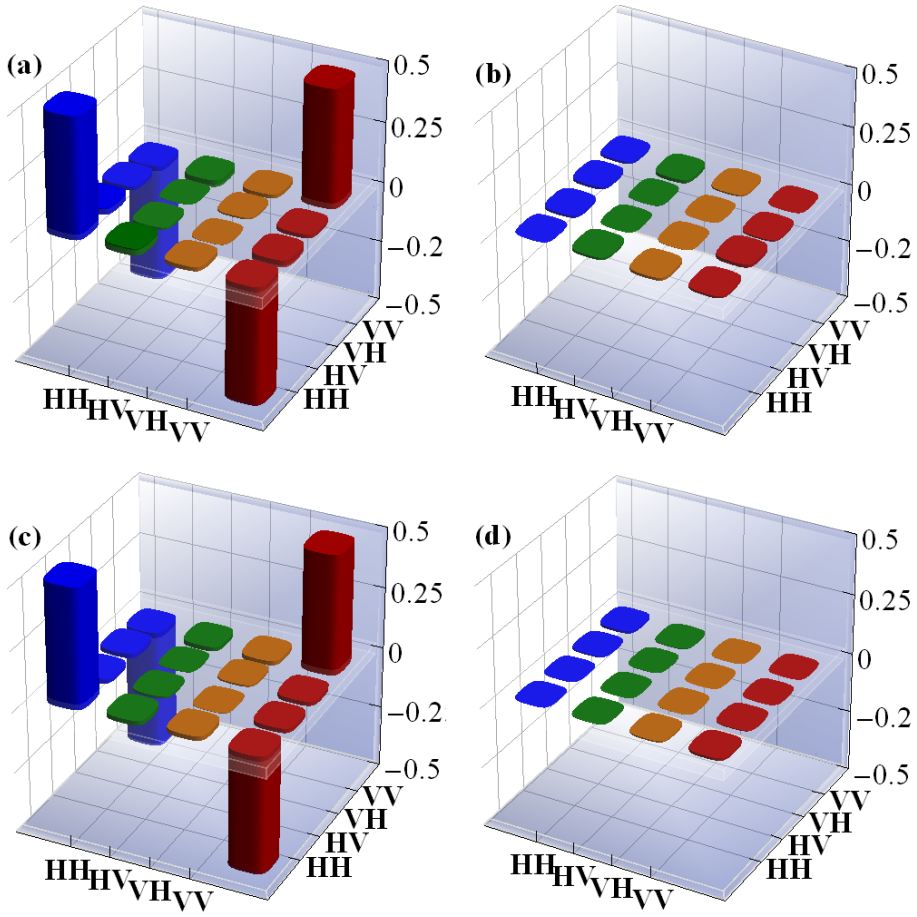


Figure 5.5: Experimentally reconstructed density matrices of our 2-photon entangled state: real part (left) and imaginary part (right). The top row {a) and b)} represents the source state, as aligned for the remote preparation of the pure states (Fig. 5.6); the bottom row {c) and d)} represents the source state as aligned (on a subsequent day) for the preparation of mixed states (states with $r < 1$ in Fig. 5.7 and Table 5.1.) The state in the top (bottom) row has fidelity $F = 0.9807 \pm 0.0004$ (0.9813 ± 0.0003) with the ideal state $|\Phi^-\rangle$, tangle $T = 0.935 \pm 0.002$ (0.932 ± 0.001), and purity $P = \mathrm{Tr}(\rho^2) = 0.9676 \pm 0.0009$ (0.9659 ± 0.0007) [81].

are used to reconstruct the two-photon density matrix [36]. On Day 1 (2) the measured state ρ_{AB} had fidelity $F = 0.9807$ (0.9813) with the ideal output $|\Phi^-\rangle$. When not in use for two-photon tomography, the first QWP on Alice's side is removed, and the HWP is set to 0°, thereby flipping the source output to $|\Phi^+\rangle$ before the POVM.

We remotely prepared and tomographically reconstructed 178 qubit states, and for each measured output density matrix ρ_m^{out} we calculate its agreement with the target state ρ^{tar} using the fidelity (Eq. 5.1). Our mean fidelity $\langle F(\rho^{\text{tar}}, \rho_m^{\text{out}})\rangle$ is 0.9951, and all but three of the 178 states have $F > 0.98$. However, following Ref. [102], we also calculate the expected remotely prepared state ρ^{exp} based on our measured imperfect two-photon entangled state ρ_{AB} as shown in Fig. 5.5, but assuming perfect operation of the POVM and unitary correction. If we then examine the fidelity $F(\rho^{\text{exp}}, \rho_m^{\text{out}})$, we obtain $\langle F\rangle = 0.9995$, with 177 out of the 178 states having $F > 0.9975$. However, in the remainder of the paper and in Figs. 5.3, 5.6, 5.7, and Table 5.1, the fidelities we report are the more stringent $F(\rho^{\text{tar}}, \rho_m^{\text{out}})$, as these are appropriate for comparison with the bounds on classical RSP.

