Stepping stones towards linear optical quantum computing

By

Till Joscha Weinhold

A thesis submitted to the University of Queensland
for the degree of Doctor of Philosophy
Department of Physics, School of Physical Sciences
April 2010

Typeset in LaTeX 2_ε.

This thesis is composed of my original work, and contains no material previously published or written by another person except where due reference has been made in the text. I have clearly stated the contribution by others to jointly-authored works that I have included in my thesis. I have clearly stated the contribution of others to my thesis as a whole, including statistical assistance, survey design, data analysis, significant technical procedures, professional editorial advice, and any other original research work used or reported in my thesis. The content of my thesis is the result of work I have carried out since the commencement of my research higher degree candidature and does not include a substantial part of work that has been submitted to qualify for the award of any other degree or diploma in any university or other tertiary institution. I have clearly stated which parts of my thesis, if any, have been submitted to qualify for another award. I acknowledge that an electronic copy of my thesis must be lodged with the University Library and, subject to the General Award Rules of The University of Queensland, immediately made available for research and study in accordance with the Copyright Act 1968. I acknowledge that copyright of all material contained in my thesis resides with the copyright holder(s) of that material.
Statement of parts of the thesis submitted to qualify for the award of another degree: None.
Statement of contributions by others to the thesis as a whole: None.
Statement of contributions to jointly authored works contained in the thesis: As detailed in List of Publications and in the appropriate chapters.

Till Joscha Weinhold

Acknowledgements

This thesis is the conclusion of my studies of physics which I started over 10 years ago and thus has certainly been a long and drawn out project. There is a number of people who's support and advice I have received during this time, and whom I would like to thank at this point. First and foremost, my family. My wife Amber, who has always supported me and dealt with the frustrations I went through during this time, and who also endures the company of people who sit at a pond and instead of enjoying feeding the ducks, analyse the ripple pattern on the water. My children Natavia, Kiana and Laiken who remind me everyday that there are other things in life but superposition states and overlap functions, and that very simple things can bring endless joy to all of us. My mother Susanne, who is a great support for our whole family and the best Omi I could have wished for and who also financially enabled me and my family to pursue my dream.

Further I would also like to thank my trinity of supervisors, Andrew, Geoff and JLo for taking me under their wing and teaching me the Ins and Outs of optical quantum computing from Hong-Ou-Mandel interference to complex models and that you should always measure the length of a fibre *before* you use it. A big thank you to Andrew for the opportunity to undertake my PhD with him and for all the support he has given me over the years. A further thank you to Geoff not only for the physics, but also the general advice on life he has shared with me and for actually reading my thesis. Thank you as well to Kevin for his patience in teaching me more about cluster states and why the Schrödinger picture sometimes is not a good choice ;-) Marco, thanks for teaching me a lot about what it means to become a post-doc and being a great mate. And the long and dark hours in the lab would have never been anywhere near as fun if Rohan would not have been about, though it did scare the -beep- out of me when you would just emerge in the dark of the lab from under the optics table after sleeping in the lab...

Also a very special thank you to my office mates Adrian, Isaac, Katrina and Marianne for enduring me and forming the best PhD office with me. Isaac, the jousting was one of the best parts of the PhD. To Kat: Pop! Adrian is always up for a philosophical discussion and if you are ever bored and want some entertainment, I suggest discussing nappies with Marianne...

Darth Doyle will return!

Oh, and it wasn't me.

List of Publications

Published works by the author incorporated into the thesis

- N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White *Demonstration of a Simple Entangling Optical Gate and Its Use in Bell-State Analysis*. Phys. Rev. Lett. **95**, 210504 (2005).

  Incorporated in Chapter 3. Data acquisition was performed by NKL,TJW, RP and KJR. Experimental design by NKL,TJW. Analysis by NKL, KJR, AG. Concepts by GJP, JLO and AGW. A more detailed description of the individual contributions is given in Chapter 3.

- K. J. Resch, J. L. O'Brien, T. J. Weinhold, K. Sanaka, B. P. Lanyon, N. K. Langford, and A. G. White *Entanglement Generation by Fock-State Filtration*. Phys. Rev. Lett. **98**, 203602 (2007).

  Incorporated in Chapter 7. Data acquisition was performed by TJW, KJR, JLO, BPL and NKL. Experimental design by TJW, KJR and JLO. Analysis by KJR, NKL and BPL. Concepts by KJR, KS and AGW. A more detailed description of the individual contributions is given in Chapter 7.

- B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White *Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement*. Phys. Rev. Lett. **99**, 250505 (2007).

  Incorporated in Chapter 6. Data acquisition was performed by BPL,TJW,NKL and MB Experimental design by TJW, BPL and MB. Analysis by AG, BPL and NKL. Concepts by DFVJ, MB, AG and AGW. A more detailed description of the individual contributions is given in Chapter 6.

- B. P. Lanyon, T. J. Weinhold, N. K. Langford, J. L. O'Brien, K. J. Resch, A. Gilchrist, and A. G. White *Manipulating Biphotonic Qutrits* . Phys. Rev. Lett. **100**, 060504 (2008).

  Incorporated in Chapter 7. Data acquisition was performed by TJW, BPL, KJR, JLO and NKL. Experimental design by KJR, TJW and JLO. Analysis by AG, NKL,KJR and TJW. Concepts by JLO and AGW. A more detailed description of the individual contributions is given in Chapter 7.

Additional published works by the author relevant to the thesis,

but not forming part of it

- M. Barbieri, T.J. Weinhold, B.P. Lanyon, A. Gilchrist, K.J. Resch, M.P. Almeida and A.G. White *Parametric downconversion and optical quantum gates: twos company, fours a crowd.* Journal of Modern Optics **56**, 209 (2009).

  Data acquisition was performed by TJW, BPL, MB, KJR and MPA. Experimental design by TJW, MB and BPL. Analysis by MB, TJW, AG. Concepts by TJW, MB and AGW.

Abstract

The experiments described in this thesis form an investigation into the path towards establishing the requirements of quantum computing in a linear optical system. Our qubits are polarisation encoded photons for which the basic operations of quantum computing, single qubit rotations, are a well understood problem. The difficulty lies in the interaction of photons. To achieve these we use measurement induced non-linearities. The first experiment in this thesis describes the thorough characterisation of a controlled-sign gate based on such non-linearities. The photons are provided as pairs generated through parametric down-conversion, and as such share correlations unlikely to carry over into large scale implementations of the future. En route to such larger circuits, a characterisation of the actions of the controlled-sign gate is conducted, when the input qubits have been generated independently from each other, revealing a large drop in process fidelity. To explore the cause of this degradation of the gate performance a thorough and highly accurate model of the gate is derived including the realistic description of faulty circuitry, photon loss and multi-photon emission by the source. By simulating the effects of the various noise sources individually, the heretofore largely ignored multi-photon emission is identified as the prime cause of the degraded gate performance, causing a drop in fidelity nearly three times as large as any other error source. I further draw the first comparison between the performance of an experimental gate to the error probabilities per gate derived as thresholds for fault-tolerant quantum computing. In the absence of a single vigourous threshold value, I compare the gate performance to the models that yielded the highest threshold to date as an upper bound and to the threshold of the Gremlin-model, which allows for the most general errors. Unsurprisingly this comparison reveals that the implemented gate is clearly insufficient, however just remedying the multi-photon emission error will allow this architecture to move to within striking distance of the boundary for fault-tolerant quantum computing. The utilised methodology can be applied to any gate in any architecture and can, combined with a suitable model of the noise sources, become an important guide for developments required to achieve fault tolerant quantum computing. The final experiment on the path towards linear optical quantum computing is the demonstration of a pair of basic versions of Shor's algorithm which display the essential entanglement for the algorithm. The results again highlight the need for extensive measurements to reveal the fundamental quality of the implemented algorithm, which is not accessible with limited indicative measurements.

In the second part of the thesis, I describe two experiments on other forms of entanglement by extending the actions of a Fock-State filter, a filter that is capable of attenuating single photon states stronger than multi-photon states, to produce entangled states. Furthermore this device can be used in conjunction with standard wave-plates to extend the

range of operations possible on the bi-photonic qutrit space, showing that this setup suffices to produce any desired qutrit state, thereby giving access to new measurement capabilities and in the process creating and proving the first entanglement between a qubit and a qutrit.

Keywords & Australian and New Zealand Standard Research Classifications (ANZSRC)

Keywords

Quantum Information, Quantum Optics, Quantum Computing, Linear Optical Quantum Computing, Pulsed Parametric Down-conversion.

ANZSRC codes

40% 020603 Quantum Information, Computation and Communication
60% 020604 Quantum Optics

Contents

List of Figures

List of Tables

1 Introduction

1.1 The Beginning

While many scientists believed physics to be nearly complete in the late 1800's, theoretical physics was struggling to explain seeming oddities, which at the dawn of the 20th century were being unveiled in experiments at an ever increasing rate. Whether the lack of electrons spiralling into the nucleus, or the wavelength dependence of the photoelectric effect, the findings where unexplainable with existing theory, yet were repeatably demonstrated in experiments. The solution came from the development of a completely new theory in the 1920's, which following Planck's finding of a discrete minimal energy step —a quantum — was given the name quantum mechanics. After nearly a full century of continuous development quantum mechanics has helped derive, explain and predict many seemingly impossible results, and has now become a well established, yet ever developing theory.

Another major development of the 20th Century, was that of an electronic computation device, the computer. Originally the size of buildings, the development of the transistor triggered an incredible development: since the 1960's computational power has approximately doubled every two years at level financial costs. This was achieved largely by further and further miniaturisation of transistors. Similarly the storage capacity of common magnetic hard disks on home computers has increased from few Megabytes at the beginning of the 1990's to up to a Terabyte in 2007, while retaining the same physical size. Again this increase was made possible through the reduction of the physical size of a data block. This development, known as Moore's Law, will run into an obvious boundary, when one bit of information will have to be stored on less than one electron or atom. However, even prior to this, the continuous decrease in size will lead to transistors on the size comparable to atomic proportions. At the latest at this point quantum effects will enter into and alter the behaviour of computer chips.

This seeming curse also holds great potential. In 1982 Richard Feynman [1] suggested that

it would be more efficient to model the evolution of a quantum system, not with a classical computer, but on a quantum computer. By doing so, he gave birth to a new concept: that of quantum computation. Instead of using a system, where information is stored and evaluated in bits limited to being either off or on, 0 or 1, one can utilise suitable quantum systems. This enables harnessing the power of the weirdness of quantum mechanics whereby the individual qubits can be in any superposition state of on and off and can become entangled with one another. While the initial idea was certainly adventurous and innovative, the lack of any suitable architecture, algorithm or further application lead to no significant research efforts until Peter Shor [2] suggested an efficient order finding algorithm for a quantum computer in 1994, followed by Cirac and Zoller indicating a potential path to quantum computing with trapped ions [3]. The order finding routine introduced by Shor is related to factoring of numbers. Factoring, or more precisely the exponential difficulty of factoring large numbers into their prime factors with a classical computer, is the mechanism on which many modern cryptographic methods, such as RSA [4], rely. While there is no vigourous proof that there is no efficient algorithm on a classical computer for the factoring problem, all efforts to derive such an algorithm so far have failed, leaving the potential existence of a classic factoring algorithm an interesting, open question. Shor's algorithm was hence not only capable of factoring numbers, but by doing so also capable of deciphering strongly encrypted information. The incredible power of this algorithm, combined with the potential path towards quantum computing and the advances towards isolating and controlling individual quantum systems, led to a flourish of both experimental and theoretical research in the young field of quantum computing. Recently an application more closely related to the idea of Feynman has been put forward, which allows the calculation of the energy states of molecules in quantum chemistry [5]. Here the addition of every additional degree of freedom becomes a substantial challenge to modern super computers, requiring a doubling of the resources. In a quantum code the addition of a single qubit would suffice to simulate the additional degree of freedom. Quantum chemistry might be the field with the lowest cross over point in terms of required qubits to demonstrate an advantage of quantum computing over a classical regime.

1.2 What it takes: The DiVincenzo Criteria

Many physical architectures have been suggested as a potential candidate for quantum computation, usually because the suggested device and associated qubit would have a particular feature beneficial for quantum computation. This diversity also led to some confusion as certain "given" characteristics in one architecture were unachievable, or achievable only with tremendous difficulty, in another. To broadly define the minimum requirements and create a common basis, David DiVincenzo published a list of capabilities a system must posses so that it would be considered suitable for potentially achieving quantum computation. The list has been compiled after years of evolving discussions on the individual requirements for the different architectures. Since his publication of the original compiled list [6], some items have been added and/or the importance of the individual points have altered. Hence many versions of the criteria exist and I do not claim that the here reprinted version is minimal or complete, but gives a good starting point. In the following we will go though the list and

discuss the individual requirements in more detail.

1. A scalable physical system with well characterised qubits.
2. The ability to initialise the state of the qubits to a simple fiducial state.
3. Long decoherence times relative to the gate operation time.
4. A "universal" set of quantum gates.
5. A qubit specific measurement capability.

When the DiVincenzo criteria were established the one paradigm for quantum computing was a circuit based model similar to that of classic computers. In such a *circuit model*, the qubits would sequentially undergo logic gate operations. Since then a fundamentally different approach has been proposed by Rausendorf and Briegel [7]. In the *cluster state model* a highly entangled input state is used as a resource and via measurement of the individual qubits and feed-forward rotations conditional on the prior measurement outcome have been proven to allow universal quantum computation. The final computation result is simply encoded in the state of the final set of qubits after the subsequent measurement and feed-forward rotations. Interestingly as the cluster state computation uses only measurement, feedforward and single qubit rotations, it requires no two-qubit gate operations. Due to this, and the inherent specific difficulty of such two-qubit gates in linear optical systems, cluster states are inherently attractive for optical quantum computing. The concept was adapted from the general theory of Rausendorf and Briegel to optics independently by Nielsen [8] and Brown and Rudolph [9]. The difficulty for cluster state quantum computing lies in the complex input state requirement. For the approach to be operational, one requires lattice like structures of entangled qubits as shown in figure 1.1. Creating this specific and highly entangled state is the intrinsic difficulty of cluster state quantum computing. If we do not limit ourselves to the sole requirements for the actual computation, but consider the complete picture with the preparation of the resources, then the requirements for circuit based and cluster state quantum computing are basically the same as the cluster state preparation with current methods would require the criteria 1 through to 4. Should however a source of a large quantity of single entangled photons become readily available, cluster state quantum computing would become instantaneously feasible in the presence of efficient measurement. In the following, I will give a brief overview over the state of the art in linear optical quantum computation with respect to the DiVincenzo criteria.

1.2.1 The qubit

Logically a "qubit" is the quantum analogue to a bit, the smallest unit of information, but unlike the classical bit which is assigned a logic value of either 0 or 1, the qubit can assume any possible superposition state of 0 and 1. The physical implementation of the logic construct qubit is in general a sufficiently isolated, individually addressable two-level quantum system. Sufficiently isolated in this case means that there are no undesired interactions between the two level system and the rest of the universe. Practically this condition is unfullfilable and

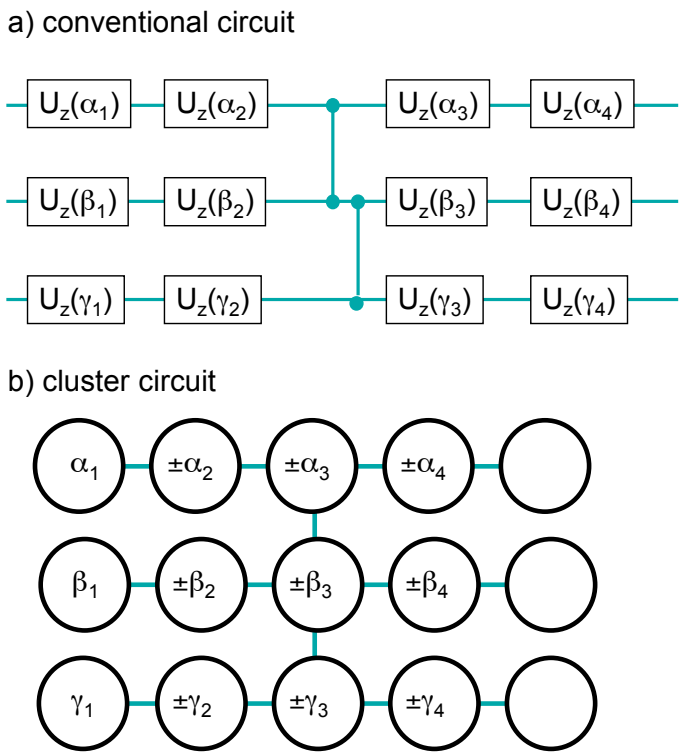


FIGURE 1.1: The two quantum computing paradigms: a) the "conventional" circuit structure. The information (and time) flow is left to right, with the qubits identified by the turquoise lines. The qubit undergoes a number of single qubit rotations U and two-qubit gates symbolised by the interconnecting wires. The final computational result is decoded by measurement (not shown) of the qubits after all gate and other processes are complete. In the cluster model of b) a large entangled state is created. The circles symbolise the qubits and the interconnecting lines the entanglement. Measuring the qubits left to right with specific settings processes the computation. Measurement settings for the second phase of qubits depend on the measurement results of the first phase and alike for subsequent phases. The final result is stored in the last qubits and can be read off with one last measurement with the required setting depending on all previous measurement results. Entanglement in a line left to right allows the passing of information in time with single qubit processes while interconnecting lines are equivalent to two qubit gates. The measurement settings in the cluster model are not related to the single qubit rotations in the circuit model despite usage of the same labels. (Used with permission of Andrew White)

thus systems where the undesired interactions are weak and occur on time scales much longer than the desired interactions and ideally the entire computation suffice. The later is one of the main difficulties in achieving scalable quantum computation in some architectures. In optical quantum computation the qubit of choice is the photon, here specifically the polarisation state of the photon. The logic 0 and 1 states are commonly encoded in the horizontal (H) and vertical (V) linear polarisation states, as off-the-shelf items such as polarising beamsplitters are commonly designed to act in this basis.

1.2.2 Initialisation of Qubits

Qubit initialisation means that prior to the computation we wish to have all our qubits in a certain state. While it is impossible to rotate a photon of unknown polarisation onto a desired state with unit efficiency, one can use polarising beamsplitters. These probabilistically project photons into one of two known orthogonal polarisation states, which are then spatially separated. While this ensures that all our qubits are in the desired input state, it operates at the cost of diminished efficiency as some qubits will be reflected out of the other port of the polarising beamsplitter. Once the polarisation state is known, any desired polarisation state can be achieved through the usage of waveplates (see section 1.3.3 for a more detailed discussion). Common commercially available devices have extinction ratios of $1 : 10^5$ and above, providing us with highly pure qubit states after this initialisation procedure.

1.2.3 The "universal" gate set

One universal set of quantum gates is formed by the combination of arbitrary single qubit rotations, and at least one two-qubit entangling gate from the Clifford group.

Single qubit gates

Single qubit gates, as the name suggest, affect the state of only a single qubit, by mapping the input state on to an output state that depends on the set angle of the single qubit gate. The set angle is usually the angle of the rotation around a fixed axis in the Poincaré sphere. It can be shown [10] that waveplates are capable of performing any arbitrary single qubit rotation on polarisation encoded qubits with very high precision. Specifically a sequence of $\lambda/4$ - $\lambda/2$ - $\lambda/4$ waveplates allows the rotation of the polarisation of a single qubit from any given pure input state to any desired pure output state as shown in section 1.3.3.

Two-qubit entangling gates

The probably best known two-qubit entangling gate is the controlled-NOT gate, where the logic state of the target qubit gets flipped, whenever the control qubit is in the logic 1 state. The truth-table of the CNOT-gate reads as follows

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle, \\ |01\rangle &\rightarrow |01\rangle, \\ |10\rangle &\rightarrow |11\rangle \quad \text{, and} \\ |11\rangle &\rightarrow |10\rangle, \end{aligned} \tag{1.1}$$

where the notation is $|CT\rangle$ identifing the logic states of the control (C) and target (T) qubit. When the control qubit is in a superposition state of $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ the output is maximally entangled. This entanglement lies at the heart of many quantum computations, either as a resource, as in cluster state quantum computation [7–9], where the required input state is highly entangled, or it is created during the computation, as in the circuit

based model. In the circuit model the computation progresses as the qubits are passed from processing element to processing element similar to the architecture of a classical computer. For optical qubits, generating such a two-qubit entangling gate poses a substantial difficulty. The interaction cross-section of visible range photons in vacuum is on the order of 10^{-72}cm^2 [11] and even in the presence of a highly non-linear crystal the achievable non-linearity at the single photon level is still many orders of magnitudes weaker than required. This has led to the wide-spread belief that optical quantum computing would remain infeasible for decades, until the development of much stronger non-linear materials. Knill, LaFlamme and Milburne (KLM) showed in a historic paper [12] that such two-qubit gates are in principle possible with linear optical elements alone. The required non-linearity arises through measurement coupled with ancilla photons and non-classical interference the best known example of this being the Hong-Ou-Mandel (HOM) interference [13]. Due to the importance of this issue, a more detailed discussion will occur in section 1.5.2.

1.2.4 Decoherence time short relative to gate time

Quantum states are subject to continuous evolution. As long as the evolution is coherent, it can be compensated for and corrected. If the state however evolves incoherently, i.e. through uncontrolled (or uncontrollable) interaction with the environment, the qubit state and thus the computation result are no longer correlated with the initial input state. This decohering action has a common, architecture dependent characteristic time, often referred to as T_2-time, on which it occurs. The origin of this labelling comes from nuclear magnetic resonance spectroscopy, where it denotes the time on which the spin vector orientation of the individual nuclei in a sample decohere after a joint initialisation and evolution in a common magnetic potential. The T_2 time is the time base after which the spin state of the nuclei is no longer coherent and any information encoded therein would be lost. Hence it is essential to complete all actions on a given qubit and its measurement in a time that is short relative to its T_2-time, so that the result has not been distorted significantly from the desired state.

Photons are virtually interaction free at optical wavelengths, as the electromagnetic environment at such frequencies is next to a vacuum. Therefore the decoherence time of polarisation encoded qubits is long. In fact, light from distant galaxies and stars which has travelled $1.5 \cdot 10^{10}$years[1] to arrive at Earth still remains partially polarised, indicating a T_2-time for polarisation encoded photons to be on the order of 10 Gyears time in partial vacuum. The gate time of photons on the other hand is governed by how long a photon remains in the gate architecture. As photons travel at the speed of light, this gate time is proportional to the gate architecture dimension. The time for a single photonic CNOT-gate has been measured to be 145ns [14]. Dividing the gate time by the T_2 time gives the order of number of gate operation that could be performed on a polarisation encoded photonic qubit before it decoheres. With the above given values, this allows for $\mathcal{O}10^{24}$ gate operations, which should suffice for any desired problem. Of course it is unlikely that an optical quantum computer would be built in the partial vacuum of outer-space, nor even in free-space as most current optical gates. A more useful data point may be taken from reference [15] where

[1] This is a trivia knowledge kind of fact publicised amongst the community by John Rarity and Andrew White.

photons were transmitted over 144 km (approximately 50μs) through the earths atmosphere and polarisation correlations of the entangled photons yielded a visibility above 95%.

1.2.5 Scalability

Scalability is the fundamental requirement that extending a basic system to a larger number of involved qubits, i.e. in order to encode and thus factor larger numbers, will not require an exponential increase in resources, either physical, temporal or financial. Should such a limitation exist, only problems involving less than the feasibly achievable maximal size of your coding space would be tractable with the given system. In Shor's algorithm the required number of bits or qubits scales with the dimension of the problem. Hence, if a quantum computer was only capable of finding the period of numbers up to a given size, any number larger than this would be "safe" and could still be used for cryptography.

Nearly every proposed architecture at the moment has a shadow of doubt hanging over it regarding the full scalability of the approach[2]. In optics these problems arise from the lack of deterministic two-qubit gates, as those based on the measurement induced non-linearities are non-deterministic, but heralded. This means that they work only probabilistically, but their success is signalled by a specific measurement outcome on the ancilla qubits, see figure 1.2a). In principle, such gates could be made deterministic, as shown in figure 1.2b), by teleporting control and target qubit states onto the successfully implemented gate, upon detection of the success signal of the gate, leading to scalable deterministic gates, but the overhead of required resources is enormous. In the cluster-state computation [7–9] the efficiency criterion for the gates can be significantly relaxed as it can be shown that a gate success probability of $> 1/2$ is sufficient to build arbitrarily large clusters [17].

A further current limitation of optical quantum computation is the lack of a true single-photon source and efficient number-resolving photon detectors. The single-photon source is a device, that emits one and only one photon in a given spatial, spectral and temporal mode when the trigger is pulled. Such devices are currently under development [18–20][3] , but due to a multitude of issues such as timing and frequency jitter, coupling efficiency and availability, a broad opinion in the community is that they are still a few years away from their feasible application to optical quantum computation. The desired detector should be capable of not only detecting photons with, ideally, unit efficiency, but also of differentiating the number of absorbed photons. In principle, just the capability of differentiating between one and many photons, while not resolving the actual number of photons (if there are more than 1) would suffice. Again substantial efforts are currently undertaken worldwide to build such devices, and individual test-bed devices have been employed [21], but they are not readily available *yet*.

[2] A general, but slightly outdated, overview over the state of the quantum computing efforts in the various architectures and their current limitations can be found in the Roadmap [16] published by ARDA in 2004.

[3] There are many, many more publications, and the here given ones are only example cases.

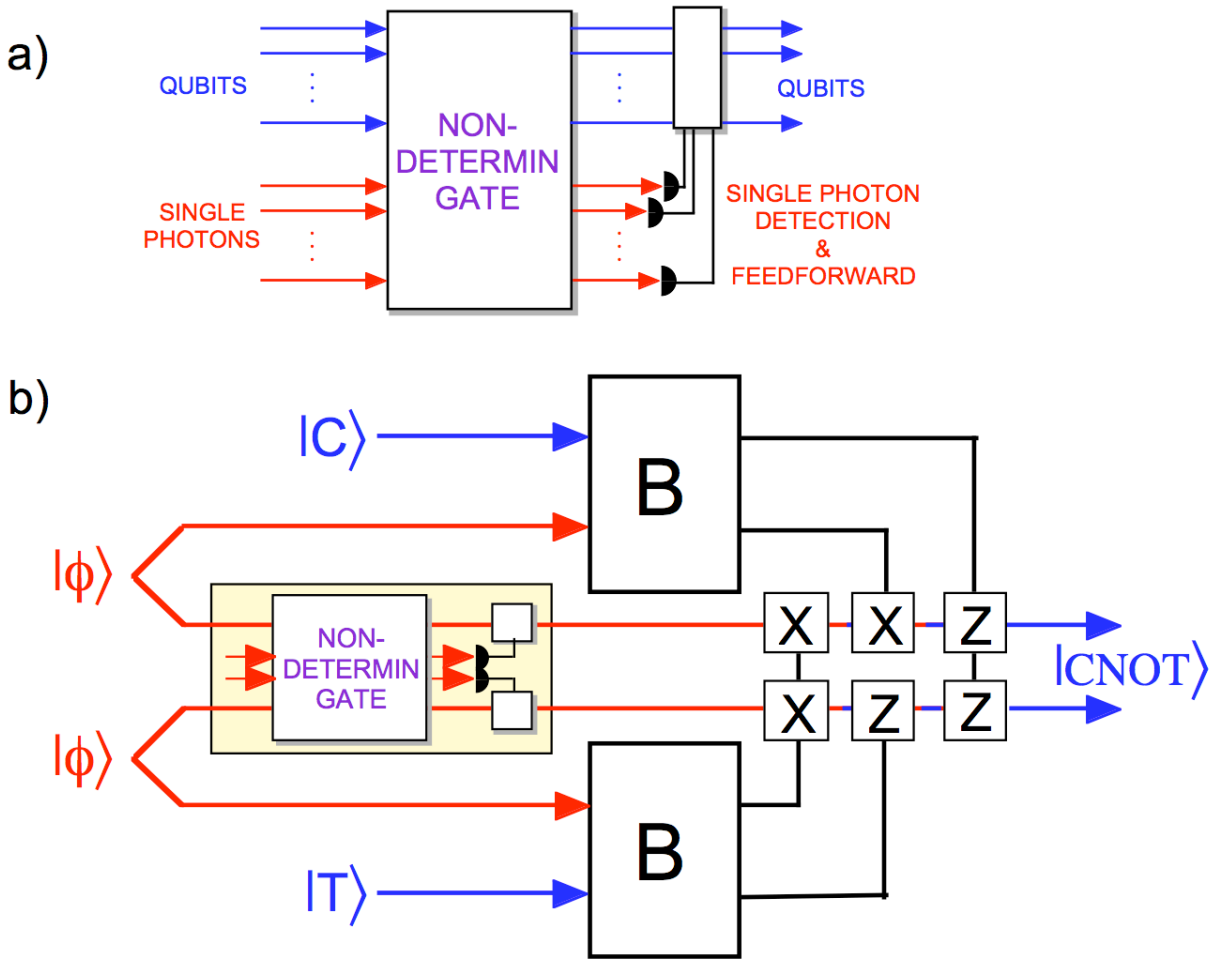


FIGURE 1.2: Schematic design of a scalable linear optics gate a) shows the basic gate as suggested in the KLM-paper [12]. The qubits and ancillas interact inside the non-deterministic gate. The success of the gate is heralded by detection of single photons in every ancilla output mode. Depending on the detected states of the ancilla photons, specific rotations are fed-forward onto the qubits, completing the gate action. If more than one photon is detected in any ancilla mode, the gate has failed and the output is discarded. b) To turn the non-deterministic gate of a) into a scalable deterministic gate, one repeats the non-deterministic gate till its success is heralded. Upon a positive signal the logic from the control ($|C\rangle$) and target ($|T\rangle$) photons are teleported onto the photons of the successful gate implementation using their entangled partner photons (The state $|\phi\rangle$ symbolises the entanglement between the photons injected into the non-deterministic gate and those used in the Bell-measurement). In the graph B denotes a deterministic Bell measurement, X and Z the (potentially) feed forward operations and $|\phi\rangle$ is a two-qubit entangled state, one photon of which is injected into the non-deterministic gate as the qubit, while the other photon is used in the teleportation process. (Figures used and adapted with permission of Andrew White.)

1.2.6 Measurement and Readout

What worth is the might of quantum computation if one is incapable of reading off the result of the computation? While this point seems trivial, it is not clear in some architectures how the measurement and evaluation of individual qubits in large ensembles is to be conducted without interfering with neighbouring qubits. In linear optical quantum computation, readout can be achieved by suitable waveplate rotations, polarising beamsplitters and photon

number counting as discussed previously. As mentioned in the sections above, all these are well understood problems for polarisation encoded qubits.

1.3 The linear optical tool box

1.3.1 The polarisation encoded qubit

As the qubit is a quantum-equivalent of the classical bit, its computational basis states are $|0\rangle$ and $|1\rangle$. Unlike the classical bit, qubits can be in states where they partially populate both the logical $|0\rangle$ and $|1\rangle$ state. The qubit is said to be in a superposition state of the computational basis states. For polarisation encoded qubits, commonly the horizontal and vertical polarisations are chosen to be the logical basis states. Without loss of generality, we assign the horizontal polarisation the logical 0 and the vertical polarisation the logical 1, $|H\rangle = |0\rangle$; $|V\rangle = |1\rangle$. What does a superposition look like? An equal superposition of the horizontal and vertical component is known as the diagonal state

$$|D\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle + |V\rangle\Big) = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big).$$

Clearly the qubit has some probability of being found in either state, when measured in the horizontal/vertical basis. Once the photon has travelled through the polarising beamsplitter, it no longer exists in the superposition state, but has been mapped onto two spatially separated modes:

$$\frac{1}{\sqrt{2}}\Big(|H,0\rangle + |V,1\rangle\Big),$$

where the second entry in the ket is now a label of the spatial mode. Commonly one does not carry the spatial mode label, and rather refers to the polarising beamsplitter as projecting the qubit from the previous superposition into the logically pure modes $|H\rangle$ and $|V\rangle$. A general qubit can thus always be written as a decomposition into the logic basis states such as

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{, where} \tag{1.2}$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad \text{, thus} \tag{1.3}$$

$$|\Psi\rangle = e^{i\gamma}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big), \tag{1.4}$$

where α, β are complex numbers and γ, θ and ϕ are all real numbers. The expression 1.4 is a very convenient method of expressing general qubit state with solely real numbers. The factor $e^{i\gamma}$ is a global phase, which is not observable and can thus be omitted [22]. The remaining representation allows the mapping of all single qubit states onto the surface of the unit sphere, with θ and ϕ the angles of the state away from the logic $|0\rangle$ state, as shown in figure 1.3. This sphere is known as the Bloch or Poincaré-sphere and is a most useful representation for a single qubit. Sadly, there is no simple extension to the multi-qubit world, as the increased dimensionality prevents a useful abstraction into 3-dimensional space. If

the logic basis states lie at the front and back of the equator of the Poincaré-sphere, the equal superposition states lie at the poles and at 90° angles to the logic basis states along the equator respectively. These states are the right- and left-circularly and the diagonally and anti-diagonally linearly polarised states. The alignment of the basis states and the representation of a qubit state in the Poincaré sphere is shown in an example case in figure 1.3.

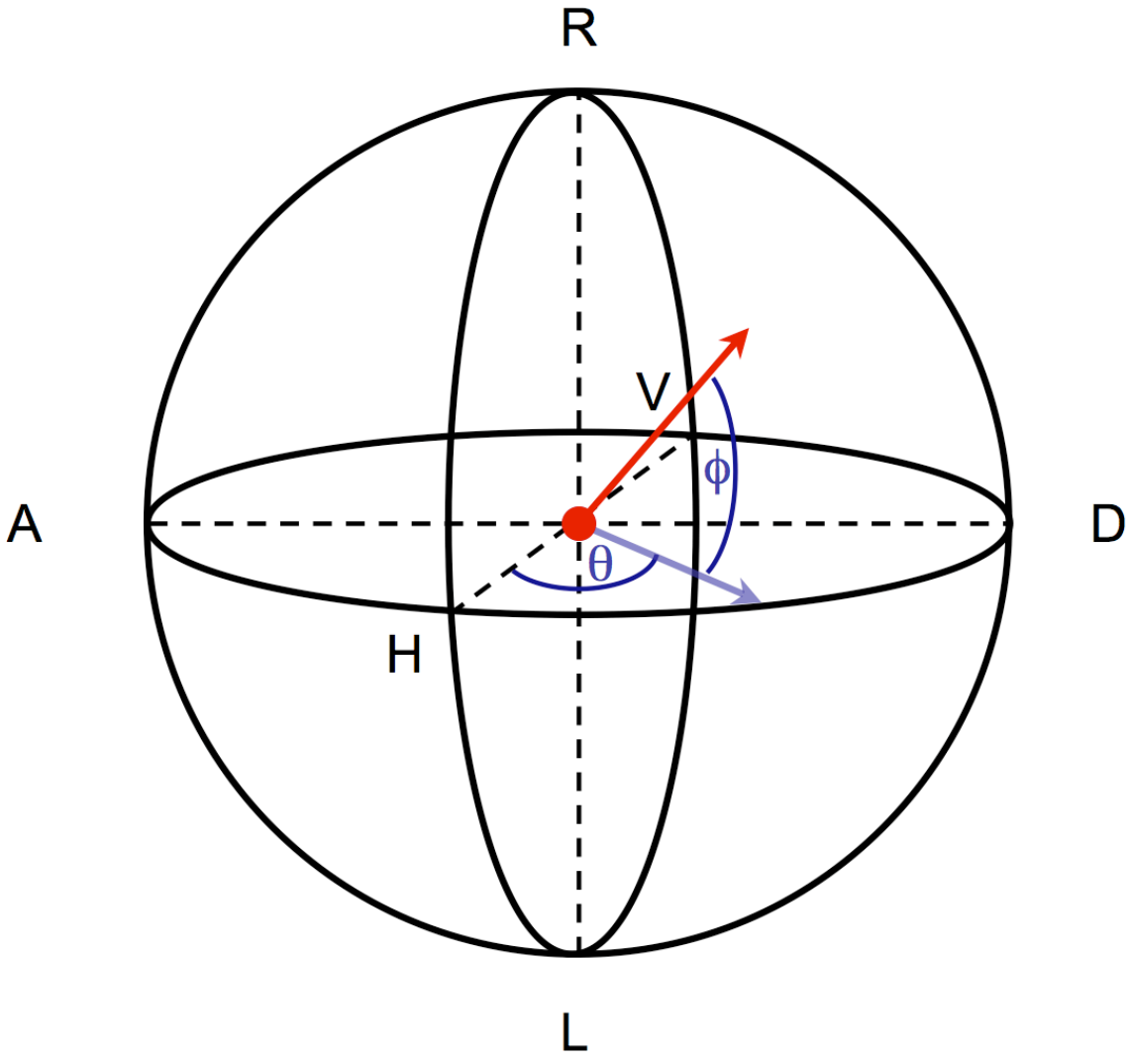


FIGURE 1.3: Mapping of a general one qubit polarisation state onto the Poincaré sphere. The red arrow indicating the state vector originates from the centre of the sphere and reaches the surface for all pure states. The faint blue arrow is the projection of the state vector in the linearly polarised plane. The two angles θ, angle in the linear plane away from the logic 0, here the horizontal state, and ϕ, angle out of the linear plane, are then fully sufficient to completely characterise any pure state. To allow arbitrary states, i.e. any mixed state, the length r of the vector also needs to be specified.

The standard set of states used through out this thesis are

$$\begin{aligned} |H\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |D\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |R\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \\ |V\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad |A\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad |L\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \end{aligned} \tag{1.5}$$

We can easily calculate the corresponding density matrices of theses states as

$$\hat{\rho} = |\psi\rangle\langle\psi|, \tag{1.6}$$

which for our standard qubits states gives us the corresponding density matrices of

$$\begin{aligned} \hat{\rho}_H &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \hat{\rho}_D = \tfrac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \hat{\rho}_R = \frac{1}{2} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} \\ \hat{\rho}_V &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \hat{\rho}_A = \tfrac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \quad \hat{\rho}_L = \frac{1}{2} \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}. \end{aligned} \tag{1.7}$$

1.3.2 What is entanglement: Two twenty line introductions to entanglement

Arguably the most intriguing attribute of a quantum system with two or more particles is the possibility of entanglement between them. A system is said to be entangled if one can no longer describe the state of the system by the tensor product of the states of the individual qubits, i.e. when the notation

$$|\Psi\rangle = |\psi_1\rangle|\psi_2\rangle|\psi_3\rangle \cdots |\psi_N\rangle, \tag{1.8}$$

where N is the number of quantum subsystems, no longer adequately describes the state. States that do fulfil equation 1.8 are said to be separable, as separate, independent wave-functions suffice to fully describe the state. The most famous two-qubit states that exhibit entanglement, i.e. are non-separable, are the four Bell-states. These are:

$$\begin{aligned} |\phi^+\rangle &= \tfrac{1}{\sqrt{2}}\big(|HH\rangle + |VV\rangle\big), \\ |\phi^-\rangle &= \tfrac{1}{\sqrt{2}}\big(|HH\rangle - |VV\rangle\big), \\ |\psi^+\rangle &= \tfrac{1}{\sqrt{2}}\big(|HV\rangle + |VH\rangle\big), \\ |\psi^-\rangle &= \tfrac{1}{\sqrt{2}}\big(|HV\rangle - |VH\rangle\big). \end{aligned} \tag{1.9}$$

The bizarre signature of entanglement is that measurements on these states yield correlations of the measurement results for the two qubits not only in the initial basis, where the output of each individual measurement is well defined, but also in any other arbitrary basis. While in these basis the measurement results on a single qubit are purely random, the perfect correlations of the measurement results for the two particles are retained if they are both measured in the same basis.

While the first definition should have satisfied the theoretically minded, it might have left those with an experimental background slightly dissatisfied as it discusses the mathematical rather than the physical properties of the states. If one looks at the information encoded onto the states, and assuming we use an extended code range where we annotate the four individual Bell States with the logic values $0, 1, 2, 3$. (Alternatively, if we want to remain in the normal bit range using only ones and zeros, we can map the four states on the bits range by using the following mapping $0_4 \rightarrow 00, 1_4 \rightarrow 01, 2_4 \rightarrow 10$ and $3_4 \rightarrow 11$.) Assuming that a priori all states are equally likely to be transmitted, then there is no information that can be gained by measuring just one qubit. Not even a separate measurement of the two qubits in the logic basis will reveal all the information. While this allows the distinction between the $\Phi^{\pm}$ and the $\psi^{\pm}$ states, it still does not identify exactly which one of the four Bell-states was sent and thus which bit value was transmitted. It is only when we measure in a basis formed by states that are orthogonal to those forming the logic basis, which leads to the measurement outcome of each individual measurement to become completely random, that we can identify the correlations of the measurements i.e. the plus or minus signs. This absurdity of having to measure in a basis in which the individual single measurement outcome yields no information, but where the joint measurement of our entangled system reveals all of the information, is the fundamental capacity of entanglement.

It is not (yet) fully understood how, why or even if entanglement is essential in quantum computing, but so far it appears that routines such as Shor's algorithm do require it at some level.

1.3.3 Single qubit operations and waveplates

The evolution of a closed quantum system can be described by the action of unitary operators on the density matrix of the initial state.

$$\hat{\rho}_{out} = \hat{U}\hat{\rho}_{in}\hat{U}^{\dagger} \tag{1.10}$$

In the case of our single qubit state matrices of equation 1.7, the corresponding unitaries are also 2×2 matrices. The most general notation of a single qubit unitary is the rotation by an angle θ around an axis defined by the orthogonal basis vectors $\vec{n}$ (omitting all hats from now on for convenience),

$$U = \quad e^{-i\frac{\alpha}{2}} R_{\vec{n}}(\theta) \quad \text{and} \tag{1.11}$$

$$R_{\vec{n}}(\theta) \equiv \quad e^{-i\theta\vec{n}\cdot\frac{\vec{\sigma}}{2}} = \quad \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z), \tag{1.12}$$

where α is a real number and θ a real angle with $\vec{n}$ the three dimensional unit vector and $\vec{\sigma}$ the vector containing the three Pauli matrices X, Y, Z. This general case can be simplified to the utilisation of three specific rotations, which suffice to emulate any single qubit unitary [22]. The required sequence is

$$U = e^{-i\alpha} \begin{pmatrix} e^{-\frac{i\beta}{2}} & 0 \\ 0 & e^{\frac{i\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-\frac{i\delta}{2}} & 0 \\ 0 & e^{\frac{i\delta}{2}} \end{pmatrix}. \tag{1.13}$$

In this decomposition all α, β, γ and δ are real numbers, and we can identify the specific rotation matrices as defined in equation 1.12 as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta). \tag{1.14}$$

The single most useful tool in the lab for altering the polarisation state of our individual photons are waveplates, which present the unitary operation applied most commonly in the lab. The common waveplates are quarter- and half-waveplates, where their label refers to the maximum retardation these birefringent optical elements impose on the extraordinarily (e) or ordinarily (o) polarised beam, in terms of their design wavelength. Mathematically we can describe their actions on the density matrices for our states by the unitary operation they encode. These are

$$U_{HWP}(\theta) = e^{i\pi/2} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} \tag{1.15}$$

for a half-waveplate (HWP) and

$$U_{QWP}(\theta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 + i\cos 2\theta & i\sin 2\theta \\ \sin 2\theta & 1 - i\cos 2\theta \end{pmatrix} \tag{1.16}$$

for a quarter-waveplate (QWP). The angle θ is defined here as to be equivalent to the physical angle for the setting of the waveplate in the lab with respect to the optic axis and not as in the Poincaré sphere, which leads to the factor of two in the argument of the trigonometric functions. In the Poincaré sphere-picture a half-waveplate thus performs a 180° clockwise rotation of the state vector around the set axis θ, while a quarter-waveplate rotates the vector by 90° clockwise around the set position for the optical axis. In the Poincaré-sphere the rotation axis lies in the plane of the equator and the angle θ is defined with respect to the polarisation state of the state vector. This can be seen in figure 1.4 where each waveplate acts on the horizontal state. In either case, if the state vector and the set position of the optic axis of the waveplate are parallel to each other, the state is not altered.

Comparing the unitaries for the HWP and QWP, we can identify the rotation unitaries similar to those needed to perform arbitrary single qubit operations. In fact, and as noted in section 1.2.3, it can be shown from this that a combination of quarter- half- and quarter-waveplate suffice to implement any single qubit unitary that transforms a pure input state to a pure output state. A more complete discussion can be found in [10].

1.3.4 General quantum operations

The following section is tightly based on the discussion in Ref. [22]. While the evolution of a closed quantum system is very nicely described through unitary operators, the process required for quantum computing will necessarily lead out of this closed space. We therefore introduce the *quantum operation* $\mathcal{E}$ to describe the evolution of open quantum systems. The quantum operation maps the density matrix ρ from the original Hilbert space H to the new density matrix $\mathcal{E}(\rho)$ in the space H'. The quantum operation must fulfil the following requirements [23]

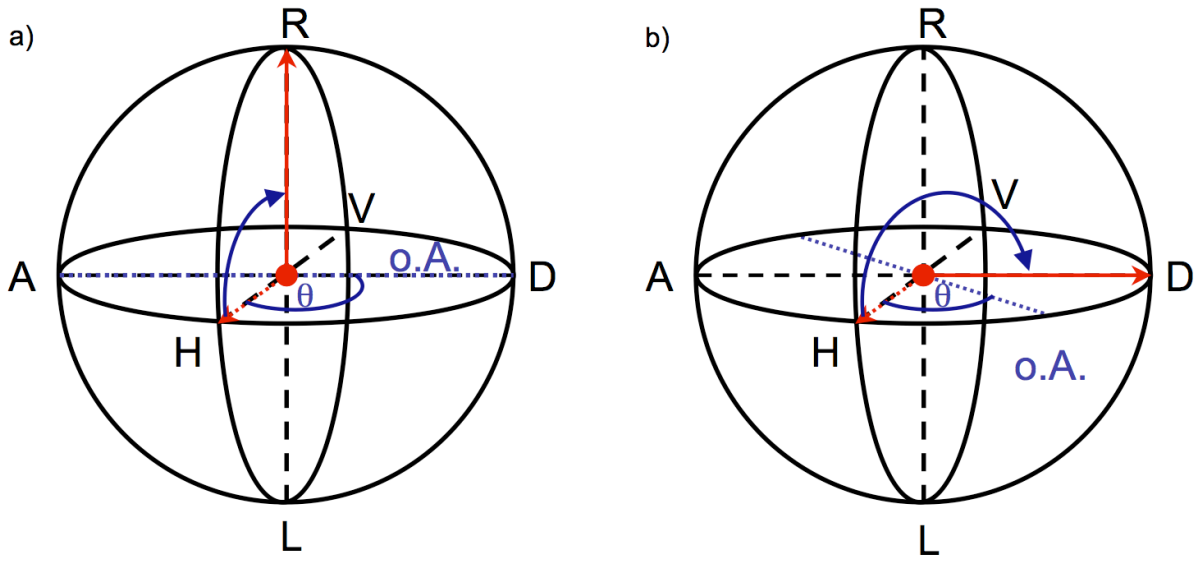


FIGURE 1.4: Actions of a) a quarter-waveplate and b) a half-waveplate set at an angle θ acting on a horizontally polarised input state. The dashed line state vector represents the horizontal state before the action of the wave-plates. The set angle for the optic axis of the waveplate is given by the dashed blue line, with the blue arrow indicates the rotation of the state. The half-waveplate causes a rotation of the state vector by 180° around the optical axis (o.A.) of the waveplate, while the quarter-waveplate rotates the state by 90°. A half-waveplate will therefore not move a state away from the equator of the Poincaré sphere, while it will also transfer right circular light to left circular light and vice versa irrespective of the set angle of the waveplate. Quarter-waveplates can be used to move a state from/to the equator.

1. $\mathcal{E}$ transforms a physical density matrix into another physical density matrix. This requires
$$\forall \rho \text{ with } Tr(\rho) = 1, \quad Tr\big(\mathcal{E}(\rho)\big) = 1.$$

2. $\mathcal{E}$ must be convex and linear.
$$\mathcal{E}\left(\sum_k p_k \rho_k\right) = \sum_k p_k \mathcal{E}(\rho_k)$$

3. The map has to be positive.
$$\mathcal{E}(\rho) > 0 \text{ , if } \rho > 0$$

4. $\mathcal{E}$ must be complete and positive. In an arbitrary space A
$$\mathcal{E}_H \otimes I_A(\rho_{H\otimes A}) > 0 \text{ , if } \rho_{H\otimes A} > 0$$

.

The quantum operation can now be seen as describing any physical process enacted on a subsystem of a larger closed quantum system. The largest possible closed quantum system (and thus most general) is the universe. We can thus evolve the universe with a unitary, in such a manner that
$$\rho' = U\big(\rho \otimes |e_0\rangle\langle e_0|\big)U^\dagger, \tag{1.17}$$

where ρ is the initial state of the subsystem we are interested in, $\{|e_k\rangle\}$ is a complete basis for the universe, which is initially in the state $|e_0\rangle$. By tracing out the remainder of the universe, we can find the state of our subsystem of interest as

$$\mathcal{E}(\rho) = \sum_k \langle e_k|\rho'|e_k\rangle = \sum_k E_k \rho E_k^\dagger, \tag{1.18}$$

where $E_k^\dagger = \langle e_k|U|e_0\rangle$ is an operator on the subspace of the system of interest. After measurement, one finds the system in the state

$$\rho_k \propto \langle e_k|\rho'|e_k\rangle = E_k \rho E_k^\dagger \tag{1.19}$$

This notation is known as the operator-sum or Kraus representation, where E_k are the Kraus operators. One can then easily see that the action of the quantum operation on the system is to randomly, with probability

$$p_k = Tr\left(E_k \rho E_k^\dagger\right), \tag{1.20}$$

replace the initial state ρ with the state ρ_k. We shall make use of this notation and decomposition when discussing the measurement of an unknown process in section 1.4.3.

1.4 Measuring states and gates

As noted in section 1.2.6, the capability to accurately determine the state of a quantum system through measurement is essential in order to read out the results of the computation. The difficulty lies in the nature of quantum physics, where any measurement that reveals some information is necessarily at least partially projective. This implies that the process of measuring the state acts on the qubit state and alters it. Furthermore, even a fully projective measurement on a single quantum system reveals only one bit of information about the state, which is that the qubit was not in a state orthogonal to the measurement result. Additionally, due to the projection our qubit is now in the state corresponding to the measurement result and no further information about the qubits initial state is available. Performing solely a single fully projective measurement on photons is thus not a suitable practice[4].

1.4.1 Stokes parameters and single qubit state tomography

If, instead of a single copy of our to be determined polarised photon, we have an infinitely large ensemble of equally prepared photons, then we can measure the Stokes-parameters to fully determine the state of this ensemble of photons. The Stokes vector $\vec{S}$ is used to describe the polarisation of a classic light field as introduced by Stokes in 1852 [24]. Its

[4]Additionally as we need to detect the photon after the projection with the PBS, unless we perform a non-demolition measurement, the qubit has been absorbed by a detector and thus is actually no longer available for a second measurement.

four components S_0, S_1, S_2, S_3 are the measures of the difference of intensity of orthogonal polarisations in the different polarisation bases.

$$\begin{aligned} \vec{S} &= \begin{pmatrix} S'_0 \\ S'_1 \\ S'_2 \\ S'_3 \end{pmatrix} \text{ , with} \qquad (1.21) \\ S'_0 &= 1 \\ S'_1 &= \frac{I_H - I_V}{I_H + I_V} \\ S'_2 &= \frac{I_D - I_A}{I_D + I_A} \\ S'_3 &= \frac{I_R - I_L}{I_R + I_L}. \qquad (1.22) \end{aligned}$$

The $'$ indicates the use of Stokes parameters normalised to the total intensity. We can immediatly relate these measures to the Poincaré-sphere by noting

$$\begin{aligned} S'_0 &= 1 \\ S'_1 &= r\cos 2\theta \cos 2\phi \\ S'_2 &= r\cos 2\theta \sin 2\phi \\ S'_3 &= r\sin 2\phi \quad \text{, where the degree of polarisation r is} \\ r &= \sqrt{S'^2_1 + S'^2_2 + S'^2_3}. \qquad (1.23) \end{aligned}$$

The Stokes vector can be used in conjunction with Mueller matrices [11] to propagate the polarisation of a light beam through various optical elements analogous to the ray matrices for Gaussian beam propagation. In the quantum picture, the same idea and measurement techniques can be used to derive the density matrix $\hat{\rho}$. By remembering that a measurement is the projection of the state $|\psi\rangle$ into the basis of the respective measurement operator, we can identify the Stokes parameters as the expectation values of measurements in their respective bases. While the actual physical measurements remain the same, we write them now as

$$\begin{aligned} S'_0 = \tfrac{|\langle H|\psi\rangle|^2+|\langle V|\psi\rangle|^2}{|\langle H|\psi\rangle|^2+|\langle V|\psi\rangle|^2} &\equiv 1 \\ S'_1 = \tfrac{|\langle H|\psi\rangle|^2-|\langle V|\psi\rangle|^2}{|\langle H|\psi\rangle|^2+|\langle V|\psi\rangle|^2} & \\ S'_2 = \tfrac{|\langle D|\psi\rangle|^2-|\langle A|\psi\rangle|^2}{|\langle H|\psi\rangle|^2+|\langle V|\psi\rangle|^2} &= \frac{\langle H|\psi\rangle\langle\psi|V\rangle + \langle V|\psi\rangle\langle\psi|H\rangle}{|\langle H|\psi\rangle|^2 + |\langle V|\psi\rangle|^2} \\ S'_3 = \tfrac{|\langle R|\psi\rangle|^2-|\langle L|\psi\rangle|^2}{|\langle H|\psi\rangle|^2+|\langle V|\psi\rangle|^2} &= \frac{i(\langle H|\psi\rangle\langle\psi|V\rangle - \langle V|\psi\rangle\langle\psi|H\rangle)}{|\langle H|\psi\rangle|^2 + |\langle V|\psi\rangle|^2}. \qquad (1.24) \end{aligned}$$

Recalling the definition of the density matirices for the states given in equation 1.7, we see

that the Stokes parameters in the quantum picture correspond to

$$\begin{aligned} S'_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv \sigma_I \\ S'_1 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \equiv \sigma_Z \\ S'_2 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv \sigma_X \\ S'_3 &= \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \equiv \sigma_Y, \end{aligned} \tag{1.25}$$

which are simply the four Pauli-spin matrices. It becomes straight-forward, how to reconstruct the measured quantum state from these, as we can use the individual spin matrices to describe all aspects of the state. The density matrix for the single photon state can thus be reconstructed as

$$\hat{\rho} = \frac{1}{2} \begin{pmatrix} S'_0 + S'_1 & S'_2 - iS'_3 \\ S'_2 + iS'_3 & S'_0 - S'_1 \end{pmatrix}, \tag{1.26}$$

revealing the state of the measured photons. One further difficulty arises: Commonly the measurement data is affected by noise, which for example could be caused by slight misalignments of the measurement apparatus or detector dark counts. This measurement noise tends to cause the derivation of unphysical states if one blindly applies the above described method. Obviously one has some natural doubts about the accuracy of the results if the reconstructed state is unphysical. A mathematical method known as maximum likelihood has been employed to prevent such unphysical results. This routine searches the space of all physical density matrices for the one which is most likely to have created the measurement results obtained. A methodology for maximum likelihood tomography is given in [25, 26] and is discussed in more detail in [10].

1.4.2 Two qubit state tomography

Two qubit state tomography is the extension of the mechanisms developed in the section 1.4.1 to the higher dimensional space in which pairs of photons can exist. The formalism is easily extended by defining the new basis states as all pair-wise combinations of the single qubit logic states. This leaves us with

$$\begin{aligned} |HH\rangle &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |HV\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \\ |VH\rangle &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |VV\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned} \tag{1.27}$$

as our new basis state vectors. The corresponding density matrices can be developed similar to the one qubit case and an example is given below for the $|HH\rangle$ state. The other states can easily be developed analogously to the example case. We expand the state

$$\begin{aligned} \rho_{HH} &= |HH\rangle\langle HH|, \text{ which equals} \\ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \rho_{HH} \end{aligned} \tag{1.28}$$

In order to determine the actual two qubit state, we have to effectively characterise each individual qubit with respect to the state of the other photon. We thus utilise the same set of measurement states for each qubit as previously in the single qubit case. This leaves us with a minimum of 16 measurements, which are constructed as $\{H, V, D, R\} \otimes \{H, V, D, R\}$. The reconstruction is again an extension of the methods used in the single qubit case, with details discussed in [26].

1.4.3 Process Tomography

This section is (again) tightly based on Ref. [22], which also contains a nice example for the single qubit process tomography on page 393.

Similar to measuring the state of a quantum particle, where a single measurement does not suffice to completely characterise the state of a qubit, the process a quantum operation enacts can not be fully characterised by using just a single input state and measuring the output state. Using the quantum operation notation introduced in section 1.3.4, we can write our arbitrary process as the action on our quantum system via the map $\mathcal{E}$. We already know from equation 1.19 that there exists a specific decomposition into a sum of certain operational elements that, when acted on the original density matrix reproduces the transformation as found by the actual operation. These operational elements $\{E_k\}$ used to describe the quantum operation usually have no sensible experimental counterpart. Therefore rather than to adopt the experimental measurements to suit an unknown process, we use a fixed set of operators $\tilde{E}_i$ that form a basis for the set of operations on the state space at hand. It must be possible then to decompose our map $\mathcal{E}$ with our basis operators so that

$$\mathcal{E}(\rho) = \sum_{mn} \tilde{E}_m \rho \tilde{E}_n^\dagger \chi_{mn} \quad \text{, where } \chi_{mn} \equiv \sum_i e_{im} e_{in}^* \tag{1.29}$$

are the complex valued elements of the χ-matrix that completely suffices to describe the operation in the given basis of operators we choose. Experimentally, we can find the entries χ_{mn} of the matrix by enacting our quantum operation on the complete basis set of states of our space and performing state tomography on the output. For a single qubit process, this requires the input of a minimum of 4 states, which can generally be written as $\left\{ |n\rangle, |m\rangle, |+\rangle = \frac{(|n\rangle+|m\rangle)}{\sqrt{2}}, |i+\rangle = \frac{(|n\rangle+i|m\rangle)}{\sqrt{2}} \right\}$, where $|n\rangle$ and $|m\rangle$ form a basis in the single qubit space. As it is possible to decompose the action on any state $|n\rangle\langle m|$ into the action

on the set of states given above, we can write

$$\mathcal{E}(|n\rangle\langle m|) = \mathcal{E}(|+\rangle\langle +|) + i\mathcal{E}(|i+\rangle\langle i+|) - \frac{1+i}{2}\mathcal{E}(|n\rangle\langle n|) - \frac{1+i}{2}\mathcal{E}(|m\rangle\langle m|). \tag{1.30}$$

Note that we do not need to reconstruct the individual states, the required data set that we need to measure however coincides with those required for the state tomographies of our input states. We can then reconstruct the states $\mathcal{E}(\rho_j)$ which can be given as a linear combination of our basis states ρ_k by

$$\mathcal{E}(\rho_j) = \sum_k \lambda_{jk}\rho_k. \tag{1.31}$$

We can expand our map $\mathcal{E}$ into the operators of our basis, such that

$$\tilde{E}_m \rho_j \tilde{E}_n^\dagger = \sum_k \beta_{jk}^{mn} \rho_k, \tag{1.32}$$

where the β_{jk}^{mn} are complex numbers which can be determined through linear algebra for the specific set of input state and operators. Combining this notation with that from equation 1.29, we arrive at

$$\sum_k \sum_{mn} \chi_{mn}\beta_{jk}^{mn}\rho_k = \sum_k \lambda_{jk}\rho_k \text{ and} \tag{1.33}$$

$$\sum_{mn} \chi_{mn}\beta_{jk}^{mn} = \lambda_{jk}, \tag{1.34}$$

which gives us a necessary and sufficient condition for our χ matrix.

Experimentally, for our polarisation encoded photonic qubits, the obvious choices for our basis states are $|H\rangle$ and $|V\rangle$ as well as $|D\rangle = \frac{(|H\rangle+|V\rangle)}{\sqrt{2}}$ and $|R\rangle = \frac{(|H\rangle+i|V\rangle)}{\sqrt{2}}$ as our superposition states. Using these states as inputs, and performing state tomography, we can use the above formalism to reconstruct the χ matrix for the operation of any black-box quantum operation. As there is no unique basis into which we have to decompose our operation, one commonly chosen basis is the Pauli bases, where the quantum operations are the Pauli spin matrices. In general, process tomography requires 2^{4n} measurements, where n is the number of qubits. This exponential increase makes the characterisation of large systems with current methods unfeasible at the present time.

Process tomography is independent of the architecture and has been first described in detail in Ref. [27] generally, and in [28] with a specific view to trapped ions as qubits. The first description of process tomography in any architecture was on an optical two-qubit gate [29], which was also the first to employ a full set of constraints on the maximum-likelihood reconstruction-technique, which ensured that despite experimental noise the reconstructed processes were physical (i.e. process is completely positive and does not increase the trace).

1.4.4 Measuring the gate performance

In the previous chapters I have introduced ways to measure the state of single and multi-photon states, and a procedure to analyse the process of a quantum black-box operation. I

will now introduce the actual measures used throughout the thesis to gauge the quality of the states and processes investigated in this thesis. The measures commonly discussed for states are the *Purity*, which is simply the trace of the square of the density matrix, thus

$$\mathcal{P} = Tr(\rho^2). \tag{1.35}$$

The *Linear Entropy*, measuring the degree of mixture of a state is defined as

$$S_L = \frac{4}{3}\big(1 - \mathrm{Tr}(\rho^2)\big), \tag{1.36}$$

and ranges from 0 for a pure state, to 1 for a maximally mixed state. The *Tangle* again varies from 0 for a completely separable state to 1 for a maximally entangled state and is a measure of the quantum coherence of a mixed quantum state. It is defined as

$$T = (\max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\})^2, \tag{1.37}$$

where the λ_i are the ordered (from biggest to smallest) eigenvalues of $\rho\tilde{\rho}$ with $\tilde{\rho}$ being the spin-flipped density matrix defined as $\tilde{\rho} = (Y \otimes Y)\rho^*(Y \otimes Y)$. All of the above measures characterise a single quantum state. When analysing the actions of the gate, it will be important to compare them with the expected ideal states. For this we use the *Fidelity*, defined as

$$F(\sigma, \rho) \equiv \big(Tr\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\big)^2, \tag{1.38}$$

for the density matrices ρ and σ. The Fidelity ranges from 0 to 1, where 1 reveals a set of identical states and 0 an orthogonal set of states. We will use the same definition to compare the χ-matrices of our processes to the ideal. Such a fidelity measure is then denoted the *Process Fidelity*, F_p. While the process fidelity is a somewhat intuitive measure revealing the closeness (or not) of the implemented operation with the desired process, it is actually not a suitable metric, as it does not obey desired chaining relations for multiple subsequent processes [30]. However it can be used to construct any of several suitable metrics such as the stabilized trace distance. As the limitations for the process fidelity arise mainly once one starts chaining multiple gates, I will retain the usage of the process fidelity as I feel that it is a more intuitively related measure of the performance of the quantum circuit. One can derive the *Average Gate Fidelity*, $\overline{F}$, from the process fidelity as

$$\overline{F} = \frac{d \cdot F_p + 1}{d + 1}, \tag{1.39}$$

where d is the dimension of the quantum system, i.e. $d = 2$ for a single qubit and $d = 4$ for two qubit systems. The average gate fidelity, contrary to the process fidelity, obeys the chaining requirement for subsequent gates and can be physically interpreted as the fidelity of all pure input states averaged over all output states. Nevertheless as it is variant under alternation of the dimensionally of the problem it still is not a suitable metric. For a more detailed discussion on state and process measures, their pros and cons, the reader is referred to [26, 30, 31].

1.5 Two photon interaction: Making it happen

One of the key reasons why photons are such good qubits, is also their downfall. The fact that photons are virtually interaction-free leads to low decoherence, but also makes the control of a single photon via another single photon seemingly all but impossible. There are no materials with non-linearities large enough to alter the polarisation state of a single photon with the power of single photons for the full π-phase shift required for fully entangling gates. Cavity quantum electrodynamics (cavity QED) is closest to this goal, with a scheme [32], where single atoms are trapped inside or floated through very high finesse cavities. The circular birefringence of the atom pumped by the first photon rotates the linear polarisation state of the target photon while it is passing through the cavity. The polarisation state of the target photon picks up a phase shift depending on which of the two upper levels of the three level atom the state of the atom was pumped to by the first photon. A significant downside of this method is the involved complexity, requiring large scale ultra-high vacuum devices, atomic beams and high-finess cavities, which as of now make the scaling to large qubit numbers infeasible.

A further scheme for optical quantum computing requires phase shifts much smaller than the full π, yet larger than currently readily available outside cavity QED. In this scheme [33], the single photons of the control and target are split spatially into two logic rails, where the logic $|1\rangle$ state of each interact with a bright coherent squeezed state, inside a strong Kerr non-linearity, thereby encoding a slight phase shift on the squeezed state. Through suitable design, the control and target encode equal but opposite phase shifts. Through a homodyne measurement after the dual interaction one either detects a phase shift, in which case an odd parity of the logic states of the control and target photon is revealed, or no phase-shift is found, indicating even parity [33]. Through appropriate feed-forward of this measurement result, entanglement between the two single photons of the control and target can be achieved and i.e. a CNOT-gate can be implemented.

The need for such currently unachievable non-linearities was circumvented by measurement induced non-linearities as suggested by Knill Laflamme and Milburn (KLM) in their ground breaking paper [12]. They devised a method which used the detection of certain events to project the general state onto a sub-state, in which the photons have seemingly interacted. By using a sophisticated network of interferometers they showed that it was possible to encode a sign-shift on the combined state of the photons for only one specific logically pure input state, while leaving all other logic input states unchanged.

1.5.1 Hong-Ou-Mandel Interference

At the core of this interaction lies the non-classical interference of single photons, first observed by Hong, Ou and Mandel (HOM) [13]. The HOM-effect occurs when two indistinguishable photons impinge on a 50:50 beamsplitter one from either side. While individually each photon has a probability of 50% to be either reflected or transmitted, the two photons will always bunch together, meaning, if one is reflected, the other one is always transmitted, leaving one mode populated with two indistinguishable photons, while the other mode is the vacuum-mode, this behaviour is depicted in figure 1.5.

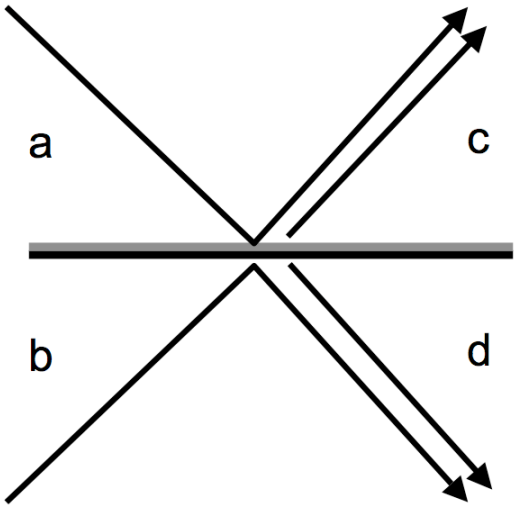


FIGURE 1.5: Schematic of the Hong-Ou-Mandel interference. when two indistinguishable photons (here arrows) impinge on a 50:50 beamsplitter, their bosonic nature forces them to bunch together and leave as a pair in either the c or d mode. Hence the double arrows in the output modes are to be understood as existing either-or.

The general mathematical description using the mode labels from figure 1.5 works as follows. If the photons are distinguishable[5] in any which way, i.e. in their arrival time, this introduces an effective mode-labelling, and there will be no interference. Hence the probability of the two photons emerging in the different modes is simply the product of the probabilities of each photon taking a certain path. Thus the probability of detecting a single photon in each output mode can be written as:

$$P_{dist} = \eta^2 + (1-\eta)^2, \tag{1.40}$$

which for the reflectivity of $\eta = \frac{1}{2}$ equals the well expected 1/2, with the two terms consisting of the two options of either reflecting both photons, η^2, or transmitting both, $(1-\eta)^2$, with all other cases not leading to a single photon in each output port. Thus for distinguishable photons one will be able to observe a single photon in each output mode in 50% of all cases.

If however two indistinguishable photons are injected in modes a and b, at the beamsplitter each photon experiences the following transformation

$$a_a^\dagger \to i\sqrt{\eta}a_c^\dagger + \sqrt{1-\eta}a_d^\dagger \quad \text{and} \tag{1.41}$$

$$a_b^\dagger \to i\sqrt{\eta}a_d^\dagger + \sqrt{1-\eta}a_c^\dagger. \tag{1.42}$$

For the input state

$$|\Psi_{in}\rangle = a_a^\dagger a_b^\dagger |00\rangle \tag{1.43}$$

the resulting state is then given by the product of the individual output states above, hence

$$|\Psi_{out}\rangle = \left(i\sqrt{\eta}\sqrt{1-\eta}a_c^{\dagger 2} + i\sqrt{\eta}\sqrt{1-\eta}a_d^{\dagger 2} + (1-2\eta)a_c^\dagger a_d^\dagger\right)|00\rangle. \tag{1.44}$$

[5]Note that distinguishability is a continuous parameter that ranges from perfect indistinguishability to perfectly distinguishability via all values in between. For example when photons of different, yet non-orthogonal polarisation interfere, they are said to be partially distinguishable, and will yield some limited interference where the interaction strength is proportional to there degree of indistinguishability.

In the KLM scheme successful operation is signalled by each of our modes being populated by exactly one photon. In principle this can be determined by a non-demolition measurement of the photon number in each mode. In practise, optical quantum computation relies on the coincident detection of photons, assuming that they are single photons, to herald the successful gate operation. Hence we are only interested in those terms, where both modes are populated, as only those will trigger a coincidence signal and thus a registered event. As the probability is the absolute square of the amplitude, the probability for a coincident detection with indistinguishable photons becomes

$$P_{indist} = |(1 - 2\eta)|^2 \tag{1.45}$$

For $\eta = \frac{1}{2}$ this term vanishes, resulting in no cases where both output modes will be populated.

By taking the difference between the probabilities of detecting one photon in each output mode for the distinguishable and the indistinguishable case, we can define the visibility of the non-classical interference[6] as

$$V = \frac{P_{dist} - P_{indist}}{P_{dist}} = \frac{(\eta^2 + (1-\eta)^2) - |(1-2\eta)|^2}{(\eta^2 + (1-\eta)^2)} \tag{1.46}$$

Experimentally the visibility is measured by the reduction in count rates between the non-interfering rate (distinguishable photons) and the one where the photons interact (indistinguishable photons),

$$V = \frac{C_{distinguishable} - C_{indistinguishable}}{C_{distinguishable}}. \tag{1.47}$$

The visibility of the Hong-Ou-Mandel-interference is therefore a measure of the degree of indistinguishability of the photons.

1.5.2 Making entangling gates

While the HOM-interference with a $\eta = \frac{1}{2}$ beamsplitter allows a measure of the degree of indistinguishability of photons, this by itself is not yet very useful for optical quantum computing. At first glance it may appear that only the maximal visibility is altered when $\eta \neq 1/2$. However when pairing the HOM-interference with a classical interferometer, as suggested by Ralph *et al.* [34] that separates the logic basis states as shown in figure 1.6, then the interaction no longer applies to all indistinguishable photons, but now only to those of horizontal polarisation, the logic $|0\rangle$ state. Vertical photons can never reach the central beamsplitter and thus even if indistinguishable in principle can never interact. The transformation applied by the circuit depicted in figure 1.6 is given mathematically by the following: The input state

[6] The more common definition if visibility is $V = \frac{P_{dist} - P_{indist}}{P_{dist} + P_{indist}}$, which is useful for signals that vary from the average both positively and negatively. For non-classical quantum interference however the coincidence count rate will only decrease and ideally to zero, hence the slightly altered definition is commonly used in this field.

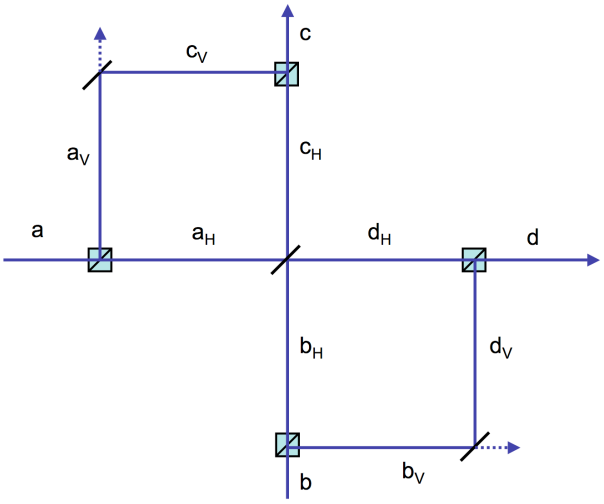


FIGURE 1.6: By separating the logic basis states H and V with polarising beamsplitters, the non-classical interaction at the central beamsplitter can only occur between horizontally polarised photons. The vertical photons are attenuated in their amplitude on the reflecting beamsplitters (loss indicated by dashed arrows) in order to retain balanced amplitudes between H and V polarised photons. After the non-classical interference for the H and the loss for the V component, the spatially separated complementary logic modes are recombined.

$$|\Psi_{in}\rangle = (\alpha a_H^\dagger + \beta a_V^\dagger)(\gamma b_H^\dagger + \delta b_V^\dagger)|00\rangle, \tag{1.48}$$

where α and β as well as γ and δ obey the normalisation conditions imposed by eqn. 1.3, gets transformed following the rules

$$a_H^\dagger \rightarrow i\sqrt{\eta}c_H^\dagger + \sqrt{1-\eta}d_H^\dagger, \tag{1.49}$$
$$b_H^\dagger \rightarrow i\sqrt{\eta}d_H^\dagger + \sqrt{1-\eta}e_H^\dagger \tag{1.50}$$

for the horizontal component, and

$$a_V^\dagger \rightarrow i\sqrt{\eta}c_V^\dagger, \tag{1.51}$$
$$b_V^\dagger \rightarrow i\sqrt{\eta}d_V^\dagger \tag{1.52}$$

for the vertical component. The loss on the vertical component is incorporated solely to retain balanced amplitudes between the horizontal and vertical components. For the general

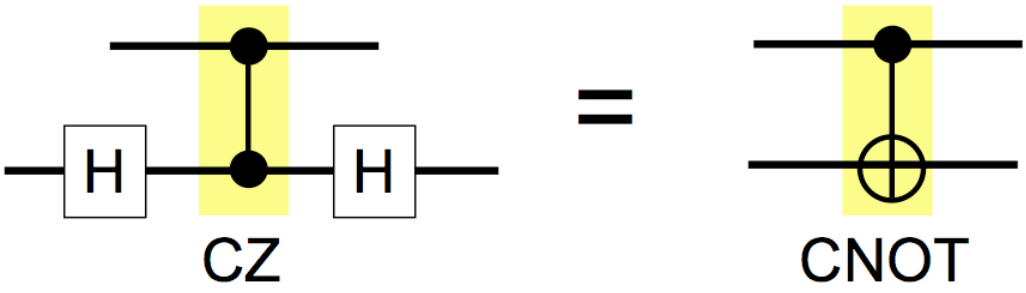


Figure 1.7: A controlled Z gate shown on the left hand side in the yellow shade equals to a controlled-NOT gate when one of the two qubits is bracketed by Hadamard gates before and after the gate action.

input state given in eqn 1.48 the resultant output state of the gate is given as

$$\begin{aligned}|\Psi_{out}\rangle \;=\Big(\;& -\alpha\gamma\eta c_H^\dagger d_H^\dagger \\ &+ i\alpha\gamma\sqrt{1-\eta}\sqrt{\eta}c_H^{\dagger 2} \\ &- \alpha\delta\eta c_H^\dagger d_V^\dagger \\ &+ i\alpha\gamma\sqrt{1-\eta}\sqrt{\eta}d_H^{\dagger 2} \\ &+ \alpha\delta(1-\eta)c_H^\dagger d_H^\dagger \\ &+ i\alpha\delta\sqrt{1-\eta}\sqrt{\eta}d_H^\dagger d_V^\dagger \\ &- \beta\gamma\eta c_V^\dagger d_H^\dagger \\ &+ i\beta\gamma\sqrt{1-\eta}\sqrt{\eta}c_H^\dagger c_V^\dagger \\ &- \beta\delta\eta c_V^\dagger d_V^\dagger\Big)|00\rangle, \end{aligned} \tag{1.53}$$

which once simplified by post-selection on cases with one photon in each output mode c and d, reduces to

$$|\Psi_{out}\rangle = \Big(\alpha\gamma\big(1-2\eta\big)c_H^\dagger d_H^\dagger - \alpha\delta\eta c_H^\dagger d_V^\dagger - \beta\gamma\eta c_V^\dagger d_H^\dagger - \beta\delta\eta c_V^\dagger d_V^\dagger\Big)|00\rangle \tag{1.54}$$

For the specific choice of $\eta = \frac{1}{3}$ the output state is not only balanced in its probabilities, but the logic $c_H^\dagger d_H^\dagger|00\rangle$ state experiences a phaseshift relative to all other states. This change in sign named this gate the controlled-sign (CSign) gate, also known as the controlled-phase or controlled-Z (CZ) gate and belongs to the class of entangling two qubit gates that is required for quantum computing to make a "universal" gate set. It is closely related to the well known CNOT-gate, a CZ gate with Hadamard-gates on the in and output of the target qubit forms a CNOT gate, as shown in figure 1.7, where the Hadamard-gate is the single qubit gate given by

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

The Hadamard gate maps the logic basis states to the equal real superposition states, in our case $\mathrm{H}|H\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = |D\rangle$. For polarisation encoded photonic qubits this action can

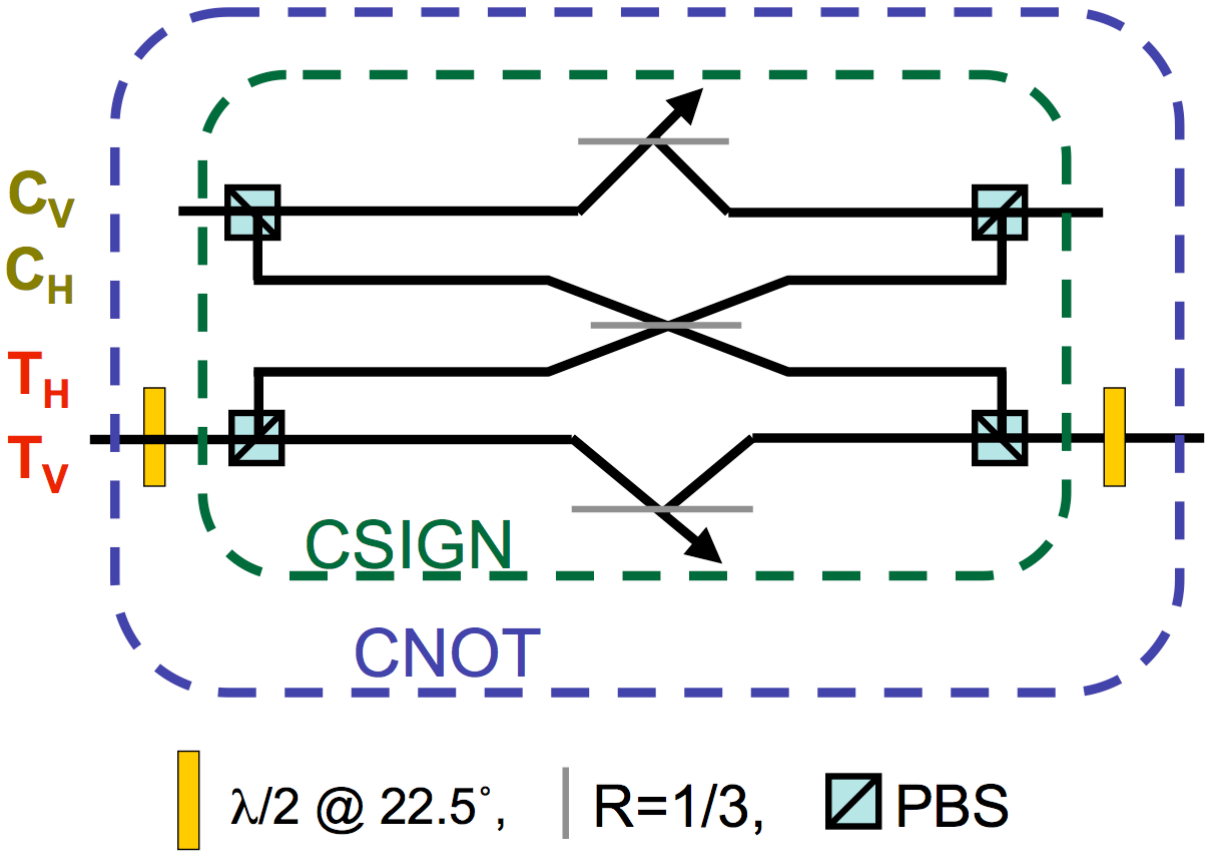


FIGURE 1.8: Experimentally the only difference between a polarisation encoded controlled Sign gate and a controlled-NOT gate is a half-waveplate set at 22.5° *before* the logic modes are split for the gate and *after* they are recombined. This waveplate acts as a Hadamard-gate converting a logically pure population into an equal superposition.

be achieved with a half-waveplate set at 22.5°. Therefore the only difference between the CNOT- and the CZ-gate in optical quantum computing is the addition of a half-waveplate on the in and output mode of the target qubit as shown in the circuit of figure 1.8. It should be noted at this point that the CZ-gate effectively has no specified control and target qubit as its action is symmetric. The phase shift gets added only when *both* input qubits are in the logic 1 state. As briefly touched upon we require that the output modes of our gates are populated by exactly one photon and that we had strictly single photon inputs. In this case the CZ gate of [34] works in post-selection on coincidenent detection of single photons in each output mode. Therefore the gate works only $1/9^{th}$ of the time, the other $8/9^{th}$ of the time the gate fails. However this failure is detectable and thus these cases can be discarded.

In principle this requires measuring the population of the output modes, and since a full projective measurement of a quantum state is destructive, we are required to incorporate a non-demolition measurement of the output mode population. Such a measurement can with some probability measure the photon number of the given mode without destroying it [35]. An alternative path is shown in the original work of KLM, where it is shown that the use of further ancilla photons can alleviate the need to detect the qubit photons: If with the appropriate circuit a single photon is detected in each ancilla mode, the gate has operated

successfully and the qubit photons remain unaffected and available for further computational steps. Furthermore, KLM shows that it is possible to increase the success rate of the gate from 1/9 to arbitrarily close to 1: the entangling step is performed between two ancilla photons. Once successful gate operation has been detected the logic state of our qubits is teleported [36–39] onto the output of the the gate. This principle operation is depicted in figure 1.2. Thus, while in its current form very resource intensive, this method in fact allows scalable quantum computation with non-deterministic gates.

A much more resource friendly method of optical quantum computation is the cluster state quantum computation paradigm. Its draw back is that it requires large entangled states as input, a resource not currently available. However the non-deterministic gates of the KLM-type can be used to create the entangled input states off-line, meaning that the gates produce the input state, and computation takes place once the cluster has reached a sufficient size for the applicable algorithm. Alternatively, future sources [40–42] might readily produce entangled photons which can then be used to build the input state for cluster computation. If either one of these methodologies can efficiently and readily produce large entangled states, cluster-state quantum computing will be the simpler computing paradigm to implement in optics as no two-qubit gates are required during the computation.

2

Single photons, and how to make them

Gates based on measurement induced non-linearities require single photon inputs for all gate and ancilla modes. This requirement is caused by the nature of the non-classical interference, which is significantly altered if more than one photon is present in one mode (see section 4.4.3 for a more detailed discussion). Ideally, this requires the abundant presence of single photon sources: devices which emit one and only one photon in a given spatial, spectral and temporal mode upon a triggering signal. Such a device does not exist (yet), though promising research is underway in various architectures [43].

2.1 The optical workhorse: Parametric down-conversion

In the absence of true single photon sources, research has turned to the next best thing: generating pairs of photons simultaneously in well defined spectral, spatial and temporal modes. This process is known as spontaneous parametric down conversion (PDC). It was first observed in 1969/1970 [44, 45] and at first appears to be the inverse of second harmonic generation (SHG), as a high energy photon decays into two low energy photons. By suitable configuration of ones experimental setup, one can design their PDC source to emit the pairs of photons in either different spatial, spectral or polarisation modes, or a combination of these which allows the separation of the photons in different logic modes for the experiments. During the work presented in this thesis the down converted photons are emitted in different spatial modes allowing their separation for the experiments.

Both of these effects, SHG and PDC, can only occur in the presence of a non-linear medium[1], where the dielectric polarisation (dipole moment per unit volume) responds in a non-linear manner to an electric field. This response can be expanded in a power series of

[1]Strictly speaking, the vacuum has a non-zero polarisabillity and is thus a very weak non-linear material, hence technically no medium needs to be present.

the electric field[2] :

$$P(t) = \chi^{(1)}E(t) + \chi^{(2)}E^2(t) + \chi^{(3)}E^3(t) + ... \tag{2.1}$$

To understand the conversion process, consider these cases: In a linear material, combining two oscillating fields of the frequency ω is similar to the sum of two sine waves of the same frequency and will hence produce a resulting oscillating field at the same frequency. Inside a non-linear material the two oscillating fields can produce the product $(E_1 \times E_2)$, which following the trigonometric identity

$$2\ \cos\omega\ \sin\omega = \sin 2\omega \tag{2.2}$$

gives rise to a field at twice the frequency (Or two fields at half the frequency, reading it right to left, as is the case in SHG, where two low energy (frequency) pump photons combine into one high energy output photon). In PDC a pump photon of high energy decays into two photons of lower energy. What is referred to as PDC throughout this thesis is more accurately named SPDC — *spontaneous* parametric down-conversion— as the parametric process is running well below threshold. As the entire process obeys energy and momentum conservation, the photons satisfy the following equations inside the non-linear material:

$$\omega_p = \omega_i + \omega_s, \quad \text{and} \tag{2.3}$$

$$\vec{k}_p = \vec{k}_i + \vec{k}_s, \tag{2.4}$$

where p denotes the pump, i the idler and s the signal photon. Furthermore the non-linear crystal can absorb or emit the energy of a phonon during this process, so that neither the energy relation nor the momentum conservation are strictly obeyed when considering only the involved photons.

The simplified view given in equation 2.1 however does not necessarily populate the modes of the signal and idler photon if one follows the classic view as these modes start from a vacuum population and hence their derivatives would necessarily have a 0 starting value. To understand the process one needs to consider vacuum fluctuations we requires us to utilise a quantised approach. A complete derivation of PDC requires a quantisation of the electric field [46], and will not be presented here, however a much simplified version based on [10, 47] is given as it will aid in the understanding of some multi-photon features and their scaling which is an central part of this thesis. For this we will describe the three-wave mixing process that is PDC using the following interaction Hamiltonian.

$$H_{int} = g a_i^\dagger a_s^\dagger a_p + g^* a_i a_s a_p^\dagger \tag{2.5}$$

Here g is a coupling constant ($\propto \chi^{(2)}$) and $a^(\dagger)_n$ is the annihilation (creation) operator for the n-th mode. We can see here that the second term describes the annihilation of two photons, one each in the signal and idler mode while a photon in the pump mode is being created — sum frequency generation, while the conjugate, the first term, destroys a pump photon and creates an idler and signal photon and gives us the quantum mechanical description of parametric down-conversion. We can now utilise this Hamiltonian to evolve the initial state,

[2]Practically the dielectric susceptibility coefficients χ are of course tensors, but for simplicity this is ignored here.

where we take our pump mode to be a coherent state $|\gamma\rangle_p$ with $|\gamma|^2 \gg 1$ and while the idler and signal modes are both vacuum modes.

$$|\psi(t)\rangle = \exp\left(\frac{-iH_{int}}{\hbar}\right)|\psi(0)\rangle \tag{2.6}$$

$$= A\sum_{k=0}\frac{1}{k!}\left(\frac{-itH_{int}}{\hbar}\right)^k |0\rangle_i|0\rangle_s|\gamma\rangle_p \tag{2.7}$$

$$= A[1 + \frac{-itH_{int}}{1!\hbar} + \left(\frac{-itH_{int}}{2!\hbar}\right)^2 - \left(\frac{-itH_{int}}{3!\hbar}\right)^3 + ...]|0\rangle_i|0\rangle_s|\gamma\rangle_p \tag{2.8}$$

$$\approx A[|0_i0_s\rangle + \frac{-itg\gamma}{\hbar}|1_i1_s\rangle + \left(\frac{-itg\gamma}{\hbar}\right)^2|2_i2_s\rangle + \left(\frac{-itg\gamma}{\hbar}\right)^3|3_i3_s\rangle + ...] \otimes |\gamma_p\rangle \tag{2.9}$$

$$= A\Big(|0_i0_s\rangle + \kappa|1_i1_s\rangle + \kappa^2|2_i2_s\rangle + \kappa^3|3_i3_s\rangle + ...]\Big) \otimes |\gamma_p\rangle \tag{2.10}$$

Here $\kappa = -itg\gamma/\hbar$ and we assume that the population of the pump mode is not significantly changed by the interaction, as can generally be assumed for a classical pump field. This treatment of the interaction shows us that there is some[3] small amplitude of generating pairs of photons in the signal and idler modes, however this is amplitude is typically small as noted earlier. This amplitude is proportional to the coupling constant and thus $\chi^{(2)}$ and the pump field amplitude. We can see from these equations, that the generation of a pair of photons is hence directly proportional to the pump power, while the production of two pairs scales with the square of the pump power and three pairs with the cube and so on. Typically these higher order terms are much much smaller than the first order term and are often neglected. However in a regime where the amplitude of the pump field is very high, these terms can be come significant. Such intense pump fields are typically generated by femtosecond pulsed pump lasers as were used during the experiments described in this thesis. Hence the effect of this multi-pair generation is a core result of this thesis and discussed in detail in Chapter 4

Due to the conservation of energy, one can operate in the degenerate case, where the two photons of lower frequency are of equal wavelength, which is twice that of the pump photon. Typically any non-linear material used for frequency conversion purposes exhibits birefringence, hence, as in SHG, there are two different down-conversion processes, the Type I and Type II process. In Type I, the idler and signal photons are of the same polarisation and will thus experience the same refractive indices, if their wavelengths are matched. In the Type II process the signal and idler photon are of orthogonal polarisation and will thus experience different refractive indices, which gives rise to a slight temporal delay of one photon with respect to the other. This delay introduces some distinguishability, which as discussed in section 1.5 will lead to a reduced visibility, which degrades the gate performance and thereby reduce the maximal achievable entanglement for our gates. For this thesis, photons with entanglement from the source are at no stage required nor desired, thus the effects of this delay are unimportant here. The conservation of momentum also makes a strict prediction of the respective output angles of the paired photons. During the course

[3]very, very, very, very ,very, very, very... (Typical efficiencies are on the order of 10^{-8} to 10^{-10})

of my experiments, I used both type-I and type-II sources, which will be discussed in more detail in the sections 2.2.1 and 2.2.2.

2.1.1 The Coincidence detection regime

Experimental optical quantum computing is marred by two main problems, the first is the absence of single photon guns as discussed earlier. This however could be tolerated if one had ideally unit efficient detectors that can resolve the number of photons that they detected. But again reality is not so kind as to provide these. In this experimentally horrific world however experimentalists are thrown a bone by PDC. Since PDC produces pairs of photons, the correct operation of the circuit can be identified when one observes simultaneous detection events on all the output modes of the experimental circuit. (Remembering that we required exactly one photon as input into each of our circuit modes). This detection regime is called the coincidence basis and limits todays experiments to proof-of-principle test-beds as the correct operation of a gate can only be assured when the output modes are detected and thus destroyed. But this limitation shall not be part of the discussion here.

Coincidence in the experimental sense means that the electronic signal from the detectors are generated (and essentially detected) within a small time window of each other. In a continuous wave experiments the exact width setting of this time window is quite important due to the possibility of creating photons at any given time and the need to ensure that the photons that triggered the electronic signals temporally overlapped in the experiment. Using a fs-pulsed laser alleviates this problem as the photons can only be emitted during the time where the pulse is physically present in the pump crystal. As this is much smaller than the temporal jitter of the detectors, coincidence windows of a total width just smaller than the temporal separation between two laser pulses can be used to give reliable coincidence readings. During the experiments in this thesis it was usually found though that a window of about 1ns would be completely sufficient to detect the maximum number of coincidences, but windows as wide as 11ns— Temporal pulse separation of the laser = 12.5ns— were used while still differentiating between subsequent pulses.

Further the Avalanche photodetectors used during the experiment exhibit dark counts, that is they trigger despite no photon being present. Typical rates for the detectors used in this thesis were on the order of 100Hz, while the background reading due to stray light would typically be on the order of $300 - 500$Hz. Such artificial counts can of course pair with events where the paired detector detected a photon and thus lead to a registered coincidence event, even if i.e. the paired photon had been lost/rejected due to circuit failure. (Of course a background count could also pair up with a background count on the other detector, however the probability for such an event is about 5 orders of magnitude smaller and can thus be safely ignored. Events where a coincidence event is registered due to a background count are referred to as accidental coincidences. While these events are very few ($\ll 1$Hz) and can typically be ignored, they can become a factor during very long detection times on measurements where theoretically no counts are expected. As there is no way of differentiating between these accidental coincidences and genuine ones, these rare events contribute to the noise and error of the obtained experimental results.

2.1.2 Pulsed parametric down-conversion

As PDC is such an inefficient process and one wants to have the highest signal rate for the experiments to perform them in the fastest possible time, it is desirable to increase the rate of coincidences. It hence looks very tempting to move away from continuous wave lasers to pulsed systems to take advantage of the high peak powers as is done commonly for SHG and other parametric wave-mixing processes. However as we saw during the quantum mechanical treatment of PDC, the amplitude of coincidence events scales linearly in the pump field amplitude. Thus moving to a pulsed source of the same pump power as a continuous source does *not* increase the number of pairs of photons being created in one mode during PDC. However the amplitude to create two pairs of photons scales quadratic with the pump field thus moving from a continuous source to a pulsed source increases the proportion of events where multiple pairs are created simultaneously.