In order to test our experimental RSP implementation against the benchmarks derived in Sec. 5.4, we prepare pure states with settings $\{\phi, \theta\}$ corresponding to the vertices of the five Platonic solids inscribed in the Bloch sphere. The orientations used for each polyhedron, along with the results for $\langle F\rangle$, are shown in Fig. 5.3. These results are compared graphically against the corresponding benchmarks for classical RSP with two and three cbits in Fig. 5.6. In all instances where the benchmark based on classical RSP is less than unity, our experimentally-determined values surpass it conclusively. This confirms that our results cannot be produced without shared entanglement, even when a comparable amount of classical communication is allowed.

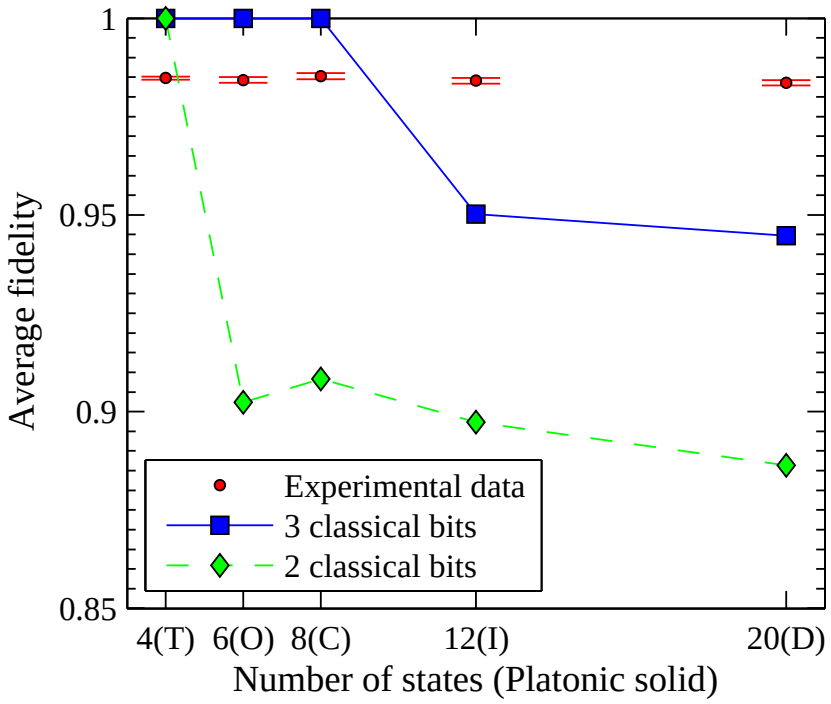


Figure 5.6: Experimentally-achieved mean fidelities $\langle F(\rho^{\text{tar}}, \rho_m^{\text{out}})\rangle$ and optimal classical benchmarks for target ensembles of pure states based on the five Platonic solids shown in Fig. 5.3. The error bars shown are the standard error of the mean. Any experimental data point above the green diamonds (blue squares) represents results that are not possible with only two (three) cbits communication and no preshared entanglement. In all cases where the classical benchmark is less than unity, the experimental results surpass the benchmarks conclusively. Note: lines are included only to guide the eye and do not represent calculated thresholds.

r	0.00	0.25	0.50	0.75	1.00
Icosahedron	0.99944 ± 0.00008	0.99967 ± 0.00007	0.99964 ± 0.00008	0.9987 ± 0.0002	0.9841 ± 0.0007
Dodecahedron	0.9995 ± 0.00006	0.99961 ± 0.00003	0.99963 ± 0.00004	0.9987 ± 0.00015	0.9836 ± 0.0007

Table 5.1: Experimentally achieved average RSP fidelities $\langle F(\rho^{\text{tar}}, \rho_m^{\text{out}})\rangle$ versus Bloch vector radius r. The data is for ensembles with settings $\{\phi, \theta\}$ corresponding to the vertices of an icosahedron and dodecahedron with varying outsphere radii r. The reported uncertainty is the standard error of the mean.

To test our ability to prepare arbitrary mixed qubit states, we use settings $\{r, \phi, \theta\}$, where ϕ and θ correspond to the vertices of the icosahedron and dodecahedron, for all $r \in \{0.00, 0.25, 0.50, 0.75, 1.00\}$. Our results for $\langle F \rangle$ are summarized in Table 5.1. In Fig. 5.7 these results are compared to the lower bounds found in Section 5.4 for classical RSP; again our data surpass the bounds on classical RSP whenever the benchmark is less than unity.

5.6 Conclusion

We have investigated the theory of remote state preparation involving only classical communication resources. Based on sets of states forming the vertices of Platonic solids we derived several fidelity-based RSP benchmarks bounding such classical protocols. We have described and implemented an experimental protocol for high-fidelity, fully deterministic remote preparation of arbitrary photonic qubit states, and compared its results with our benchmarks. The results show a clear violation of all the classical thresholds whenever the classical protocols do not trivially allow for a perfect RSP strategy. We also examined the special cases where the states to be remotely prepared are i) chosen uniformly from all pure qubit states and ii) mixed qubit states, all with Bloch radius r. We provided appropriate benchmarks in these cases, and our experimental fidelity values once again surpass all sub-unity benchmarks.