While there is no gain in efficiency by utilising pulsed pump lasers for PDC when seeking to generate only a pair of down-converted photons, there is one attribute of pulsed laser systems do drastically improve the behaviour of parametric down-conversion. PDC occurs purely at random, hence if one is pumping PDC with a continuous wave laser, the stimulated PDC events are scattered randomly in time. In this sense, PDC is similar to radioactive decay, where the probability of observing a decay is proportional to the number of available atoms, but the occurrences are statistically distributed. The number of PDC events per time unit is proportional to the pump power, hence the photon number, but the events are again statistically scattered. This behaviour is obviously counter productive when more than one pair of photons is required simultaneously. This problem can be alleviated with a pulsed laser: Assuming the laser has the same average power as a the before mentioned continuous wave laser, then the average rate of PDC-events remains the same, but the pulsing of the laser now introduces a clock and down-conversion can only occur while the pump pulse is present inside the non-linear crystal. By using a pulsed laser, the time span where the pump pulse is present inside the crystal is given by the length of the crystal divided by the speed of light inside the crystal. Furthermore femto-second lasers commonly have repetition rates on the order of 100MHz with pulse length on the order of 100fs. The on-off ration is thus on the order of $1 : 10^5$, which equals the gain in probability of inciting multiple simultaneous down-conversion events through the usage of a pulsed system, compared to a continuous wave laser of equal average power.

The down-side of pulsed parametric down-conversion lies in the Energy-Time uncertainty relation. A shorter, more well defined pulse length requires, following the Fourier-transform, a spectrally broader pulse. Pulses on the sub-hundred femto-second scale correspond to bandwidths on the order of ten nanometers. This extreme bandwidth creates a new problem for the non-classical interference: Revisiting our momentum conservation relation 2.4, and remembering that the refractive index of a material continuously changes with the wavelength, the solution for $\vec{k}$ changes across the pulse causing again distinguishability[48]. Effectively the coherence length of the pulsed light becomes so short, that the extra-ordinary and the ordinary beam are no longer coherent with each other by the time they leave the down-conversion crystal. The solution is to simply utilise spectral filters, narrower than the spectral pulse width, artificially increasing the coherence length and restoring good visibility, however filtering means damping and thus loss. The application of these filters reduces

the count rate and thereby partially undoes the benefit of increased simultaneous multi-pair events gained by utilising the pulsed pump. The selected filter bandwidth thus represents a compromise between count rate and maximum possible indistinguishability. In all our experiments we applied interference filters centred at 820nm with a full wave half maximum (FWHM) bandwidth of 3nm.

2.2 The experimental photon sources

2.2.1 Version 1: The naive approach

In the beginning Newport created the optical table. And the table was without form, and void; and darkness was upon the face of the deep. And the spirit of Andrew moved upon the face of the labs. And Andrew said, Let there be light: and we started setting up a Titanium Sapphire (Ti:Sa) laser, and shortly thereafter, there was light[4].

To be precise, the laser system used for all experiments was the Spectra-Physics Tsunami laser with a 10W Millenia X frequency doubled Nd:YAG system, setup to emit approximately 70fs long pulses with a repetition rate of 82MHz and average output power that varied from 1.2 to 1.6W at the central wavelengths of 820nm. The variations where mainly caused by slow deposition of dust on the cavity surfaces and misalignments with time. The mentioned drift thus occurred on the scale of months. As the photon detectors that we utilised (Perkin-Elmer SPCM-ARQ-14 silicon avalanche photodiodes) have their best response near 700nm, we would like to have our photons near this wavelength. This requires us to first up-convert our Ti:Sa laser beam before then generating down-converted photons at 820nm. We choose 820nm rather than a wavelength closer to the detection peak, as this is a secondary standard wavelength in telecommunications, meaning some items are pre-fabricated and do not have to be custom made. In the original setup shown in figure 2.1 we used type-I SHG in a BBO-crystal to up-convert the light from the Ti:Sa.

After measuring the transverse beam-profile of the Ti:Sa output pulse, the optimal lens was calculated [11] as

$$L_c = 2.9\frac{\pi w_0^2}{\lambda_{inc}} \quad \text{for the optimal crystal length, with} \tag{2.11}$$

$$w_0 = \frac{f\lambda}{w_{lens}\pi} \quad \text{, thus giving the optimal focal length as} \tag{2.12}$$

$$f_{opt} = \sqrt{\frac{L_c w_{lens}^2 \pi}{2.9\lambda_{inc}}} \tag{2.13}$$

Due to the elliptic shape of the pump beam and since the equation holds true only for monochromatic light, which, given a bandwidth of 12nm at 65fs long pulses, is at best a poor representation, the calculation was repeated for multiple extreme data sets returning values in the range from 28mm to 48mm for the optimal focal length. The three available lenses in this region were tested by trial and error, revealing the best conversion efficiency for the f=35

[4]My PhDs version of Genesis 1.1

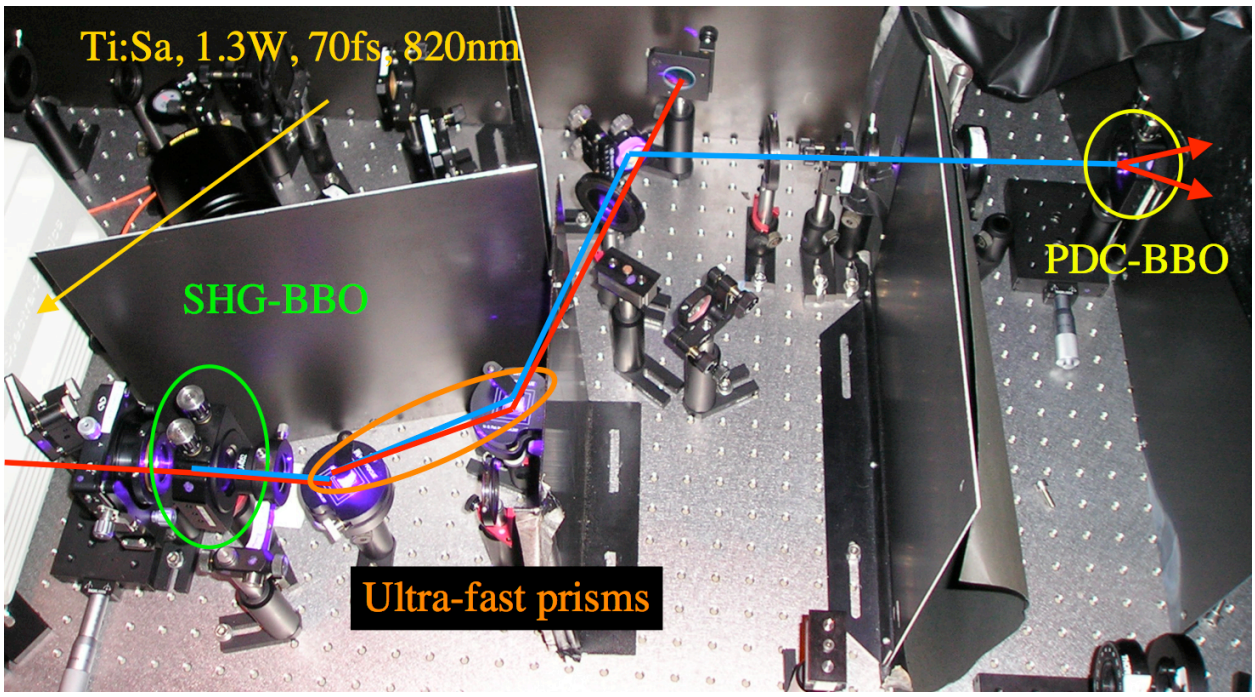


Figure 2.1: Photograph of the original second harmonic generation and down-conversion setup. As can be seen from the bright spots, the ultra-fast prisms, have relatively high losses due to scattering, thus also requiring extensive light shielding. Two of these prisms where needed to maximise the separation on a short spatial distance. The translation stage on the down-conversion crystal was used to translate the crystal whenever crystal damage due to the high UV intensities occurred The SHG-BBO could not be optimally retroreflected as the reflected pulse propagated back into the cavity of the Ti:Sa and partially depleted the inversion and thereby suppressed mode-locking of the laser.

mm lens ($\eta_{25.4mm} = 17\%, \eta_{35mm} = 26\%, \eta_{50mm} = 22\%$), which was subseqquently used in this setup. The non-linear crystal used in this first SHG source was a $(8 \times 8 \times 2)\text{mm}^3$ β-barium borate crystal (BBO) with its optic axis cut for type-I SHG at perpendicular incidence.

This very fact caused some obstruction to the optimal design. When perfectly retro-reflecting the crystal to guarantee perpendicular incidence of the pump light, the crystal - despite an anti-reflection coating at 820nm - would reflect sufficient amounts of light back into the cavity, that the Ti:Sa would not maintain mode-locking. Ultra-short pulsed lasers, such as the Ti:Sa fs-lasers, use a third order non-linear effect known as Kerr-lensing or self-focusing to instigate mode-locking. In this case a random power fluctuation of the spontaneous emission possesses enough power to excite a sufficiently strong focussing effect in the Ti:Sa crystal. Due to this focusing the mode can pass without loss through a slit or mode aperture and complete the round trip with total net amplification in the cavity. Other modes that do not undergo sufficient self focussing will suffer too much loss at the aperture to experience amplification during a round trip and are hence suppressed. The propagating pulse will deplete the available inversion upon each round trip and suppresses thereby the existence of any other pulses in the same cavity. As the pulse requires all modes to be present inside the non-linear crystal simultaneously to generate enough Kerr-lensing,

it also guarantees the mode-locking for femtosecond pulsing. The pulse that is reflected back into the cavity from the SHG-crystal now depletes some of the available inversion and thus stops the original pulse from acquiring enough amplification and consequently experiences not enough self-focusing to maintain its unattenuated propagation inside the cavity, and the laser will no longer remain mode-locked and pulsed operation.

There are two ways to counter this problem. The first is to build an optical diode involving a polarising beamsplitter and a Faraday-rotator. The advantage of this design is that subsequent optics can all be aligned perfectly with respect to the pump orientation, and the isolation against back scatter is very high. The disadvantage, that this system itself has a significant loss and decreases the available power. Furthermore, for a short pulsed system, the crystal inside the Faraday-rotator creates a large amount of dispersion, temporally lengthening the pulse and thus reducing the peak power — clearly undesired side effects.

Option two is to not retro-reflect the SHG-crystal. In this case the optimal conversion efficiency can never be achieved, but due to the tilt of the crystal the back-scatter of all optics downstream from the crystal is deviated and thus does not couple back into the cavity. Due to the ease of the installation, and absence of loss and dispersion, we chose option two.

After passing through the SHG crystal, the light is collimated with a second lens one focal length (50mm) away. This second lens was part of a custom made UV-grade fused silica lens kit from Thorlabs. The kit was custom AR coated to cover the range from 350 to 900nm with reflection minima at 410nm and 820nm. PDC is the degenerate case of four-wave mixing, where the second input field is the vacuum. In the presence of a second pump field, either sum frequency generation or difference-frequency generation would dominate. It is therefore essential to dump all remaining unconverted (820nm) light from the Ti:Sa laser and pump with only the up-converted pulse. Separation of the two light fields was achieved with two dispersion compensating prisms followed by a UV-cold mirror, which reflects UV-light at 45°, while transmitting light above 720nm which also steered the pump pulse onto the down-conversion crystal.

A $(8 \times 8 \times 3)\text{mm}^3$ BBO crystal cut for type-II down-conversion was used in this first setup. Commonly type-II down-conversion is associated with the emission of the two photons along two cones, which can intersect. As one cone is of horizontal and the other of vertical polarisation, as in the diagram in figure 2.2 this source design allows for the collection of entangled photons from the intersecting regions. For the work of this thesis, polarisation entanglement from the source is neither required nor desired. Tilting of the optic axis of the crystal with respect to the pump vector varies the opening angle of the cones, without moving the centre point of the individual cones, thus the cones can be fully collapsed, where the inner boundaries of the rings touch each other and the emission spot has an approximately Gaussian spatial intensity distribution in their cross-section, instead of the normal donut. We chose this setup, as the down-converted signal was to be coupled into single mode fibre, and a significant improvement in coupling efficiency was expected due to the Gaussian beam-profile of the to be coupled light. A picture taken with a single photon sensitive CCD-camera (MicroMax from Princeton Instruments) of the collapsed cone down-conversion is shown in figure 2.3 confirms the collapsed cone emission. The improvement in coupling efficiency was smaller than expected and did not compensate the loss in down-conversion efficiency

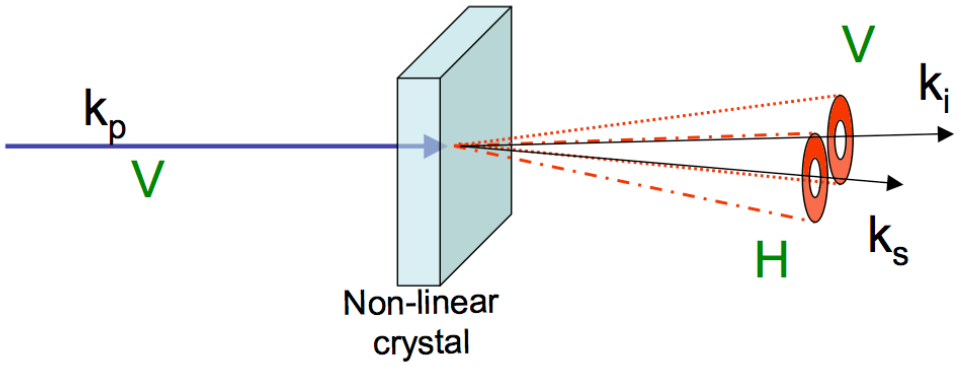


Figure 2.2: Schematic of type-II parametric down-conversion. Black letters are momentum vectors, green letters identify the polarisation of the respective beam. In the collapsed cone regime, the two cones shrink to the point where the inner boundaries touch and the intensity profile is approximately a Gaussian profile. The paired photons are emitted along the individual cones, at points symmetric around the pump axis, in such a manner that the momentum is conserved. The crystal in our experiment was a β-barium borate crystal.

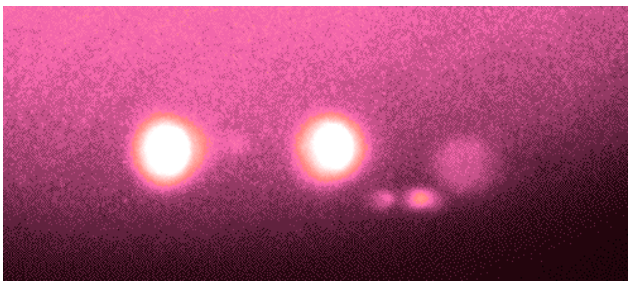


Figure 2.3: False colour image of the type-II collapsed cone source, obtained with a single photon sensitive CCD camera. The two bright spots are the actual emission cones. The three lighter spot to the right (one large and two small ones) are reflection on the imaging lenses and interference filter. The general background is caused by scattering. Exposure time of the image is 0.1s. The interference filter (IF) is centred at 820nm with a full width half-maximum bandwidth of 3nm and is placed directly in front of the CCD. Prior to the IF, multiple slides of RG715, a red glass from Schott, are placed to absorb the remaining pump photons. A UV cold mirror directly after the PDC crystal was used to deflect the majority of pump light to a beam dump, as it caused significant fluorescence in the RG715, of which some was at 820nm and thus created a large background signal.

that arose from this unfavourable crystal alignment. There is an ideal angle at which the momentum and energy conservation relationships are generally "easily" fulfilled and the phase matching function is large. The collapsed cone regime however is the edge of the angle range for which down-conversion can occur and thus the phase matching function is small and vanishes if the optical axis is tilted even further from the ideal angle.

Once beam-like emission was confirmed with the CCD camera, free space single photon detectors were set up to collect the down-converted modes. Once one detector for each mode was successfully installed and coincident detection of photons was confirmed, the emission

cone propagation directions were identified by the placement of irises, while monitoring the down-conversion signal. A visible laser diode was then aligned to the beam path identified by the irises and thereby to the mode of the down-converted light. The laser diode light was steered onto the PDC-mode via two flipper mirrors, allowing easy alternation between normal down-conversion operation or the laser diode alignment setup. Once the light from the diode overlapped with the beam path of the down-conversion, a further two flipper mirrors were used to steer the beam to free-space fibre launchers (Thorlabs KT110), to couple the down-converted photons into single mode optical fibres, allowing convenient guiding of the PDC photons to any experimental setup.

Despite the lower than expected efficiency and the lack of improvement on other down-conversion arrangements known to yield better efficiencies [49],the source was used for the experiments described in chapter 3.

2.2.2 Down-conversion Source Version 2.0: The V2

When one of the pump diodes for the Nd:YAG pump laser burned out, a complete realignment of the source was required. Instead of reproducing the inefficient collapsed cone setup, we grasped the opportunity to completely overhaul the source, and installed a new SHG crystal remedying the retro-reflection problem. A detailed schematic diagram of the new source design can be seen in figure 2.4 and is described in the section below.

The first significant change was swapping from type-II to type-I down-conversion as it is intrinsically more efficient, as a different and higher non-linear coefficient for the crystal is being exploited. Since the original PDC-crystal was cut with an angle of the optical axis suitable for type-II, a new BBO-crystal cut for type-I down-conversion was installed. In type-I, the two down-converted photons have the same polarisation. If they are further degenerate (same wavelength) this leads to them being emitted on the same cone but on opposite sides.

Simultaneously we trialled a new non-linear crystal for the SHG. Instead of using a BBO crystal, a newly acquired Bismuth-Borate (BiBO)-crystal was used. This recently developed crystal has a larger non-linearity, but has a narrower acceptance angle for the phase matching. We tested this new crystal in comparison to another new BBO crystal, with both the BBO and the BiBO cut at the appropriate angle for type-I SHG + 5°. Cutting the crystals away from ideal the ideal angle for SHG at perpendicular incidence causes the maximum conversion efficiency to be achieved when the crystal front-face is tilted relative to the pump beam axis. Thereby any back reflected light is as before reflected at an angle to the pump beam and thus can not re-couple to the cavity of the Ti:Sa . Further, the lenses focusing onto and collimating the light from the crystal were replaced with achromatic lenses rather than the previously used bi-convex lenses, giving a better focus and thus a higher intensity for the up-conversion. This intensity was further increased through realignment of the Ti:Sa laser cavity after installation of the new pump diode bar, resulting in a much higher output power, 1.6W compared to 1.2 W previously. To gauge the difference in the conversion efficiency of the two crystals, the new system with the achromatic lenses was trialled with both the BiBO and the BBO crystal. We found optimal performance for the BBO crystal with the 50mm achromatic lens, resulting in a maximal output power of 620mW or an efficiency of

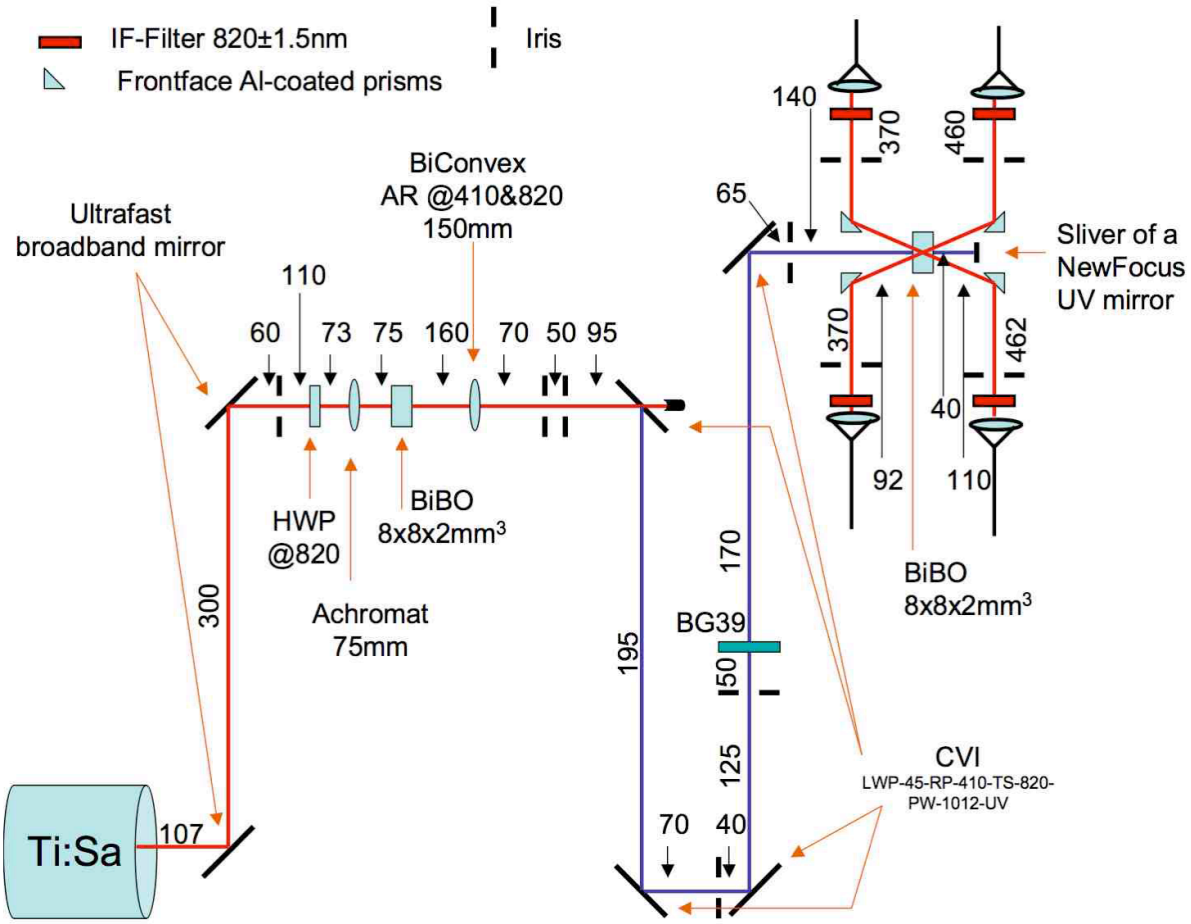


Figure 2.4: General layout of the V2 source and subsequent sources, with altered crystals. The figure shows the latest configuration, including the BiBO-PDC crystal. All crystals and lenses are mounted in five-axis mounts to give maximum degrees of freedom for fine adjustment. The biconvex lens is additionally mounted on a 50mm translation stage. The last two CVI mirrors are in high-precision tilt mounts (Newport LP-1), to allow compensation of beam-steering down-stream, i.e. due to cavity realignment, reducing amount of realignment required on the fibre couplers. The BG39 is in a flipper mount. During normal operation it is down (off). While trying to get first PDC signal fibre coupled, the BG39 is used to suppress 820nm scatter. The SHG BiBO crystal is cut 5° away from ideal angle, to avoid back reflection, both crystals are dual AR coated and cut for type-I operation. The BiBO up-conversion crystal prefers slightly longer pulses and a less tightly focused beam for ideal SHG than BBO due to a smaller acceptance angle for the phase matching. The fibre couplers are mounted on x-y translation stages to give access to all degrees of freedom during alignment. Irises in the beam path are placed to reduce scatter, whereas the irises between the prism mirrors and fibre couplers are used to allow coupling from a forward pass coupler to a backward pass coupler. Distances for the fibre couplers are given as mirror to fibre tip, others as front edge to front edge. All distances are given in mm.

nearly 40%. With the BiBO crystal and a 75mm achromatic lens we achieved a peak power of 930mW, giving us a single-pass conversion efficiency of 58%. To obtain these results the Ti:Sa laser was pushed to run on the edge of the stable mode-locking region producing slightly

longer than optimal pulses, reducing the bandwidth and thereby easing the phase matching condition for the BiBO crystal. This mode of operation led to the laser frequently dropping out of mode-locking and an oscillation of output power. As the planned experiments required long term stability (weeks rather than hours) maximum power was traded for stability by using slightly shorter - spectrally broader - pulses. The narrow acceptance angle of the BiBO crystal limited the conversion efficiency yielding output powers at 410nm of approximately $650 - 750$mW.

A further alternation in the pump design was the replacement of the dispersion compensating prisms, which were found to be relatively lossy due to scattering and reflection of the surfaces. Instead we used custom dichroic mirrors with a reflectivity above 99.5% at 410nm and a high transmission ($T \geq 80\%$) at 820nm. A total of four of these harmonic separators were needed before the intensity of residual 820nm the pump beam was below the measurable threshold of our power-meter. Obviously measuring the remaining fundamental without the second harmonic is non-trivial. By flipping the polarisation of the fundamental before the SHG crystal from vertical to horizontal, the phase-matching condition is no longer fulfilled and no up-conversion occurs. This allows us to measure an upper bound for the remainn 820nm light in the pump path, as now none of the power at 820nm was converted to 410nm. We also measured the amount of leaking blue light to ensure that our dichroic mirrors were within their specs. We grew suspicious as after the first mirror a blue beam was observable on a white card. By splitting this spot from the overlaying fundamental with a prism we concluded that the intensity was below the threshold of the power meter (less than 1mW), and the mirrors where found to be well with in their specs.

As mentioned above, the down-conversion crystal was replaced with a BBO crystal of the same dimensions, with the optic axes cut for type-I PDC at a 3° opening angle. The collection of the down conversion photons was also altered. Instead of using a two-mirror setup to steer the beam towards a fibre launcher, a platform with two front-surface metal coated prisms was used to reflect two opposite parts of the down-conversion cone at right angles to the pump beam, towards the fibre launchers. While not offering as many degrees of freedom for the steering of the down-conversion photons, this setup proved significantly more stable and required very little maintenance once configured. The pump beam was allowed to pass between the two prisms, removing the need for spectral filtering at this stage and reducing the scattered pump light. The fibre launchers were also swapped from the Thorlabs free-space launchers to NewFocus (9131-FS-FC), which provided far superior stability, requiring only fortnightly tweaking of the alignment compared to the daily adjustment for the Thorlabs launchers.

2.2.3 The 4-photon source

The V2-Source described in the previous section was later upgraded to allow the collection of four photons, as indicated in Figure 2.4. The pump pulse was retroreflected with a UV mirror after passing through the crystal. Throughout the course of this thesis, the labelling of the down-conversion modes will be in reference to the pump creation direction. The *forward* pass shall here indicate the first pass through the crystal, whereas the *backward* pass or direction shall indicate the pump pulse travelling back on its on path after reflection on the mirror

after the non-linear crystal. In order to balance the down-conversion probabilities, the focus of the 410nm pump pulse was set to be approximately at the retro-reflecting mirror, so that both passes would have near identical local intensities, beam profiles and a similar range of k-vectors.

To collect the down-conversion light generated in the backward pass, two further front surface coated right-angled prisms were placed on the front side (towards the laser) of the crystal. To ensure that photons with similar wavelength and momentum range would be collected, we shone a diode laser through the collection fibre of the forward pass couplers. As the forward couplers already collected coincident photons from the forward pass, the light sent back through the fibre, impinged at the prescribed angle of 3° on the crystal and overlapped with the pump light inside the crystal. It further ensured, that the light travels again at 3° to the pump beam after exiting the crystal and thus identifies the suitable places for the backward-pass prism mirrors and subsequently the fibre couplers which collect the down-conversion photons. The backward fibre-couplers were than aligned to collect the light from the 820nm diode laser injected by the forward couplers. Upon achieving high efficiency coupling from the forward to the backward couplers we not only immediately had down-conversion signal in the backwards pass, but also some coincidences. The success of this alignment method not only saved many hours compared to the usual trial and error method, but also minimised the the optimisation required to obtain the maximum collection efficiency and coincidence rates.

2.2.4 Of flying ants and blue light

The 4-photon source proved to be a very stable and reliable setup, that is as long as we managed to keep ants out of the lab. One day, the sun was out, the wind was low and the air was dry, when the flying ants of a nearby colony said their last good-byes and flew of, cruising through the air looking for queen ants to mate with. Some of them were misled and made their way into our lab and while to the best of my knowledge I am sure that we have no queen ants there, have no direct explanation for the why, ants seem to be attracted by blue/UV light, as many ants kept running madly across optics that scattered blue light in both the fs-setup and the Ar^+ section of the lab. However, some ants are known to use the polarisation of light to navigate, and ants like bees are capable of detecting light in the UV range, thus I assume that the presence of vast amounts of strongly polarised light in the lab led to their disorientation. However, this behaviour has only been proven with foraging ants [50], and I do not know if it expands to flying ants. A further discovery of this day was, that when ants choose to walk straight thorough half a Watt of blue, fs-pulsed laser light, they seem to disappear. Closer inspection revealed that of course the ants did not just vanish as if abducted by aliens, but rather left a smudged burned spot on whatever optic they choose to walk across... In our case, this was both of our crystals and two of our harmonic separators. None survived. Neither the ants nor the optics. I have recently discovered that a patent has been issued in the US in 1997 [51] for a method based on applying pulsed UV-laser pulses to fruit, as a non-invasive pesticide. Specifically it was found and proven that ants (among other insects) tend to explode after exposure to only a few pulses of UV light.

Once the replacement crystals and optics had arrived, and the ants had finished their migration either naturally or induced by ant-rid, we replaced the burned elements, we grabbed the opportunity and, encouraged by the improved SHG efficiency with BiBO over BBO, trialed a BiBO crystal for the down-conversion as well. We used the exact same setup as previously and had the BiBO crystal cut so that the type-I PDC photons again would have a 3° opening angle outside of the crystal. The change proved to be a major success, increasing our down-conversion rate approximately by a factor of 2. Apart from the new optics and PDC-crystal, the setup remained unchanged.

Lessons learned: Ants are a vital part of the ecosystem but seem to yield only minimal use in quantum information.

2.3 In fibre HOM-Interference: Green lights for the Gates

While parametric down-conversion had been used for many different quantum optical schemes, and non-classical interference had been proven numerous times, the emergence of ultra short pulses had led to some difficulty arising from the duration of the pulses with respect to the length of the crystals used to generate the down-converted photons. It was shown that if the coherence time of the signal and idler photon becomes shorter than the pump pulse duration that the observed non-classical interference degrades [52]. The coherence time can be estimated by the dispersion of the group velocities in the non-linear medium, hence

$$t_{coh} = \left(\frac{1}{u_e} - \frac{1}{u_o}\right) L_{crystal}, \tag{2.14}$$

where t_{coh} is the coherence time, $u_{o(e)}$ is the group velocity of the (extra)ordinary beam and $L_{crystal}$ is the length of the crystal. This distinguishability can be suppressed by spectral filtering, as the maximally different group velocities become limited and the coherence time is subsequently increased.

For our ultra-fast system we intended to use interference filters centred at 820nm with a full width half maximum (FWHM) bandwidth of 3nm. While such a filter should suffice in order to reestablish sufficient visibility of the non-classical interference for the desired quantum gates, a proof-of-principle experiment was conducted to measure the non-classical interference in a 2x2 fibre-port beamsplitter. This is a beamsplitter with two fibres each as in and output, where the two fibres have been melted (fused) together in the interaction region to achieve an effective polarisation-independent beamsplitter with reflectivity $\eta = 0.5$.

I conducted this test with the original collapsed cone source and a fused-fibre beamsplitter obtained from JDS-Uniphase. As it is essential for the photons to be completely indistinguishable, it is necessary for both photons to have the same polarisation in the interaction region. As the source was a type-II source, the emerging down-converted photons have orthogonal polarisations. However as both photons prior to the interaction region have to first pass through about 2m of single mode optical fibre which does not preserve the polarisation, the input polarisation is not the defining element for the polarisation state at the interaction region. It does not suffice to simply inject two photons of the same polarisation into the two fibres.

To experimentally ensure that both photons have the same polarisation in the interaction region I applied the following procedure: I measured the horizontal polarisation intensity at one of the outputs, while blocking one of the inputs. Using fibre polarisation controllers (aka bat-ears), I rotated the polarisation of the active input *before* the interaction region, till the output was purely horizontally polarised, indicated by a maximum intensity after a Glan-Taylor polarising beamsplitter cube in the horizontal port. This procedure was then repeated with the other input, while blocking the first input. It is essential to continue to measure on the same fibre output-port, as now the fibre of this output is a common path. Thus any polarisation rotation occurring on a photon from one input in this output fibre also occurs on the photons from the other input. Hence if both photons have the same polarisation at the common output, they must also have the same polarisation in the interaction region, fulfilling this precondition for indistinguishability.

A further requirement is that both wave-packets must temporally overlap in the interaction region. To ensure this, one fibre coupler was mounted on a motorised translation stage allowing a slow gradual scan of the free-space path length prior to this input of the fibre beamsplitter, altering the arrival time of photons coming thorough this port. While this appears to be a straightforward "turn the handle and it works" method, measuring the actual length of the individual fibre pigtails is strongly suggested to ensure that a sufficient range of free-space path length can be scanned. We observed fibre length deviations on 2m fibres as large as 148mm, or 7.4%. Once the correct delay was found, the expected HOM-dip was observed and is shown in Fig. 2.5. The visibility of the dip is $94.1\pm0.4\%$ and thus close to the optimal 100%. Though not measured at the time, the degradation is likely a combination of spectral mode mismatch, higher-order photon terms (see section 4.4), and also in part due to the different dispersion inside the non-linear crystal for the e and o-beams even within the filter bandwidth, as recently pointed out to me by Thomas Jennewein from the University of Vienna. However the visibility is high and gives us a green light (for our infrared photons) to proceed with the implementation of an entangling quantum gates with photons from femtosecond pulsed down-conversion.

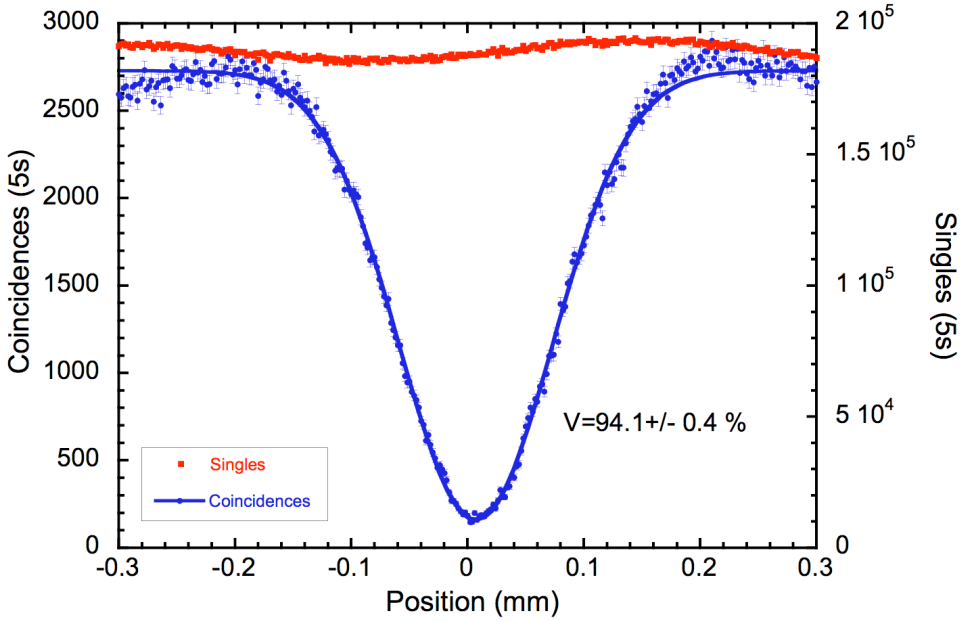


FIGURE 2.5: Hong-Ou-Mandel interference of photons generated in type-II parametric down-conversion with a femtosecond pulsed laser in a fused fibre beamsplitter. Error bars for the singles rates are smaller than the symbol-size. The visibility as derived from the fitted Gaussian dip is 94.1±0.4%. The background rate (with no light input into the fibres) is ≈ 30 per 5s, and has not been corrected for in the visibility calculation.

3

A robust and simple controlled-Sign gate

This chapter discusses the first implementation of a two-qubit entangling gate with a novel piece of optics: the partially polarising beamsplitter (PPBS). This type of cube beamsplitter utilises a specifically engineered dielectric stack between two right-angle prisms. The stack is designed to be perfectly reflective for the vertical polarisation while reflecting (ideally) only 1/3 of the horizontal component. As only the horizontal polarisation mode of each qubit can thus interfere non-classically, the PPBS makes classical interferometers for mode separation of the orthogonal polarisations redundant. We implemented controlled-sign gates with both a pulsed down-conversion source and a continuous-wave source and compared their performance to investigate any potential degradation in gate performance due to the application of spectrally broad and temporally short pump pulses . We further analysed the pulsed gate both with free-space detection of the qubits after the gate and with single-mode fibre coupled detectors, where the single-mode fibres act as strong spatial filters. It was found that there is no significant degradation of the gate performance due to the utilisation of photons generated through pulsed PDC rather than continuously pumped PDC. In actual fact the pulsed gate outperformed the continuously pumped one slightly. Additionally it was discovered that spatial filtering of the output modes of the gate with single mode fibres improves the gate performance while only slightly reducing the count rate.

Work on the free-space pulsed gate was conducted by myself with assistance from Geoff Pryde and Jeremy O'Brien. The subsequent single-mode fibre coupled version was implemented and analysed by myself in close co-operation with Robert Prevedel and Kevin Resch. The continuous wave gate was investigated by Nathan Langford with help from Geoff Pryde and Jeremy O'Brien. Some data analyses was handled by all involved members, the final process tomographic reconstruction and rotational optimisation was the work of Alexei Gilchrist and Nathan Langford. Our work was published as a triple back-to-back publication in Physics Review Letters [53] together with groups from Munich [54] and Hokkaido [55] who performed similar experiments independently. Our publications is included at the end of the

chapter and replaces the appropriate subsection in this chapter detailing the experiments described in the paper. The remaining sections of this chapter give underlying details and insights additional to those published in the paper.

3.1 A brief history of optical two-qubit entangling gates

After the publication of the seminal paper by Knill, Laflamme and Milburn in 2001 [12] circumventing the need for very large non-linearities in optical quantum computing, the path towards a two-qubit entangling optical gate was clear. The difficulty for polarisation encoded photonic qubits, lay in the need to let the individual logic modes interact independently of the other logic mode of the qubits, i.e. have non-classical interference between the horizontal components of two photons, but not their vertical components. A gate design for this was suggested in [34], which first spatially separated the two polarisation modes with classic interferometers and later, after the non-classical interaction, recombine them. This required a classical interferometer for the separation and recombination of the polarisation modes for both qubits, and non-classical interference between two of these modes. A schematic of this kind of gate design is included as Figure 1a) in the publication attached at the end of this chapter. Stabilising two classic interferometers and a non-classical interference is a difficult task. The first implementations using the common interferometers were too unstable to yield convincing and conclusive results without active locking of the classical interferometers. It took till 2003 and the re-discovery of a nearly forgotten intrinsically stable interferometer, with which a successful implementation was reported [56]. This controlled-NOT gate used a Jamin-Lebedeff interferometer comprised of calcite beam-displacers, making it insensitive to any kind of translation of the elements in the interferometer. Nevertheless the gate performance was still limited by the visibility of the classical interference. It had been noted by Geoff Pryde that if an element existed which would have the desired reflectivities for the different polarisations, that this would be a significant simplification and would yield potentially significantly higher gate fidelities. Other implementations of two-qubit logic gates were also published during this time [57, 58], which do not require classic interferometers, but do require entanglement between each of the interacting photons and an additional ancilla photon. Due to this inherent significant difference in the designs, these gates and their implementations are not discussed in this thesis.

3.2 Building a gate with partially polarising beamsplitters

In 2004 our research group obtained the first sets of such partially polarising beamsplitters from two different suppliers. One of the sets was designed to operate at 702.2nm, the wavelength of down-converted photons from PDC crystals pumped by an argon-ion-laser (Ar^+), and was obtained from Asahi (Japan). The second set, obtained from Special Optics (USA), was designed for operation at 820nm, for the photons generated by the fs-pulsed Ti:Sa system. This set of partially polarising beamsplitters (PPBS) turned out to have reflectivities far from the specified values. For ideal gate operation it is required to have perfect reflection

for vertically polarised photons and 1/3 reflectivity for horizontally polarised photons. The obtained PPBS had reflectivities of η_V=0.99±0.01 and η_H=0.28±0.01. This deviation limited the visibility of the non-classical interference to approximately $V_{ideal} = 67\%$ as opposed to $V_{ideal} = 80\%$ for the ideal case and thereby also limited the accuracy of the gate action. While promising, the original set of data was not of the desired quality and a redesign of the gate was conducted to include single mode fibres to collect the photons after the gate. Single mode fibres act as spatial filters. As the photons were injected into the gate by single mode fibres as well, this allowed very accurate control of the spatial modes active in the gate, simply by optimising the coupling from the input to the output couplers. Photons that were not coupled into the detectors could not trigger a detection event, thus not incite a coincident count. As far as the gate is concerned they never existed. This high degree of spatial filtering thus selected only an idealised Gaussian mode that coupled to the single mode fibre from all possible spatial modes in the gate. This introduced a much more stringent limitation on the detected spatial mode as the injection through single mode fibres and while this inevitably reduced the count rate, it led to a much improved visibility of the non-classical interference and a subsequently much improved gate operation. The data published in the subsequent paper was acquired with the setup using the single mode fibres acting as spatial filters, and worked of the revamped source described in section 2.2.2. As the gate requires no longer any spatial separation of the logic modes of the qubits, the number of optical elements in the gate is drastically reduced. A schematic of this novel gate design is displayed as figure 1b) in the publication at the end of this chapter. The only necessary element is the PPBS for the non-classical interference, however in order to balance the probabilities for a modes in the gate, half-waveplates after the interaction PPBS flip the logic modes i.e. $|H\rangle \rightarrow |V\rangle$ and vice versa prior to another set of PPBSs, one in each arm of the gate. These PPBSs act as the dump ports where the previously unattenuated $|V\rangle$ mode, which has been flipped to $|H\rangle$ now experiences loss, but as there is no other photon injected in the other input port of this PPBS that our initial photon could non-classically interfere with at this beamsplitter, it does not receive a phase shift.

The deviation of the splitting ratio of the PPBS was deemed intolerable and was clearly limiting the results, hence a new set of PPBSs was ordered from the company that provided the original set for the Ar^+-laser, as this set was ideal within the measurement accuracy. The new set proved significantly better, but was still not ideal with reflectivities of η_V=0.99±0.01 and η_H=0.35±0.01. As these beamsplitters were not delivered till October 2005, they were installed in the gate after publication of our paper which is attached at the end of this chapter. The experiments in chapter 4 and onwards were all conducted with the PPBS-set obtained from Asahi in conjunction with post gate single mode fibre coupling as spatial filters.

3.2.1 Towards the implementation

After constructing the gate as shown in the paper, the non-classical interference had to be established. For this measurement, the polarisation of the input states was set to horizontal, allowing interaction of the photons at the PPBS. The scan of the interference visibility just before the collection of the data in the paper is shown in Fig. 3.1. As the PPBSs were found

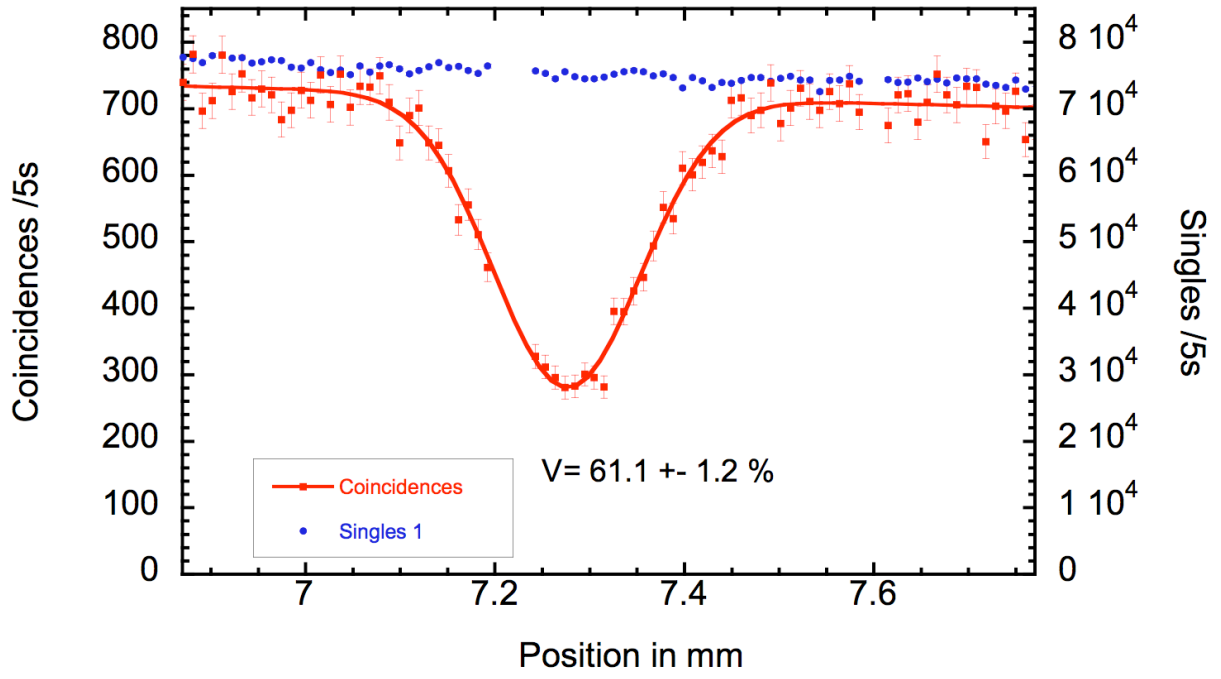


Figure 3.1: Hong-Ou-Mandel interference of the horizontally polarised photons on the central PPBS of the controlled-Z gate taken just prior to the data collection for the process reconstruction. Error bars for the singles rates are smaller than the symbol-size and the visibility as derived from the fitted Gaussian dip is 61.1±1.2%, yielding a relative visibility of 91%. Missing points are caused by communication failure where the data from the counter is not received by the computer.

to be leaking some vertically polarised photons, we also took a interference measurement with the vertical polarisation, which is shown in Fig. 3.2, however no conclusive dip was observed and it was hence concluded that no significant interference of the vertically polarised photons occurred.

In the ideal case the maximal visibility is limited by the reflectivity of the beamsplitters to $V_{ideal} = 80\%$ for horizontally polarised photons. With $\eta_H = 0.28$ this limit drops to $V_{ideal} = 67\%$. Rather than quoting the total visibility, it becomes sensible to quote the measured value relative to the maximal possible or ideal value, thus

$$V_{rel} = \frac{V_{meas}}{V_{ideal}}, \tag{3.1}$$

which leads to a much better appreciation of the quality of the non-classical interference achieved. For the published controlled-Z gate implementation, the relative visibility achieved with spatial filtering with single mode fibres and the spectral filtering with the interference filters with $\Delta\lambda_{\mathrm{FWHM}}$=3nm was 91%. At the time the imperfections were attributed chiefly to remaining mode-mismatch, spatial or spectral. As the results obtained with the pulsed laser system equalled the previous best demonstration of a photonic entangling two-qubit gate and surpassed that of the continuous wave system, spectral mode mismatch was thought to be insignificant.

The gaps in the data for the HOM-dips are artefacts of the LabView acquisition program with the Ortec counting modules. The program would send the desired integration time to

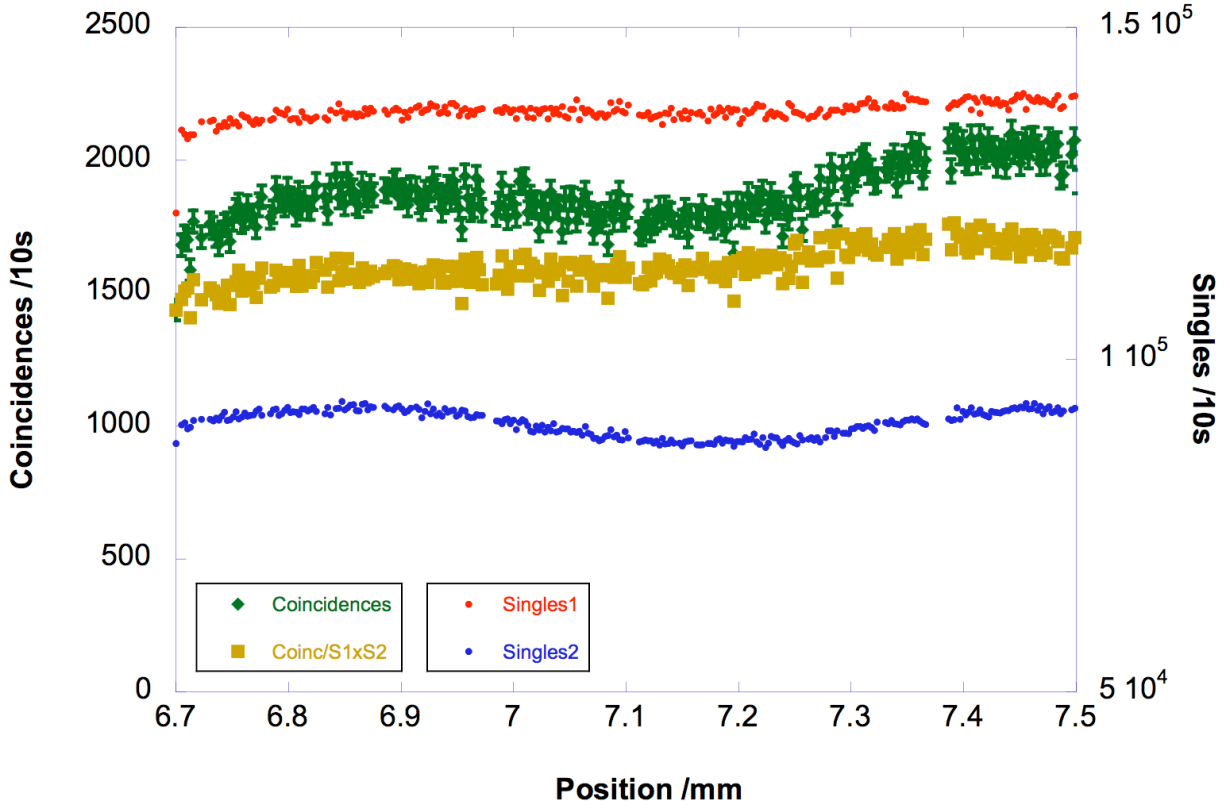


Figure 3.2: Searching for Hong-Ou-Mandel interference of the vertically polarised photons in the PPBS-CZ gate. There is no observable dip. The drop of coincidences towards the middle of the graph is completely explained by the temporal fluctuation of the singles rates, as can be seen by the brown curve showing the coincidence rate divided by the singles rates and re-scaled to approximate count rate level. The expected dip position is the same as in the HH case shown in Figure 3.1, at 7.277mm. Clearly there is no significant drop in coincidence count rate.

the counter, which would automatically count for the desired time period and then send the counts back to the computer via GPIB and a GPIB/Ethernet converter. Upon reception of the number of counts, these would be added to a file with the current time stamp. Due to occasional drop outs of the Ethernet connection some data points would not be properly written, and the measured counts for that interval lost. As the translation stage operated independently, it would continue to run at a constant speed. The position for the data points is calculated from the elapsed time, multiplied by the known speed of the stage and its starting point. Therefore the counts in the gaps are due to the data lost during the communication of the counting card to the LabView program. This behaviour initially distorted the data acquisition of the state tomographies as well, an additional loop was added in the tomography program to confirm the receipt of data, else the point would be retaken, until the data was received. Therefore there is no effect on the state tomography data from this undesired feature. Such an additional loop in the program was not possible for the scanning of the HOM-dip, as the program did not control the translation stage (It did control the waveplates for the tomographies though).

The acquisition of a new controller and counting card during the extension of the source to the four photon source led to a completely new LabView acquisition program for all data

acquisitions that did contain appropriate steps to ensure the correct reception and logging of all data.

3.3 The effect of spatial filtering

The paper (shown at the end of this chapter) emphasises on the difference between the pulsed/cw implementation and the application of the gate as a Bell-state discriminator and as the effect of the spatial filtering, while a major result is barely discussed in the paper due to the space confinement, hence I will give more detailed results in this section.

3.3.1 State Tomographies

To obtain the most detailed analyses of the gate action, we conducted full process tomography on the gate. However, as pointed out in section 1.4.3, state tomographies form a subset of the data taken for process tomography. The setup of our gate (shown in the paper as Fig. 1a) consisted of motorised rotation mounts for the analyses waveplates and manual input waveplates, which allowed the automation of the state tomographies. For complete process tomography a total of 256 measurements (Sets of 4x4 input states (H, V, D, R)x(H, V, D, R) while measuring sets of 4x4 output states for each input state) is the minimal set required to completely characterise the process. It has been shown in the past, that taking an over-complete set of 576 measurements (16 input $\times$ 36 output), drastically improved the reliability and quality of the results [10], as temporal fluctuations of count rates can be normalised out in individually sets of positive operator measurements (POVM) (i.e. HH, HV, VH, VV or DR, DL, AR, AL), rather than having a single normalisation for the entire data set per input state. We thus used the set $\{H, V, D, R\} \otimes \{H, V, D, R\}$ as input states (i.e. HH, HV, HD, HR, VH, VV, ..., RR) while taking the complete set of output states $\{H, V, D, A, R, L\} \otimes \{H, V, D, A, R, L\}$ (i.e. HH, HV, HD, HA, HR, HL, VH, VV, ..., RR, RL). State reconstruction were handled by Mathematica and Matlab routines. The Mathematica routine was written by Kevin Resch, while the Matlab program was developed by Nathan Langford and was part of his thesis [10].

While the setup of the gate remained unchanged, there were two different implementation of the CZ gate with the pulsed source. During the original tomography run no spatial filtering was applied after the gate . The spatial alignment was optimised on a best effort basis by spatially overlapping the outputs of the single mode fibres that injected the photons into the gate. For this a visible laser diode was shone through the input fibre. Overlapping of the two spots (one from each input coupler) at the interfering PPBS and then adjusting the angle till they also overlapped also after letting the beams propagate to the wall (approximately 1.5m from the PPBS) was used to give a first rough alignment of the two beams. As we used light from the same diode laser in both input ports to the gate as we split the diode light with a non-polarising beamsplitter prior to fibre coupling it, we could then search for classical interference of the spots after the PPBS. The classical interference is an indicator that good transverse spatial and momentum overlap between the two input ports was achieved. Once breathing of the interference modes (slow changes from light to dark spots at the centre of the beam due to thermal drift of the couplers) was observed, we then swapped the visible

laser diode for a laser diode at 820nm, the wavelength of the down converted photons and repeated optimised the magnitude of the classical interference while measuring the power of the beam in one arm after the PPBS. The IR diode was mainly used to optimise the focusing coming out of the single mode fibres and into the gate. The detectors used during this original process tomography were free-space single photon detectors with a interference filter (820 ± 1.5nm) and a 35mm achromatic lens mounted directly in front of the detectors. To allow coupling optimisation the detectors were placed on x-y-z-translation stages. However these detectors could not be aligned to only collect light from the ideal spatial mode from the gate, but would also collect a much larger angle and thus more background photons and more importantly scattered and rejected photons which never went through the gate. While the probability for such events was minimised by alignment and shielding, it remained non-zero. The PDC photons for the initial investigation were generated by the naive source (section 2.2.1).

The final and published tomography was conducted using the V2Source (section 2.2.2), and the gate after it underwent a major reconstruction. This comprised compacting it in size, rerouting light paths to have a better spatial arrangement, minimising scatter onto different detectors and the installation of single mode fibres and fibre coupled detectors after the gate to perform stringent spatial filtering. The latter was by far the main improvement, as verified by my colleagues when they upgraded the cw-gate to spatial filtering as well. This new detection technique also altered the alignment method. As the single mode detection fibres could be unplugged from the single photon detector, we could measure the power coupled into and guided by the single mode fibre with a powermeter while using the IR diode of above as input through our input couplers. This method is significantly more reliable as it allows a direct measurement of the achieved coupling and thus alignment quality. It was found to give best results when the fibre of the first detector (either detector) would be optimised with respect to the stationary input, i.e. the one not translated during HOM-scans, followed by optimisation of the second input to the first detector and finally the last detector while using both inputs simultaneously. As this alignment procedure could use the IR diode throughout the entire alignment process, alternation of the distance of the coupling lenses in the fibre couplers when switching beween the IR diode and the visible diode was no longer necessary, making it by far easier to achieve identical spot sizes at the interference point. The achieved relative visibility for the HOM-interefernce subsequently rose from $87 \pm 1\%$, to $91 \pm 1\%$.

This improvement is also evident in the individual data taken for the two gates during the course of the process tomography. The individual state tomography pictures are shown for comparison in the Figures 3.3-3.6 for the original gate implementation without the single mode fibres as filters, and Figures 3.7-3.10 with the fitering. Both show the uncorrected state, where the phase shift induced by the beamsplitter has not been accounted for in the final analysis. The purity, linear entropy and the tangle of the individual states are also shown in Table 3.1 & 3.2. The improvement of the fibre filtered gate is eminently clear in every measure. The purity ranges from 99% to 80% for the spatially filtered gate, while the original gate achieves purities in the range from again 99% but dropping as low as 68%. Not surprisingly the linear entropy also shoots up reaching a maximal value of 42% unfiltered compared to 26% with the single mode fibres as filters. The maximal tangle also climbed to new heights reaching consistantly over 60% for all four states (DD, DR, RD, RR) that

should produce a maximally entangled output states, with a maximum of 67% (DD). Prior to the gate upgrade, the tangles ranged from 41% to 56%.

Input State	Purity	Linear Entropy	Tangle
HH	0.954 ± 0.005	0.061 ± 0.006	0.0005 ± 0.0005
HV	0.951 ± 0.010	0.065 ± 0.014	0.006 ± 0.004
HD	0.825 ± 0.013	0.233 ± 0.018	0.003 ± 0.002
HR	0.737 ± 0.013	0.351 ± 0.017	0.001 ± 0.001
VH	0.935 ± 0.013	0.086 ± 0.017	0.006 ± 0.004
VV	0.944 ± 0.012	0.075 ± 0.016	0.003 ± 0.002
VD	0.976 ± 0.008	0.032 ± 0.011	0.004 ± 0.003
VR	0.992 ± 0.005	0.010 ± 0.007	0.002 ± 0.002
DH	0.788 ± 0.013	0.283 ± 0.017	0.0006 ± 0.0012
DV	0.962 ± 0.011	0.051 ± 0.015	0.016 ± 0.006
DD	0.780 ± 0.018	0.29 ± 0.02	0.56 ± 0.04
DR	0.693 ± 0.018	0.41 ± 0.02	0.46 ± 0.03
RH	0.829 ± 0.013	0.229 ± 0.018	0.0004 ± 0.0011
RV	0.936 ± 0.013	0.086 ± 0.017	0.021 ± 0.007
RD	0.683 ± 0.015	0.42 ± 0.02	0.41 ± 0.03
RR	0.721 ± 0.015	0.37 ± 0.02	0.53 ± 0.03

Table 3.1: Purity, Linear Entropy and Tangle of the individual state tomographies conducted during for the process tomography of the CZ gate implemented with PPBSs, without the spatial filtering of the output modes. See text for details.

Input State	Purity	Linear Entropy	Tangle
HH	0.991 ± 0.001	0.0127 ± 0.001	0.0001 ± 0.0001
HV	0.805 ± 0.004	0.2600 ± 0.005	0.0061 ± 0.0014
HD	0.917 ± 0.004	0.1110 ± 0.005	0.0012 ± 0.0004
HR	0.868 ± 0.004	0.1762 ± 0.005	0.0001 ± 0.0001
VH	0.883 ± 0.004	0.1562 ± 0.005	0.0042 ± 0.0012
VV	0.973 ± 0.005	0.0354 ± 0.006	0.0001 ± 0.0001
VD	0.943 ± 0.003	0.0765 ± 0.004	0.0016 ± 0.0006
VR	0.945 ± 0.003	0.0732 ± 0.003	0.0011 ± 0.0004
DH	0.891 ± 0.004	0.1451 ± 0.005	0.0012 ± 0.0005
DV	0.876 ± 0.005	0.1656 ± 0.006	0.0065 ± 0.0014
DD	0.836 ± 0.005	0.2183 ± 0.006	0.667 ± 0.010
DR	0.802 ± 0.004	0.2636 ± 0.006	0.619 ± 0.009
RH	0.864 ± 0.004	0.1819 ± 0.006	0.0002 ± 0.0002
RV	0.872 ± 0.005	0.1702 ± 0.007	0.023 ± 0.003
RD	0.869 ± 0.005	0.1741 ± 0.007	0.675 ± 0.008
RR	0.834 ± 0.004	0.2214 ± 0.006	0.648 ± 0.010

Table 3.2: Purity, Linear Entropy and Tangle of the individual state tomographies conducted during for the process tomography of the CZ gate implemented with PPBSs, after the source had been upgraded and single mode fibres and single mode fibre-coupled detectors were used for spatial filtering of the output modes. Significant increases in purity and tangle and a decrease in linear entropy for superposition input states were obtained. The reduction of the error magnitude is not a result of the improved gate alignment, but an effect of the brighter source leading to larger count numbers and thus better statistics.

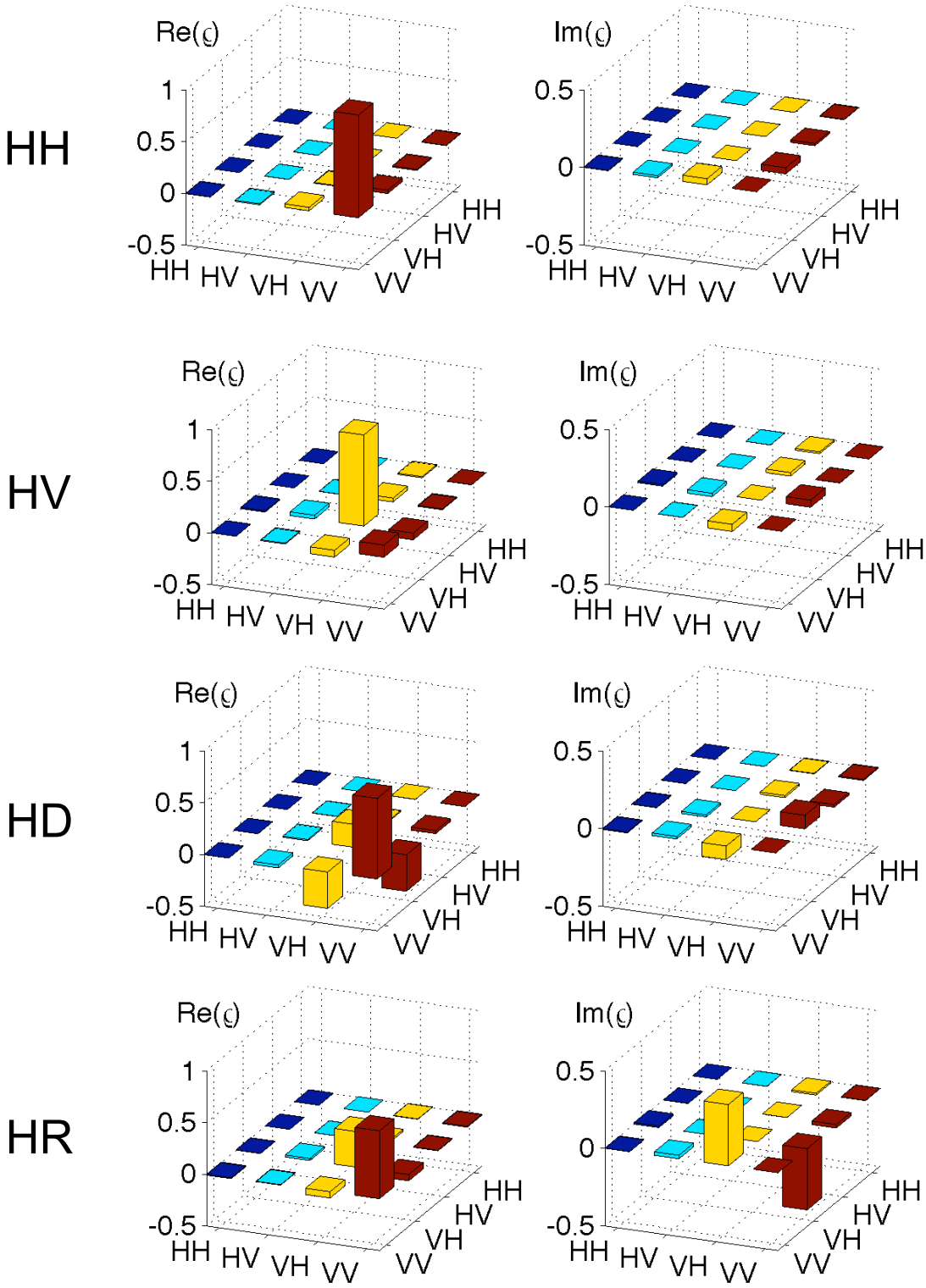


Figure 3.3: State tomographies for the input states HH,HV,HD and HR into the CZ-Gate using free-space detectors and no spatial filtering of the output modes. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate. The shift of the coherences from real to imaginary and vice versa in the HD and HR case are chiefly caused by the phase-shift of the PPBS. The occurrence of coherences in the HH and HV state is not caused by the PPBS and is discussed at a later stage (Section 4.4).

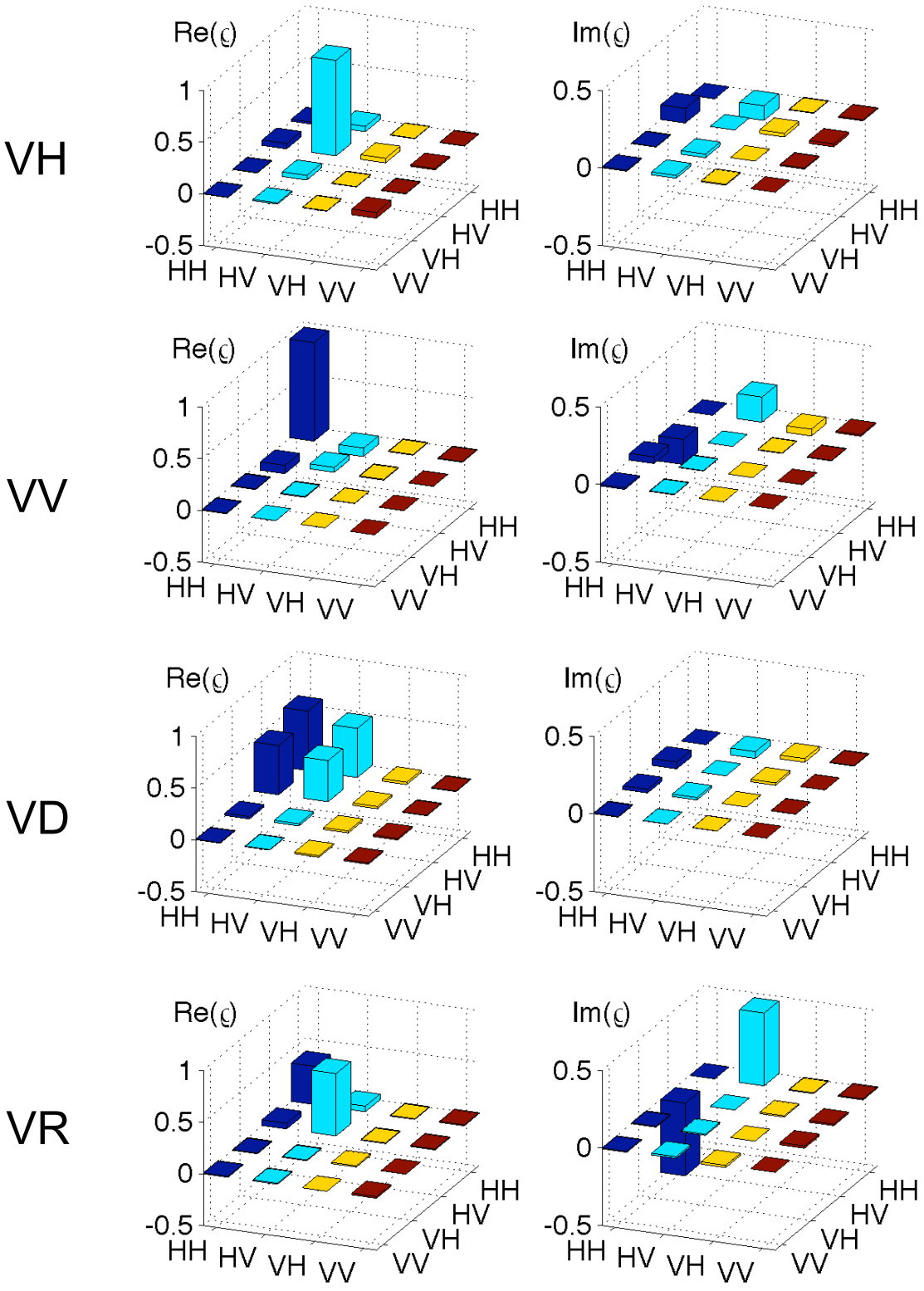


Figure 3.4: State tomographies for the input states VH,VV,VD and VR into the CZ-Gate using free-space detectors and no spatial filtering of the output modes. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate.

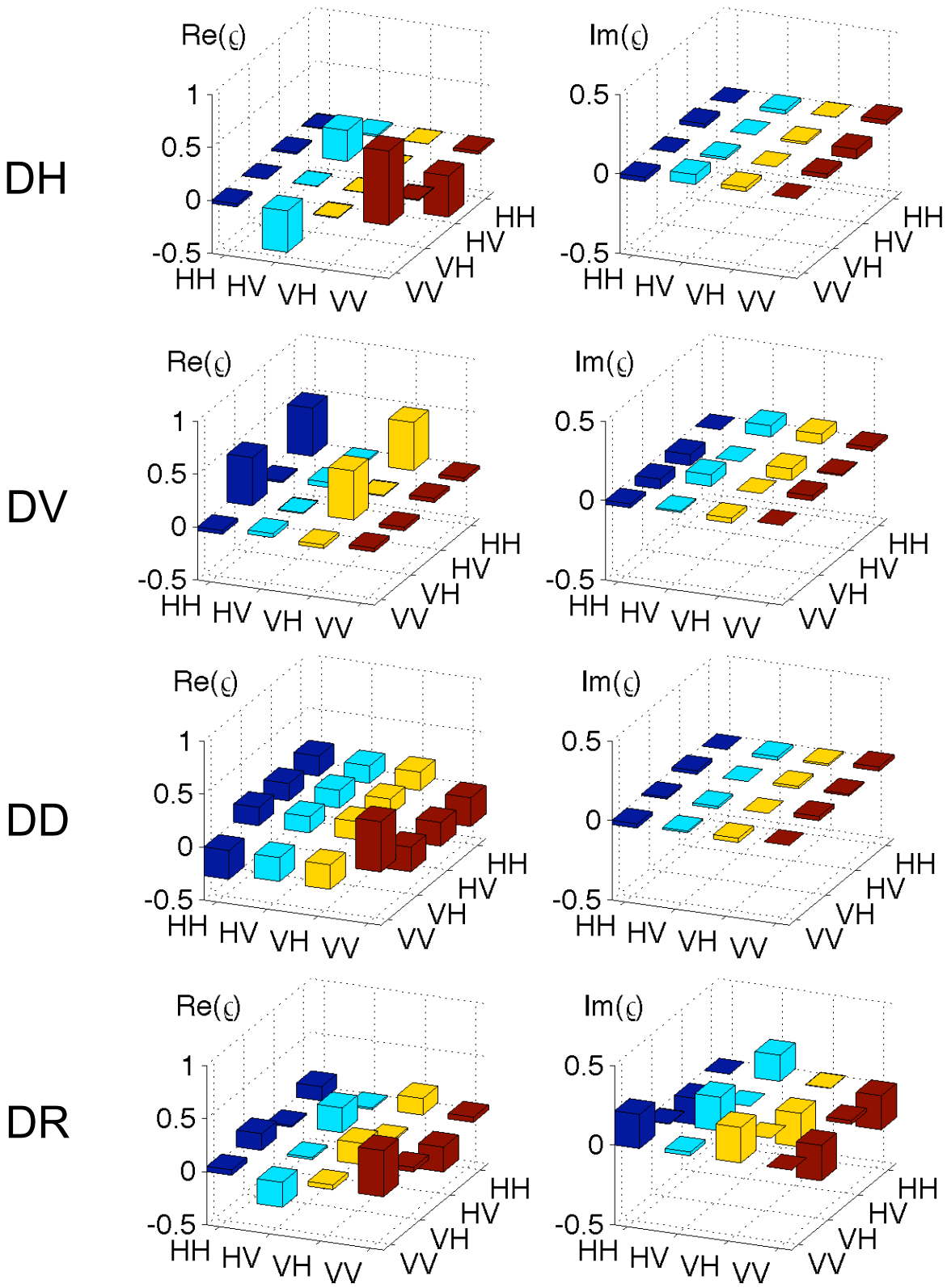


Figure 3.5: State tomographies for the input states DH,DV,DD and DR into the CZ-Gate using free-space detectors and no spatial filtering of the output modes. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate. The output for the DD and DR states are expected to be maximally entangled.

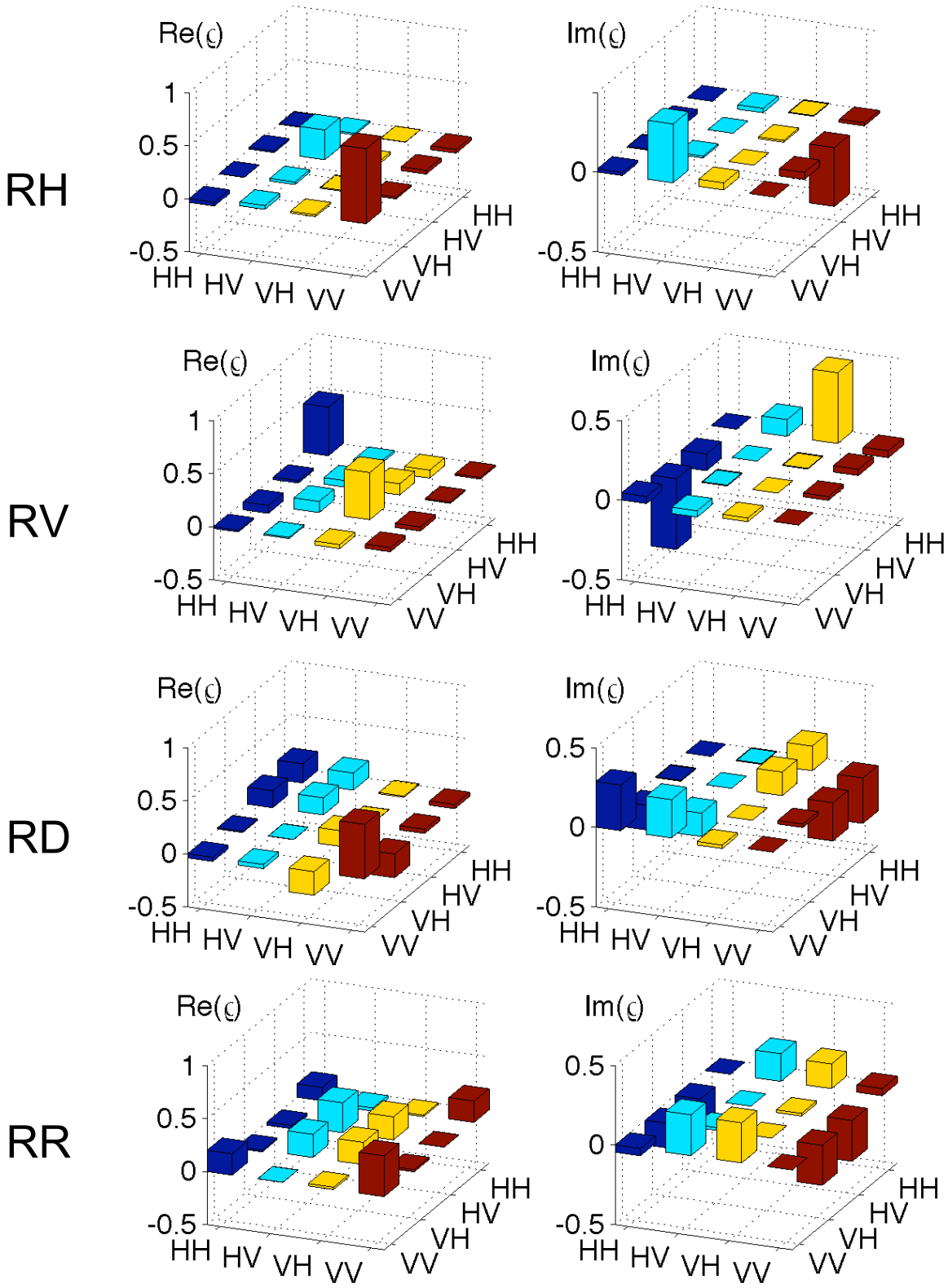


Figure 3.6: State tomographies for the input states RH,RV,RD and RR into the CZ-Gate using free-space detectors and no spatial filtering of the output modes. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate. Maximally entangled outputs are expected for the RD and RR state are

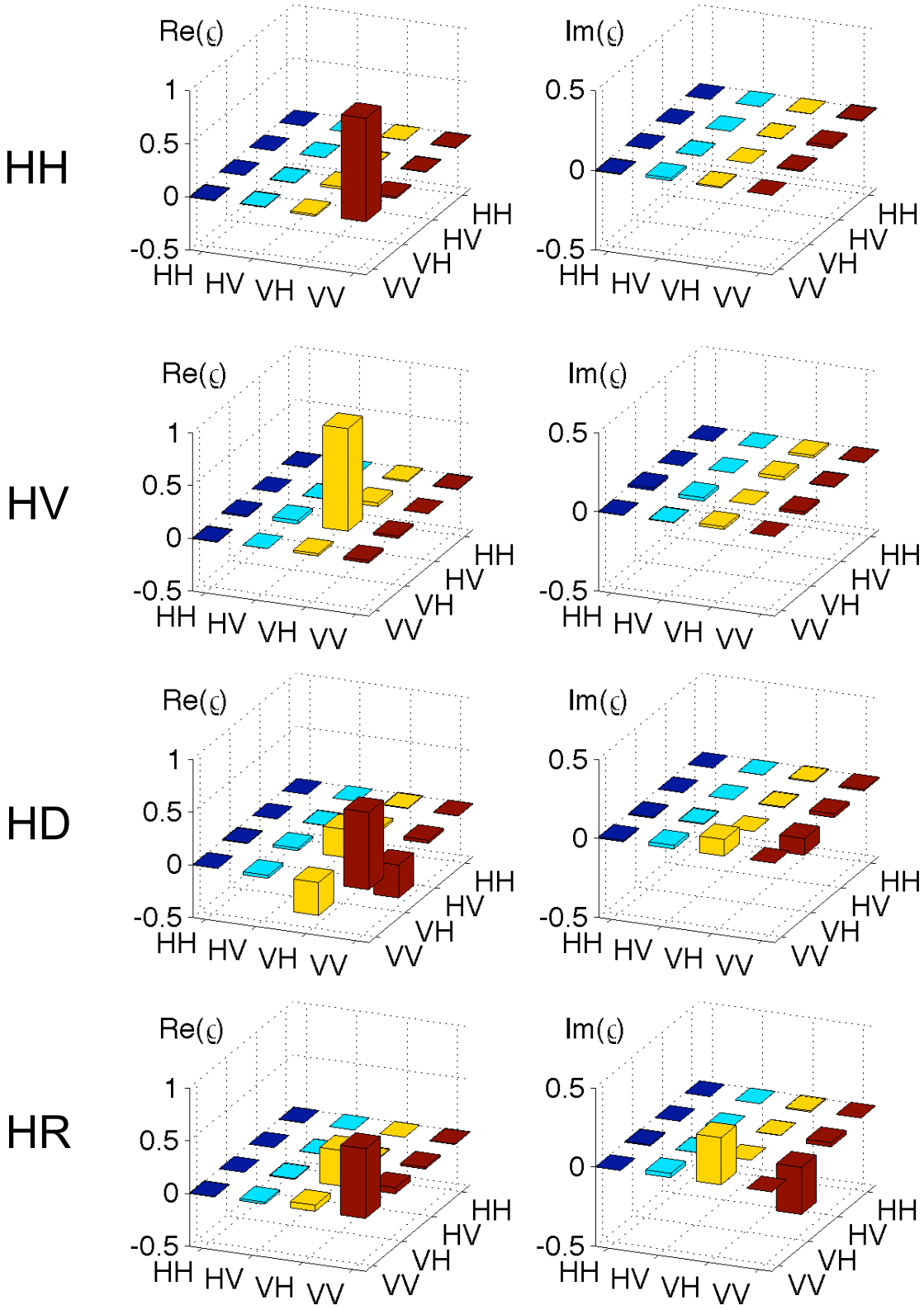


Figure 3.7: State tomographies for the CZ-Gate using single mode fibre coupled detectors for spatial filtering of the output modes. Input states are HH,HV,HD and HR. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate. In comparison to the unfiltered data it becomes immediately obvious that the states are in general of higher quality. Especially in the logically pure states HH and HV the lower rate of undesired populations and coherences is evident.

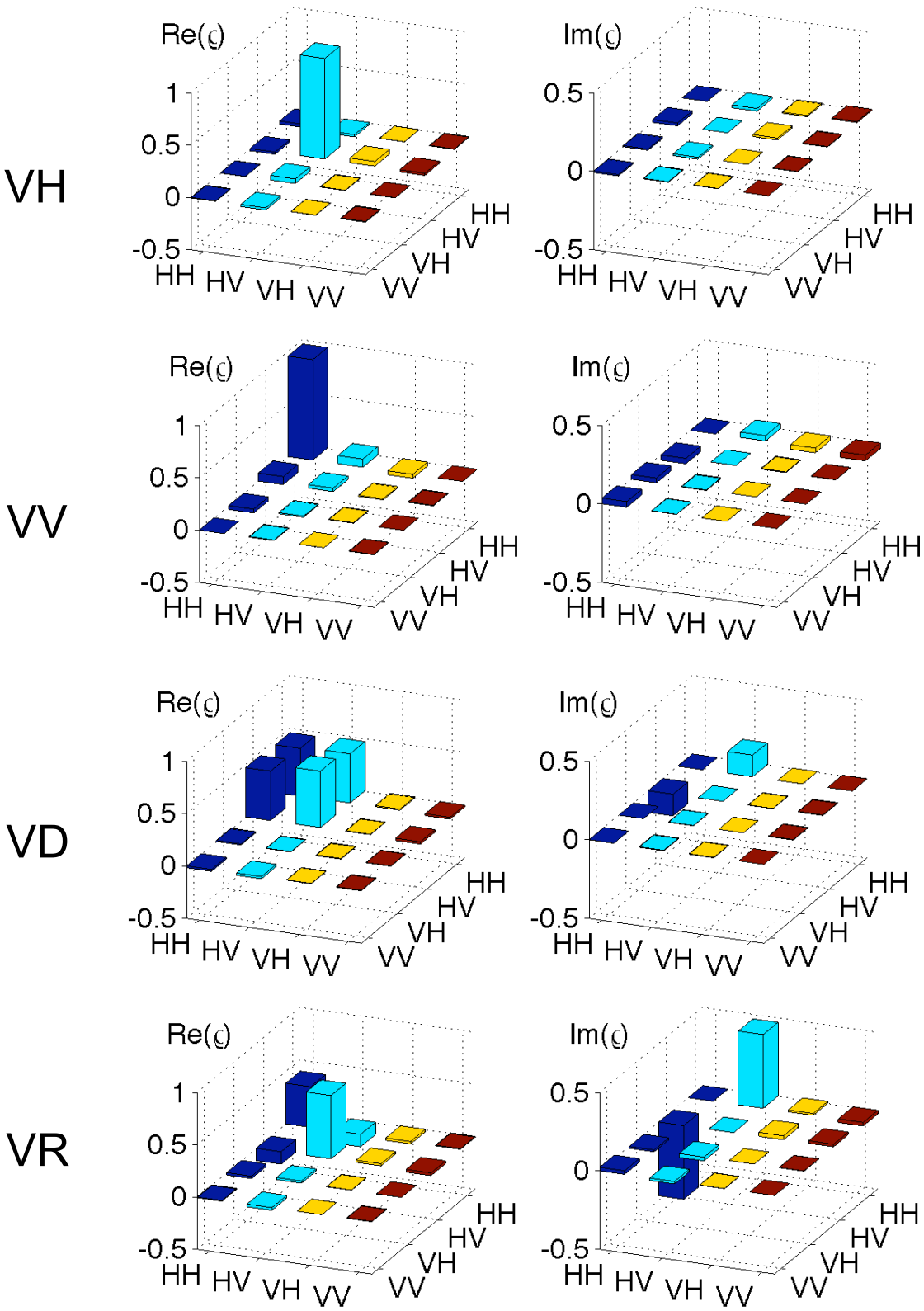


Figure 3.8: State tomographies for the CZ-Gate using single mode fibre coupled detectors for spatial filtering of the output modes. Input states are VH,VV,VD and VR. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate.

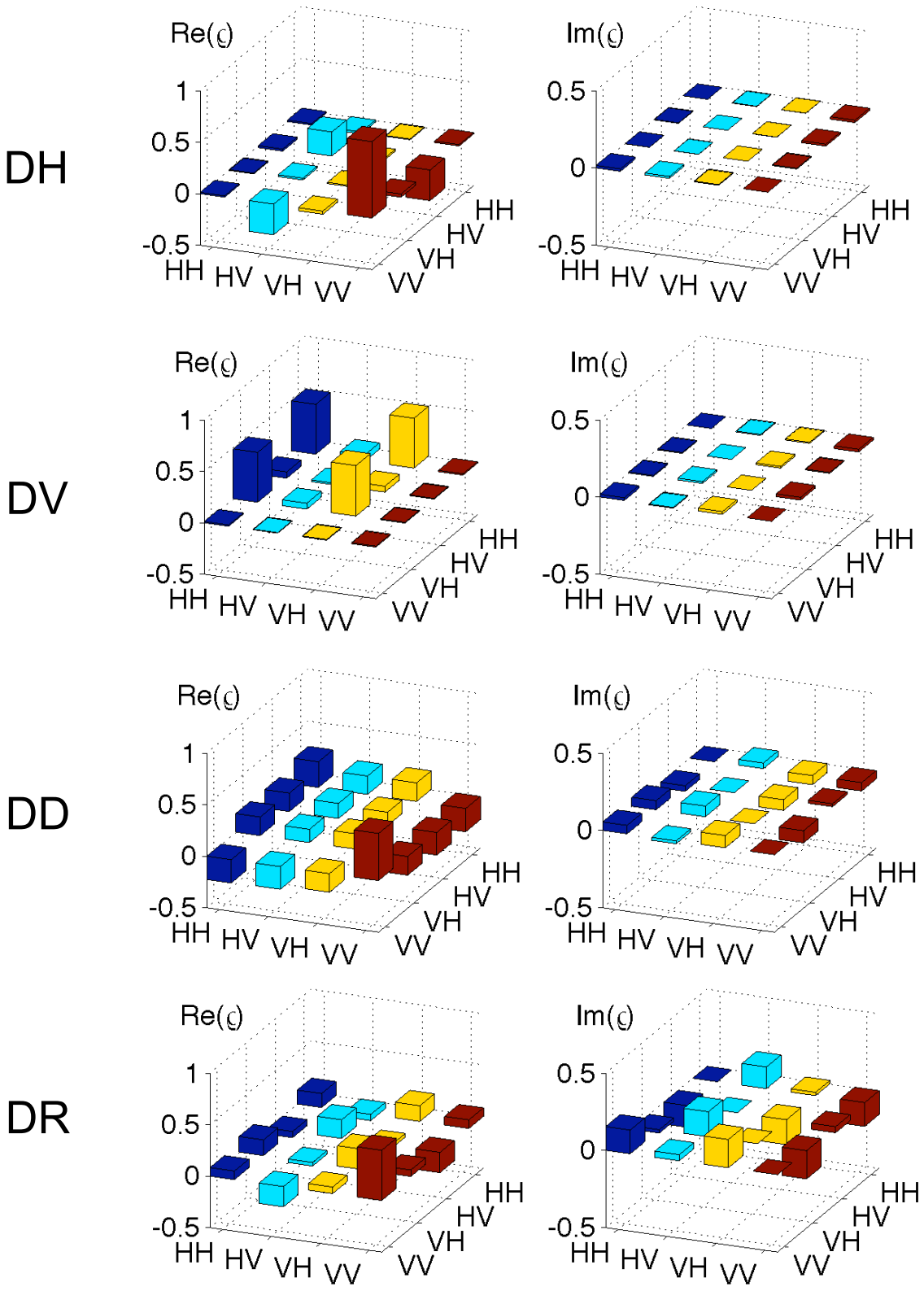


Figure 3.9: State tomographies for the CZ-Gate using single mode fibre coupled detectors for spatial filtering of the output modes. Input states are DH,DV,DD and DR. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate. Both the DD and DR state achieve tangles well above the 60% mark.

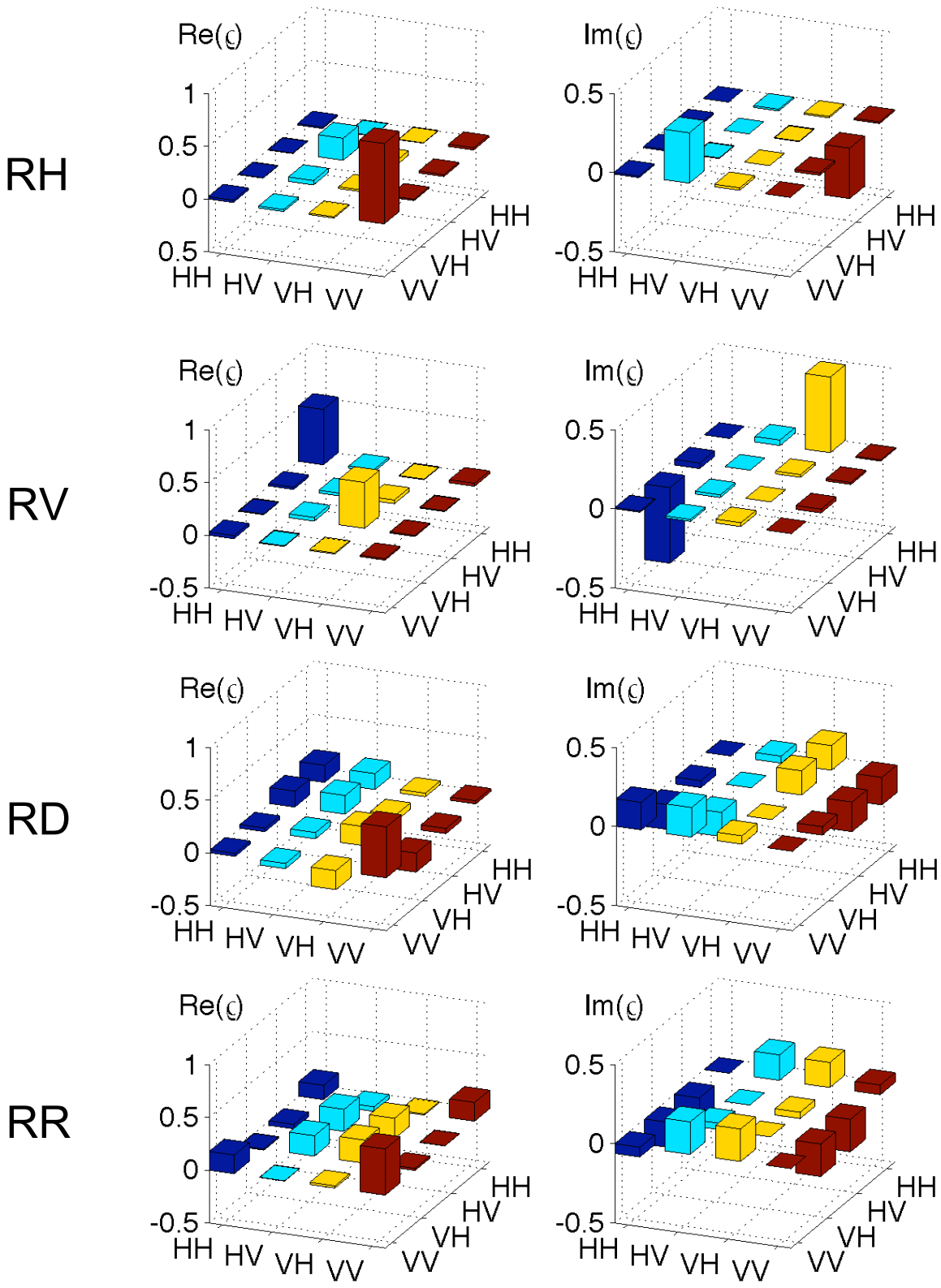


Figure 3.10: State tomographies for the CZ-Gate using single mode fibre coupled detectors for spatial filtering of the output modes. Input states are RH,RV,RD and RR. No compensation was made for the phase shift imposed by the PPBS or the additional bit flip imposed by the gate. Both the RD and RR state show significant tangle, with the DR state yielding the highest tangle of all states during this chapter at 67.5%.

3.3.2 Process Tomographies

As we can see from the tables and state density matrices, the quality of the reconstructed output states improved significantly due to the spatial filtering. Naturally this also improves the quality of the process that the gate implemented. For the process tomography conducted with free space detectors and thus without the additional spatial filtering, we find a process fidelity of $F_p = 76.2\pm0.6\%$ which equates to an average gate fidelity of $\overline{F} = 81.0\pm0.5\%$, where as after the introduction of the single mode fibre coupling at the gate output, the process fidelity rose to $F_p = 84.0 \pm 0.1\%$ with the average gate fidelity reaching $\overline{F} = 87.2 \pm 0.1\%$. The reconstructed χ-matrices are shown in figures 3.11 and 3.12 for the gate without and with the spatial filtering respectively. While the difference might be hard to spot with the naked eye, the (desired) coherences of the processes in the matrix with the spatial filtering in place are significantly higher and closer to the ideal value of 0.25.