An interesting extension to this work would be to deal with the problem of post-selection. Because of device inefficiencies and losses, many more photons are used in the experiment than are actually counted in the final analysis. Carefully counting the lost photons and allowing Alice and Bob to use them as comparable classical resources, without loss, would lead to more difficult benchmarks. Yet it would also provide even stronger support for claims that an experiment evidences genuine quantum behaviour. As well, a comparison of experimental data with the classical thresholds, which were derived for ideal conditions, necessarily has to assume fair sampling [108, 109].

Acknowledgements

We thank G. O. Myhr, D. Hamel, and G. Weihs for valuable discussions, and Z. Wang for designing and building our TTL logic. D.B. and R.K. are thankful for support from the

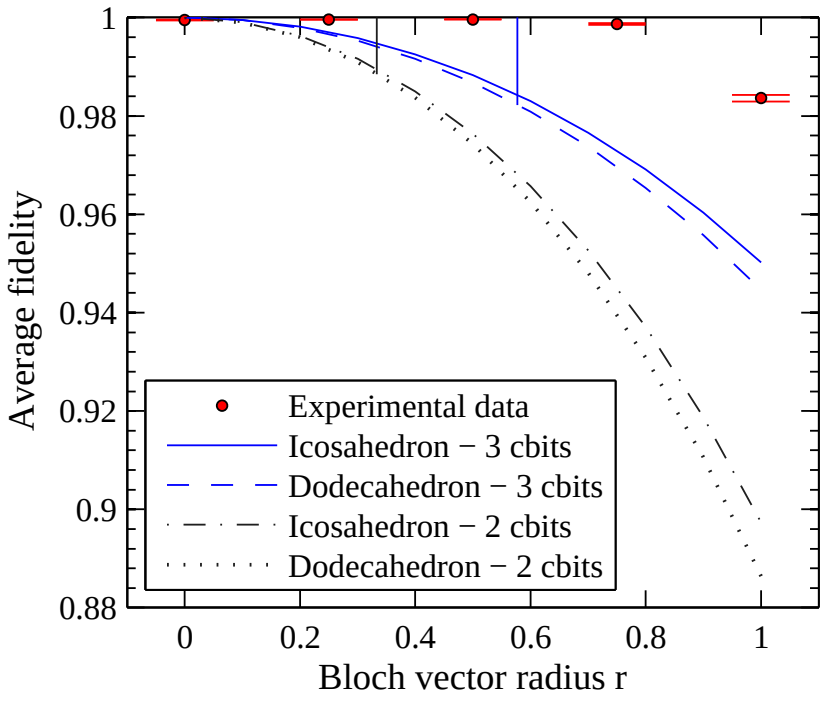


Figure 5.7: Experimentally-achieved mean fidelities and optimal classical thresholds versus Bloch vector radius. The target ensembles consist of uniform distributions of states of Bloch radius r which form the vertices of either an icosahedron or dodecahedron. The lower (upper) pair of lines are bounds on the classical average fidelity arising from specific two (three) cbit classical strategies. Within each pair, the higher bound is for the icosahedron. Experimental data must lie above and to the right of the bounds to be in the quantum regime, but even points in this region may be possible to achieve without pre-shared entanglement by some non-deterministic classical strategy. Experimental data points for the icosahedron ensembles are similar but were not plotted because at this scale they are not distinguishable from those of the dodecahedron.

Mike and Ophelia Lazaridis Fellowship and IQC, respectively. We are grateful for financial support from NSERC (Discovery Grant and QuantumWorks), OCE, and CFI.

Chapter 6

Conclusions and Avenues for Further Research

Quantum measurement and entanglement are among the most fundamental concepts in quantum information theory. Generalized quantum measurements allow greater experimental freedom than standard projective measurements, in particular the ability to have more possible measurement outcomes than the dimension of the state space of the measured system, and the lifting of the restriction to an orthogonal set of outcomes and output states. As many of the most famous and useful ideas in quantum information physics stem at heart from measurements on entangled systems, it seems both useful and interesting to investigate the effects and applications of implementing generalized measurements on such systems.

In this thesis I have presented background material relevant for understanding generalized quantum measurements on pairs of entangled photons, as well as the construction and operation of experimental equipment for the production of such entangled photons, the realization of a tunable four-outcome POVM on a polarization-encoded photonic qubit, and the implementation of fast-switchable correction operations on the other photon based on the POVM outcome. Furthermore I have described two experiments employing these concepts and experimental techniques.

The first experiment concerns the power of generalized measurements when applied in place of projective measurements in the cluster-state model of quantum computation. Our results show that properly-chose POVMs work well in extending the computing power of a two-qubit cluster to that normally obtained by a three-qubit cluster, and that the

method can be implemented with quite high fidelity and an error rate comparable to recent thresholds for fault-tolerant cluster-state computing. In the future it would be interesting to see this method used to implement the addition of two 'virtual' qubits to the cluster instead of only one, and also to see it applied to larger clusters and even to multiple input qubits. Finally, there may perhaps be some utility to implementing POVMs on qubits in the middle of the cluster computation ('body qubits') instead of only the input qubits, and I hope such theoretical avenues are investigated further.

The second experiment realizes the preparation of an arbitrary pure or mixed known qubit state at a remote location via the transmission of only two classical bits, and is enabled by a previously-shared entangled pair and a tunable POVM. I present the derivation of bounds on the achievable average fidelity of so-called 'classical' remote state preparation, limited to classical communication with no entanglement. Such bounds can provide thresholds for examining whether the results of a particular experiment demonstrate advantages to quantum communication or could be equally well achieved using only classical resources. Our results demonstrate the preparation of both pure and mixed states with very high fidelity, and in fact conclusively surpass all derived bounds where perfect remote state preparation could not be achieved with classical resources alone. Related future investigations might include the utility of similar techniques and experimental apparatus for optimal remote state preparation with imperfectly entangled states, as well experimental implementations of optimal quantum steering, wherein Alice's implementation of a suitably-chosen generalized measurement on one qubit from a not-necessarily-maximally-entangled pair, including e.g. Werner states which cannot exhibit Bell-inequality violations, may nonetheless be used to affect the probability distribution of outcomes of Bob's measurements on his photon [77, 110].

Further applications and protocols will doubtless be developed and further questions encountered as physicists and other quantum information scientists continue to explore the application of generalized measurements on entangled systems. I hope that the concepts explored and the experimental tools developed in this thesis help to inspire new avenues for implementations of generalized measurements and to experimentally test resulting protocols and address the questions encountered in these explorations.

Appendices

Appendix A

Proofs Regarding Thresholds for Classical RSP

A.1 Proof of bound for continuous case

In this appendix, we proof two claims from section 5.4.2 used to find upper bounds on the classical threshold for states on the Bloch sphere.

Claim 1

Define a circular cap as the set of points on the surface of the Bloch sphere lying north of some fixed latitude or any rigid spherical rotation of this. Amongst all partitions of surface area $A > 0$, a circular cap has the longest average Bloch vector.

Proof

Consider an arbitrary partition of total surface area $A > 0$ (we do not assume that this partition is connected). This partition, which we call Γ, defines some average Bloch vector $\vec{r_\Gamma}$. We will compare partition Γ with a circular cap of area A centred along the direction of $\vec{r_\Gamma}$, which we shall denote by C. Partition C has an average Bloch vector $\vec{r_C}$. If $\vec{r_\Gamma}$ is the zero vector, then $r_C \geq r_\Gamma = 0$. If not, then without loss of generality we can assume $\vec{r_\Gamma}$ points along the z-axis. By construction, $\vec{r_C}$ must also point along the z-axis. Using Γ and

C, the Bloch sphere can be divided into four disjoint regions: $R_1 = \Gamma \cap C$, $R_2 = \Gamma - C$, $R_3 = \Gamma^c \cap C$, and $R_4 = \Gamma^c - C$. Each of these regions has average Bloch vector $\vec{r_i}$ and area A_i, $i = 1, ..., 4$. Also note that we must have $A_2 = A_3$.

Since $\Gamma = R_1 \cup R_2$, and $C = R_1 \cup R_3$, we must have

$$\vec{r_\Gamma} = \frac{A_1}{A_1 + A_2}\vec{r_1} + \frac{A_2}{A_1 + A_2}\vec{r_2}, \text{ and} \tag{A.1}$$

$$\vec{r_C} = \frac{A_1}{A_1 + A_2}\vec{r_1} + \frac{A_3}{A_1 + A_3}\vec{r_3}. \tag{A.2}$$

From this we conclude that

$$\vec{r_C} = \vec{r_\Gamma} + \frac{A_2}{A_1 + A_2}(\vec{r_3} - \vec{r_2}), \tag{A.3}$$

i.e. that the vector $\vec{r_3} - \vec{r_2}$ also lies along the z-axis. However, it might point in the negative z-direction.

But the boundary of C lies at some fixed height H_C on the z-axis. By construction, every state in R_3 has a z-component higher than H_C and every state in R_2 has a z-component lower than H_C. Then the z-component of $\vec{r_3}$ must be larger than that of $\vec{r_2}$. Therefore, their difference $\vec{r_3} - \vec{r_2}$ has a positive z-component. From Eq. (A.3), we can conclude that $\vec{r_C}$ is longer than $\vec{r_\Gamma}$. Thus, for fixed area A, a circular cap gives the longest average Bloch vector.

Claim 2

Knowing that a circular cap gives the optimum Bloch vector length for fixed area A, we want to optimize the objective function

$$\sum_{k=0}^{2^c-1} \langle F \rangle_{A_k}^{\max} = \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} p_k r_k^{\max}\right) \tag{A.4}$$

subject to the constraint

$$\sum_{k=0}^{2^c-1} A_k = 4\pi. \tag{A.5}$$

We claim that this is optimized when all areas are equal.