As briefly mentioned in our publication, we observed fixed rotations on our single qubits. The nature of the rotation meant that in all states where the output states where not logic states (H or V), the coherences where shifted. The four states seeking to create a maximally entangled state (DD, DR, RD, RR Figures 3.5,3.6,3.9,3.10) subsequently suffer the most. After an extensive analyses of our gate with single qubit tomographies conducted at various points in our circuit, we concluded that the phase shifts were caused by the PPBSs. As the PPBSs consisted of two glued together right angle prisms, with the dielectric stacks in the centre, we were striking the dielectric stack at an angle of 45°, which is known to potentially cause such phaseshifts. As these rotations are a fixed phase shift between the horizontal and vertical component of our qubits, only superposition states are affected. There are two possible methods to eradicate the effect of theses phase shifts. The first one is by installing a equal and opposite phase shift in the gate before the analyser i.e. waveplate at its optic axis, however tilted with respect to the beam. The incorporated phase shift could then be adjusted until single qubit tomography on a superposition state no longer indicates a phase shift. Option two is not altering the physical implementation of the gate but optimising the measured and reconstructed two-qubit state by an optimal single-qubit rotation mathematically. In principle these methods are identical as both find a single qubit rotation that optimises the state. As our measurements were completed by the time we had pinpointed the problem we chose to use the mathematical optimisation. We used the average gate fidelity ($\overline{F}$) as our optimisation parameter. While these optimisations did increase the gate measures (as stated in the paper), we chose to display the reconstructed states and processes without these optimisations for our publication and following suit the reconstructed states and processes in this chapter are also derived without the correction of the undesired rotations induced by the PPBS.

A further major difference of the two process tomographies (with and without the spatial filtering) was the individual duration. While both tomographies consisted of 576 measurements, the original tomography was conducted with 20 second integration time per point, thus consuming a total of 192 minutes or 3 hours and 12 minutes excluding the time it took to alter the waveplate angles in between measurements. It was calculated that the motorised changing of waveplates for the state analyses took on average 5s, adding a further 48 minutes to the total duration. Manually altering the input state and readying the acquisition system for the next input state, takes on average about 3 minutes each, bringing the total

duration to 4 hours and 45 minutes. The total time overhead, the time during which no data was acquired thus totals to nearly one and a half hours. After the source improvement the count rate was so drastically increased, that the per point integration time was reduced to 10 seconds, thus halving the active acquisition time to just 1 hour and 36 minutes. An even shorter acquisition time would have been feasible, but due to the unalterable time overhead through waveplate rotations, we chose to not reduce the acquisition time any further and rather improve the counting statistics, leading to the much improved errors as can be seen in Table 3.2.

3.3.3 Noise sources for the PPBS-CZ gate

While the found process fidelity was the highest recorded for linear optical quantum computing to this point, it still leaves the question where the noise comes from and what can be done to improve the gate operation. Historically imperfect visibility of the non-classical interference, and hence non-ideal gate operation, has been chiefly attributed to poor mode matching, bee this temporal spatial or any other mode. In this experiment however the spatial, temporal, spectral and polarisation modes are very well defined, raising the question what else can contribute to the non-ideal gate operation. This question will be addressed and answered in detail in the following chapters (Chapters **??**). As a quick preview it shall be mentioned here, that the accidental generation of multiple photons in the same spatio-temporal mode, the detector inefficiency and the non-ideal beamsplitter reflectivity are now the leading sources of process imperfection.

3.4 Conclusions from this experiment

- We implemented the first optical CZ-gate free of classical interferometers by using partially polarising beamsplitters.
- We demonstrated the gate with both a pulsed PDC source and a continuous wave source, finding no degradation of the gate performance due to the pulsed source. In fact, the results obtained with the pulsed source surpassed those from the cw-source.
- We implemented spatial filtering after the gate with single mode fibres. This increased all measures of the gate performance, Most notably the process fidelity rose by 7.8% to 84.0%, equalling the highest gate fidelity achieved in an optical gate up to this point. An investigation into the sources of the imperfect gate operation and the sources of the noise is conducted and presented in Chapters **??**.
- Single qubit rotations due to the dielectric stack of the PPBS were identified and compensated for mathematically.
- Future outlook: The PPBS gate has been shown to operate at least as accurately as gates using classical interferometers. This is especially noteworthy as the utilised PPBSs were non-ideal with respect to their reflectivities. More accurate PPBSs will lead to a further improvement to the gate performance. The fact that no classical

interferometers are needed makes the realisation of these type of gates much more feasible with view to a large scale implementation. Nevertheless these gates still only have a success probability of 1/9 and will require a quantum non-demolition measurement to become scalable.

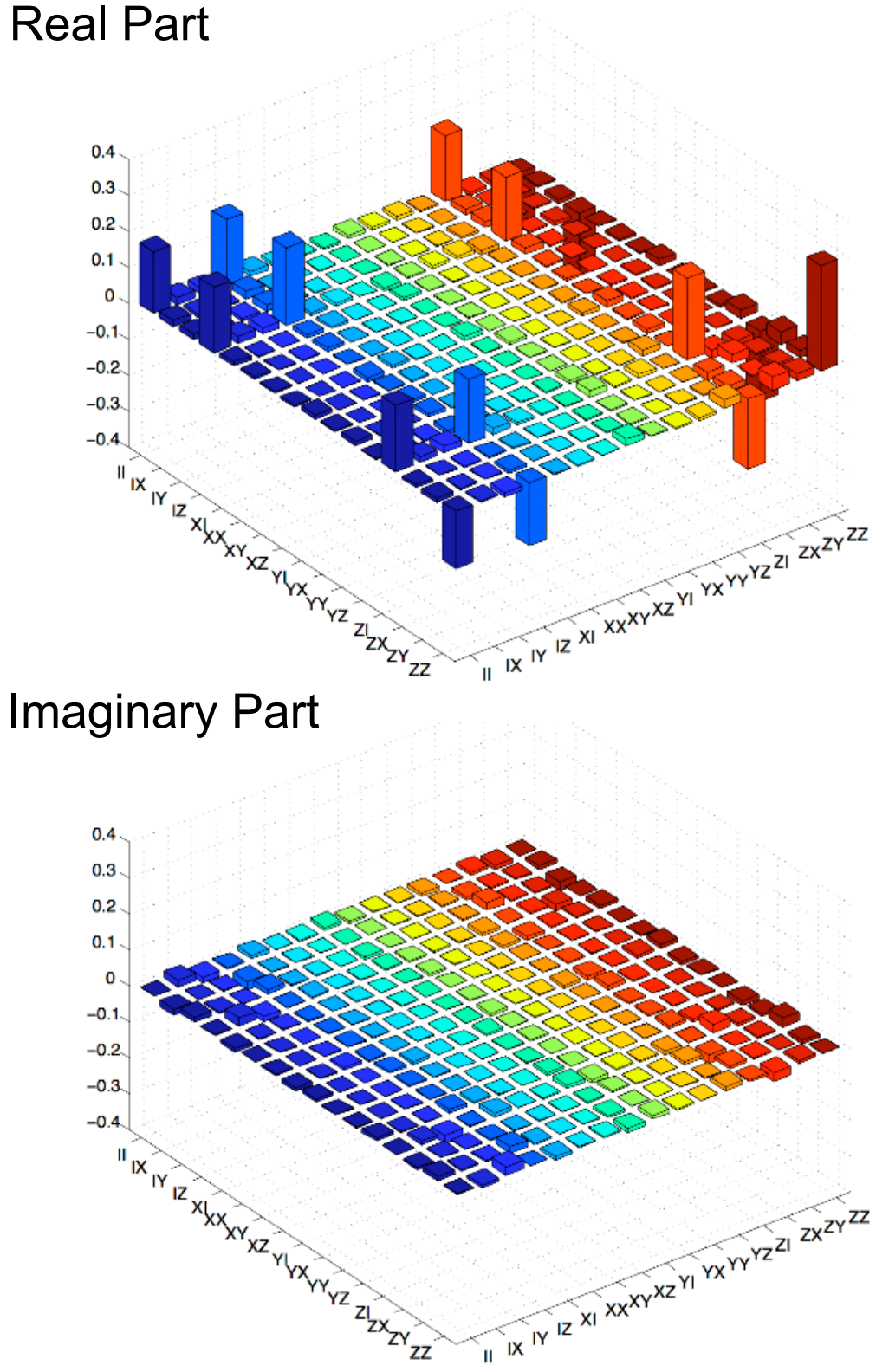


Figure 3.11: Real and imaginary part of the χ-matrix for the original CZ-Gate implementation without the spatial filtering, shown in the Pauli basis. The ideal gate operation (shown in the paper), should consist of equal populations in the II,IZ,ZI and ZZ element and coherences between them.

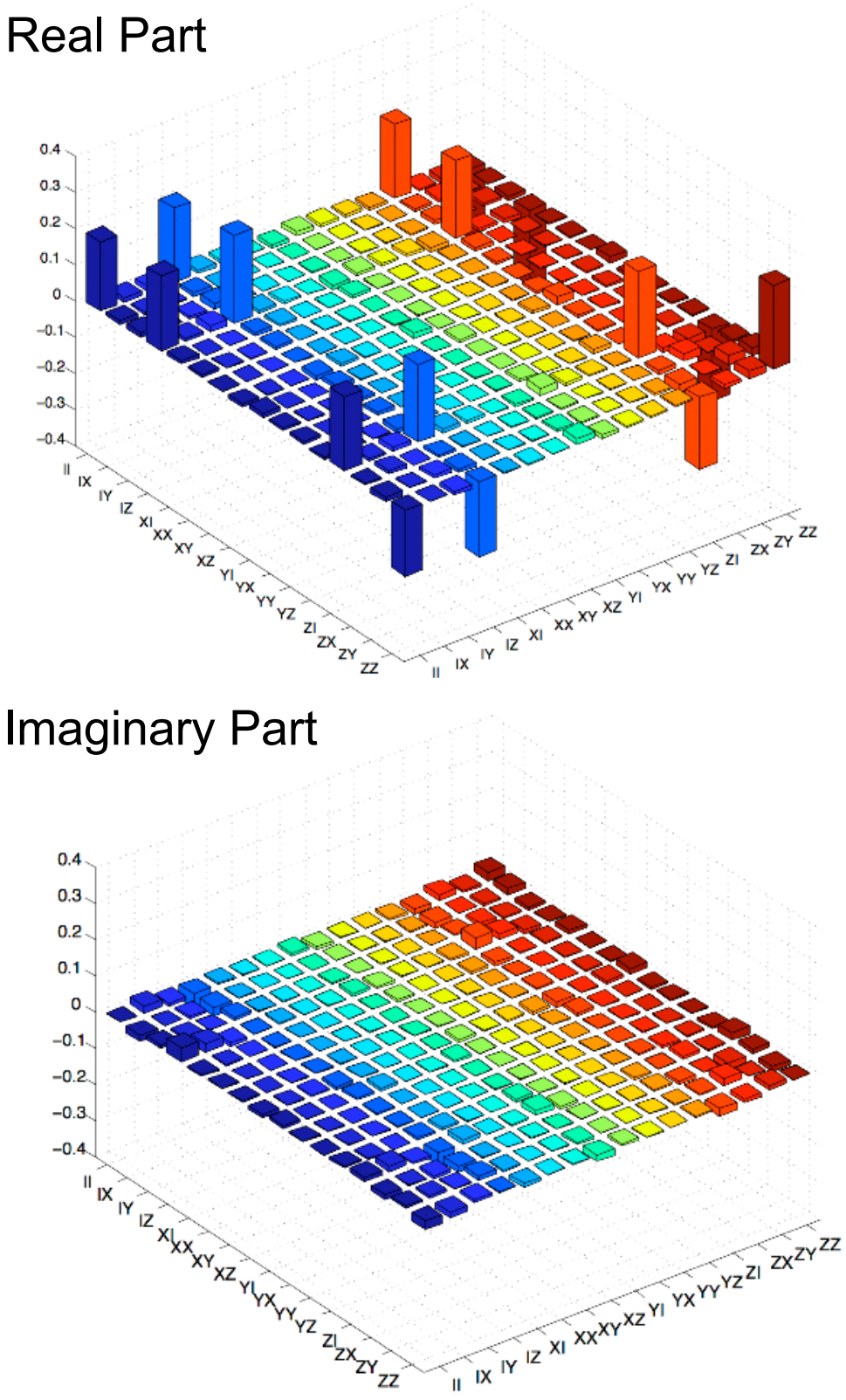


FIGURE 3.12: Real and imaginary part of the χ-matrix for the CZ-Gate in the implementation with the single mode fibres as spatial filters shown in the Pauli basis. The ideal gate operation (shown in the paper), should consist of equal populations in the II,IZ,ZI and ZZ element and coherences between them.

3.4.1 The paper — Demonstration of a simple entangling optical gate and its use in Bell-state analysis

PRL 95, 210504 (2005) PHYSICAL REVIEW LETTERS week ending 18 NOVEMBER 2005

Demonstration of a Simple Entangling Optical Gate and Its Use in Bell-State Analysis

N. K. Langford,[1,2] T. J. Weinhold,[1,2] R. Prevedel,[1,2,3] K. J. Resch,[2] A. Gilchrist,[1,2]
J. L. O'Brien,[1,2] G. J. Pryde,[1,2] and A. G. White[1,2]

[1]*Centre for Quantum Computer Technology, University of Queensland, Brisbane QLD 4072, Australia*
[2]*Department of Physics, University of Queensland, Brisbane QLD 4072, Australia*
[3]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Vienna, Austria*
(Received 30 June 2005; published 18 November 2005)

We demonstrate a new architecture for an optical entangling gate that is significantly simpler than previous realizations, using partially polarizing beam splitters so that only a *single* optical mode-matching condition is required. We demonstrate operation of a controlled-Z gate in both continuous-wave and pulsed regimes of operation, fully characterizing it in each case using quantum process tomography. We also demonstrate a fully resolving, nondeterministic optical Bell-state analyzer based on this controlled-Z gate. This new architecture is ideally suited to guided optics implementations of optical gates.

DOI: 10.1103/PhysRevLett.95.210504 PACS numbers: 03.67.Lx, 03.65.Wj, 03.67.Mn, 42.50.Dv

A key resource for using entanglement in quantum information protocols is gates that are capable of entangling or disentangling qubits [1]. Entangling gates lie at the heart of quantum computation protocols, for example, and disentangling gates used in Bell-state analyzers are required for quantum teleportation. Conceptually, the simplest such two-qubit gate is the controlled-Z (CZ) gate, which in the logical basis produces a π phase shift on the $|11\rangle$ term, (i.e., $|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$; $|10\rangle \rightarrow |10\rangle$; $|11\rangle \rightarrow -|11\rangle$). This is a maximally entangling gate which, when coupled with single-qubit rotations, is universal for quantum computing [2].

In 2001, Knill, Laflamme, and Milburn proposed a scheme for linear optical quantum computing which used measurement to nondeterministically realize the optical nonlinearity required for two-qubit entangling gates [3]. They also showed that deterministic versions of these gates could be achieved using teleportation [4], which requires Bell-state measurement. Since then, there have been a number of demonstrations of quantum logic gates derived from this concept [5–9] and further theoretical development of linear-optics schemes [10–14]. In particular, there is a recent suggestion to use nondeterministic CZ gates to construct cluster states for demonstrating optical cluster-state quantum computation [15].

Here we report an experimental demonstration of a nondeterministic linear-optics CZ gate and its application as a Bell-state analyzer. This CZ gate is the simplest entangling (or disentangling) linear-optics gate realized to date, requiring only three partially polarizing beam splitters (PPBSs), two half-wave plates, no classical interferometers, and no ancilla photons. It is nondeterministic, and success is heralded by detection of a single photon in each of the outputs. We demonstrate the operation of this type of gate using photons generated both by continuous-wave (cw) and by femtosecond-pulsed parametric down-conversion—we find that temporal mode mismatch was not a significant factor in the gate's performance. We fully characterize the operation in both regimes using quantum process tomography, and we also demonstrate the use of this kind of gate for fully resolving Bell measurements. This simple entangling optical gate is promising for micro-optics or guided optics implementations where extremely good nonclassical interference is realizable.

The best performing entangling gate implementations to date have been interferometric: A conceptual schematic of an interferometric optical CZ gate, composed of three partially reflecting beam splitters with reflectivity $\eta = 1/3$, is shown in Fig. 1(a). Each polarization qubit input to the gate is split into two longitudinal spatial modes via a polarizing beam splitter. The horizontally polarized modes meet at a 1/3 beam splitter, and nonclassical interference means that, for an arbitrary input state, the entire circuit performs

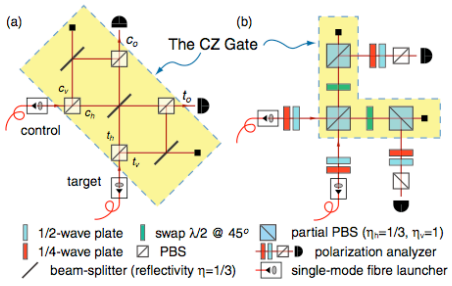


FIG. 1 (color). (a) Interferometric CZ gate based on the approach of Refs. [13,14]. Gate operation is enabled by transforming each qubit from polarization to spatial encoding and back again. This requires high interferometric stability and spatiotemporal mode matching for correct operation. (b) Partially polarizing beam splitter gate. The qubits can remain polarization encoded, since the vertically polarized modes are completely reflected by the first PPBS and do not interact. Nonclassical interference occurs between the horizontally polarized modes, with $\eta = 1/3$. The subsequent PPBSs give the required losses in the c_V and t_V modes as shown in (a).

PRL 95, 210504 (2005) PHYSICAL REVIEW LETTERS week ending 18 NOVEMBER 2005

the transformation: $\alpha|HH\rangle + \beta|HV\rangle + \gamma|VH\rangle + \delta|VV\rangle \rightarrow \frac{1}{3}[-\alpha|HH\rangle + \beta|HV\rangle + \gamma|VH\rangle + \delta|VV\rangle] + \cdots$, where H and V refer to horizontal and vertical polarization, respectively, and the terms not shown correspond to the failure mode of the gate (i.e., the control and target output ports do not each contain one photon). With probability 1/9, the circuit performs the CZ operation (using the logic-basis definitions $0 \equiv V$ and $1 \equiv H$). After the network of 1/3 beam splitters, the two spatial modes of the control and target must be recombined to return to polarization-encoded qubits. Since the phase relationship between the logical modes must be maintained throughout this operation, interferometric stability is required between the control and target modes. Inherently stable interferometers have previously been used [6,7] to achieve this—however, these may not be suitable for scaling to large numbers in micro- or integrated-optical realizations. Here we take an alternative approach which does not require interferometric stability.

The experimental setup for the CZ gate we have developed is shown schematically in Fig. 1(b). We use PPBSs with reflectivities of 1/3 and 1 for horizontally and vertically polarized light, respectively [16]. As in Fig. 1(a), only the H modes interfere nonclassically at the first PPBS. The V inputs are then flipped to H by half-wave plates—single-qubit X gates—and are attenuated by the remaining two PPBSs to balance the losses. The circuit of Fig. 1(b) therefore performs a CZ gate with additional X gates on the control and target qubits. These X gates could be corrected with wave plates in the outputs or by relabeling the logical states of the outputs—here we chose to relabel. The key advantage of the PPBS gate is that the polarization modes are never spatially separated and recombined, and, consequently, no classical interference conditions are required. A single nonclassical interference at the first PPBS is, therefore, the gate's sole mode-matching condition.

To test multiqubit circuits, multiphoton sources are required. The current gold standard for generating two or more photons is pulsed parametric down-conversion: Pump power densities far greater than those possible with cw sources lead to significantly higher probabilities of multiphoton events. Down-converted photons from short pump pulses can display more complex interference effects with reduced visibility. Thus, any new gate architecture should be shown to be compatible with both cw and pulsed sources. We tested the PPBS architecture with both cw and femtosecond-pulsed sources, which produce pairs of energy degenerate single photons via spontaneous parametric down-conversion in a β-barium-borate crystal (Table I). The photon pairs were collected into single mode optical fibers to improve the spatial mode and injected into the CZ gate [Fig. 1(b)]. In the pulsed case, mode-matching was also improved by collecting the gate output into single mode fibers. A pair of half- and quarter-wave plates at the output of each fiber was used for input state preparation. A coincidence window of ~5 ns was used, and no correction for accidental counts was made. The gates were completely characterized via quantum process tomography [7,18].

TABLE I. Photon source parameters.

Parameter	cw	Pulsed
Pump source	Ar^+	Doubled Ti:Sa
Pump wavelength	351.1 nm	410 nm
Crystal arrangement	Type I sandwich [17]	Type I single
Photon wavelength	702.2 nm	820 nm
Interference filters	±0.18 nm	±1.5 nm
Output state	Separable ↔ entangled	Separable

A convenient representation of the measured process is the χ matrix, which is a complete and unique description of the process relative to a given basis of operators. The χ matrix for ideal CZ gate operation in the Pauli basis is shown in Fig. 2(a) (all the components are real). The experimental results for the cw gate are shown in Fig. 2(b), those for the pulsed gate in Fig. 2(c). By using the method of Ref. [7], we are guaranteed physical χ matrices requiring no extra normalization. In the cw case, the II term is 0.36 instead of the expected 0.25 due to imperfect nonclassical interference resulting from mode mismatch.

Gate performances can be quantified by calculating the process fidelity $F_P = \mathrm{Tr}[\chi_{\mathrm{meas}}\chi_{\mathrm{ideal}}]$ or the average gate fidelity, which is the fidelity between expected and actual output states, averaged over all pure inputs, $\bar{F} = (4F_P + 1)/5$ [7,19]. The cw and pulsed gates have process fidelities of 74.6 ± 0.3% and 84.0 ± 0.1%, respectively, and average gate fidelities of 79.7 ± 0.2% and 87.2 ± 0.1%, respectively [20]. Despite more stringent temporal mode-matching requirements in the pulsed regime, the extra spatial filtering led to better gate operation, equivalent to the previous best demonstration [7].

In our experiment, we observed systematic, fixed polarization rotations, probably due to birefringent effects in nonideal PPBSs. In practice, these have no effect on gate quality and, if necessary, could be compensated for with appropriate wave plates. To demonstrate this, we modeled their effect numerically, identifying single-qubit unitary corrections which increased the cw and pulsed process fidelities to 77.0 ± 0.3% and 86.6 ± 0.2%, respectively, and average gate fidelities to 81.6 ± 0.2% and 89.3 ± 0.1%, respectively.

A potential drawback of the PPBS architecture is that the beam splitting ratios are fixed at manufacture—in contrast to schemes where the setting of a half-wave plate determines the effective beam splitter reflectivity [6,7]. While the PPBSs for the cw gate (optimized for 702.2 nm) were measured to be within ±0.01 of the required reflectivities, for the pulsed gate (820 nm), the values for the three PPBSs were $\eta = 0.28$, 0.28, and 0.29 (±0.01; normalized to output power). Modeling a gate using 0.28 reflectivities, we find the optimum process fidelity that can be obtained is $F_P^{0.28} = 96\%$—near ideal. As originally shown in

PRL 95, 210504 (2005) PHYSICAL REVIEW LETTERS week ending 18 NOVEMBER 2005

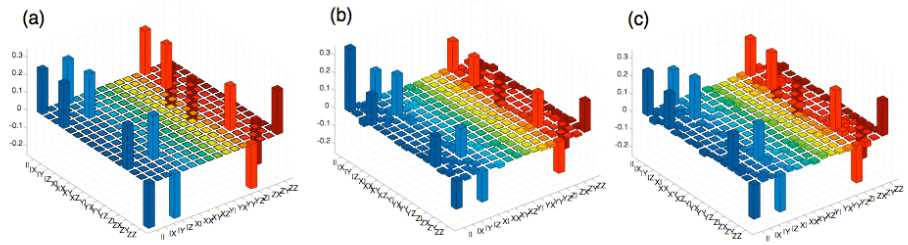


FIG. 2 (color). Quantum process tomography of the CZ gate. Real components of the χ matrix for the: (a) ideal, (b) cw, and (c) pulsed CZ gates. The imaginary components of the experimental matrices are not shown: A few elements are on the order of 0.05; the average is ~0.005.

Ref. [13], the CZ gate is relatively forgiving of the exact splitting ratios, making it an eminently suitable gate to be realized with a PPBS architecture. Performance of the PPBS gates is limited almost exclusively by mode matching, primarily spatial, making these gates promising candidates for micro- or integrated-optical implementations, where nonclassical mode matching in excess of 99% can be expected [21].

We further test the CZ gate by operating it as a Bell-state analyzer of the entangled continuous-wave input states [17]. Because of the geometry of the source, and birefringence and geometric effects in the single mode fibers, the near-maximally entangled state produced is of the form $|HH\rangle + e^{i\varphi}|VV\rangle$. We use quantum state tomography [22,23] to characterize the source state [Fig. 3(a)]. The tangle $T = 0.93 \pm 0.01$ and linear entropy $S_L = 0.05 \pm 0.01$ show that this state is highly entangled and highly pure; the fidelity with a maximally entangled state is $F = 98.0 \pm 0.4\%$. We determine that $\varphi = -2.094$ radians, and, by using the input wave plates [Fig. 1(b)] to perform appropriate single-qubit unitaries on each qubit, we can transform the state of Fig. 3(a) to any desired maximally entangled state of linear polarization. In Fig. 3(b), we have produced the state $|HH\rangle + |VV\rangle$ with fidelity $F_{\phi^+} = 96.1 \pm 0.2\%$; $T = 0.96 \pm 0.01$ and $S_L = 0.02 \pm 0.01$.

To quantify the performance of the CZ gate as a Bell-state analyzer, we produced the four maximally entangled states: $|\psi'^{\pm}\rangle = |HA\rangle \pm |VD\rangle$; $|\phi'^{\pm}\rangle = |HD\rangle \pm |VA\rangle$,

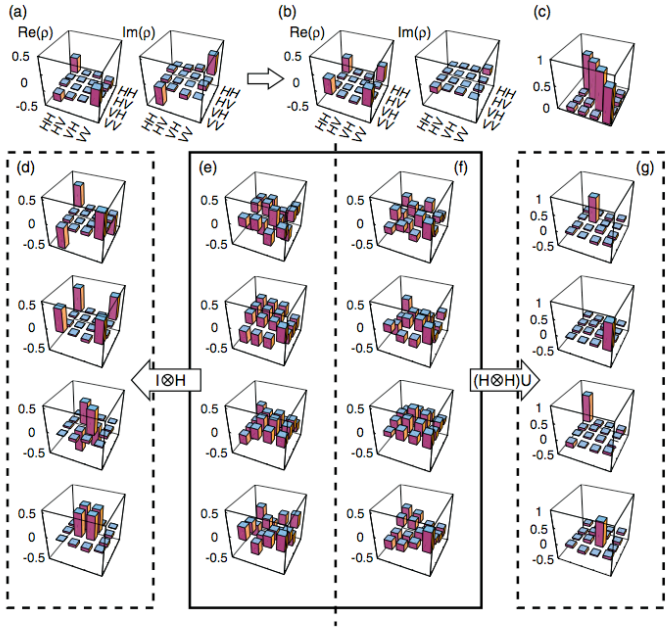


FIG. 3 (color). The CZ gate operating as a Bell-state analyzer. (a) The two-qubit entangled state at the output of the fibers and (b) transformed to the ϕ^+ Bell state. (c) The measured truth table: The average probability of success is 0.78 ± 0.03. (d)–(g) Transformation of near-maximally entangled states to near-separable states by a CZ gate Bell-state analyzer. (d) The input Bell states determined from (e) the measured input states with the second qubit rotated by a Hadamard. (f) The measured output states, (g) transformed by applying local rotations to each qubit (see text).

where $D \equiv (|H\rangle + |V\rangle)/\sqrt{2}$ and $A \equiv (|H\rangle - |V\rangle)/\sqrt{2}$. These are just the usual four Bell states, with the second qubit rotated by a Hadamard so that they can be discriminated by the CZ gate. The four experimentally produced density matrices are shown in Fig. 3(e): The average of their fidelities is $\overline{F} = 95.8 \pm 0.7\%$; the average of the tangles and linear entropies are $\overline{T} = 0.94 \pm 0.02$ and $\overline{S}_L = 0.04 \pm 0.01$, respectively. For ease of visualization, we have numerically rotated these states into the more familiar form by applying a Hadamard gate to the second qubit [Fig. 3(d)].

An ideal CZ gate would take the four maximally entangled states $|\psi'^{\pm}\rangle$, $|\phi'^{\pm}\rangle$ to the four separable orthogonal states: $|DD\rangle$, $|AD\rangle$, $|DA\rangle$, and $|AA\rangle$, respectively. For the four input states in Fig. 3(e), the measured output density matrices are shown in Fig. 3(f). In fact, they are close to the four orthogonal separable states $(|H\rangle \pm e^{i\varphi_1}|V\rangle) \otimes (|H\rangle \pm e^{i\varphi_2}|V\rangle)$, where $\varphi_1 = -3.07$ and $\varphi_2 = 0.32$ as determined by a best fit. For ease of visualization, we have rotated these states into the logical basis in Fig. 3(g). The average of the fidelities between all combinations of the measured output states is $24 \pm 5\%$ (ideally zero), demonstrating that the states are close to orthogonal. Their average tangle $\overline{T} = 0.04 \pm 0.05$ and linear entropy $\overline{S}_L = 0.42 \pm 0.07$ indicate that they are unentangled, albeit somewhat mixed. This circuit is working quite well as a Bell-state analyzer.

The average fidelity of the measured output states with the above separable states is $F = 79 \pm 3\%$: If we analyzed the output of the circuit in this rotated basis, we would correctly identify the Bell state with a probability of 79%. More directly, we can measure each of the separable states for each Bell-state input by explicitly analyzing in the rotated basis, which gives the directly measured truth table for the CZ gate when operated as a Bell-state analyzer. The results are shown in Fig. 3(c), and the average probability of success is $78 \pm 3\%$, in agreement with the tomography results.

It is interesting to note that, whenever a postselected event occurs, the Bell measurement has effectively discriminated one of four input wave plate settings applied to a single input qubit. That is to say, 2 bits of classical information (representing the four wave plate settings) have been encoded into a single qubit. This is reminiscent of quantum dense coding [24–26], although, because the Bell measurement is nondeterministic, a protocol using this gate would be less efficient than ordinary classical communication. Nevertheless, this still demonstrates the power of entanglement for dense coding given a deterministic Bell analyzer, such as can be constructed, in principle, using measurement-induced nonlinearity.

In summary, we have proposed and demonstrated a new architecture for entangling optical gates. The key advantage of this new gate architecture is its simplicity and suitability for scaling—it requires only one nonclassical mode-matching condition and no classical interferometers. This is very promising for micro-optic and integrated-optic realizations of this gate, where extremely good mode matching can be expected. Finally, we have demonstrated the operation of this gate as a Bell-state analyzer which has the advantage of higher success probability and no ancilla compared to alternative recent demonstrations [9,27].

This work was supported by the Australian Research Council (ARC), the Queensland Government, and the U.S. Advanced Research and Development Agency (ARDA). R. P. acknowledges support from the Austrian Science Foundation (FWF). We acknowledge Rohan Dalton for valuable discussions.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] The more familiar CNOT gate is formed by applying a Hadamard gate H to the target qubit before and after a CZ gate.
[3] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[4] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[5] T. B. Pittman *et al.*, Phys. Rev. A **68**, 032316 (2003).
[6] J. L. O'Brien *et al.*, Nature (London) **426**, 264 (2003).
[7] J. L. O'Brien *et al.*, Phys. Rev. Lett. **93**, 080502 (2004).
[8] S. Gasparoni *et al.*, Phys. Rev. Lett. **93**, 020504 (2004).
[9] Z. Zhao *et al.*, Phys. Rev. Lett. **94**, 030501 (2005).
[10] T. C. Ralph *et al.*, Phys. Rev. A **65**, 012314 (2002).
[11] E. Knill, Phys. Rev. A **66**, 052306 (2002).
[12] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. Lett. **88**, 257902 (2002).
[13] T. C. Ralph *et al.*, Phys. Rev. A **65**, 062324 (2002).
[14] H. F. Hofmann and S. Takeuchi, Phys. Rev. A **66**, 024308 (2002).
[15] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[16] The PPBSs are cube beam splitters with appropriately specified multilayered dielectric stacks purchased from Asahi Spectra (702.2 nm) and Special Optics (820 nm).
[17] P. G. Kwiat *et al.*, Phys. Rev. A **60**, R773 (1999).
[18] This involves inputting identical ensembles of 16 separable states into the circuit and performing a set of 36 measurements for each—36 measurements form an overcomplete set which increases accuracy.
[19] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).
[20] The errors were estimated by doing a 1000 run Monte Carlo simulation of the whole process tomography analysis, with Poissonian noise added to the count statistics in each run.
[21] T. B. Pittman and J. D. Franson, Phys. Rev. Lett. **90**, 240401 (2003).
[22] A. G. White *et al.*, Phys. Rev. Lett. **83**, 3103 (1999).
[23] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
[24] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[25] T. Schaetz *et al.*, Phys. Rev. Lett. **93**, 040505 (2004).
[26] K. Mattle *et al.*, Phys. Rev. Lett. **76**, 4656 (1996).
[27] P. Walther and A. Zeilinger, Phys. Rev. A **72**, 010302(R) (2005).

4

Controlled-Sign gate between independent photons

In this chapter of the thesis I discuss methods for increasing the number of qubits and thus number of photons used in quantum circuits. This involves both a slight redesign of the gate and a source of more than two simultaneous photons. While the investigation of a many (i.e. more than two) qubit entangling gate fails initially, this leads to the intensive investigation of behaviour of a controlled-sign gate with independently generated photons. We do this both experimentally and by deriving a full model of the gate with all of its parameters determined from the experimental setup. We find that our model describes the experiment with very high accuracy and allows a detailed analyses of the magnitude and effect of the observed noise sources. Surprisingly, undesired multi-photon emission is identified as the leading noise source, degrading the process fidelity by 15.8%.

Kevin Resch, Geoff Pryde and Jeremy O'Brien assisted me in the experimental realisation of the multi-photon gates. Kevin Resch also assisted in the measurement and analyses of the independent photon gate and in the debugging of the Mathematica^{TM}model for the independent gate. Alexei Gilchrest lead the reconstruction and mathematical optimisation of the process tomographies and also helped me debug my Mathematica code and provided me with an important insight in some of Mathematica's functions and flaws.

4.1 Scaling up the gates

The Di Vincenzo-criteria for quantum computing demand that to be suitable, an architecture should be scalable, meaning that without large overheads the number of utilised qubits can be increased indefinitely. The issue of scalability can not be answered positively with certainty in any architecture yet. In linear optical quantum computing, the potential path to scalable quantum computing is clear at least in principle [12]. The first step towards optical quantum

computing was successfully taken through the demonstration of two-qubit entangling gates [53–59], the next major step was to address the issues on the path to scalability. While the challenges optical quantum computing face in this respect are manifold, the individual limitations must each be addressed. Thus demonstrating the extension from entangling two-qubits to a larger number of qubits becomes the next aim. The demonstrated two-qubit CSign gate of chapter 3 is, like all other optical quantum gates demonstrated so far, only probabilistic, with a success probability of 1/9. Chaining such gates to circuits rapidly reduces the success probability to unfeasible realms especially when paired with the ever decreasing probability of generating the appropriate photon number via spontaneous PDC.

One improvement was suggested by Ralph [60]. Instead of simply chaining the gates and feeding one output into the next gate as input as shown in figure 4.1a), one combines the the second gate action into the dump-port of the first gate as shown in figure 4.1b). This reduces the portion of the signal that is dumped and thus improves the success rate from 1/81 for two chained CSign gates, to 1/27, or by a factor of 3. Even better, this method can be expanded infinitely, leading to a circuit success probability $P_{circ} \approx (1/3)^N$ (instead of $(1/9)^N$, where N is the number of involved qubits. While this obviously does not solve the problem of ever decreasing success probability for large N, it certainly improves the feasibility of test circuits operating in the small N limit. The downside of this gate logic is that as the two interactions are both controlled in part by the input state of the central qubit (CZ action imposes the sign shift if and only if both qubits are in the logic $|1\rangle$ state), and since the logic of the bottom gate is inverse to that of the top gate, the gates are not as flexible as individual gates. For example it is not possible to place a single unitary rotations between the two gates to alter the action of the qubit that is interacting in both gates.

There are several challenges to be overcome in implementing such a gate experimentally: First and foremost, it requires three qubits. A single PDC event will thus not suffice and as PDC is spontaneous and terribly inefficient, this drastically reduces the rate at which the circuit can be operated. A second difficulty lies in the fact that photons from a single down-conversion event share certain correlations through their shared mother (pump) photon, which reduces the required effort to make them perfectly indistinguishable for the non-classical interference at the heart of our quantum gates.

For a proof-of-principle demonstration one can replace one of the inputs to such a three qubit gate with a strongly attenuated coherent state [61, 62], which has to contain on average less than one photon per pulse. As our circuit started of with a pump laser at the appropriate frequency for the quantum logic, one could use the unconverted light of the Ti:Sa laser for this coherent state input as it is by definition at the correct wavelength and the same repetition rate. After attenuating the fundamental that passed through the second harmonic separator in fig 2.4 with multiple stacked neutral density filters followed by crossed polarises with a half-waveplate between them for tuneability and finally an interference filter of the same kind as used on the PDC photons to ensure the same spectral properties, the unconverted light from the Ti:Sa laser was coupled into a single mode fibre and sent to the gate as the third photon for out three qubit gate. The experimental setup is shown in figure 4.2 schematically and a photograph of the setup is provided in figure 4.3. Measurements with fibre-coupled SPCMs confirmed 10^4 to 10^7 photons/s in the weak pulse, depending on the attenuation set by the setting of the HWP. Clearly we achieved the precondition of an average photon

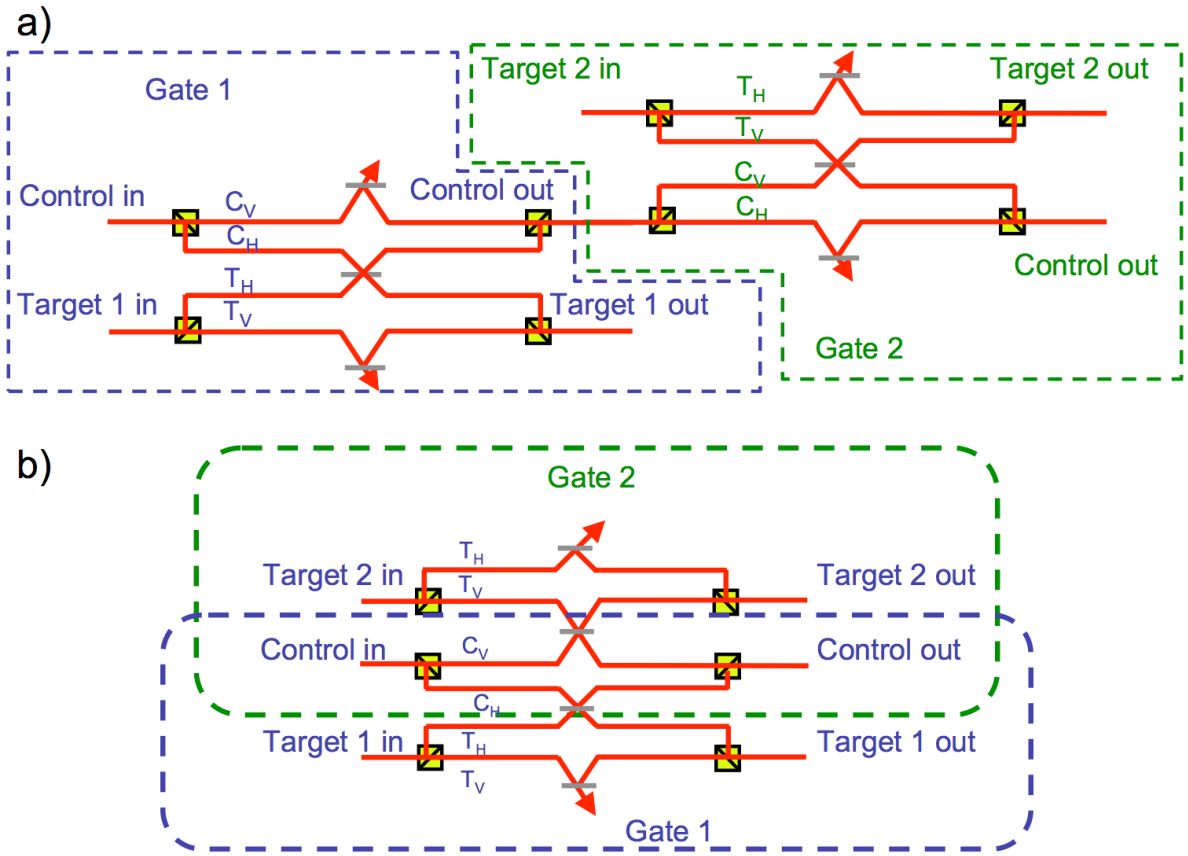


Figure 4.1: Chaining of CZ gates. In the dual rail picture the polarisation encoded qubit gets split across two rails one per logic mode. In a) one naively uses the output of the control qubit of the first gate as the input for the control qubit in the second gate. The success rate of a single CZ gate of this kind is 1/9 leading to a total success probability for chained gates of $(1/9)^N$, where N is the number of implemented gates. b) In the scheme suggested by Ralph [60] a significant improvement is achieved by simultaneously interacting multiple qubits on the different logic rails. As this makes the dump port redundant for all but the two outer most qubits, the success probability becomes $\propto (1/3)^N$. This scheme can be readily expanded to an arbitrary qubit number.

number of less than 1 photon per pulse given our 82MHz repetition rate. While we managed to find non-classical interference between the weak coherent state and the PDC photons on the second PPBS (HOM-dip shown in figure 4.4), the signal was very noisy (See section 4.2.3 for a discussion why the noise increased) and the reconstructed states were very mixed and far from ideal.

At first the lack of a high visibility was believed to be due to some poorly understood property of the source of the photons. As one photon was generated in a non-linear crystal via parametric down-conversion, while the other photon was emitted by Ti:Sa crystal during stimulated emission and subsequently interacted with many optics, it was thought to be very possible that distinguishing information in some degree of freedom was imprinted through these differences. Therefore a second pass of the laser pulse through the down-conversion

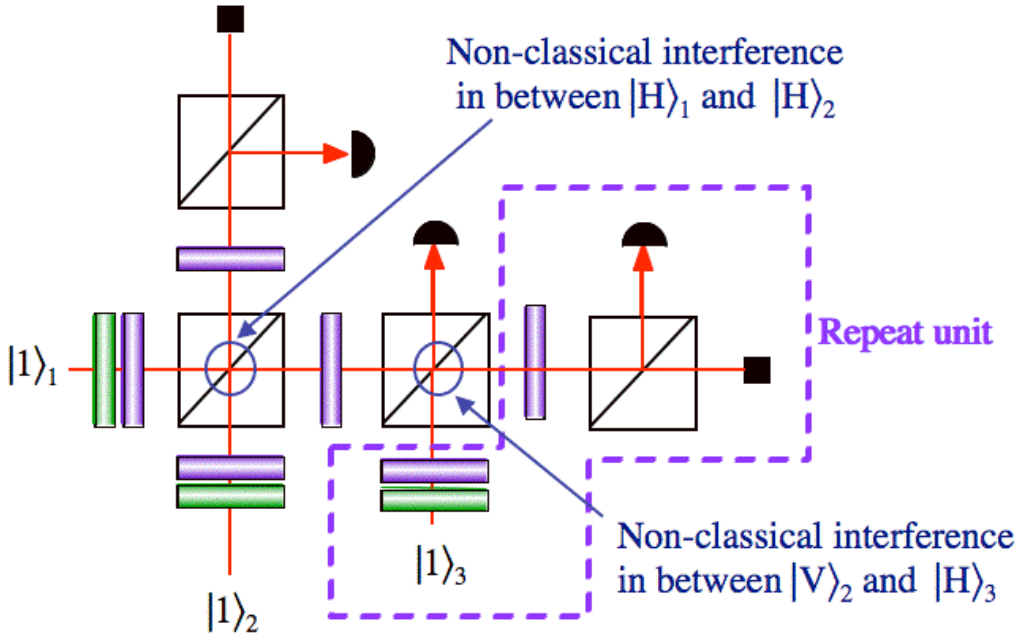


FIGURE 4.2: Schematic depiction of the experimental setup of the three qubit CSign gate following the scheme suggested by Ralph [60], we use the dump PPBS for a further interaction. This can be extended indefinitely by adding the elements in the "Repeat unit" to the last PPBS in either arm. Half-waveplates (purple blocks) between the PPBS switch the logic ensuring that a) each logic mode experiences the same attenuation and that each input mode can only interact with its next neighbours. The success probability is increased by a factor of 3 compared to chaining of independent gates.

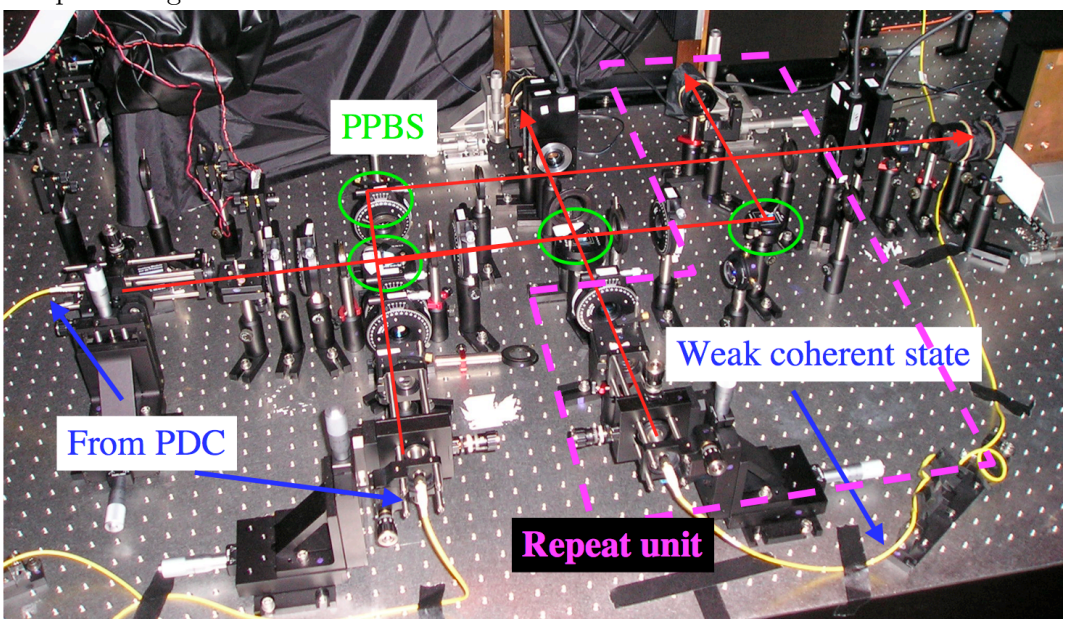


FIGURE 4.3: Experimental realisation of the 3 qubit gate. Again the added "Repeat unit" is highlighted. The basic gate is the same as used in the CSign-gate of the chapter 3 before the upgrade to single mode fibre collection.

crystal was set up and down converted photons in the backward direction were collected as described in section 2.2.2. But even after replacing the weak coherent state input with a down-conversion photon, and continuing to collect threefold coincidences, the quality of the results did not improve. Subsequently the attempt of implementing a three qubit gate was deferred as it became obvious that an investigation of the source of the degradation of the gate performance was necessary to allow further progress with this kind of gate. The PPBS-type CZ gate had been successfully implemented not only in our experiment of chapter 3, but simultaneously by two further groups [54, 55]. It was thus known, that these gates are capable of very high quality performance. The main difference we faced was trying to interact photons generated independently from each other. We hence set out to investigate the performance of a single controlled sign gate with photons generated in independent down-conversion events. As these are effectively independent photons, this experiment was dubbed the Independent Photon Gate, or IPG for short.