Proof

To obtain the optimal Bloch vector as a function of area, we temporarily centre a spherical cap on the z-axis and integrate up to some final angle ϕ_k^f,

$$\begin{aligned} r^{\max}(\phi_k^f) =& \frac{1}{A_k}\left|\int_{\theta=0}^{2\pi}\int_{\phi=0}^{\phi_k^f}\sin(\phi)\cos(\phi)d\theta d\phi\right| \\ =& \frac{1}{A_k}\pi\sin^2(\phi_k^f). \end{aligned} \tag{A.6}$$

Reparameterizing using $A_k = 4\pi\sin^2(\frac{\phi_k^f}{2})$, we end up with

$$r^{\max}(A_k) = 1 - \frac{A_k}{4\pi}. \tag{A.7}$$

The corresponding probabilities are given by $p_k = \frac{A_k}{4\pi}$. We can group the objective function (A.4) together with the constraint (A.5) into the following Lagrange function:

$$\begin{aligned} \Lambda(A_k,\lambda) =& \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1}\frac{A_k}{4\pi}\left(1-\frac{A_k}{4\pi}\right)\right) \\ &+\lambda\left(\sum_{k=0}^{2^c-1}\frac{A_k}{4\pi} - 1\right). \end{aligned} \tag{A.8}$$

Solving this Lagrange problem for the maximum yields $A_k = \frac{4\pi}{2^c}$ for every k. Hence, the optimal distribution of areas occurs when all they are all equal.

A.2 Proof of optimal average fidelity for mixed states

In this appendix, we prove the optimality of Eq. (5.16). Since we are dealing with qubits, we can make use of an alternative formula for fidelity found in [111], namely

$$F(\sigma,\tau) = \mathrm{Tr}(\sigma\tau) + \sqrt{1-\mathrm{Tr}(\sigma^2)}\sqrt{1-\mathrm{Tr}(\tau^2)}. \tag{A.9}$$

Under the assumptions that the target states all have the same Bloch vector length r and that the message strategy is deterministic, the average fidelity is

$$\begin{aligned}\langle F\rangle =& \sum_{\alpha} p_\alpha F(\rho_\alpha^{\text{tar}}, \rho_{m(\alpha)}^{\text{out}}) \\ =& \sum_{k=0}^{2^c-1} \sum_{\alpha\in k} p_\alpha F(\rho_\alpha^{\text{tar}}, \rho_k^{\text{out}}) \\ =& \sum_{k=0}^{2^c-1} p_k[\text{Tr}(\overline{\rho_k}\rho_k^{\text{out}}) \\ &+ \sqrt{\frac{1-r^2}{2}}\sqrt{1-\text{Tr}((\rho_k^{\text{out}})^2)}]. \end{aligned} \tag{A.10}$$

As before, $p_k = \sum_{\alpha\in k} p_\alpha$ is the probability of sending message k and $\overline{\rho_k} = \frac{1}{p_k}\sum_{\alpha\in k} p_\alpha\rho_\alpha$ is the weighted average of states where message k is sent. The quantity in square brackets will be denoted by

$$G_k[\rho_k^{\text{out}}] = \text{Tr}(\overline{\rho_k}\rho_k^{\text{out}}) + \sqrt{\frac{1-r^2}{2}}\sqrt{1-\text{Tr}((\rho_k^{\text{out}})^2)}. \tag{A.11}$$

For each k, we need to find the choice of ρ_k^{out} which optimizes G_k. Working in the eigenbasis of $\overline{\rho_k}$, we have

$$\rho_k^{\text{out}} = \begin{bmatrix} a & b \\ b* & d \end{bmatrix}, \tag{A.12}$$

with $a, d \in \mathbb{R}, b \in \mathbb{C}$. From the above expression for the fidelity, the optimal choice of ρ_k^{out} should be simultaneously diagonal with $\overline{\rho_k}$, i.e. $b = 0$. Equivalently, the Bloch vectors of $\overline{\rho_k}$ and the optimal ρ_k^{out} should be parallel. Denoting the magnitudes of these Bloch vectors by r_k and s_k, respectively, we are left with

$$\begin{aligned} G_k =& \frac{1}{4}\left[(1+r_k)(1+s_k) + (1-r_k)(1-s_k)\right] \\ &+ \sqrt{\frac{1-r^2}{2}}\sqrt{\frac{1-s_k^2}{2}} \\ =& \frac{1}{2}\left(1+r_k s_k\right) + \sqrt{\frac{1-r^2}{2}}\sqrt{\frac{1-s_k^2}{2}}. \end{aligned} \tag{A.13}$$

Since r_k is fixed by the choice of target state partitioning, we differentiate G_k with respect to s_k and find where this derivative equals zero. The result is

$$s_k = \pm\frac{r_k}{\sqrt{r_k^2 + 1 - r^2}}. \tag{A.14}$$

The positive root will give the maximum of G_k, which works out to be

$$G_k^{\max} = \frac{1}{2}\left(1 + \sqrt{r_k^2 + 1 - r^2}\right). \tag{A.15}$$

Collecting all the terms together yields Eq. (5.16).