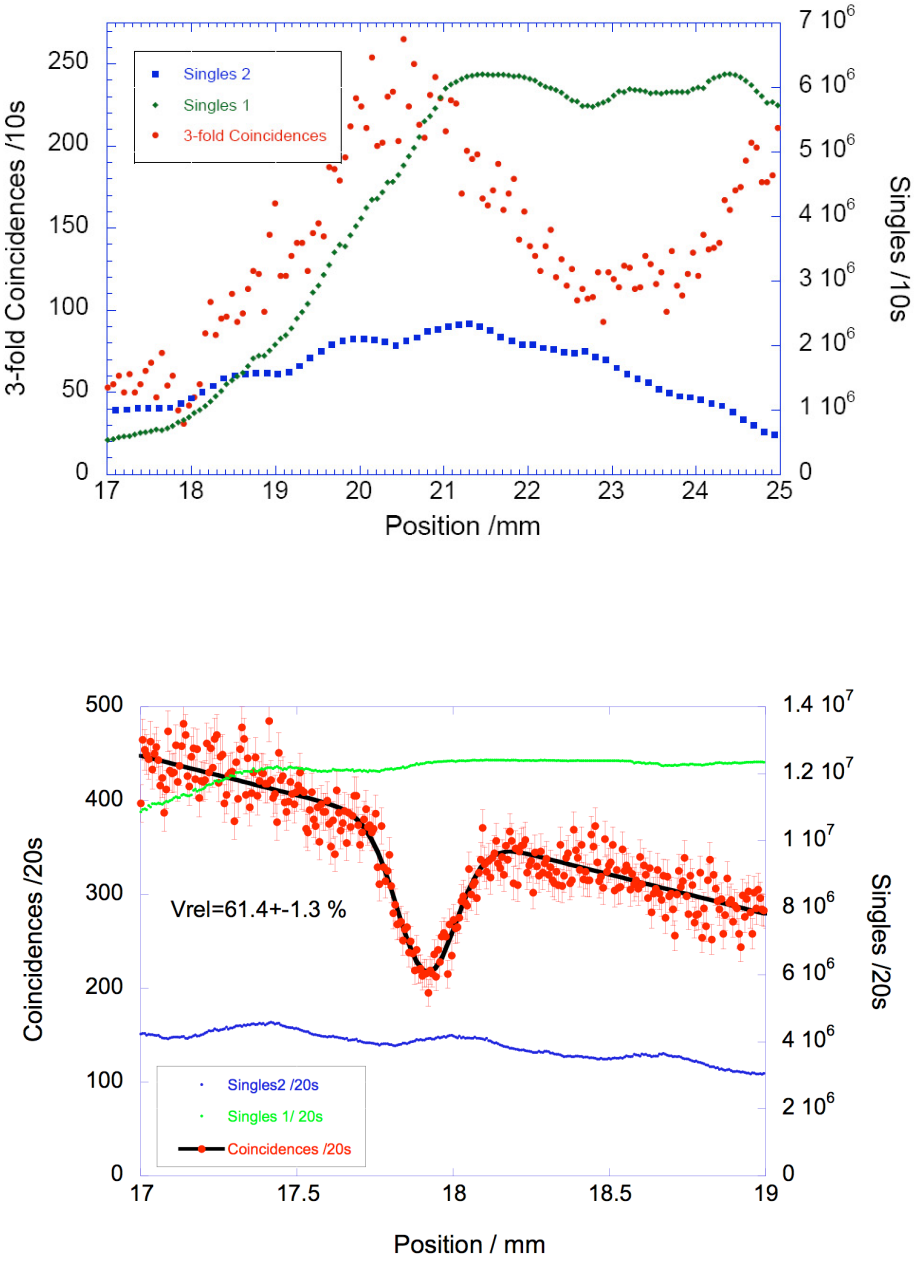


FIGURE 4.4: Finding a needle in the Haystack: (Top) Graph of the original scan finding the HOM-interference between one photon generated by PDC and a weak coherent state. This graph is to demonstrate the significant difficulty of finding this interference feature in front of large background variations. The HOM-dip is the small drop at the beginning of the graph at approximately 18mm. Singles 1 is the coherent state, while singles 2 is the down converted photon. The delay of the coherent state is scanned. The coupling efficiency of the scanned input to both detectors varies significantly during the scan. This is due to the non-perfect alignment of the translation stages with the beam path and gives rise to the large change in count-rates. The correlation between total singles and expected rate of coincidences is also varying due to this effect, giving a non-trivial relationship between the observed singles count-rates and the coincidence rate, leading to the drop in coincidences around the 21 to 24 mm region while the singles rates do not drop significantly in this regime. Error-bars for the singles are smaller than the symbol size. For clarity of the graph, only every 20th measurement point is displayed and the error bars for the coincidence signal have been omitted. (Bottom) HOM-Interference between one photon generated by PDC and a weak coherent state after optimisation of the alignment and scanning over a much shorter range, thus reducing the drift. The signal is fitted with a Gaussian + linear function to compensate for the sloping of the coincidence signal due to the altering coupling efficiency of the scanned weak coherent state.

4.2 The Independent Photon Gate

Investigating the action of a quantum gate with independent photons is significantly more important than it might seem at first glance: a full scale quantum computer will require thousands of gates and thus thousands of individual qubits, here photons. Individual single photon sources are currently being developed [18–20], but suffer from a variety of undesired effects, such as low success probabilities, changes in spectral characteristics or jitter in the timing of the photon creation to name only a few of the problems. They are currently not at a level which would allow their implementation into such multi-qubit gates. Therefore all implementations use the current gold-standard of creating single photons via parametric down-conversion (PDC), a process in which one mother photon spontaneously decays into two correlated daughter photons. The draw back of this mechanism is the extremely low probability to create a single pair of photons and its even lower probability to create multiple pairs, coupled with an increase in relative background from the next highest emission order when the intensities are increased. Thus PDC allows the principal study of required elements and gates, but is rendered unsuitable for the implementation of many concatenated gates as needed for a quantum computer.

We explored the consequences of moving from dependent to independent photons in optical quantum computation. Moving to independent sources will most likely mean to depart from the correlations that down-converted photons share and the eased requirements to ensure indistinguishability[1]. In fact independent sources have been used to demonstrate non-classical interference, and found to perform worse than a pair of dependent photons, the difference being attributed to higher-order photon terms and spectral mismatch [63] and timing and spectral mismatches [64]. These are striking results, as non-classical interference lies at the heart of optical quantum computation. Indeed, entangling gates using independent downconversion sources achieved entangled-output state fidelities up to 78% [58] and 79% of ideal [65], worse than the dependent photon counterparts, with fidelities up to 87% [56].

The gate we used is effectively the same two qubit gate as described in detail in chapter 3, the main alteration being, that we now use single heralded photons from different down-conversion events as inputs into our gate. To generate them, we use the four-photon version of the V2-source as described in section 2.2.3. The emitted PDC photons were coupled into single mode fibres, collecting about 35kHz (30kHz) coincidences in the forward (backward) direction. One fibre of each direction was directly fed into a silicon avalanche photon detector (SAPD) while the other fibre injects its photon into the gate as shown in figure 4.5b). Hence the photons used to interact in the gate come from to separate down-conversion event and thus do not share the correlations which exist in between the two paired photons of a single event. In this context the photons can be thought of as independent. However they do share the common laser pulse generating them and thus have a fixed time delay between each other and also share the polarisation reference frame through the polarisation of creating laser pulse. These however are correlations that might well carry across to novel sources through i.e, reference beams and electronic trigger signals.

Furthermore to emulate the behaviour of different future photon sources more accurately,

[1] Namely the spectral overlap in the degenerate case, polarisation correlation, the fixed timing relation, and even the spatial correlation defining where the paired photons can be found.

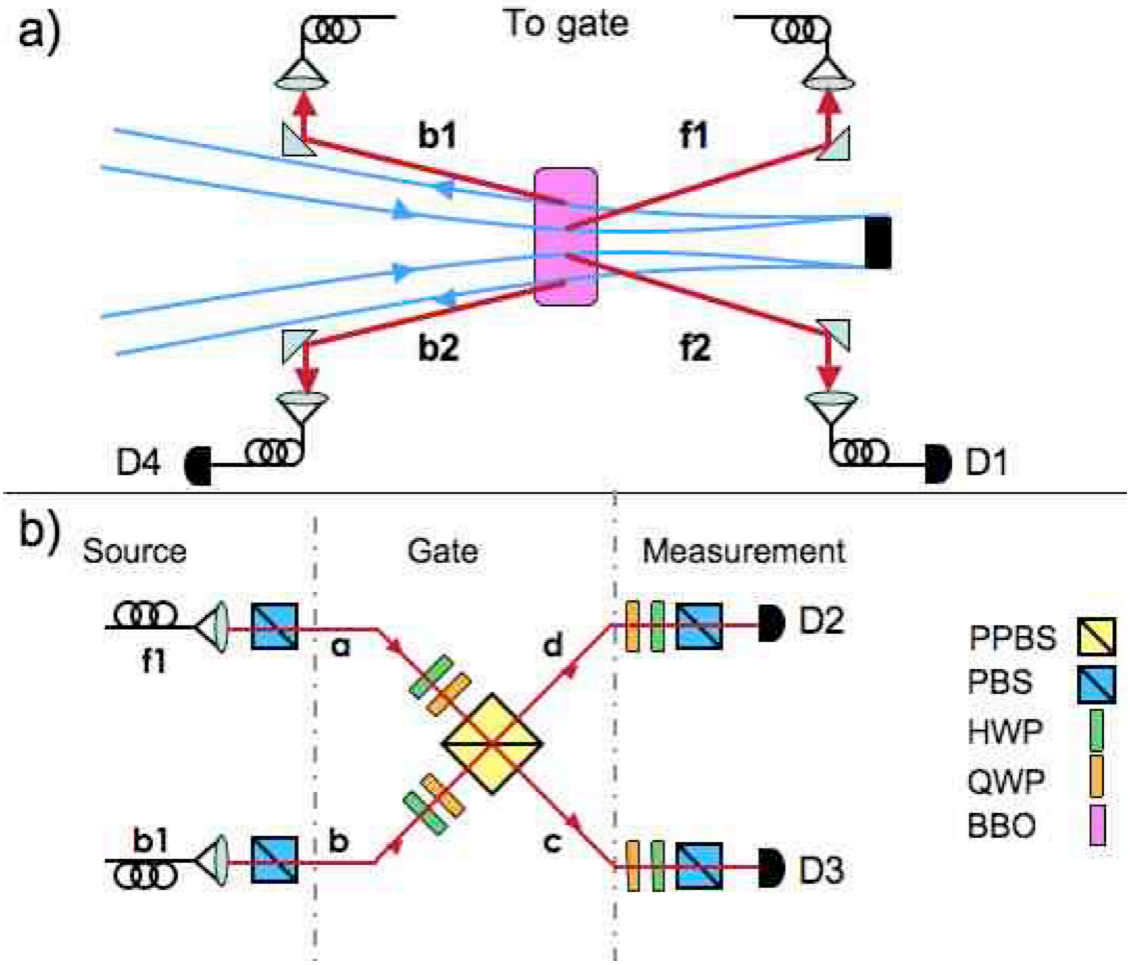


FIGURE 4.5: a) The pump is reflected after passing through the down-conversion BBO-crystal and travels through it a second time in the opposite direction. Therefore pairs can be emitted either in the forward or backward direction or in both as required for our gate. One photon per pair is detected immediately at D1 and D4 to herald the photons that travel on to the gate. As the focus of the pump beam lies before the retro-reflecting mirror, the emission probability for the forward pass is higher than the backward pass. b) schematic of the gate: The conjunction of half and quarter waveplate and polarising beamsplitter allow the controlled input (detection) of any desired state. The partially polarising beamsplitter is ideally perfectly reflective for vertical polarisation, while reflecting 1/3 of the horizontal component.

we altered the source in such a manner, that the waist of the focus for the pump pulse is no longer half way between the forward and backwards pass on the retro-reflecting mirror, but is moved closer towards the forward pass, as shown in figure 4.5a), simulating independent sources of unequal emission probabilities.

4.2.1 Non-classical interference of independent photons

We measured the non-classical interference for the potentially interfering $|H, H\rangle$ input state and achieved a visibility of 76.8%±1.2% as shown in figure 4.6. As we are using beamsplitters

with a reflectivity of $\eta_H = 0.35$, the maximum visibility V_{max} that could be achieved is limited to 82%. We hence use the relative visibility $V_{rel} = \frac{V}{V_{max}}$, which allows easy comparison to those experiments where a 50:50 beamsplitter($V_{max} = 100\%$) was employed. We achieved a $V_{rel} = 93.7\% \pm 1.4\%$, which is the highest relative interference visibility for independent photons reported to date. While we used spatial filtering with single mode fibres after the gate, the previous best mark of $90.8 \pm 1.7\%$ [61], was achieved with a fused fibre-beamsplitter, effectively removing any spatial mode matching imperfections. It is hence specially noteworthy that we manage to surpass this mark and indicates the quality of our setup and again the power of the spatial filtering with the single mode fibres.

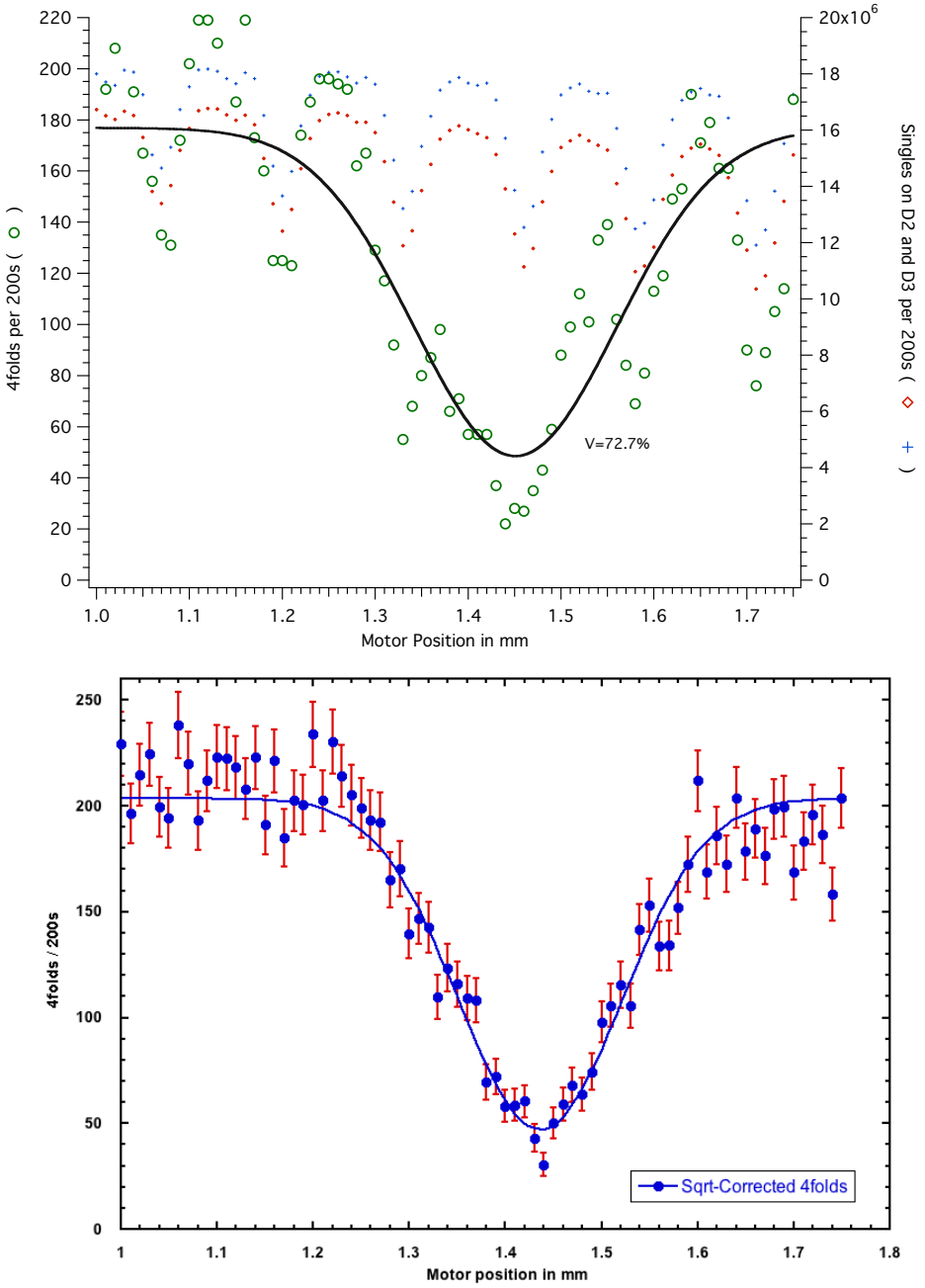


FIGURE 4.6: Hong-Ou-Mandel Interference between independent heralded photons. As the photons interfere on a 0.35:0.65 beamsplitter the maximum visibility is limited to 82%. (Top) Due to thermal oscillations the coupling efficiency varied drastically during the scan causing the sharp drop in count rates. (Bottom) This effect can however be undone by normalising the measured 4 fold rate to the singles rates.The four-fold count rate is divided by the square root of the product of the contributing singles rates and has then be rescaled to actual count rate level. This correction does not alter the visibility, which is found to be 72.7% which is a record high relative visibility of 93.4% for independent photons.

4.2.2 Beating the clock: Iterative (Process) Tomography

Moving from a two photon or one down-conversion event experiment to a multi-pair setup has one significant impact, which is the probability with which such events occur. While we have on the order of 10^4 coincidences/s even after the lossy gates with two photons, this drops to about 1/s when using four photons. Even not registering the fourth photon and thereby evading the loss probability for it, does not significantly improve this rate, but in turn makes the signal significantly more susceptible to noise (See Section 4.2.3 for details). While the obvious solution to this arising problem is to simply integrate for a longer period of time, this gives rise to the revival of the temporal stability issue. While the overcomplete tomography helps with short term fluctuations of i.e. the laser output power through additional normalisation possibilities as discussed earlier, it is not capable of addressing long time scale issues that arise as a more physical manifestation, i.e. the ghosts of thermal drift or simple stress relaxation in any translation stage or any of the optical fibres as these actually alter not the counting statistics, but the quality of the alignment and thus of the non-classical interference. This can not be undone mathematically. One example of such effect can be seen in the HOM-scan shown in figure 4.6. Here both the singles and subsequently the coincidence signals undergo a periodic sharp drop in count rates with sharp recovery. As each point in the graph corresponds to 200s integration time, one can derive that the effect has a period of 40 minutes. Thus in the rapid two-photon tomography with a total active time of approximately 100 minutes such an effect would have been barely visible. For the four-photon coincidence circuits there would be a significant effect on every 4th measurement. For the Hong-Ou-Mandel scan this effect can be undone by normalising to the single count rates as discussed in the figure caption. For tomography data such a mathematical compensation is not feasible.

Nevertheless these effects can be countered with a relatively simple approach. Instead of measuring each output state for a long time, i.e. 10 minutes/point in one iteration, we use our automated routine, to continuously cycle through all measurements and collect data for only a short period ($<$ 1min.) and simply repeat this multiple times, until each measurement had again been integrated for the desired total duration of 10min. The benefit of this iterative tomography is that short term drifts can be compensated for via normalisation, and the effect of long term drifts is damped as it is spread equally over all output states.

At a later stage, when additionally to the already automated analyses the input state generation was also automated, the iterative tomography was further extended from state to process tomography, where all required settings for one process tomography would be repeated iteratively with a short duration each time.

4.2.3 Why *not* detecting every photon hurts

It has been mentioned earlier that the attempt to utilise an attenuated laser beam as a photon source degraded the gate performance, as did the detection of only three (or even two) photons in the independent photon gate. The cause of this might not be immediately clear, but now in conjunction with understanding the error modes of the gate should become more obvious. Neither of these methods alter the gate architecture, hence the alignment is all the same. All use the same lossy detectors, so the solution lies in the source. As we have

discussed in section 4.4.3 there is a non-zero probability of generating multiple photons in one spatio-temporal mode this probability is equal to that of generating two pairs of photons in different spatio temporal modes. If one of these modes is then injected into a gate where there is a non-zero probability of the photons reaching the two output modes, even thought they are injected in a single input mode, than this can lead to a coincidence count. The state of the photons however will not be governed by the gate dynamics as the photons never interfered or where even influenced by the state preparation in the second input. The obvious solution is to detect not only the gate output modes but also the trigger photons, i.e. the paired photons that are not injected into the gate. These will then herald that a photon was actually created in each input mode for the gate. Again detecting only one of the trigger photons opens one up to the same failure mode, however limited to only one PDC direction as the multi-pair event had to occur in the direction where the trigger was detected. As the trigger photons never overlap or interact, they can not be replaced or mistaken for a photon from any other source.

For the case where an attenuated laser beam was used that had on average less than one photon in its mode, the same problem occurs, where such a coherent state always has a non-zero probability of containing more than one photon and additionally lacks the paired photon production that allows one to trigger of it. For experiments with independently generated photons it is hence imperative to detect all photons that one wants to create (not just all that one wants to utilise) to ensure highest gate fidelity.

4.2.4 Prebiased state generation: The making of the 'ishes

In this experiment we pre-bias the input states. into the gate to obtain higher count rates as in the implementation described in chapter 3. We do not flip the polarisation after the interaction and employ dump PPBSs to balance the probabilities for horizontal and vertical components of superposition states in the H-V-bases. Thus the partial-polariser unbalances input states, e.g. a single diagonally-polarised photon input in mode $\mathbf{a}$, $(\mathbf{a}_H^\dagger+\mathbf{a}_V^\dagger)/\sqrt{2}$, becomes in mode c, $(\mathbf{c}_H^\dagger+\sqrt{3}\,\mathbf{c}_V^\dagger)/2$. To balance the state, we employ pre-biasing [35, 55]. While the former requires no knowledge of the input state, it lowers the success probability to 1/9 compared with 1/3 for the state dependent pre-biasing. While pre-biasing is an acceptable procedure for characterising these small scale gates and allow us to obtain a much increased count rate, it is unsuitable for large scale implementation with concatenated gates. For example, a diagonally polarised output state in mode c can be achieved by sending $(\sqrt{3}\,\mathbf{a}_H^\dagger+\mathbf{a}_V^\dagger)/2$ in mode $\mathbf{a}$ (mode labels as in figure 4.13). These pre-biased states were named 'ishes, as in Dish and Lish[2]. In order to generate such pre-biased states, some non-standard waveplate settings had to be found. A HWP set to $\pm 15^\circ$ will generate the desired Aish or Dish states from a pure H input. As in our setup the half-waveplates were followed by a quarter-waveplate (QWP), we also needed to rotated the QWP by $\pm 30^\circ$ in order to align its optic axis with the polarisation vector in the Bloch-sphere and thus have the QWP not affect the state. In order to create the Lish or Rish states the same procedure was used for the half waveplate, but the quarter waveplate was left at the 0° position.

[2]This labelling is analogous to the word creations such as largish which mean kind of large. A Dish state is kind of diagonally polarised.

4.2.5 State Tomographies of the IPG

The measurement process is identical to that used in the dependent two-photon gate described in chapter 3. The process tomography was subdivided in the 16 state tomographies and again we observed fixed rotations of the superposition states, which were corrected for numerically after the completion of the experiment. The gate design in the dependent case balanced the probabilities of the horizontal and vertical component of superposition states by flipping the logic polarisations with a half waveplate and subsequently propagating the photons through a further PPBS. This resulted in the flipped output states to what one would naively expect as seen in Figures 3.3 to 3.10. As we here pre-bias our input states, this flipping of the logic populations is no longer necessary and the obtained output states are as originally expected.

The record breaking high visibility of our non-classical interference easily leads to the expectation of a gate performance similar to that of the dependent CSign gate, albeit with a slightly lower fidelity as the relative visibility was not quite as good. However, while the tangle of states in the dependent gate ranged in the mid sixties, only one state for the independent gate managed to surpass the 50% mark and all other measures were significantly lower as well. State fidelities range from the high nineties (VV) to only 68% for LH, with the average of the state fidelities being 81%. The reconstructed states of the individual state tomographies are shown in figures 4.7-4.10, and the results for state fidelity, purity tangle and linear entropy are summarised in table 4.1.

Input State	Purity	Linear Entropy	Tangle	Fidelity with ideal
HH	0.954	0.062	0.015	0.95
HV	0.847	0.203	0.016	0.88
HD	0.710	0.386	0.012	0.75
HL	0.656	0.458	0.038	0.70
VH	0.878	0.163	0.11	0.88
VV	0.927	0.098	0	0.98
VD	0.876	0.166	0.018	0.79
VL	0.924	0.101	0.014	0.90
DH	0.621	0.506	0	0.76
DV	0.897	0.138	0.008	0.88
DD	0.667	0.444	0.478	0.74
DL	0.720	0.374	0.523	0.78
LH	0.606	0.525	0	0.68
LV	0.940	0.081	0.020	0.94
LD	0.704	0.395	0.471	0.71
LL	0.727	0.365	0.595	0.72

Table 4.1: Summary of the results of the state tomography for the CZ gate between independent photons. The general output state quality is worse than when operating the same gate with dependent photons, as shown in table 3.2.

The high fidelities and low linear entropy values for the states with two equal and pure logic inputs (HH, VV), as well as the high fidelity of any state that contains a vertical input

are noteworthy. The relatively high linear entropy values and low fidelities of the logically pure HV and VH states are also surprising. While it is easy to understand the better-than-average results for states that contain a vertically polarised state on the basis that vertically polarised photons do not under go any interaction and thus are seemingly unaffected by the gate, the argument becomes some what stressed when trying to explain why the gate performs significantly worse when using the HV and VH inputs, which not only contain a vertically polarised photon, but are still logically pure. As we will see these degradations arise from a plain violation of one of the fundamental assumptions of the gates relying on non-classical interference: single photon inputs. This and other noise effects will be discussed in detail in section 4.4.

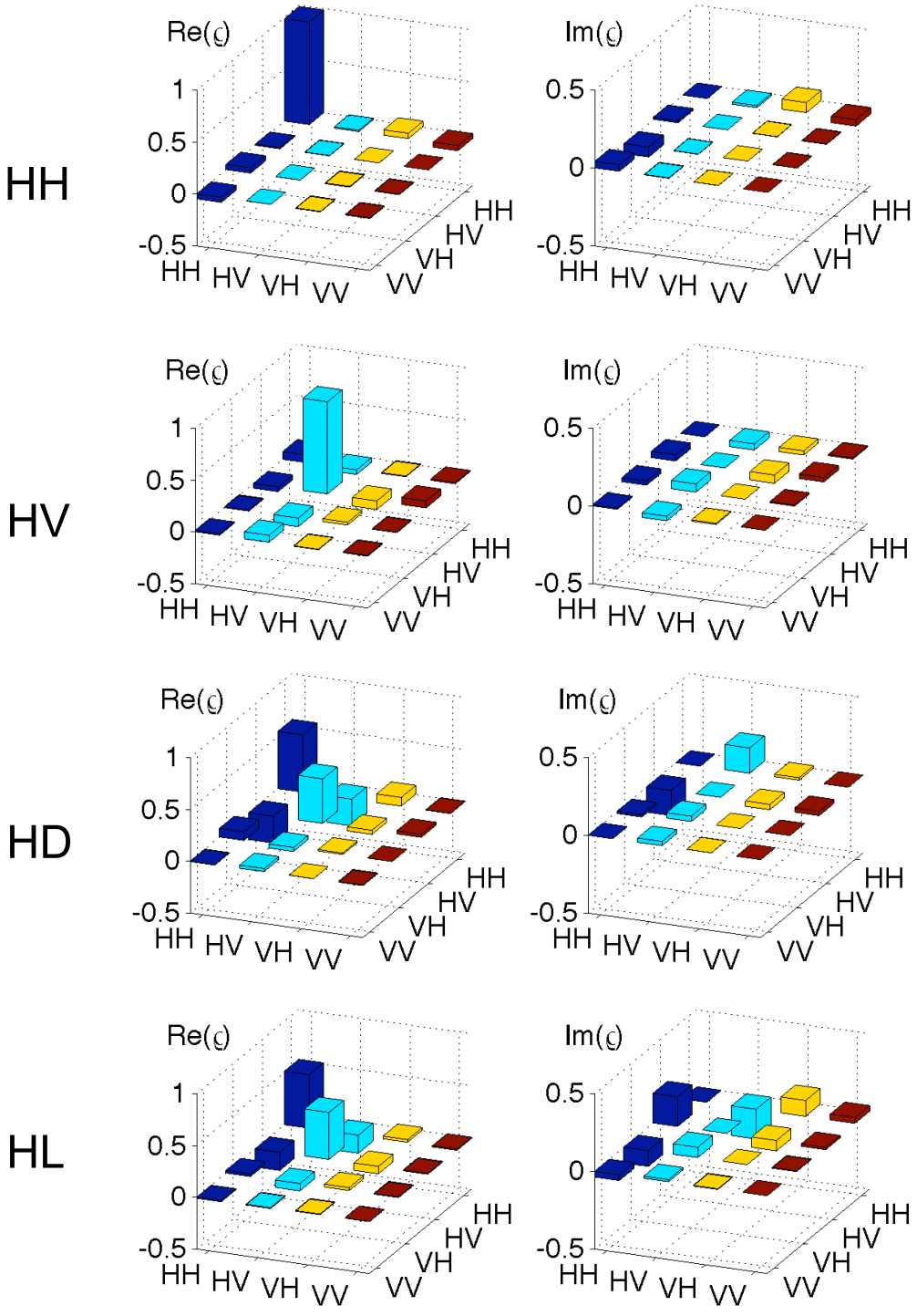


Figure 4.7: Density matrices derived from the state tomographies of the independent CZ gate for the input states HH, HV, HD, HL. The rotations of the PPBS have been corrected for, by finding the optimal single qubit rotation that gives the highest average fidelity for all input states with the ideal output states. As this gate also uses pre-biasing of input states to balance the output populations, the output state has not been flipped as was the case for the dependent gates of chapter 3.

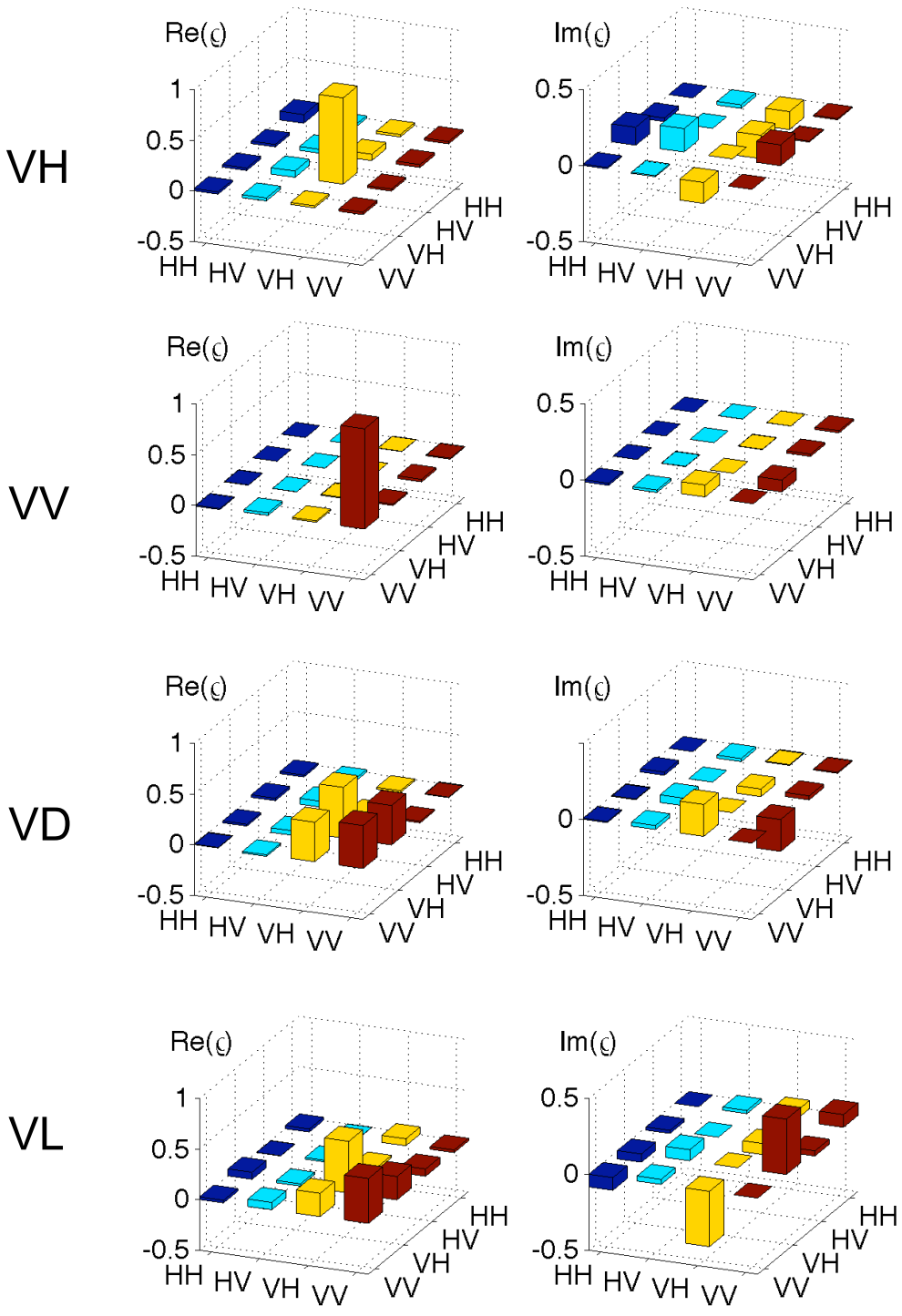


FIGURE 4.8: Density matrices derived from the state tomographies of the independent CZ gate for the input states VH, VV, VD, VL. The rotations of the PPBS have been corrected for, by finding the optimal single qubit rotation that gives the highest average fidelity for all input states with the ideal output states. As this gate also uses pre-biasing of input states to balance the output populations, the output state has not been flipped as was the case for the dependent gates of chapter 3.

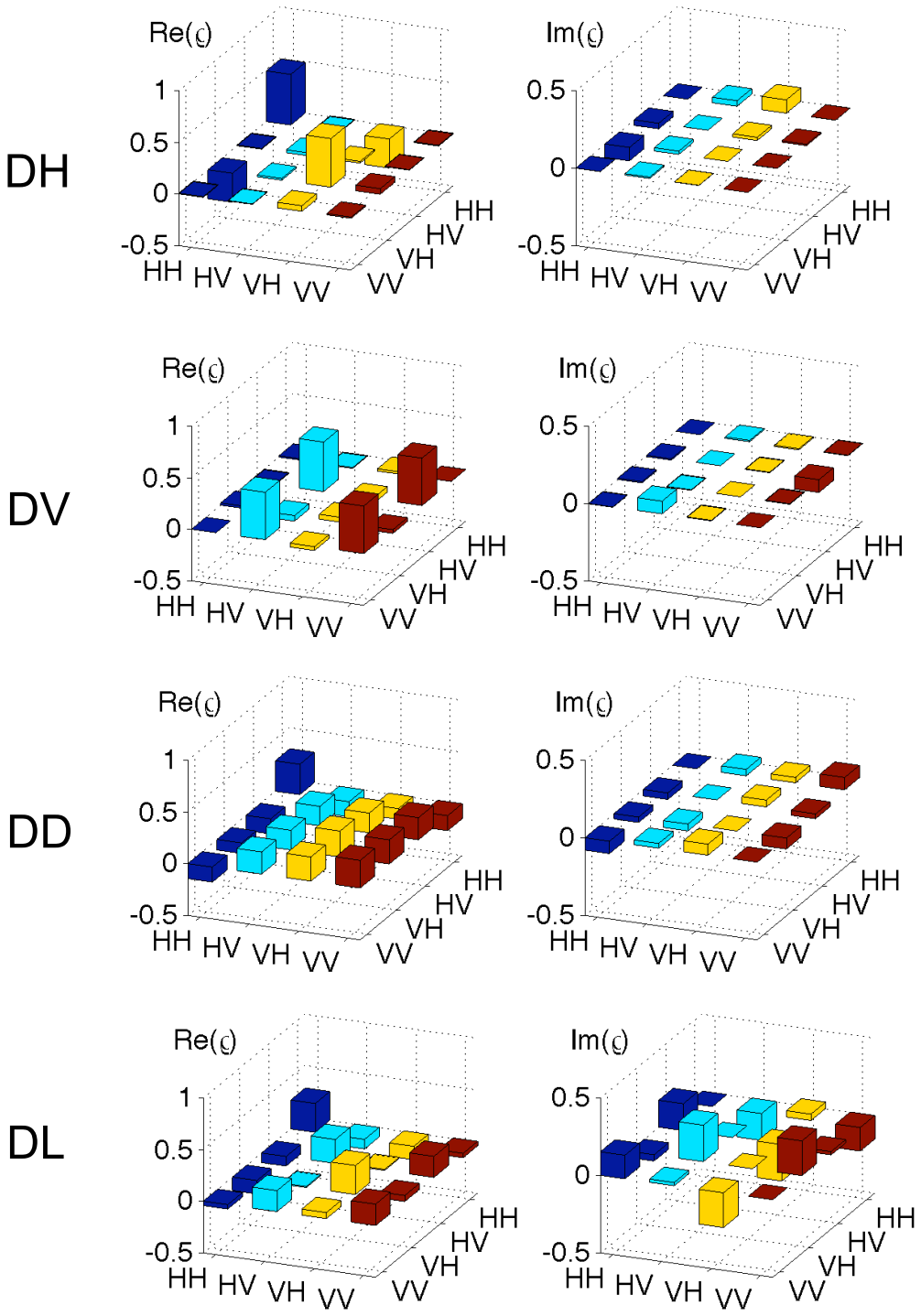


Figure 4.9: Density matrices derived from the state tomographies of the independent CZ gate for the input states DH, DV, DD, DL. The rotations of the PPBS have been corrected for, by finding the optimal single qubit rotation that gives the highest average fidelity for all input states with the ideal output states. As this gate also uses pre-biasing of input states to balance the output populations, the output state has not been flipped as was the case for the dependent gates of chapter 3.

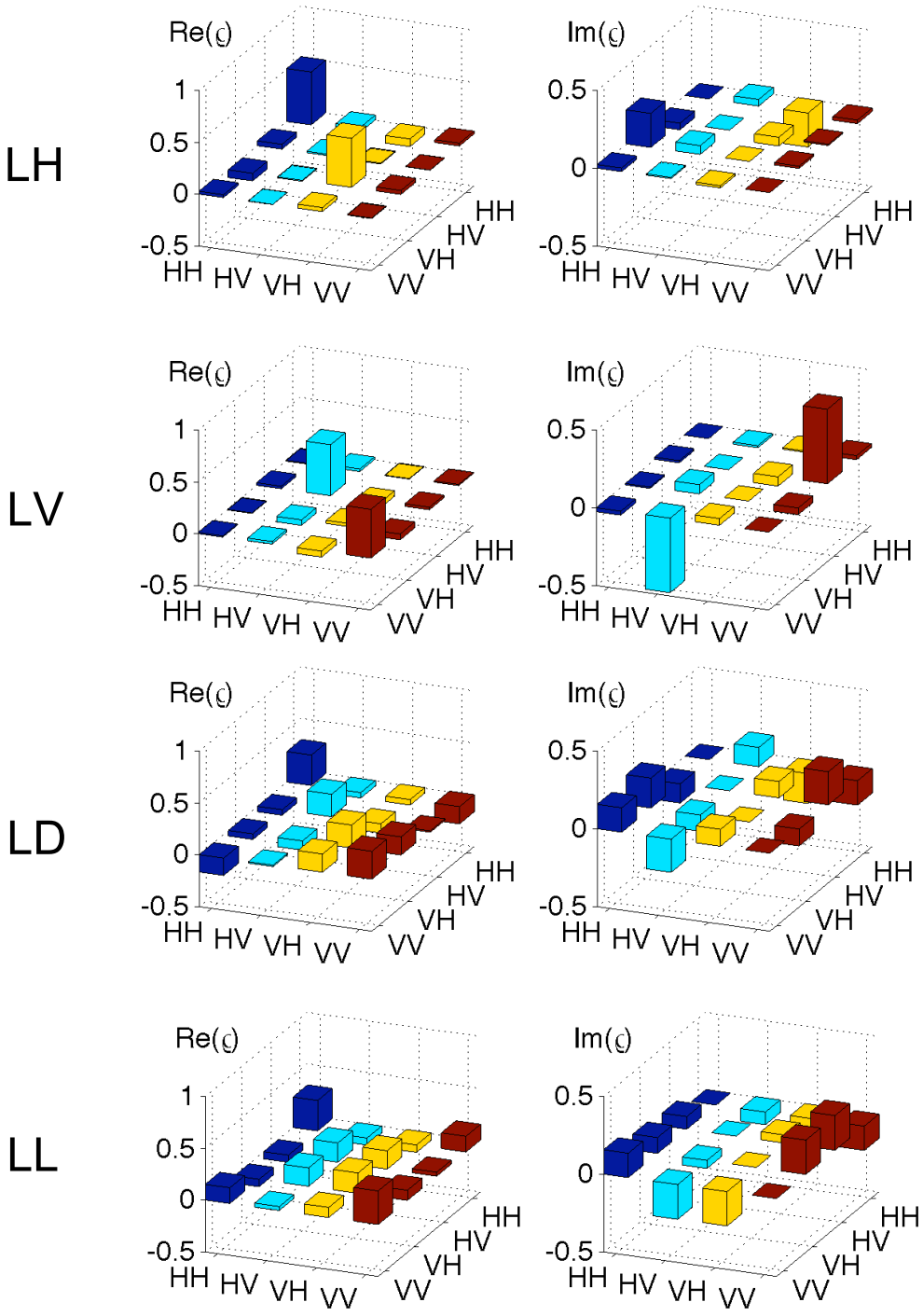


FIGURE 4.10: Density matrices derived from the state tomographies of the independent CZ gate for the input states LH, LV, LD, LL. The rotations of the PPBS have been corrected for, by finding the optimal single qubit rotation that gives the highest average fidelity for all input states with the ideal output states. As this gate also uses pre-biasing of input states to balance the output populations, the output state has not been flipped as was the case for the dependent gates of chapter 3.

4.2.6 Process Tomography of the IPG

Using the measurements for the process characterisation of the IPG and reconstructing the χ matrix for the process gives us the first full analysis of a two-qubit entangling gate performed with independently generated photons. Due to the pre-biasing of the gate, certain input states have higher signal rates leading to different integration times for the individual state tomographies to achieve the same counting statistics. However due to technical failure and environmental impact[3] the integration time was not adequately adjusted for all states. Nevertheless, the imbalance in detection efficiencies can of course be accounted for mathematically by adequately weighting of the individual counts. It was found however, that the reconstructed process had the same fidelities within the error irrespective of whether this correction was applied or not. Hence the here presented data does not contain the readjusted weighting of the individual state tomography data sets. The ideal process is shown in figure 4.11, while the real and imaginary components of the reconstructed chi matrix for the experimentally implemented gate are shown in figure 4.12. We find a process fidelity of $78.2 \pm 1.5\%$, staggering 11% worse than for the dependent gate. The average gate fidelity is found to be $82.5 \pm 1.5\%$ As the fidelity is known to be a relatively forgiving measure, the steep drop in comparison to the equivalent gate with dependent photons is thus most surprising since the achieved relative visibility for the Hong-Ou-Mandel interference was only on the order of 5% worse. As the HOM-Interference only characterises the distinguishability of the interfering photons, this drastic difference in fidelities lead to the question what other effects contribute in what way to the degradation of the gate performance.

[3]The air-conditioning in our lab was found to be faulty and caused large temperature fluctuations. The installation of a replacement system took approximately eight months, by which time the experimental aims of the group had moved on.

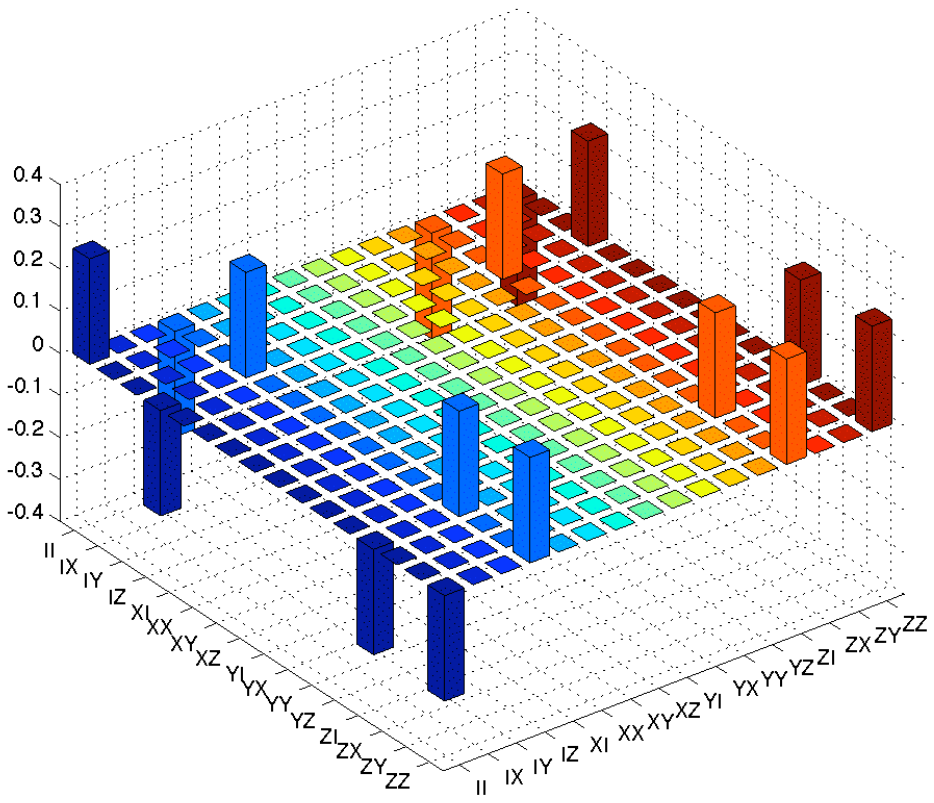


FIGURE 4.11: Process matrix of the ideal CZ operation in the Pauli-basis. The real part of the matrix is shown, the imaginary part is identically 0. The shown matrix here is actually for a CZ gate with an additional bit-flip, i.e. $CZ(X_1 \otimes X_2$. The standard CZ gate is an equal superposition of the II+IZ+ZI−ZZ processes and full coherences between them.

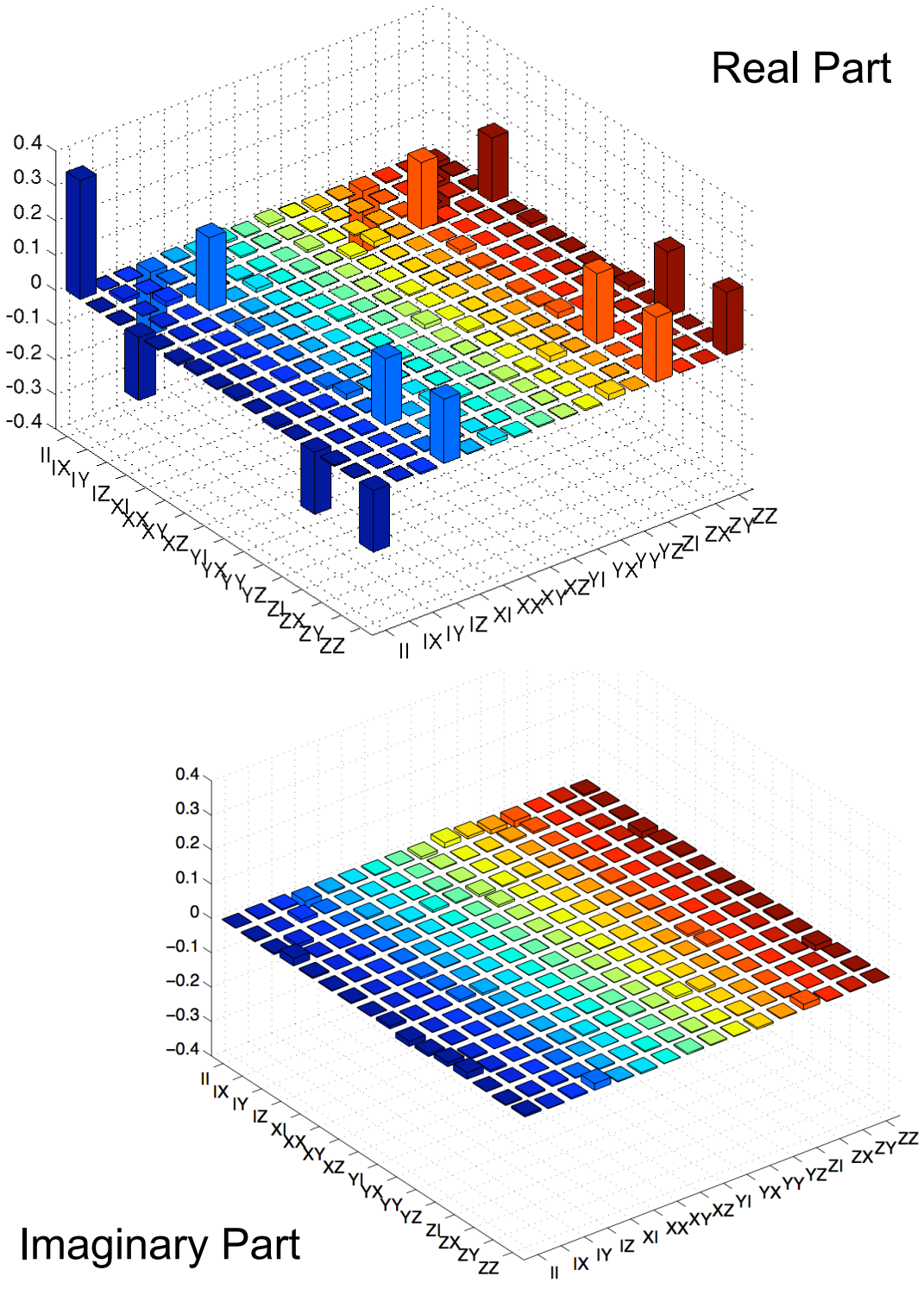


Figure 4.12: Real and imaginary part of the reconstructed experimentally determined χ matrix. While a quick visual inspection seems to indicate good agreement to the ideal case, a closer inspection indicates undesired populations and coherences and lower than desired coherences where desired. After optimisation over all local unitary single qubit rotations, $F_p = 78.2 \pm 1.5\%$.

4.3 Modelling the Independent Photon Gate

In order to get an understanding for the effects that degraded the gate performance in the IPG gate, a complete model of the gate, except for the effects of mode mismatch, was constructed. The model accurately describes the generation of photons through double pass (independent) PDC, the actions of the gate with realistic beamsplitters, photon loss, and last but not least employs the same projective measurements as experimentally employed to analyse the data and subject it to the same density matrix reconstruction as for the

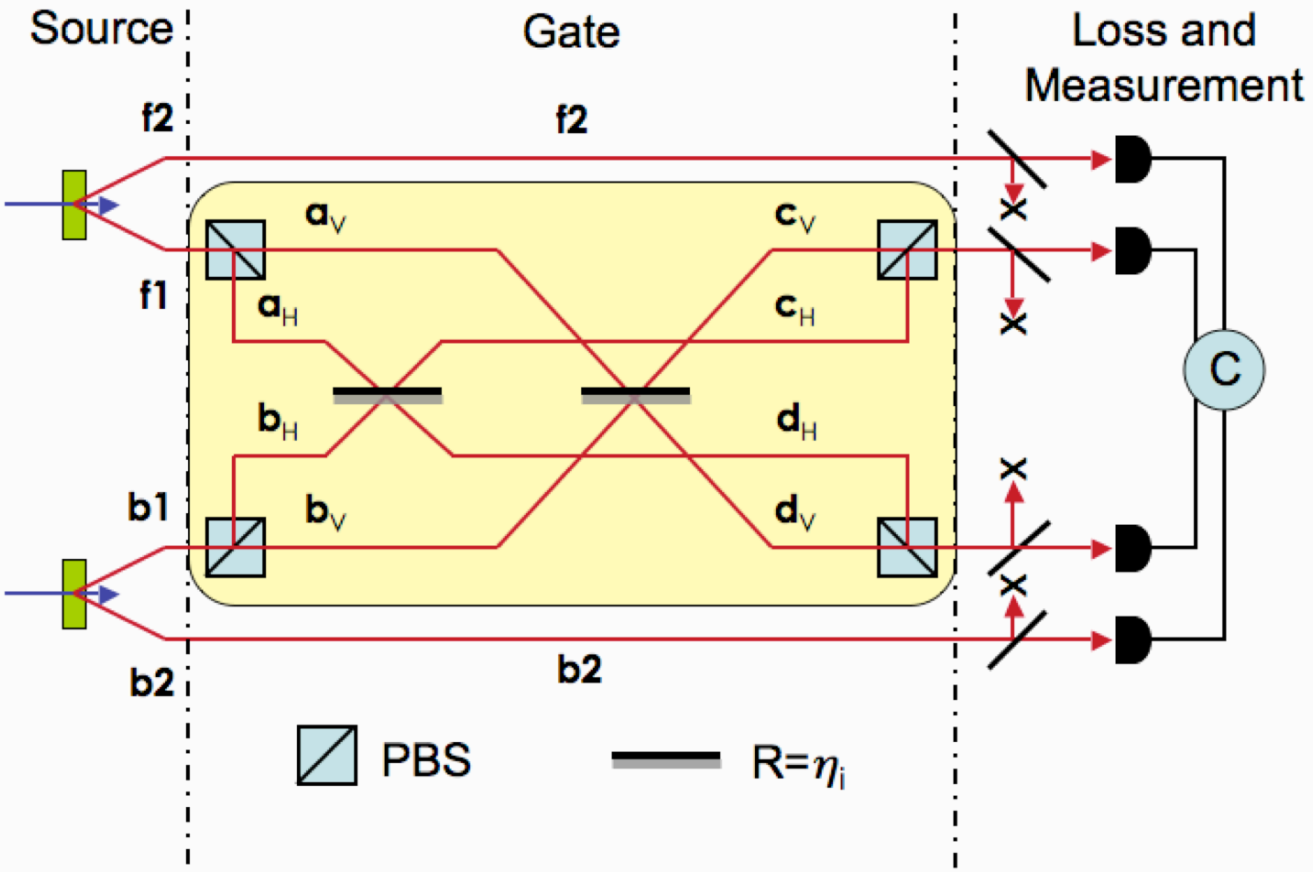


FIGURE 4.13: Schematic of the circuit used to model the independent photon gate. Photon pairs are independently generated into the modes f1 & f2 and b1 & b2 through parametric down conversion. One photon per pair is immediately detected to herald its partner photon, which is injected into the gate. Polarising beamsplitters (PBS) and waveplates allow the generation of any desired input state. The polarisation modes are separated at the PBS and interact separately at beamsplitters of reflectivities η_H and η_V. The separated polarisation modes are then recombined spatially, and a further beamsplitter of reflectivity k_i emulates the effect of photon loss. The detection is preceded by tomographic measurements with a set of quarter and half waveplates and a PBS.

Parametric down-conversion can be described by the evolution of the vacuum state by

$$|\psi(t)\rangle = U_{int}|\psi(0)\rangle = e^{i\mathbf{H}_{int}t/\hbar}|\psi(0)\rangle, \tag{4.1}$$

where if we want to describe two down-converters simultaneously i.e. in the forward and backward direction, the interaction Hamiltonian becomes

$$\mathbf{H}_{int} = A_f \mathbf{f1}^\dagger \mathbf{f2}^\dagger \mathbf{p}_f + A_b \mathbf{b1}^\dagger \mathbf{b2}^\dagger \mathbf{p}_b + H.C. \tag{4.2}$$

where A_b and A_f are the probability amplitudes for the forward and backward creation of a photon pair; $\mathbf{p}_i$ and $\mathbf{f}_i^\dagger$ and $\mathbf{b}_i^\dagger$ are the pump-annihilation and downconversion-creation operators in direction i, respectively; and $H.C.$ is the Hermitean conjugate. Taking the Taylor expansion, and retaining only terms where at least one pair of photons are emitted into f & b (emission into only one will not cause a trigger event and are disregarded), and ignoring pump field depletion, we obtain the source terms,

$$\begin{aligned} U_{int} \approx A_f\, A_b \mathbf{b1}^\dagger \mathbf{b2}^\dagger \mathbf{f1}^\dagger \mathbf{f2}^\dagger + \\ (A_f A_b^2 \mathbf{b1}^{\dagger 2} \mathbf{b2}^{\dagger 2} \mathbf{f1}^\dagger \mathbf{f2}^\dagger + A_f^2 A_b \mathbf{b1}^\dagger \mathbf{b2}^\dagger \mathbf{f1}^{\dagger 2} \mathbf{f2}^{\dagger 2})/2. \end{aligned} \tag{4.3}$$

The first term describes creation of one pair of photons into each the forward and backward modes, whereas the last two terms describe production of 2+1 and 1+2 photon pairs respectively. The contribution from terms higher than these have been found to be negligible and are hence ignored.

We encode logical 0 & 1 in vertical and horizontal polarisations, V & H, respectively. The input modes to the gate, $\mathbf{f1}^\dagger$ and $\mathbf{b1}^\dagger$, are projected with a polarising beamsplitter,

$$\begin{aligned} \mathbf{f1}^\dagger &\rightarrow \alpha\, \mathbf{a}_H^\dagger + \beta\, \mathbf{a}_V^\dagger, \\ \mathbf{b1}^\dagger &\rightarrow \sigma\, \mathbf{b}_H^\dagger + \tau\, \mathbf{b}_V^\dagger, \end{aligned} \tag{4.4}$$

and the action of the controlled-Z gate is described by,

$$\begin{aligned} \mathbf{a}_j^\dagger &\rightarrow -\sqrt{\eta_j}\, \mathbf{c}_j^\dagger + \sqrt{1-\eta_j}\, \mathbf{d}_j^\dagger, \\ \mathbf{b}_j^\dagger &\rightarrow \sqrt{\eta_j}\, \mathbf{d}_j^\dagger + \sqrt{1-\eta_j}\, \mathbf{c}_j^\dagger, \end{aligned} \tag{4.5}$$

where $j{=}H, V$. Ideally, the reflection probabilities are $\eta_H{=}1/3$ and $\eta_V{=}1$, implementing the maximally entangling controlled-sign operation [66, 67]. Photon loss is modelled by additional beamsplitters, with reflectivity k_i. As the entire circuit is linear and all loss mechanisms are indistinguishable, the location of this loss operation is arbitrary assuming that it is polarisation independent: without loss of generality we model it before the detectors. Measurement of both the trigger and gate photons is modelled by ideal projective measurements with non-number-resolving detectors. Thus our model describes the existence and strength of higher order pair emission, deviations in gate beamsplitter reflectivities, and photon loss: all effects observed in our experiment. A quantitative comparison of our model and experiment requires values for the down-conversion amplitudes, A_f, A_b, the beamsplitter reflectivities, η_i, and the losses, k_i. The reflectivities are easily obtained from direct measurement either with a suitable laser or the down-converted photons themselves. The other values need to be derived from specific measurements made using input states designed to extract these quantities.

4.3.1 Deriving the experimental parameters

To derive the values for the down-converision amplitudes, consider the situation where one pair of photons is emitted in both the forward and backward directions. The probability of detecting a fourfold event with measurement settings $\{r, s\}$, where $r, s \in \{H, V, D, A, R, L\}$, is,

$$\vec{P}^{11} = A_f^2 A_b^2 \left(\prod_{i=1}^{4} (1 - k_i) \right) \vec{\gamma}^{11}, \tag{4.6}$$

where the superscript on P refers to the photon number in each gate input mode, a & b; k_i is the probability of photon loss in modes $\{i\}=\{f2, c, d, b2\}$, and $\vec{\gamma}^{11}$ is the vector of overlap probabilities between the gate output and the measurement setting rs, $\vec{\gamma}^{11}=\{\langle rs|\mathbf{U}_{gate}^{\dagger}|\psi_{in}\rangle\}^2$. Without loss of generality we choose $|\psi_{in}\rangle=\mathbf{a}_D^{\dagger}\mathbf{b}_D^{\dagger}|00\rangle$ in the following discussion, so as to equally populate the logical states.

Experimentally it is tempting to obtain $\vec{P}^{11}$ by inputting $|DD\rangle$, and forming a vector of the resulting probabilities, $P^{11}=\{C_{rs}/C_{tot}\}$, where C are counts and C_{tot} is the number of total counts in the appropriate POVM (i.e. $C_{HH}+C_{HV}+C_{VH}+C_{VV}$, $C_{DD}+C_{DA}+C_{AD}+C_{AA}$ ...). However, this does not account for events where 2 pairs of photons are emitted in the one direction and 1 pair in the other—a non-negligible background. These terms cannot be measured directly, though they can be estimated in the following manner. Consider the 2 pair emission in one direction, e.g. forward, and stop the photons from the other direction from entering the gate, e.g block mode b. The probability-vector of detecting a fourfold event now is,

$$\vec{P}^{20} \;=\; \frac{1}{4} A_f^4 A_b^2 \left(\prod_{i=1}^{4} (1 - k_i) \right) (1 + k_{f2})\, \vec{\gamma}^{20}, \tag{4.7}$$

where $\vec{\gamma}^{20}=\{\langle rs|\mathbf{U}_{gate}^{\dagger}|\psi'_{in}\rangle\}^2$ and $|\psi'_{in}\rangle=\mathbf{a}_D^{\dagger}\mathbf{a}_D^{\dagger}\mathbf{b}_D^{\dagger}|00\rangle$. (Swapping the roles of the forward and backward directions gives $\vec{P}^{02}$ & $\vec{\gamma}^{02}$). Experimentally we obtain $\vec{P}^{20}$ & $\vec{P}^{02}$ by blocking in turn one of the gate inputs, while continuing to count four-fold events—since there is only one gate input active at a time, and both gate detectors fire, two photons must have been injected in the same input. In the case of perfect detection efficiency, the total number of events where two-forward and one-backward pairs are created is $N^{20}=\vec{C}^{20}\vec{\gamma}^{20}$. This of course is the same whether mode b is blocked or not, i.e. $N^{20}=N^{21}$ and

$$\vec{C}^{20}\vec{\gamma}^{20} \;=\; \vec{C}^{21}\vec{\gamma}^{21}. \tag{4.8}$$

From the ratio of eqns 4.7 & 4.6 the forward amplitude is,

$$A_f^2 \;=\; \frac{1}{1 + k_{f2}} \sum_{r=1}^{4} \sum_{s=1}^{4} \frac{P_{rs}^{20} \gamma_{rs}^{11}}{P_{rs}^{11} \gamma_{rs}^{20}}. \tag{4.9}$$

Remembering that P_{rs}=C_{rs}/C_{tot}, this becomes,

$$\begin{aligned} A_f^2 &= \frac{1}{1+k_{f2}} \sum_{r=1}^{4} \sum_{s=1}^{4} \frac{C_{rs}^{20}\gamma_{rs}^{11}}{C_{rs}^{11}\gamma_{rs}^{20}} \\ &= \frac{1}{1+k_{f2}} \sum_{r=1}^{4} \sum_{s=1}^{4} \frac{C_{rs}^{20}\gamma_{rs}^{11}}{(C_{rs}'^{11} - C_{rs}^{21} - C_{rs}^{12})\gamma_{rs}^{20}}, \end{aligned} \tag{4.10}$$

where C'^{11} is the measured number of four-fold events, C'^{11}=C^{11}+C^{21}+C^{12} and, from equality 4.8, C_{rs}^{21}=$C_{rs}^{20}\gamma_{rs}^{20}/\gamma_{rs}^{21}$ and similarly for C^{12}. (Swapping the forward and backward roles in the above argument yields A_b). From our measurements we determined A_f=0.137 and A_b=0.208 in the no-loss limit, k_i=0. Note that in the high loss limit, $k_i \to 1$, our estimate of the down-conversion amplitudes A_i will *decrease* by a factor of $\sqrt{2}$. This somewhat counter-intutitive result highlights the critical role of loss in the presence of higher-order photon terms: the combination causes errors, in this case an overestimation of the downconversion probability.

We estimated the loss probabilities of our experiment using the following method. We input a pair of vertically-polarised photons, which ideally both reflect from the PPBS, and measure with the analyser in the VV setting. We measured the singles rate of each detector, S_i and the two-fold coincidences, C_{12} & C_{34}, caused respectively by pairs generated in the forward and backward directions. Accounting for background singles counts, B, and coincidence accidental counts, Acc, the loss in mode i is,

$$k_i = 1 - \frac{C_{ij} - Acc_{ij}}{S_j - B_j} \tag{4.11}$$

where $i, j \in \{1, 2\}$ or $\{3, 4\}$. We obtained, k_{f2}=0.904, k_c=0.953, k_d=0.970, and k_{b2}=0.911. Clearly we are in a high-loss regime: the downconversion amplitudes become A_f=0.116 and A_b=0.177.

4.4 Learning from the model: Signatures of the errors

Having successfully determined all input values for the model, we can extract the same kind of results from the model as we obtained from the experiment. By reconstructing the individual states as predicted by the model we can not only compare them to the experimental values, but as the model gives us the option to vary any parameter, we can simulate every individual error source or choose to turn it off, by replacing the experimentally obtained value with the respective ideal value. A summary of all values, ideal and experimentally determined, is given in Table 4.2.

By turning off all error sources bar one, we can learn the individual signatures of specific errors. One of the most instructive cases is the HV input to the gate. While it neither seeks to create entanglement, nor does it contain a superposition state, it still has a population of both logic modes. In principle the expected output state is very easily understood and a single spike on the HV population is expected, as shown in figure 4.14a). For comparison the experimentally obtained state was shown in figure 4.7 as the second diagram from the

Quantity	Variable	Value	
		Ideal	Exper.
PPBS reflectivity for H	η_H	1/3	0.35
PPBS reflectivity for V	η_V	1	0.99
Loss probability, mode f2	k_{f2}	0	0.904
Loss probability, mode b2	k_{b2}	0	0.911
Loss probability, mode c	k_c	0	0.953
Loss probability, mode d	k_d	0	0.970
Measured forward amplitude	A_f	0.137	0.116
Measured backward amplitude	A_b	0.208	0.177

Table 4.2: Summary of values used as input parameters for the model. When modelling the presence of a given error the experimental value is utilised; to switch the error off, the ideal value is used. To suppress the higher-order down-conversion events for the ideal source case a post-selection on terms with only one pair generated in either direction is forced.

top. In the following section we will look specifically at the contribution of each individual error source.

4.4.1 Non-ideal beamsplitter reflectivities: You get what you pay for

To investigate the effect of the non-ideal splitting ratios of the PPBS, we use realistic values only for the beamsplitter ratios, while using the ideal values of table 4.2 for all other parameters and suppressing multi-photon events. We reconstruct the state, which is shown in figure 4.14b) and observe that, while the spike of the desired HV population dominates, there is a non-zero population in the VH mode and significant coherences between them. The obvious cause must now lie in the wrong beamsplitter reflectivity. In this case, taking the ideal two photon input into the gate and splitting them into the modes $\mathbf{a}_H\mathbf{b}_V$ gives us the state before the interaction beamsplitter. Clearly there is no interference as the two photons are in different modes . While the H photon always had some probability of leaving the gate in either the $\mathbf{c}_H$ or the $\mathbf{d}_H$ mode, the V input photon should always leave the gate in the reflected mode if $\eta_V = 1$. While we only allow for a 1% transmission probability, it is this small deviation that now allows detection of the $|VH\rangle$ rather than the $|HV\rangle$ state. Obviously the probability of detecting the vertically photon having "slipped" through the beamsplitter appears amplified with respect to the desired state as the probability for the horizontal photon being transmitted is approximately twice that of it being reflected. It also is immediately obvious that this must be a coherent process as the transmission through a beamsplitter introduces no mixture to the state and preserves coherences.

4.4.2 Photon loss: Have you got all your marbles

Visualising the effect of photon loss is significantly more difficult than the effect of the wrong beamsplitter reflectivity. The main problem is that photon loss has no effect if there are no

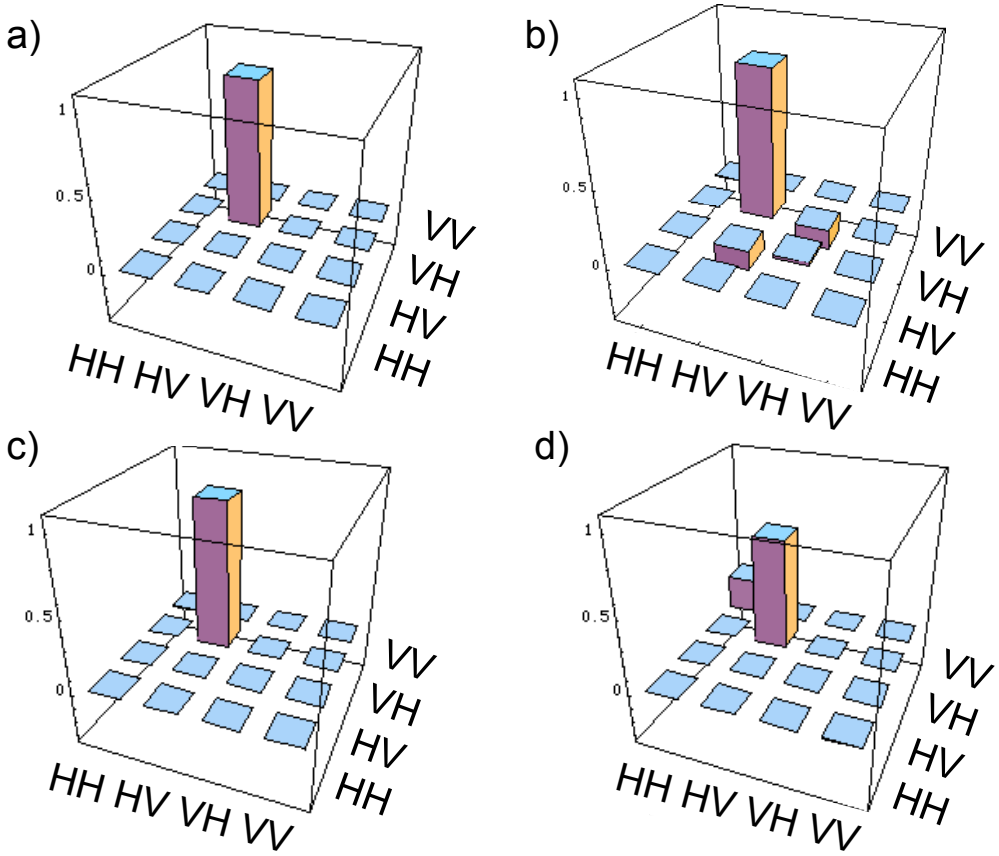


Figure 4.14: Results of the modelling of the HV input state with the various error sources turned on individually: a) shows the ideal state, with a single population in the HV mode of magnitude 1. b) shows the effect of the wrong beamsplitter reflectivities, which lead to some population of the VH mode and significant coherences between the HV and VH modes. For the diagramms c) and d) the multi-pair emission has been turned on. While c) shows the state whith only the multi-pair emission and an ideal beamsplitter leading to a very small population in the HH mode arising from cases where two H photons where injected in the a mode of the gate. To make this contribution of the higher order terms more obvious, d) shows the state as created by multi-photon events exclusively and is thus ignoring cases where only one photon per gate input is injected. Clearly the state contains a significant population in the HH mode, but shows no coherence with the HV population. This is due to the fact that the input state is effectively a mixture of the HH and HV mode and is not created by a unitary rotation of a pure HV state.

additional photons (higher order terms) in the system as long as we are using post-selection on four-fold coincidences[4], because the four fold coincident detection will not register an event if one of the four detectors fails to fire. Therefore we are discussing photon loss in the presence of multi-photon emission events.

Naively one might expect that the only effect loss has would be to dampen the total detection probability. However when we do allow for photon loss and multi-pair emission

[4]Hence the degradation of the experimental results when we tried using only one trigger photon to increase our count rate (See section 4.2.3) The individual heralding of our inputs contributes significantly to the high fidelity.

events, we notice that loss appears to amplify the effects of multi-pair emission. Again a brief and generalised inspection of the photon behaviour in the gate helps to clarify this. Assuming approximately equal probability of losing any one of the photons in the circuit, we can always obtain a signal as long as one photon reaches each detector. Having created an additional pair in one down-converter thus gives us a second bite at the cherry for detecting a trigger photon, should we have lost the original one. Therefore the probability of any output state of the gate when there is more than one trigger photon, is amplified relative to the ideal input. The same effect slightly reduces this effective over-counting, if both photons take the desired path, one has a second chance to detect the sought after state. However, due to beamsplitter reflectivities and the non-classical interference between the photons in the gate, this effect is generally weaker than the possibility at over-counting the "wrong" state due to the doubled trigger photon.

4.4.3 Higher order photon terms: Too much is never enough...

If the gate is ideal and loss-less and the only error is the occasional creation of multiple photons in one of the down-converters, the expected output state for a HV-input is shown in figure 4.14c) and d). We can clearly identify some population occurring in the HH output mode. Where does this population come from? Obviously as the only allowed error is that of multi-pair emission, this must be the source of error, but how? While in the ideal case there are only two photons in the gate, and the coincident detection requires the registration of both, and since a vertical photon is always perfectly reflected at the interaction beamsplitter, the only possible output state in the ideal case is HV. Allowing two photons to populate the input mode $\mathbf{a}_h$, than these photons have a 4/9 chance of splitting at the interaction beamsplitter central in the gate. The vertical photon injected from the other input mode still leaves the gate in the desired output mode $\mathbf{d}$, however it is now overlapped with the second horizontally polarised photon, so that we have $\mathbf{c}_H(\mathbf{d}_H+\mathbf{d}_V)$ (without paying attention to the actual amplitudes or normalisation). When utilising state tomography, there now is a non-zero probability of measuring a fourfold coincidence (two photons from the gate plus the two trigger photons) during the $|HH\rangle$ output state-measurement. This gives rise to the HH population in figure 4.14c), therefore one can easily see now that higher order photon term cause the occurrence of output states initially thought to be impossible.

A second way in which non-single photon input states effect the gate behaviour has already been discussed in section 4.3.1. If photons impinge on both sides of the interaction beamsplitter, than they would usually undergo the desired interference, that is reducing the amplitude of a certain state by a set amount. If multiple photons impinge from one side and a single one from the other side, the behaviour of the interference is altered[5] and the output amplitudes are different to the desired ones [68]. Furthermore, as mentioned above higher order pair emissions also combines with photon loss. Thus multi-pair emission becomes like the Hydra that has multiple ugly heads that pop up and disrupt your experiment and the more you investigate them to cut them off, the more ways you find in which they hurt your

[5]See section 7.1 for more details on how the non-classical interference behaviour is altered due to the presence of more than one photon in one of the interfereing modes.

precious[6] results.

4.5 Model vs. Experiment

The model does not just unveil the individual contributions of the errors, but is obviously capable of predicting the output state for any given input under any given circumstances for the modelled errors. By calculating the expected output state for the same set of input states and modelling the individual measurements, we can generate the same data set as we experimentally obtained to perform both state and process tomography for any combination of modelled noise sources, but most interestingly for the gate with the noise sources as determined experimentally. We hence expect a very good overlap between the modelled and experimental data. After calculating the process matrix of the model with (**H**)igher-order photon terms, photon (**L**)oss and actual (**B**)easmplitter reflectivities[7] for the PPBS we reconstruct the χ_{HLB}-matrix which should be the most accurate description of the experimental situation. Calculating the process Fidelity between the HLB-Model and the ideal CZ gate, we find $F_p = 81.4\%$, close to that of the experiment and the ideal at $78.2 \pm 1.5\%$. To confirm that our model has not simply derived an equally bad, yet completely different, process to that observed in the experiment, we calculate the process fidelity between the modelled and experimentally derived process matricies after we optimise the experimental data again over local unitary single qubit rotations with respect to the model, to compensate for the phase-shift of the PPBS (not modelled). We find a process fidelity between the two χ-matrices of $96.7 \pm 1.5\%$. The remarkably good agreement between the model and the experiment highlights the accuracy of our model and rewards the efforts in deriving the highly detailed model and the required input values for it. As the model allows the individual investigation of all errors, we have derived the χ matrices for all error combinations and calculated the fidelity between them and the ideal and model. The values for both the process fidelity and the average gate fidelity are shown in tables 4.5 and 4.4 respectively. Here the comparison of the fidelity of the modelled χ-matrices lets us explore the impact of each individual error source on the process and average gate fidelity.

We can see, that while loss has, as expected from section 4.4.2, no impact on the gate performance by itself, the imperfect beamsplitters used during the experiment caused a 2.8% drop in process fidelity by themselves. Higher order photon terms alone already degrade the gate performance by 6.8%, which gets blown out to a stunning 15.8% once one considers that loss is activated only due to the presence of multi-pair emission. Furthermore it is noteworthy, that the contribution of the individual error sources is by no means linear, meaning you can not simply determine the individual effect and perform either a sum or product to derive the combined effect. Finally the difference between the HLB-model and the experiment of 3.3% is attributed to mode mismatch, as it is the only known error source in optical quantum computing that is not modelled here. Prior to this experiment, all modelled error sources where well known, but all, especially the effect of multi-photon inputs, were considered less

[6] my precious...

[7] The bold, capital letters are used in labelling the different results obtained from the model, results from the model with i.e. multi-pair emission and photon loss at realistic levels will be referred to as the HL-model. They should not be confused with the non-bold letters H and L labelling the polarisation states.

Model settings	F_p with ideal	ΔF_p (wrt ideal)	F_p with experiment	ΔF_p (wrt exp)
ideal	100%	0%	78.2%	21.8%
L	100%	0%	78.2%	21.8%
B	97.2%	2.8%	80.2%	19.8%
BL	97.2%	2.8%	80.2%	19.8%
H	93.2%	6.8%	92.1%	7.9%
HB	88.0%	12.0%	94.9%	5.1%
HL	87.2%	12.8%	94.4%	5.6%
HBL	81.4%	18.6%	96.7%	3.3%
experiment	78.2(±1.5)%	21.8%	100%	0%

Table 4.3: Process Fidelities, F_p, between the models with all possible error source combinations and the ideal (column 1 & 2) and the experimentally determined (column 3 &4) processes. As can be seen from the differences, the significant deterioration of the gate performance is caused by the higher order photon terms. There is a very good agreeance between the model with all error sources and the experiment, achieving a fidelity of 96.7%. (wrt =with respect to)

Model settings	$\overline{F}$ with ideal	$\Delta\overline{F}$ (wrt ideal)	$\overline{F}$ with experiment	$\Delta\overline{F}$ (wrt exp)
ideal	100%	0	82.5%	17.5%
L	100%	0	82.5%	17.5%
B	97.8%	2.2%	84.2%	15.8%
BL	97.8%	2.2%	84.2%	15.8%
H	94.6%	5.6%	93.7%	6.3%
HB	90.4%	9.6%	94.9%	5.1%
HL	89.8%	10.2%	95.5%	4.5%
HBL	85.1%	14.9%	97.4%	2.6%
Experiment	82.5% ±1.5%	17.5% ±1.5%	100%	0%

Table 4.4: Average gate fidelities, $\overline{F}$, for the models with respect to (wrt) the ideal (column 1 & 2) and the experiment (column 3 &4). Terms that can be turned on in the model are: Loss **L** , given by measured losses in the experiment; Beamsplitter reflectivity **B**, given by the measured beamsplitter reflectivities in the experimental gate; and the higher-order photon terms **H**, a model of the source based on measurement that includes higher-order photon terms. In the *ideal* case there is no loss, ideal beamsplitter reflectivities, and no higher-order photon terms in the source. The overlap between χ-matrices is the process fidelity, F_p, it gives: $\overline{F}$=dF_P+1/d+1, where d is the state dimension, here 4.

important and secondary to the effect of mode mismatch due to the very low probability of emitting one more pair than needed thanks to the natural inefficiency of down-conversion. This model contradicts this common belief and points to the few multi-photon events as

the main culprit for imperfect gate performance, making the development of either photon number resolving detectors or genuine single photon sources the main requirement for the successful future of linear optical quantum computing.

This new finding also explains, why despite record high visibility for the Hong-Ou-Mandel interference for independently generated photons, the individual states and subsequently the gate performance was considerably worse than was to be expected from the results obtained, when implementing the gate with dependent photons.

5

Exploring the realm of fault-tolerance

For quantum computing to become feasible and scalable one of the main feats to achieve is that of fault-tolerance . Through a specific encoding and correction scheme a certain level of gate failure—known as error probability per gate (EPG)—becomes tolerable and can be corrected for using specific fault tolerant quantum codes. The error probability per gate that can be sustained depends on a variety of assumptions [69], such as the specific error correction code, the available resources and the distribution and kind of errors. Many different thresholds have been derived for various combinations of assumptions of available resources, however no effort has been made to compare these theoretically derived bounds to experimentally realised gate performance. In this chapter we introduce two specific error models, one which has yielded the highest reported threshold value to date and one that assumes the most general errors. These two models will serve as our upper and lower bounds for the fault-tolerance threshold respectively. We demonstrate how to compare the performance of experimentally characterised gates to these thresholds using a method that can be applied to any quantum computing architecture. Further we analyse the predicted behaviour from our modelled gate to identify the required technological advances to reach the realm of fault tolerance.

The work presented in this chapter was conducted by myself in close collaboration with Alexei Gilchrist, Andrew Doherty and Andrew White. The idea for the optimisation of the error bound for our experiment with respect to the gremlin model was thought of by Andrew Doherty and implemented and optimised by Alexei Gilchrist.

5.1 Principles and Classic examples

Fault tolerance is the basic concept of retrieving information accurately despite the presence of noise. Even though a given process is not error free, it is possible to encode the signal in such a way that it becomes possible to detect some errors and correct them, so that the

final process outcome is error free.

There are two basic concepts for fault-tolerance: one is feedback or feed-forward, which seeks to actively compensate occurring errors, the other is redundant encoding, which protects the information by storing it in multiple copies.

Feedback is applied in everyday life in many places and relies on measurement of a certain parameter to determine whether or not an error has occurred. One common example is controlling the room temperature via an air-conditioner. If a temperature sensor detects that the room temperature deviates from the desired or set temperature, the system adjusts by either increasing or decreasing its cooling efforts. This mechanism works very well, if the desired state is known, and an efficient measurement of a suitable indicator is possible. When measurement is impossible or no a priori information is held about the expected or desired state, this lack of information makes it impossible to determine if a deviation from the desired state has occurred— errors are undetectable.

If feedback is unsuitable, redundancy commonly is the answer. This technique is, besides others, used in modern digital communication i.e. digital and mobile phones, which face a very noisy environment. Using analogue encoding, the effect of a noisy telephone line was, well, noise in the line. The change to digital data transfer required some way of compensating for the possible errors. In the analogous case, noise in form of a voltage fluctuation would lead to additional frequencies and thus squeaking in the line. Moving to the digitalised world, where all information is encoded in bits with values of either one or zero, such fluctuations could swap 1's into 0's and vice versa. Thereby it not only adds unwanted noise, but potentially alters the transmitted signal to a point where the information is falsified. Redundant encoding protects against this by transmitting the same information an odd number of times. Should one of the code bits flip a simple vote by majority of all code bits retrieves the state of the underlying logic bit. This method has a high success probability, as long as the probability of a bit-flip up to the correction point is less than one half. Using more code-bits either increases the probability of successfully decoding the logic bit or leads to tolerance of higher noise levels with the same success probability.

Modern classical error-correction mechanisms are far more sophisticated[22] than described here, but the two methods described above are the underlying concepts on which error-correction and thus fault-tolerance are based.

5.2 Quantum error correction and fault-tolerance

The attributes of qubits that lead to the might of quantum computing are also their drawback when trying to shield the computation against errors through noise. Feedback or feed-forward[1] in a quantum system faces the difficulty that each measurement causes back action onto the state itself. While the strength of the measurement can be varied [35], this also changes the amount of information that can be gained from the measurement. The choice ranges from a fully projective measurement with maximal information gain, to a completely

[1]Forward here means forward in time, but back onto the very qubit that was measured, thus correcting the measured state. The alternative feedback would feed the information about the experienced deviation back onto the process seeking to correct the interaction process so that future qubits will be more likely to be in the correct state.

interaction free measurement that subsequently also reveals no information about the quantity of interest. Feedback or feed-forward also requires knowledge of the expected state, which generally is not given during a quantum computation.

This measurement back action also makes encoding into multiple qubits difficult due to the no-cloning theorem[2]. The theorem states that it is impossible to create exact copies of a quantum state, without destroying the original copy, making it impossible to posses multiple copies of the same qubit. It was hence thought that a quantum computer would have to consist of independently perfect steps, as it would be impossible to detect errors in the code and compensate for them during one computational run. It came as a surprise when Shor presented a code [70] that could correct for both bit-flip (X-) errors and phase (Z-) errors. Capability to correct these two error types in principle suffices to correct any error. Shor's code required a total of nine physical qubits to encode a logic qubit, and was able to correct for one error in the gate operation and one error during the error correction, which defines the class of distance-5 codes. Steane independently discovered a code with only 7 physical qubits [71], which still could correct for 2 errors in a logic gate step. These two papers sparked research into the optimal fault tolerance methodology which soon revealed, that with improved error correction schemes, distance-3 codes (capable of correcting one error during gate operation or error correction) would suffice to reach fault tolerant quantum computation.

To do a full computation, one will need many thousands of gates, with the total error rate for the computation scaling with the number of implemented gates. The absence of error correction would require the individual gate error rate to decrease further and further for longer and longer[3] computation to sustain the same success probability. By applying redundant encoding and error correction after every single logic gate one can prevent the spreading of errors through the computational code, removing the requirement for ever improving architectures. Larger computations will still require better gates as the total error probability scales with the probability of an error not being corrected at which obviously scales with the number of implemented gates where this could occur. Of course the encoding is not limited to the initial logic qubits, but can be applied again to the code qubits. As the original code allowed for one error in our code qubits, we can now allow one error in our code qubits, and to still correctly identify the state of our logic qubits. Since we can tolerate again one error and still correctly retrieve the logic qubits, we have therefore increased our tolerable error rate. More specifically, if the probability of an error on any one physical qubit in the first encoding is p, this becomes the maximum tolerable error rate, as two errors in our encoding of the logic qubit would lead to an unrecoverable error. If we encode the code qubits of the initial encoding again, the failure probability decreases to p^2, before we will fail to recover our logic qubit. This further encoding comes at a price: there is an overhead in operations and thus additional locations where errors can occur. These extra steps lead to a constant overhead c for this encoding [22, 69]. The new total error probability becomes $\varepsilon = cp^2$. If cp^2 is smaller than p, we have increased the probability of successfully computing a result. This can of course be repeated, by encoding the encoded code qubits again, picking up another factor of c for the overhead and p for the additional physical errors that we can

[2]For a nice proof see Ref. [22] page 532.

[3]Using more gates.

tolerate. The error rate after k concatenation steps thus becomes

$$\frac{(cp)^k}{c}$$

. We can then identify a threshold condition of the kind

$$\frac{(cp)^k}{c} \leqslant \frac{\xi}{G(n)}, \tag{5.1}$$

where $G(n)$ is the number of gates in our circuit for a problem of the dimension n. $G(n)$ must be polynomial in the size of n, and ξ is the final accuracy we would like to achieve. For a concatenation level k we must achieve

$$p \leqslant p_{th} \equiv \frac{1}{c}.$$

The significance of this equation is that once we achieve a error probability below the threshold, we can achieve any desired total error rate ξ by applying concatenated encoding. While p_{th} is the error per gate rate at which fault-tolerant quantum computing will be in principle possible, the price tag of this manifold encoding—due to the required resources—is going to influence the level of concatenations that are practically feasible. This might lead to a feasability threshold larger than the theoretically predicted $p_{feasable} > p_{th}$. Recently it was found that close to the threshold, the required concatenation level blows out exponentially, while for values away from the error threshold a significant large region exists, where the increase in required encoding levels is relatively flat [72]. For practical fault-tolerant quantum computing, the goal must be to achieve an EPG (error probability per gate) not only lower than the threshold, but in this flat region.

A complete discussion of quantum error correction and fault tolerant circuitry is beyond the scope of this thesis, but the inclined reader is referred to Chapter 10 of Ref. [22] and Refs. [73, 74]. For the upcoming chapter it is sufficient to know that quantum error correction is in principle possible and that schemes for fault-tolerant quantum computing exist.

5.3 Where do fault-tolerance thresholds come from

As diverse as the approaches towards quantum computing are, as manifold are the fault-tolerance results thresholds. Their multitude is caused by the variety of assumptions used to derive thresholds. It is not clear which assumptions (if any) are actually necessary to derive the most general or even an universal threshold and while some conditions are easily met in one architecture, they might be completely infeasible in another. A brief discussion of this can be found in [69].

Further complication arises from the difficulty of calculating these thresholds theoretically. In some cases. a mathematically derived boundary can be proven, though commonly at the price of very conservative assumptions, leading to thresholds that are likely to be pessimistic. Because of the difficulties in obtaining analytical proofs, numerical simulations are usually used to infer asymptotic values for tolerable errors. There are two problems with

this method: it always leaves the possibility of an oversight in the model which could render the simulation useless; and the simulations usually struggle with many concatenation levels, thereby potentially undershooting the threshold. Nevertheless the values achieved with such models provide a basis as to the likely order of tolerable error rates. In the past, thresholds inferred from such simulations are usually higher than proven thresholds, commonly by a factor of ≈ 10. A third option is an analytical approach, making assumptions about leading contributors to error rates and mechanisms. These usually result in value between the simulated and proven values, further indicating that the pegged out range appears to be correct. A brief and recent summary of the current state of the art of fault-tolerance, with specific details on these problems, can be found in [69].

5.3.1 The Knill error threshold

Most error-thresholds are in the range from 10^{-6} to 10^{-3}, depending on the assumptions and used methods. In 2005, a paper by Emmanuel Knill [75] stunned the community by inferring an error threshold as high as $5-6\%$ or 5×10^{-2}, with the proven (through simulation) threshold at 3%. This is the highest reported threshold value to date, and is achieved by departing from error correction and applying an error detection code which dumps a subset of the computation when an error is indicated. It also uses a C4/C6-architecture, where the first level of concatenation is using 4 qubits and the further levels use 6 rather than the common symmetric encoding. Knill points out that the code can tolerate error rates of the same order as $1 - F$ for the fidelities of entangled states created in experiments with ion-traps [76, 77]. The required resource overhead at EPG-levels close to the error-threshold of this scheme is enormous due to the dumping, which has earned this code the nickname "ancilla-factory".

A further limitation of Knill's result, like most other thresholds, is the specific selection of allowed noise, which here is assumed to be that of a independent stochastic noise source giving random Pauli rotations. This means that all errors are random and equally likely to occur while there is no correlation between specific errors either in the individual gate or in concatenated gates.

5.3.2 The general gremlin model

Like the Knill model, any other derived threshold has been gained by making some assumptions[4] about the errors to be faced. The reason for a specific error choice is usually to make modelling easier, as it allows more specialised compensation methods. While these methods are in wide-spread use, these assumption can make the threshold somewhat artificial and its application very limited. We hence ideally want the most general threshold possible. Aliferis, Gottesman and Preskill [78] managed to *prove* a threshold for in a model with non-markovian noise which allows for the most general errors. It effectively allows the actions of a gremlin, who has complete freedom in its noise action. He can thus correlate the errors in

[4]More assumptions than just the error source are usually needed, i.e. the availability and relative speed of classical computing power or the presence of abundant ancilla qubits. These will likely be architecture dependent and solutions depend on the engineering. We thus focus here on the error sources.

such a way that the errors of subsequent gates add coherently, maximising their impact. He could even add entangled errors. While such coherent addition is in principle possible, it is highly unlikely to occur without a organising force—the gremlin in the experimental implementation. This model is therefore considered a worst case scenario and the proven bound for the error threshold of 2.73×10^{-5} can be considered a lower bound for the correctable error threshold for a future quantum computation device.

The two introduced models, Knill's ancilla-factory approach and the gremlin model are current extreme cases for fault-tolerance thresholds. As the exact threshold value for fault-tolerant quantum computing is yet to be found, we use these two results, the proven value from the gremlin and the inferred threshold in the ancilla factory model as our upper and lower bounds. If the achieved EPG is lower than Knill's threshold of 5×10^{-2} fault tolerant quantum computing might be possible, while an EPG below the gremlin-threshold guarantees fault-tolerant quantum computation.

Practical quantum computing is likely to require not only an EPG *at* the threshold, but *well below*, in order to limit the overhead blow out that occurs near the threshold value. The exact point at which quantum computing will become feasible will depend on the availability and both the physical and temporal cost of the resources required for concatenated error encoding and correction. The aim for experimental implementations thus has to be to achieve an EPG below 2.7×10^{-5}, but failing this, to at least surpass Knill's threshold and then have a closer look at the real noise sources and specific correction methods.

5.4 Bridging the gap: Comparing experimental gate performance to the theoretical thresholds

While derived, inferred and proven thresholds are plentiful for various combinations of assumptions, there has been little to no effort in relating the experimentally demonstrated gates and their performance to the theoretically derived thresholds. One obvious cause for this is the lack of a methodology for comparing experimental gate performance measures to the theoretically derived threshold values. As mentioned, Knill [75] related his threshold to the achieved fidelity of creating an entangled state in an ion-trap implementation [76, 77]. But as discussed in section 1.4.3, the fidelity of generating an individual output state can hardly serve as a measure for the gate performance and can thus not be a rigorous value for the EPG.