References

[1] E. Schrödinger. Discussion of probability distributions between separated systems. *Proc. Camb. Phil. Soc.*, 31:555, 1935. 1, 69

[2] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935. 1, 14

[3] J.S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195–200, 1964. 1, 13, 14

[4] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992. 1

[5] C.-H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dualclassical and Einstein- Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993. 1, 80

[6] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991. 2, 14

[7] Tomohisa Nagata, Ryo Okamoto, Jeremy L. O'Brien, Keiji Sasaki, and Shigeki Takeuchi. Beating the standard quantum limit with four entangled photons. *Science*, 316:726, 2007. 2

[8] Hans J. Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86:910–913, 2001. 2, 22, 67

[9] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, May 2001. 2, 22, 67

[10] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(2):022312, Aug 2003. 2, 22, 25, 67

[11] Asher Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128:19, 1988. 2

[12] S. J. Freedman and J. F. Clauser. Experimental Test of Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 28:938–941, 1972. 2

[13] J. F. Clauser and A. Shimony. Bell's theorem. Experimental tests and implications. *Rep. Prog. Phys.*, 41:1881–1927, 1978. 2

[14] A. Aspect, J. Dalibard, and G. Roger. Experimental Test of Bell's Inequalities Using Time-Varying Analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 1982. 2

[15] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the ekert protocol. *Phys. Rev. Lett.*, 84(20):4733–4736, 2000. 2

[16] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.*, 84(20):4737–4740, 2000. 2

[17] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997. 2

[18] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434:169, 2005. 2, 31, 67, 68, 69

[19] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge Univ. Press, Cambridge, 2000. 5, 8, 9, 12, 19, 79, 85

[20] Richard Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41:2315–2324, December 1994. 12, 73, 74, 81

[21] Asher Peres. *Quantum theory: concepts and methods*. Dordrecht: Kluwer, 1993. 13, 67, 68

[22] D. M. Greenberger, M. A. Horne, and A. Zeilinger. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, pages 73–76. Kluwer, Dordrecht, 1989. 13

[23] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880, 1969. 14

[24] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, 1982. 14

[25] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequalities under strict Einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, 1998. 14

[26] M.A. Rowe, D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland. Experimental violation of Bell's inequality with efficient detection. *Nature*, 409:791–794, 2001. 14

[27] C.H. Bennett and G. Brassard. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, New York, 1984. 14, 69

[28] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992. 14

[29] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3, 1992. 14

[30] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 75:145–195, 2002. 14

[31] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.P. Poizat, and P. Grangier. Single photon quantum cryptography. *Phys. Rev. Lett.*, 89:187901, 2002. 14

[32] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Petersonn. Practical free-space quantum key distribution over 10km in daylight and at night. *New Journal of Physics*, 4:43.1, 2002. 14

[33] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.*, 89:101122, 2006. 14

[34] S. J. van Enk, N. Lütkenhaus, and H. J. Kimble. Experimental procedures for entanglement verification. *Phys. Rev. A*, 75(5):052318, 2007. 14

[35] Nathan K. Langford. *Encoding, Manipulating and Measuring Quantum Information in Optics*. PhD thesis, University of Queensland, 2007. 15, 16, 17, 36, 38, 43, 47

[36] Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. Measurement of qubits. *Phys. Rev. A*, 64(5):052312, Oct 2001. 16, 73, 99, 100

[37] Phillip Kaye, Raymond LaFlamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford Univ. Press, Oxford, 2007. 18, 22

[38] M. A. Nielsen. Cluster-state quantum computation. e-print arXiv:quant-ph/0504097v2, 2005. 26

[39] R. Raussendorf and H.J. Briegel. Computational model underlying the one-way quantum computer. *Quant. Inform. Comput.*, 2:344–386, 2002. 28

[40] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hansch, and I. L. Bloch. Controlled collisions for multi-particle entanglement of optically trapped ions. *Nature*, 425:937–940, 2003. 31

[41] Michael A. Nielsen. Optical quantum computation using cluster states. *Phys. Rev. Lett.*, 93(4):040503, Jul 2004. 31

[42] Nikolai Kiesel, Christian Schmid, Ulrich Weber, Géza Tóth, Otfried Gühne, Rupert Ursin, and Harald Weinfurter. Experimental analysis of a four-qubit photon cluster state. *Phys. Rev. Lett.*, 95(21):210502, Nov 2005. 31, 67, 68

[43] Chao-Yang Lu, Xiao-Qi Zhou, Otfried Guhne, Wei bo Gao, Jin Zhang, Zhen sheng Yuan, Alexander Goebel, Tao Yang, and Jian-Wei Pan. Experimental entanglement of six photons in graph states. *Nature Phys.*, 3:91, 2007. 31, 67, 68

[44] Kai Chen, Che-Ming Li, Qiang Zhang, Yu-Ao Chen, Alexander Goebel, Shuai Chen, Alois Mair, and Jian-Wei Pan. Experimental realization of one-way quantum computing with two-photon four-qubit cluster states. *Physical Review Letters*, 99(12):120503, 2007. 31, 67, 68, 69

[45] Giuseppe Vallone, Enrico Pomarico, Paolo Mataloni, Francesco De Martini, and Vincenzo Berardi. Realization and characterization of a two-photon four-qubit linear cluster state. *Phys. Rev. Lett.*, 98(18):180502, 2007. 31, 67, 68

[46] Giuseppe Vallone, Enrico Pomarico, Francesco De Martini, and Paolo Mataloni. One-way quantum computation with two-photon multiqubit cluster states. *Phys. Rev. A*, 78(4):042335, 2008. 31, 67, 68, 69

[47] Michael A. Nielsen and Christopher M. Dawson. Fault-tolerant quantum computation with cluster states. *Phys. Rev. A*, 71(4):042323, Apr 2005. 31

[48] R Raussendorf, J Harrington, and K Goyal. Topological fault-tolerance in cluster state quantum computation. *New J. Phys.*, 9(6):199, 2007. 31, 68, 74

[49] J. D. Franson. Bell inequality for position and time. *Phys. Rev. Lett.*, 62(19):2205–2208, May 1989. 35

[50] C. K. Law, I. A. Walmsley, and J. H. Eberly. Continuous frequency entanglement: Effective finite hilbert space and entropy control. *Phys. Rev. Lett.*, 84(23):5304–5307, Jun 2000. 35

[51] Julio T. Barreiro, Nathan K. Langford, Nicholas A. Peters, and Paul G. Kwiat. Generation of hyperentangled photon pairs. *Phys. Rev. Lett.*, 95(26):260501, Dec 2005. 35

[52] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412:313–316, 2001. 35

[53] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 80(6):1121–1125, Feb 1998. 35, 80

[54] Taehyun Kim, Marco Fiorentino, and Franco N. C. Wong. Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer. *Phys. Rev. A*, 73(1):012316, 2006. 37, 39, 70, 71, 96, 97

[55] Alessandro Fedrizzi, Thomas Herbst, Andreas Poppe, Thomas Jennewein, and Anton Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Exp.*, 15:15377, 2007. 37, 39, 70, 71, 96, 97

[56] D. C. Burnham and D. L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Phys. Rev. Lett.*, 25:84–87, 1970. 36

[57] Alessandro Fedrizzi. *Fundamental experiments with a high brightness source of entangled photons*. PhD thesis, Universität Wien, 2008. 36, 39, 42

[58] Kevin J. Resch. *Making photons talk to each other—Nonlinear optics in the quantum domain*. PhD thesis, University of Toronto, 2002. 36

[59] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, 1987. 43

[60] Zbigniew Ficek and Mohamed R. Wahiddin. *Quantum Optics: Fundamentals and Applications*. International Islamic Univ. Malaysia, Gombak, 2004. 43

[61] Eugene Hecht. *Optics*. Addison Wesley, San Francisco, fourth edition, 2002. 43

[62] B.E.A Saleh and M.C. Teich. *Fundamentals of Photonics*. John Wiley & Sons Inc., Hoboken, N.J., second edition, 2007. 43, 44, 48

[63] Rtp pockels cells datasheet, 2009. http://leysop.com/100khz_rtp_q-switch.htm. 49

[64] 100 kHz RTP Pockels cell Q-switch system, 2009. http://leysop.com/rtp_pockels.pdf. 49

[65] S. M. Barnett and E. Riis. Experimental demonstration of polarization descrimination at the helstrom bound. *J. Mod. Opt.*, 44(6):1061–1064, June 1997. 55, 67, 85

[66] E. Jeffrey, N. A. Peters, , and P. G. Kwiat. Towards a periodic deterministic source of arbitrary single-photon states. *New Journal of Physics*, 6:100, 2004. 55, 80, 84

[67] S. E. Ahnert and M. C. Payne. General implementation of all possible positive-operator-value measurements of single-photon polarization states. *Phys. Rev. A*, 71(1):012330, Jan 2005. 55, 67, 85

[68] W. Rosenfeld, S. Berner, J. Volz, M. Weber, and H. Weinfurter. Remote preparation of an atomic quantum memory. *Phys. Rev. Lett.*, 98(5), 2007. 55, 80, 84

[69] W.-T. Liu, W. Wu, B.-Q. Ou, P.-X. Chen, C.-Z. Li, and J.-M. Yuan. Experimental remote preparation of arbitrary photon polarization states. *Phys. Rev. A*, 76(2), 2007. 55, 84

[70] Wei Wu, Wei-Tao Liu, Ping-Xing Chen, and Cheng-Zu Li. Cluster-state quantum computing enhanced by high-fidelity generalized measurements. e-print arXiv:0909.2570, 2009. 55, 84

[71] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning. Demonstration of an all-optical quantum controlled-not gate. *Nature*, 426:264, 2003. 55, 72, 98

[72] SPCM-AQ4C datasheet, 2009. http://optoelectronics.perkinelmer.com/content/DataSheets/DTS_SPCMAQ4C.pdf. 59

[73] P. J. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A*, 60:R773–R776, 1999. 61, 62

[74] Robert Prevedel, Philip Walther, Felix Tiefenbacher, Pascal Bohi, Rainer Kaltenbaek, Thomas Jennewein, and Anton Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445:65, 2007. 67, 68, 70, 73, 84

[75] John Preskill. Lecture notes for physics 229: quantum information and computation, 1998. 69

[76] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White. Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nat. Phys.*, 5(2):134–140, 2009. 69, 98

[77] L. Hughston, R. Jozsa, and W. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A*, 183:14–18, November 1993. 69, 107

[78] R. W. Spekkens and T. Rudolph. Optimization of coherent attacks in generalizations of the bb84 quantum bit commitment protocol. *Quantum Inform. Compu.*, 2:66, 2002. 69

[79] Terry Rudolph and Robert W. Spekkens. Quantum state targeting. *Phys. Rev. A*, 70(5):052306, Nov 2004. 69

[80] T. B. Pittman, B. C. Jacobs, and J. D. Franson. Demonstration of feed-forward control for linear optics quantum computation. *Phys. Rev. A*, 66(5):052305, Nov 2002. 70

[81] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat. Exploring Hilbert space: Accurate characterization of quantum information. *Phys. Rev. A*, 65(1):012301, Dec 2001. 73, 100

[82] D. Bouwmeester, A. Ekert, and A. Zeilinger. *The Physics of Quantum Information*. Springer, Berlin, 2000. 79

[83] H. K. Lo. Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. *Phys. Rev. A*, 62(1):012313, Jun 2000. 80, 83, 84

[84] A. K. Pati. Minimum classical bit for remote preparation and measurement of a qubit. *Phys. Rev. A*, 63(1):014302, Dec 2000. 80, 83

[85] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional Quantum Teleportation. *Science*, 282(5389):706–709, 1998. 80

[86] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble. Criteria for continuous-variable quantum teleportation. *J. Mod. Opt.*, 47:267–278, 2000. 80

[87] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock. Quantum versus classical domains for teleportation with continuous variables. *Phys. Rev. A*, 64(2):022321, Jul 2001. 80

[88] H. Barnum. PhD thesis, University of New Mexico, 1998. 80, 93

[89] V. Bužek, M. Hillery, and R. F. Werner. Optimal manipulations with qubits: Universal-NOT gate. *Phys. Rev. A*, 60(4):R2626–R2629, Oct 1999. 84

[90] D. W. Leung and P. W. Shor. Oblivious remote state preparation. *Phys. Rev. Lett.*, 90(12):127905, Mar 2003. 84

[91] A. Hayashi, T. Hashimoto, and M. Horibe. Remote state preparation without oblivious conditions. *Phys. Rev. A*, 67(5):052302, May 2003. 84

[92] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, , and W. K. Wootters. Remote state preparation. *Phys. Rev. Lett.*, 87(7):077902, 2001. 84

[93] P. Hayden, R. Jozsa, and A. Winter. Trading quantum for classical resources in quantum data compression. *J. Math. Phys.*, 43(9):4404–4444, 2002. 84

[94] A. Abeyesinghe and P. Hayden. Generalized remote state preparation: Trading cbits, qubits, and ebits in quantum communication. *Phys. Rev. A*, 68(6):062319, Dec 2003. 84

[95] D. W. Berry and B. C. Sanders. Optimal remote state preparation. *Phys. Rev. Lett.*, 90(5):057901, Feb 2003. 84

[96] M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo. Faithful remote state preparation using finite classical bits and a nonmaximally entangled state. *Phys. Rev. A*, 69(2):022310, 2004. 84

[97] D. W. Berry. Resources required for exact remote state preparation. *Phys. Rev. A*, 70(6):062306, Dec 2004. 84

[98] C. H. Bennett, P. M. Hayden, D. W. Leung, P. W. Shor, and A. J. Winter. Remote preparation of quantum states. *IEEE Transactions on Information Theory*, 51(1):56–74, 2005. 84

[99] X. Peng, X. Zhu, X. Fang, M. Fengand M. Liu, and K. Gao. Experimental implementation of remote state preparation by nuclear magnetic resonance. *Phys. Lett. A*, 306:271–276(6), 2003. 84

[100] S. A. Babichev, B. Brezger, and A. I. Lvovsky. Remote preparation of a single-mode photonic qubit by measuring field quadrature noise. *Phys. Rev. Lett.*, 92(4):047903, Jan 2004. 84

[101] Marie Ericsson, Daryl Achilles, Julio T. Barreiro, David Branning, Nicholas A. Peters, and Paul G. Kwiat. Measurement of geometric phase for mixed states using single photon interferometry. *Phys. Rev. Lett.*, 94(5):050401, Feb 2005. 84

[102] N. A. Peters, J. T. Barreiro, M. E. Goggin, T.-C. Wei, and P. G. Kwiat. Remote state preparation: Arbitrary remote control of photon polarization. *Phys. Rev. Lett.*, 94(15):150502, Apr 2005. 84, 101

[103] G.-Y. Xiang, J. Li, B. Yu, and G.-C. Guo. Remote preparation of mixed states via noisy entanglement. *Phys. Rev. A*, 72(1):012315, Jul 2005. 84

[104] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:657, 1949. 85

[105] F. Morgan. *Real analysis and applications: including Fourier series and the calculus of variations*. AMS Bookstore, 2005. 93

[106] Devon N. Biggerstaff, Terry Rudolph, Rainer Kaltenbaek, Deny Hamel, Gregor Weihs, and Kevin J. Resch. Deterministic remote preparation of arbitrary photon polarization states. e-print arXiv:0909.2843, 2009. 98

[107] T. C. Ralph, K. J. Resch, and A. Gilchrist. Efficient Toffoli gates using qudits. *Phys. Rev. A*, 75(2):022313, 2007. 98

[108] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969. 104

[109] J. F. Clauser and M. A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10(2):526–535, 1974. 104

[110] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde. Experimental EPR-steering of Bell-local states. *e-print arXiv:quant-ph/0909.0805*, 2009. 107

[111] J. A. Miszczak, Z. Puchala, P. Horodecki, A. Uhlmann, and K. Zyczkowski. Sub- and super-fidelity as bounds for quantum fidelity. *Quant. Inf. Comp.*, 9(1&2):0103–0130, 2009. 111