In chapter 4 we measured the performance of a linear optical entangling gate under conditions close to those expected when attempting large scale fault-tolerant quantum computation with current technology. The highly accurate model that we derived during that chapter will give us access to the effects of real error sources. In the following we will develop a method for comparing our experimental gate performance and to these fault-tolerance thresholds. We will analyse the quality of the derived experimental error probability for our gate and utilise our model to pinpoint the advances needed to reach the realm of fault tolerance with photonic quantum computing. We choose the ancilla factory by Knill and the gremlin model of Aliferis, Gottesman and Preskill, as these present the two extreme cases as

detailed in the previous section. In order to find suitable measures to compare the experimental gates to the threshold, we will have a closer look at the individual noise assumptions and their implications on the gate behaviour.

5.4.1 Pathfinding part I: Comparing to Knill's threshold

To identify a suitable approach to compare our experimental gate performance to threshold derived by Knill, it pays off to look at the assumptions Knill uses to derive his threshold. He assumes that all errors are independent products of Pauli-opperations with an unbiased probability distribution. What does this mean?[5] First of all, if the errors are all products of Pauli-errors, and since our representation of χ-matrices (see chapters 3 and 4) is in the Pauli-basis, this should allow an easy comparison to our process fidelities. However we want to be in a basis where the ideal gate operation is a single element (and not broken up in it's Pauli-operations) and all errors show up as additional operations. We hence rotate the basis in which we represent the process matrix[6] in such a manner that the basis vectors are no longer the Pauli operators $\{I, X, Y, Z\} \otimes \{I, X, Y, Z\}$, but instead the product of the desired CZ-gate action with the Pauli-operators, $CS \times (\{I, X, Y, Z\} \otimes \{I, X, Y, Z\})$. (We use here CS as the operator for a controlled-sign gate and avoid using the CZ from the text as to avoid misinterpretation of the Z as the Pauli Z operator.) In this basis, the first element of the matrix becomes the desired gate operation followed (or preceded) by the identity operation on both qubits, which leaves it at the ideal gate operation. The $(2, 2)$-element $(CS \times IX)$ now becomes the ideal gate operation followed (or preceded) by the identity operation on qubit one, and a X-rotation (phase-shift) on qubit two. All of the diagonal elements are subsequently the CZ-gate action followed or preceded by a combination of Pauli-errors on one or both qubits. The off-diagonal elements in this matrix are coherences between different processes. The ideal CZ gate operation is shown in fig.5.1a) and b), where a) is in the Pauli basis and b) after rotation in the *"gate" basis*. As this is the ideal operation, the only population in the gate basis is in the $(1, 1)$ element. However, if there were errors, the Knill model demands that the errors should be independent of each other. Hence while we should now see populations along the diagonal axis, we should not see *any* off diagonal elements, i.e. coherences between the individual populations in the process matrix. Furthermore Knill demands that the errors are randomly distributed. As our χ-matrices are reconstructed from a large number of measurements, we should therefore expect the populations in the gate-basis to be of equal magnitude except for the $(1, 1)$-element, which gives us the probability p of having performed the gate correctly. The sum of the remaining populations should hence yield the error probability

$$\sum_{i=2}^{16} \chi_{i,i} = \varepsilon_p = (1-p), \tag{5.2}$$

which should be equal or less than the error threshold value

$$\varepsilon_p \leqslant \varepsilon_0 = 5 \times 10^{-2}, \tag{5.3}$$

[5] I am quite aware that any inclined theorist is by now terribly bored, but this section is meant to provide an understanding for naive experimentalists like me.

[6] Remembering that the choice of basis is arbitrary, Section 1.4.3

to make fault tolerant quantum computing in principle possible.

So far we have reconstructed the χ-matrices in the Pauli-basis to allow some intuition of the applied actions of the gate. We need to find the suitable rotation to convert our matrices from the Pauli-basis to the gate-basis. To obtain the matrix that maps the Pauli-basis onto the gate basis, we calculate the bit-wise tensor product of the individual basis vectors of the Pauli-basis with the ideal CZ-Gate action. The resultant vector for the 16 individual basis vectors are then strung together to form the matrix that transforms the Pauli basis to the gate basis. With the bit-flipped gate operation

$$CS = (-II + IZ + ZI + ZZ)/4, \tag{5.4}$$

the individual vectors for the transfer matrix become

$$\begin{aligned} II{\times}CS &= \frac{1}{\sqrt{4}}(-II + IZ + ZI + ZZ) \\ IX{\times}CS &= \frac{1}{\sqrt{4}}(-IX - iIY + ZX - iZY) \\ IY{\times}CS &= \frac{1}{\sqrt{4}}(-IY + iIX + ZY + iZX) \\ IZ{\times}CS &= \frac{1}{\sqrt{4}}(-IZ + II + ZZ + ZI) \end{aligned} \tag{5.5}$$

$$\begin{aligned} XI{\times}CS &= \frac{1}{\sqrt{4}}(-XI + XZ - iYI - iYZ) \\ XX{\times}CS &= \frac{1}{\sqrt{4}}(-XX - iXY - iYX - YY) \\ XY{\times}CS &= \frac{1}{\sqrt{4}}(-XY + iXX - iYY - YX) \\ XZ{\times}CS &= \frac{1}{\sqrt{4}}(-XZ + XI - iYZ - iYI) \end{aligned} \tag{5.6}$$

$$\begin{aligned} YI{\times}CS &= \frac{1}{\sqrt{4}}(-YI + YZ + iXI + iXZ) \\ YX{\times}CS &= \frac{1}{\sqrt{4}}(-YX - iYY + iXX - XY) \\ YY{\times}CS &= \frac{1}{\sqrt{4}}(-YY + iYX + iXY - XX) \\ YZ{\times}CS &= \frac{1}{\sqrt{4}}(-YZ + YI + iXZ + iXI) \end{aligned} \tag{5.7}$$

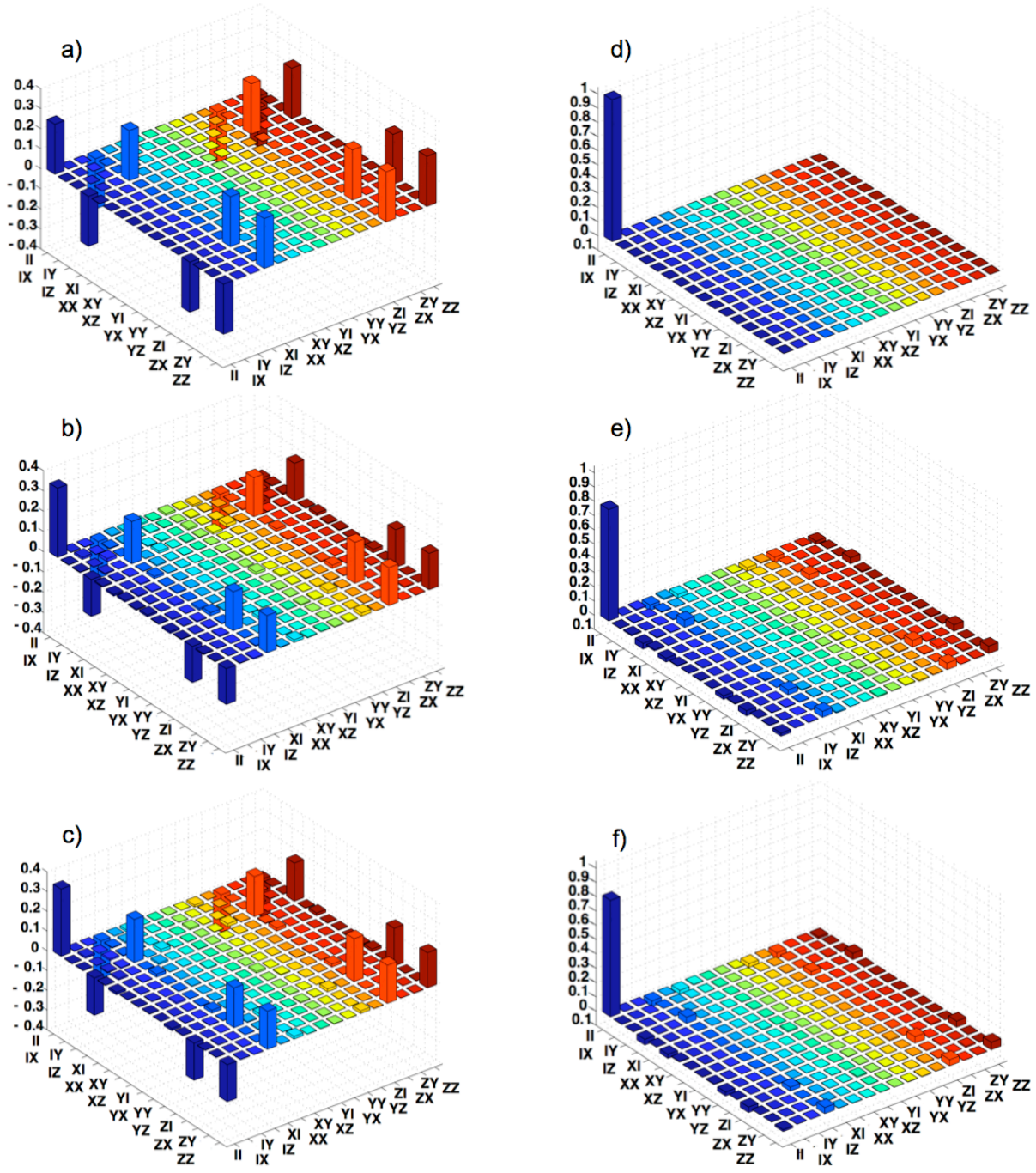


Figure 5.1: Process matrices of a bit-flipped CZ gate in the commonly used Pauli basis a)-c) and after basis rotation in the gate basis d)-f). The matrices are for the ideal gate a) and d) and those reconstructed from the experimental data b),e) and from the HLB-model c),f). The Pauli-basis is instructive to understand the actions of the gate, while the gate-basis allows a fast and easy analyses of non-ideal results, as the first element becomes the process fidelity, with every other diagonal element being a Pauli-error.

$$\begin{aligned} ZI{\times}CS &= \frac{1}{\sqrt{4}}(-ZI + ZZ + II + IZ) \\ ZX{\times}CS &= \frac{1}{\sqrt{4}}(-ZX - iZY + IX - iIY) \\ ZY{\times}CS &= \frac{1}{\sqrt{4}}(-ZY + iZX + IY + iIX) \\ ZZ{\times}CS &= \frac{1}{\sqrt{4}}(-ZZ + ZI + IZ + II) \end{aligned} \tag{5.8}$$

The transformation that we seek to imply is thus

$$\chi_{Gate} = U_{P2G}\,\chi_{Pauli} U_{P2G}^{\dagger} \quad \text{, with} \tag{5.9}$$

$$U_{P2G} = \Big[\{II{\times}CS\}, \{IX{\times}CS\}, \{IY{\times}CS\}, ..., \{ZZ{\times}CS\}\Big] \tag{5.10}$$

Applying this transformation to the ideal χ-matrix of figure 4.11, we obtain the matrix for the ideal CZ-Gate in the gate-basis. This matrix is 1 in the $(1,1)$ element and 0 elsewhere, indicating that the only process that is occurring is the perfect CS gate action. We can see immediately that the overlap of this matrix with any other matrix is simply the value of the $(1,1)$ element of the second matrix. As the overlap of the ideal gate action with the χ-matrix of another process is defined to be the process fidelity, we can identify the value of the first element of any χ-matrix in this gate basis to be the process fidelity with the ideal CZ-gate.

The graphical representation of the χ-matrices shown in figure 5.1 displays the real parts of the ideal a),d), the experimental b),e) and the modelled c),f) data before a)-c) and after d)-f) the transformation. As discussed above, any population except for the $(1,1)$ element is an undesired gate operation and can thus be ascribed to noise and the population elements (representing additional Pauli rotations) reveal the actions of the encountered noise. While it might not bear much comfort to the experimenter to see the individual effects of errors, it leads to an open and interesting question of whether an optimal correction exists for the measured noise, which might tolerate an even higher EPG. An indication of this is a recent paper by Aliferis and Preskill [79], which yields a higher threshold for a certain model if, in this specific case, phase errors dominate by several orders of magnitude.

After the transformation we can read off the probability of incorporating the desired CZ gate action as the population of the first element for both the model and the experiment that we discussed in chapter 4, which, as expected, equal the previously found process fidelities of 78.2% for the experimental data and 81.4% for the model. As any population that is not in the first element of the matrix is an error in the Knill model, we can identify the error per gate probability p as the part of the process fidelity (population of the first element) missing to 100%, thus

$$\begin{aligned} F_p &= (1-p) \\ p &= 1 - F_p. \end{aligned} \tag{5.11}$$

The values of $p_{exp} = 21.8\%$ and $p_{HLB} = 18.6\%$ (see table 4.5) are considerably larger than the tolerable 5% EPG found by Knill. As we already observed in the previous chapter, switching off individual error sources drastically increases the process fidelity with the ideal

operation. We use this capability to now estimate the EPG rates that could be achieved with technological advances that eliminate the error arrising from an imperfect photon source. Using Eq.5.11 and the third column of table 4.5, we can immediately read off the error probability for the various combinations of errors. It is worthy noting that losing one photon in this post-selection based method would not yield any errors if we had either perfect sources or unit efficient number resolving detectors. Thus eliminating multi-pair emission effectively remedies two error sources and thus allows an instantaneous leap to an EPG of 2.8% caused only by the wrong beamsplitter reflectivity puts this approach on the doorstep to fault tolerant quantum computing. As noted in Chapter 4 the model does not consider mode mismatch, which was attributed with the discrepancy between the model and the experimentally determined χ-matrices (3.2%). We thus expect that the elimination of the multi-pair emission error source will leave optical quantum computing with an combined EPG of 2.8+3.2%, which still leaves us with an EPG in the vicinity of fault-tolerant quantum computing. Clearly there is also no physical reason, why the reflectivity of our PPBS need to deviate from the ideal[7] and as discussed in Chapter 3, the set of PPBSs in the cw gate at the PDC wavelength for the Ar^+-laser were ideal within measurement accuracy. It is thus feasible that this specific error source could also be eliminated, leaving only the mode-missmatch, $p = 3.2\%$, as the governing error source. This would put the EPG of optical quantum computing in the range where fault tolerant quantum computing could be possible. Whether it would be feasible would depend on the specific conditions at hand, especially the cost of adding ancilla qubits and the associated operations, especially in the light that the demonstrated optical gates are non-deterministic.

5.4.2 Testing the fault tolerant conditions

It is important to check the consistency of our experimental results with the assumptions made by Knill to derive his model. The main assumption was that the errors should be independent random Pauli rotations. As acknowledged above, the gate basis allows immediate appreciation of the occurring noise in terms of Pauli errors. This also reveals that the distribution is not random, as there are specific errors (IZ, ZI, ZZ) that dominate.

Furthermore coherences between individual error terms become immediately apparent in the gate-basis representation. A brief inspection of both the experimental and modelled process matrix (Fig. 5.1) e) and f)) shows not only populations indicating the predominant errors to be any additional Z rotations on the gate, i.e. IZ, ZI, ZZ but also significant coherences between these noise populations and the ideal gate action, as well as with the other noise terms. With coherences it is however not the magnitude themselves that holds all the information about the strength or degree of coherence, as the maximal value for a coherence is given by the product of the square roots of the respective populations, using the complex conjugate of one of the two. While this gives the maximal strength of the coherence, this value will be a small, if one or both of the populations are small. Nevertheless, the *degree of coherence* between the two populations might still be significant. We define the degree of coherence as the ratio between the maximal value for a given coherence and the observed

[7] Clearly achieving the correct beamsplitter reflectivities is a problem of the kind Quality $\propto$ log(Money) clearly showing that there is no physical reason why the ideal reflectivity can not be achieved.

value. To calculate the degree of coherence matrix we calculate

$$C_{ij} = |\chi_{ij}|(1 - \delta_{ij})/\sqrt{\chi_{ii}\chi_{jj}}, \tag{5.12}$$

where i, j are indices of the χ-matrix. Entries in the resulting coherence matrix vary between 0, no coherence, and 1, maximal coherence. The coherence matrix for the experiment is shown in Fig. 5.2 a), clearly showing non-zero coherences everywhere. It is noteworthy that the coherences of the ideal operation with any error term is relatively low. The coherences between the IZ and the other dominant errors ZI, ZZ are above average, but the degree of coherence between the ZI and ZZ error and, surprisingly, the ZX and ZY error are unsurpassed—they are nearly perfectly coherent! Remembering that coherences show how populations got redistributed, we can identify that this would result from phase shifts, Z rotations, added onto identity operations as $Z \otimes I \to Z$ or onto X-rotations ($Z \otimes X \to Y$). The other significant coherences appear on terms that relate to the primary error terms identified earlier, with an additional phase shift (Z) on one or both of the qubits. As the Z-rotation is a coherent process, it is not surprising to find strong coherences in these terms.

Figure 5.2 b) is the degree of coherence matrix as predicted by the model. While similar patterns can easily be identified as in the experimental degree of coherence matrix, the general level of coherence is significantly higher than in the experimental data set. Since so far we observed outstanding agreement between the model and the experiment, we now have to ask what gives rise to the large discrepancy in coherences. We start by looking at the degree of coherence that occur due to the individual error terms of the model.

Looking only at the effects of the imperfect circuitry in the model (as discussed in section 4.4, with the degree of coherence matrix shown in figure 5.2 c)) we can see that the errors caused by this kind of noise are highly coherent. As the imperfect beamsplitter reflectivity can also be described as a slight rotation of the output state, this is by no means surprising. On the other hand, the multi-pair emission causes errors by giving rise to processes that would and could not be populated otherwise[8]. As there is generally no rotation that allows us to obtain the states obtained due to the multi-pair emission, the degree of coherence of these errors is low. We find exactly this behaviour for this kind of error, as can be seen in figure 5.2 d). The only terms that have significant coherences in this modelled result are the ZI and ZZ, the ZX and ZY and the ZZ and ZI terms. These are exactly the terms that have the most significant coherences in the experimental data set, hinting again that the multi-pair emission appears as the leading error source in optical quantum computing.

While this inspection was highly instructive, it has not explained the discrepancy between the full model and the experiment. We must hence conclude that of the modelled errors could lead to the lower coherence, but remembering the discussion of the details of the model, we see that the model was designed to account for higher order pair emission, wrong beamsplitter reflectivities and photon loss. The only known error source that was not included was mode mismatch. Mode mismatch causes distinguishability between the photons which leads to the lack of coherent interaction[9]. Therefore by definition the action of mode mismatch is

[8]The effect of loss is mainly a scaling effect on this multi-pair behaviour and will not be discussed individually here.

[9]It also allows some coherent, but incorrect operation, i.e. the passing of a vertically polarised photon instead of perfectly reflecting it is clearly coherent.

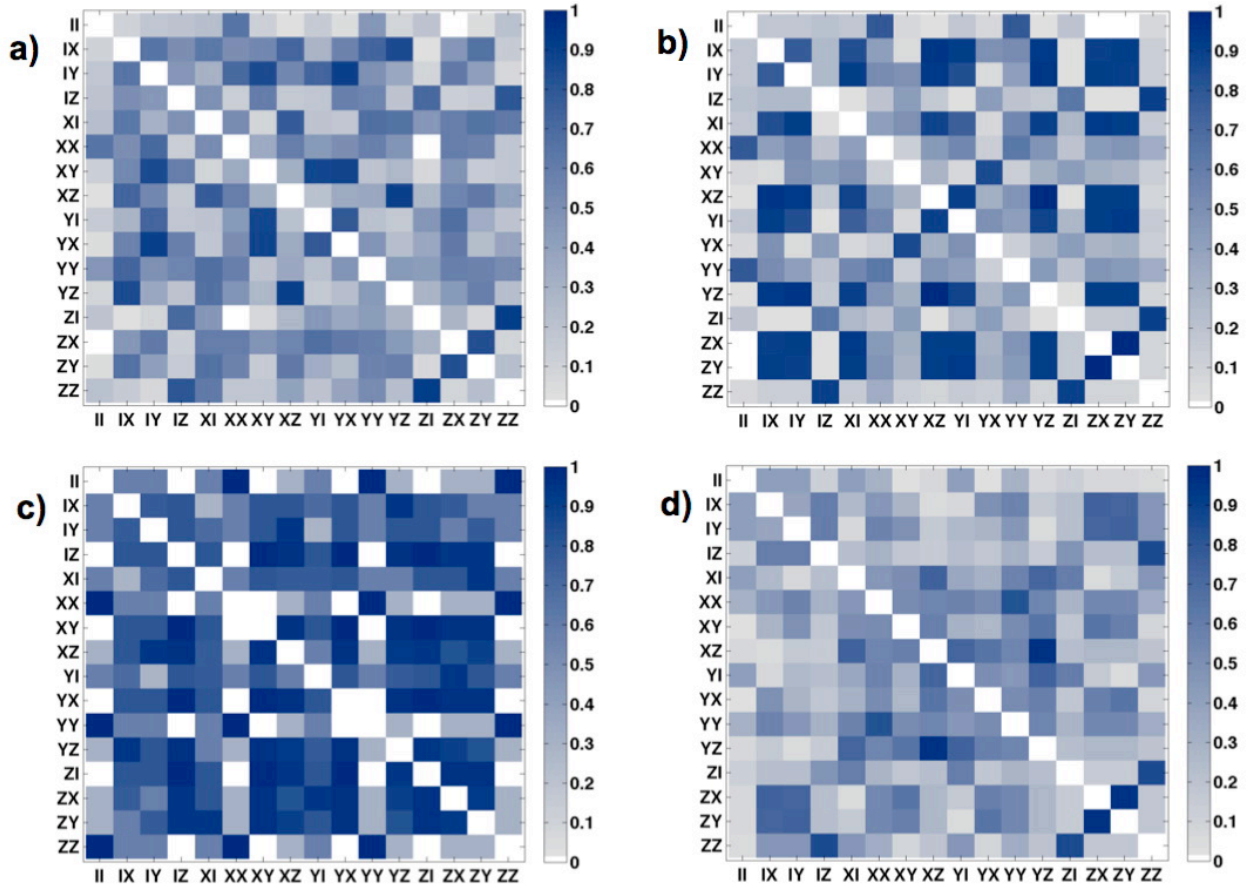


Figure 5.2: Coherence matrices showing the degree of coherence for a) the experiment, b) the full model, c) modelling only the effect of imperfect circuitry and d) modelling only the effect of higher order photon numbers. Coherence values vary between 0, no coherence, and 1, full coherence. The coherence patterns of the experiment and model are similar: as the experiment suffers decoherence due to mode mismatch we expect it to have lower coherences than the model, as is observed. c) and d) highlight that, while the effects of non-ideal circuitry is highly coherent, the errors due to the non-ideal source are not.

incoherent. We thus expect that even small amounts of mode mismatch lead to the loss of coherences between the processes. Since it is observed that the experiment suffers from additional[10] mode-mismatch, we expect the experiment to have generally a lower degree of coherence than the complete model.

5.4.3 Summary for the Knill model

We have learned that rotating the process matrix into the gate-basis instantaneously reveals the kind of errors faced and gives first clues at the coherence of the processes. However as gates continue to be optimised, and their performance approaches the ideal, the graphical representation is going to be dominated by the first element which also gives the process

[10] Additional to the error sources modelled.

fidelity. What remains challenging will be to appreciate the degree of coherence between the ever increasing process fidelity and the decreasing error populations and of course between the error populations themselves. We therefore introduce the degree of coherence matrix, which gives an easy representation of the level of coherence relative to the individual maximal value. By inspecting the graphical representation of these new methods, we can see two things immediately which contradict the assumptions used for Knill's ancilla factory:

- The distribution of errors is not random, the Pauli-errors do not occur with equal likelihood.
- The occurring Pauli errors are not independent. While the process matrix in the gate basis already reveals some coherences, the degree of coherence matrix resolutely rebuts this assumption.

We therefore have to conclude that while it is relatively easy to derive the experimental EPG value for comparison with the Knill threshold, the threshold itself does not apply to the current gates and their intrinsic noise sources in optical quantum computing.

5.4.4 Pathfinding Part II: How to compare to the gremlin threshold

While the comparison of the gate performance to the Knill model is rather straight forward, as it is directly related to the process fidelity, we also noted that the chosen error model is so specific that it is unlikely to apply in general and indeed does not apply for our specific gate. As the gremlin model made absolutely no assumptions on what errors would occur, a comparison to the threshold for this model is very desirable. The model permits any error that can be written as a completely positive process. We can decompose the experimentally determined χ-matrix into the gremlin process and the ideal process, so that

$$\chi_{exp} = p\chi_{gr} + (1-p)\chi_{ideal}. \tag{5.13}$$

To avoid the unhelpful solution that our implemented process is, while sharing some overlap with the desired process, just simply always wrong, we need to describe the action of the gremlin as the kind of action that leads to the observed statistical behaviour, but gives a process with very low overlap with the ideal in the few cases where the gremlin acts. In summary instead of having the gremlin *always* cause a *small* error, we find the situation where the gremlin acts in the *least* amount of cases, but then with the *strongest* possible error. Thus altering the kind of gremlin process so that we minimise p in this equation finds the minimal error probability for the gate, which we will label p^*. A visualisation of this method is given in figure 5.3. By choosing a process for the gremlin process that is as far away from the ideal process as possible, we minimise p, and thus optimise the EPG, as the distance from the ideal process can be linked to the process fidelity, thus the further away two process are in our visuallisation the lower the fidelity between these two processes. The ideal decomposition finding the p^* that minimises the contribution of the gremlin process will thus use the gremlin process that lies on the boundary of the space of completely positive

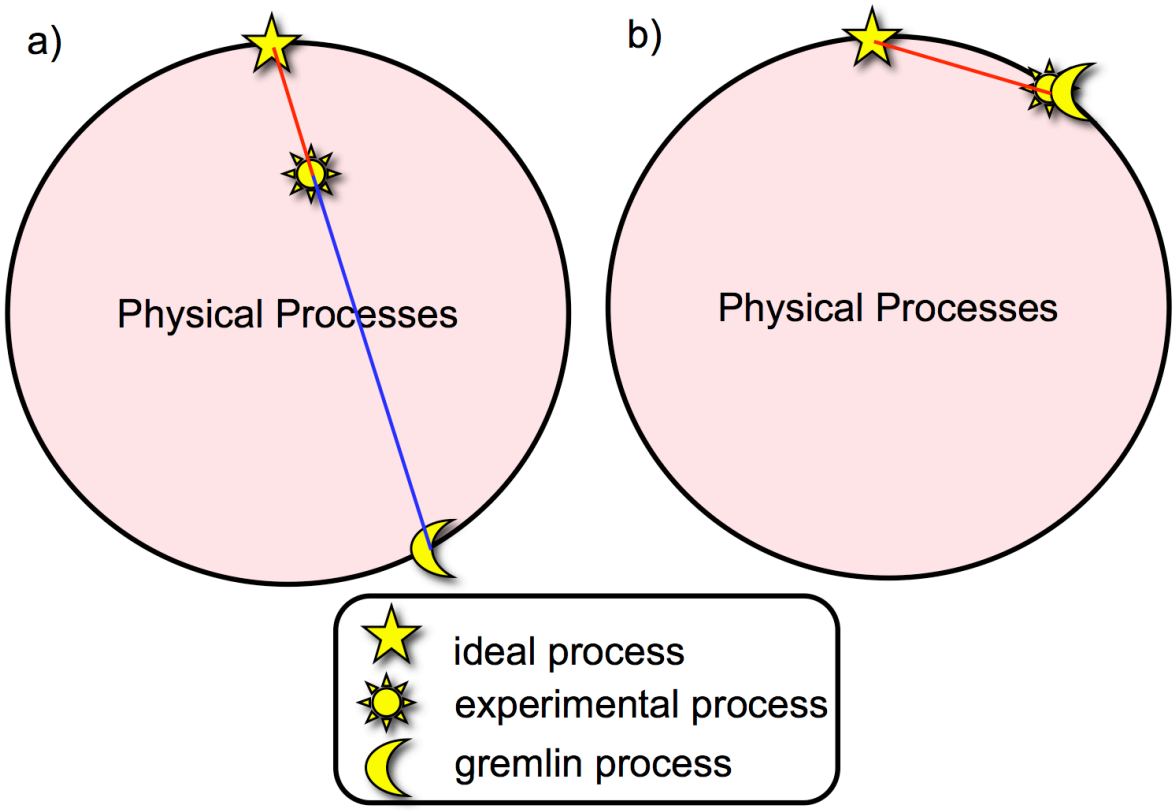


Figure 5.3: Visualisation of the minimisation of the contribution of the gremlin process. All three processes, the ideal, the gremlin and the experimental live necessarily on the space of the physical processes, which is bounded by processes that have at least one zero eigenvalue. Further reduction of this eigenvalue would led to a negative eigenvalue and thus an unphysical process. The ideal process has a zero eigenvalue and thus lies on the boundary. In a) the measured physical process has all eigenvalues larger than zero and lies inside the physical process space, not touching the boundary. By selecting the gremlin process that lies as far away from the ideal process and inline with the experimental and ideal process, the magnitude p of the contribution of this error process is minimised. b) The maximum likelihood reconstruction technique recreates the experimental process inside the space of the physical processes by setting any negative eigenvalues to zero. The processes hence lie on the boundary, and no gremlin processes can be found that lie inline with the ideal and experimental process that is farther away from the ideal than the experimental. Thus the only conclusion would be that the gremlin is always active, meaning the Error probability per gate goes to $p = 1$ and we always implement the wrong process.

processes directly adjacent to the ideal process and inline with the measured experimental process as shown in figure 5.3a)

We thus seek to decompose χ_{exp} into $(1-p)\chi_{\text{ideal}} + p\chi_{\text{gr}}$ where p is the probability of a gremlin reducing the gate to an arbitrary (and possibly adversarial) quantum process χ_{gr}. We want to find the minimum-p, p^*, such that χ_{gr} still represents a physical, trace-preserving process - that is, we require that all eigenvalues are non-negative and that $\text{Tr}_A \chi_{\text{gr}} = I/d$[11]

[11]Remembering from Section 5.3.2 that we want to assume the worst possible case. Hence we are allowing the Gremlin to perform entangling operations and thus use the partial trace here.

The optimisation we need to solve is then the following,

$$\min\ p,\ \text{such that}\ p\chi_{\text{gr}}=\chi_{\text{exp}}-(1-p)\chi_{\text{ideal}}\geq 0 \tag{5.14}$$

Note that since both χ_{exp} and χ_{ideal} represent physical process matrices, the partial-trace condition for χ matrices is automatically satisfied and has been omitted[12]. This optimisation is in the form of a *semidefinite program*, which is a convex optimisation problem, which enjoys several advantages, such as being particularly amenable to numerical solution, and that every local optimum is a global optimum [80].

The *primal* optimisation of eq. 5.14 possesses a *dual* optimisation problem

$$\begin{aligned}\max\ d=&\text{Tr}\chi_{\text{ideal}}Z-\text{Tr}\chi_{\text{exp}}Z,\\ \text{such that}\ Z\geq 0,\ &\text{Tr}\chi_{\text{ideal}}Z=1\end{aligned} \tag{5.15}$$

where the optimisation variable is a Hermitian matrix Z. The primal and dual problems are related by a condition known as weak-duality, which asserts that any solution p of the primal problem is always greater than a solution d of the dual problem, and in particular these sandwich the optimal solutions p^* and d^*: $p \geq p^* \geq d^* \geq d$.

The dual problem can often be used to derive lower bounds on the primal optimum. For instance, the trial solution $Z=\chi_{\text{ideal}}$ is a valid solution, and hence $p^*\geq d=1-F_p$. In general this solution is not optimal so the bound is not saturated, this can be seen by checking the conditions for the primal problem when $p=1-F_p$. The bound *is* saturated if, in the gate basis, the first element of the χ_{exp}, corresponding to F_p, shares no coherences with any other element, making $p^*=1-F_p$ the optimal solution as is the case in Knill's ancilla factory.

While in principle the solution of this optimisation problem is a fast numerical problem, in practise there is a significant difficulty which arises from the way the process matrices are derived from the experimental data. Due to the noise commonly encountered during measurements, the reconstructed processes are typically non-physical. To prevent the reconstruction of such unrealistic processes, a technique called maximum likelihood is employed [29], which finds the closest (thus most likely) *physical*[13] process that would have led the obtained data set. If initially the process would have been unphysical, maximum likelihood will converge on a process that lies on the boundary between the physical and unphysical processes. The boundary has the, in this case unfavourable, attribute that at least one eigenvalue of the process is equal to zero. Conversely, any process that possesses at least one zero eigenvalue exists on the boundary of the space of the completely positive processes and the non-physical processes, as any further decrease of the zero eigenvalue would violate the positiveness and thus place this process outside the space of physical processes. In this case, decomposing the experimental matrix in the ideal and the gremlin matrices no longer yields sensible results, as the $\chi_{gremlin}$ can not be chosen to be more distant to the ideal than the reconstructed χ_{exp} and thus the only way to satisfy the primal condition of equation 5.14 is to let $p = 1$ and thus $\chi_{gremlin} = \chi_{exp}$. This means that we always encode the wrong process, and never the ideal, and that the minimal error per gate probability p^* is bound from above by 1—Clearly not a useful bound.

[12]The sum of two physical processes is necessarily a physical process

[13]Processes are physical if all eigenvalues larger or equal to zero.

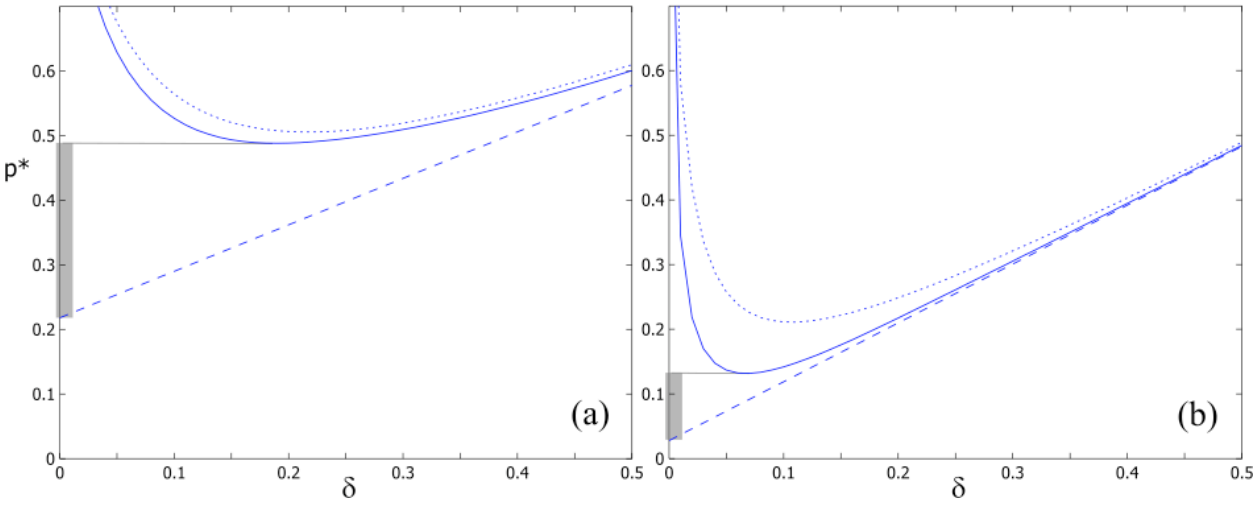


Figure 5.4: Derivation of the upper and lower bounds for the error-probability per gate p^* through the addition of deliberate noise with varying strength δ, so that the reconstructed experimental process, is of the form $(1-\delta)\chi_{\text{exp}}+\delta\chi_{\text{noise}}$. The lower bound (straight dashed line) is $1-F_p$. The dashed curve results from adding depolarising noise, the solid curve from optimising the form of the noise. These curves are upper bounds on the true p^* since we are deliberately adding extra noise to the experiment. a) For the experimentally measured gate shown in Fig. 5.1b),e), the error per gate probability is bound by $21.8\% \leq p^* \leq 48.8\%$. These bounds reduce drastically as shown in b) when assuming true single photon sources as in the modelled gate shown in Fig. 5.1c),f), the bounds improve to $2.8\% \leq p^* \leq 13.2\%$.

To overcome the trivial solutions imposed by the zero eigenvalues in the reconstructed χ matrix, we deliberately add noise to the process. By choosing the noise so that it could be generated and added with high fidelity in the lab, the resulting p^* will be an upper bound for the error probability per gate of our investigated gate, as we could add this noise in practice, and any additional noise will necessarily further dampen the process fidelity with the ideal unless the implemented process was close to orthogonal to the ideal process. We will consider noise generated by the following procedure — with probability δ we replace the gate output with a fixed state. If we use the maximally mixed state, the added noise is depolarising noise, shown as the dashed curve in figure 5.4. In general we will optimise over the fixed state for this noise process χ_{noise}, still leaving the entire optimisation, strength and kind of noise, as well as gremlin process, as a semi-definite program. In figure 5.4 we plot the upper and lower bounds. The lower bound for the process fidelity is shown in the dashed straight line, while the upper bound for the optimised noise is the solid curve. The lowest point of this curve, irrespective of noise strength δ becomes then the upper bound for our experimental EPG. Figure 5.4a) shows these bounds for the experimental state derived in Chapter 4, finding the EPG bound by $21.8\% \leqslant p^* \leqslant 48.8\%$ (shaded region on the side of the graph). Obviously the upper bound of the EPG is significantly worse than the $1 - F_p$ our lower bound. Paired with the much tighter threshold value of $p_{th} = 2.73 \times 10^{-5}$ the hopes of fault tolerance in the near future seem relinquished. Applying the same methodology as above to our model described in the previous chapter and again hoping for the timely

development of single photon sources, we find the bounds for the error probability for the modelled gate. The corresponding graph is shown in figure 5.4b). We find that the EPG is now bound much tighter with $2.8\% \leqslant p^* \leqslant 13.2\%$ and also note that we have to add much less noise to find the upper bound. Again the upper bound is still outside the threshold value derived by Knill. We note though that the bound has become much tighter, spanning only 10.4% compared to the 27.0% for the experiment. Also the fact that we have to add noise to find sensible bounds indicates that the real bounds might be much lower, if the reconstructed states would not commonly be reconstructed on the boundary. One technique that might circumvent this is based on Bayesian analysis. However, this technique is not yet in widespread use [81]. Nevertheless our procedure described here allows the direct estimation of the gate errors for any given experimental gate, irrespective of its architecture. We expect a much tighter upper bound if the problem of zero eigenvalues can be solved. Together with the architecture-dependent modelling introduced in the last chapter, we expect this technique to become of major importance in identifying required technological improvements en route to quantum computing with any architecture. Furthermore it allows direct comparison to the fault tolerance thresholds, and thus closes this gap between experimental and theoretical work in this field.

5.5 Summary of this chapter

- We have discussed two different thresholds for fault tolerant quantum computing and developed tools that allow the comparison of experimental gates to these thresholds.
- Error probabilities per gate for modern optical gates are many standard deviations away from the fault tolerance thresholds.
- Making use of our model developed in Chapter 4, we infer that alleviation of the multi-pair emission problem will render optical quantum computing within striking distance of the fault-tolerance threshold as derived by Knill.
- The ramification of current source problems and the application of high precision optics would lead to mode mismatch becoming the leading error source. As mode mismatch causes random and uncorrelated errors, the Knill threshold would apply. Specifically such gates are already today within reach of this fault tolerance threshold, albeit right near the limit, requiring by far more resources than readily available.

6
Tackling Shor's algorithm

In this chapter the gates developed during chapters 3 and 4, paired with the understanding that we gained from our model developed in chapter 4 about how different error sources affect the gate, allowed us to complete a successful implementation of the three qubit gate we initially attempted in chapter 4. Such a gate allows us to implement a proof-of-principle implementations of Shor's algorithm [2] to factor the smallest non-trivial number: 15. Further this experiment was made possible by the discovery of compiling techniques, which reduce the number of required qubits. Thus we were able to evaluate the order finding routine, which is at the heart of Shor's factoring algorithm with two different co-primes 2 and 4, with two two-qubit gates and one three qubit gate respectively. While we achieve near ideal algorithm performance (fidelity of the output state with the expected output state), a closer analyses of the states during the computation indicates lower performance values.

The experimental implementation was conducted by Marco Babieri, Nathan Langford, Ben Lanyon and myself (in alphabetical order), while data analyses was conducted by Nathan Langford and Ben Lanyon. The original idea for the compilation steps stemmed from Prof. Daniel James (University of Toronto) and was further developed by Marco Barbieri, Alexei Gilchrist and Andrew White. Simultaneous with our publication a group from Hefei, China independently implemented the three qubit circuit [82] as well. Both papers have been published back to back in Physical Review Letters.

6.1 Shor's algorithm, the (not so) basics

One of the most intriguing attributes of a functioning quantum computer is the capability of executing Shor's factoring algorithm, which allows the breaking of a number of widely used classic encryption codes. These codes in general rely on what is known as a trap door function, that is a function that is easily executed in one direction, but difficult to reverse. In this case the function is multiplying and factoring of numbers. While it is relatively easy to

multiply two numbers, even if they are very large, finding the two prime factors to a number is very difficult. In fact, factorising a number into its prime factors is exponentially difficult on a conventional classic computer, meaning that the number of computational steps to solve the problem scales exponentially with the bit length of the input value. This means that with a modest increase in bit length the time to decipher a code increases exponentially. This feature guarantees the pseudo-security of the standard encryption protocols used in every day live, i.e. for internet banking, as when ever the computing power of classical computers is increased, reducing the time to break the encryption, the strength of the encryption can be increased by a manifold with the same increased computing power. While it is not proven that factoring is necessarily exponentially difficult with classical algorithms, extensive efforts to find an algorithm scaling polynomial in the input bit length have failed and thus such an algorithm is now believed to not exist.

Utilising the weirdness of quantum mechanics, namely the capability of entangling the individual qubits gave rise to what is now known as Shor's algorithm. By entangling the qubits, one can effectively query all possible solutions of the factoring problem simultaneously and at the end of the routine use the interference of the phases of the qubit to cancel out everything but the one solution and it's multiples. The algorithm consists of multiple computational steps, but only one of them requires the aid of quantum computing to gain the computational advantage. The required quantum routine in Shor's algorithm consists of three parts: the circuit initialisation, modular exponentiation and the inverse quantum Fourier transform (QFT). The qubits utilised during the computation are split into two groups, the argument and the function register. During the initialisation state the argument register is placed into an equal superposition of all possible states, which requires a single qubit Hadamard-gate to be applied to each qubit, in linear optical quantum computing this is simply a waveplate as mentioned in section 1.5.2. The function register is then initialised in the $|1\rangle_f$ state. This means that all qubits are set to their logic $|0\rangle$ value, except for the last qubit, which is set to $|1\rangle$. After the initialisation, the argument and function register are entangled via subsequent application of the unitary action of the modular exponentiation function, U, transforming our input state

$$|\psi\rangle_{in} = \sum_{x=0}^{2n-1} |x\rangle_a |0\rangle_f^{\otimes m-1} |1\rangle_f \text{ , to} \tag{6.1}$$

$$U|\psi\rangle = \sum_{x=0}^{2n-1} |x\rangle_a |C^x \mathrm{mod} N\rangle_f. \tag{6.2}$$

Here C is a co-prime to N the number we are seeking to factor. After creation of this complex state, a inverse quantum Fourier transform is performed on the argument register followed by measurement of the argument register, which effectively identifies the periodicity of the function, thus revealing the order r, satisfying

$$C^r \mathrm{mod} N = 1, \tag{6.3}$$

which allows us to find the prime factors of N as the greatest common (non-trivial) divisors of N and $C^{r/2} \pm 1$. Details on the Quantum Fourier Transform and the modular exponentiation can be found in Ref. [22].

Like all algorithms, the required resources scale with the size of the input problem, and Shor's algorithm is no exception. Implementation of all steps of Shor's algorithm to factor a number N which is k-bits long when expressed in binary, requires $72k^3$ elementary gates acting on $5K + 1$ qubits [83]. The first meaningful number that can be factored with Shor's algorithm is 15, as it is the first number where its prime factors do not include the trivial solution 1. As 4 bits are required to encode the number 15, this would mean 4608 gate operations acting on 21 different qubits to implement the smallest *general* version of Shor's algorithm. As all quantum computing architectures are currently limited to only a few gates, and trapped ion quantum computation has achieved the largest entangled state at 8 qubits [84], 4608 gate operations as well as control over 21 qubits are still well beyond the grasp of experimental quantum computing.

The resource blow-out is, in part, caused by the fact that the modular exponentiation function depends on the number to be factored and the chosen co-prime C. To have a circuit that can thus accommodate this step for any given choice of values for C and N up to the maximum bit-length that can be encoded, then the circuit needs to be extremely flexible and thus much more complex than strictly necessary for an specific individual set of C and N. Thankfully ref. [83] not only derives this dooming resource demand, but also indicates a way of circumventing it, while not compromising the validity of the results, nor requiring any knowledge not usually available when tackling a factoring problem. It uses the publicly known number N that we are desiring to factor and the chosen co-prime to reduce the demands on both the available qubit number and gate operations by compiling the circuit, so that only the essential operations are conducted. This kind of compiling is essential to reduce the resources to a level that allows a proof-of-principal experiment and even then limits us to the simplest cases. The only demonstration of Shor's algorithm so far was demonstrated in a nuclear magnetic resonance (NMR) experiment [85]. There is a significant shadow of doubt over this implementation due to the NMR technique being incapable of preparing pure states [86] and the fact that the dynamics can be modelled classically [87]. This means that the entanglement at the core of the algorithm can not be implemented in NMR.

In the paper at the end of this chapter, we present two different implementations of Shor's algorithm using different levels of compiling. Both versions allow us to factor $N = 15$, and implement the only two relevant co-primes $C = 4$ and $C = 2$ for the choice of $N = 15$.

6.1.1 Compiling the circuit for $C = 4$

To determine the minimum size of our argument register, we need to identify the maximum value of x in our function $y(x) = C^x \mathrm{mod} N$. Equally, the maximum value of $y(x)$ determines the required size of our function register. A further requirement for the argument register is determined by the QFT. To find the periodicity of a function with certainty, we need to observe a minimum of two full periods. For the specific choice at hand ($C = 4, N = 15$), we

thus evaluate the function and find

$$\begin{aligned} y(0) &= 4^0 \text{mod} 15 = 1, \\ y(1) &= 4^1 \text{mod} 15 = 4, \\ y(2) &= 4^2 \text{mod} 15 = 1, \\ y(3) &= 4^3 \text{mod} 15 = 4. \end{aligned} \tag{6.4}$$

By inspection we see that our argument register needs to be able to count up to 3, requires two bits ($0 \rightarrow 00$, $1 \rightarrow 01$, $2 \rightarrow 10$, $3 \rightarrow 11$), while our function register needs to be able to count up to four, which requires three bits ($0 \rightarrow 000$, $1 \rightarrow 001$, $2 \rightarrow 010$, $3 \rightarrow 011, 4 \rightarrow 100$). While experiments with gates between five photonic qubits have been demonstrated and up to six qubits have been demonstrated [88], the difficulty of generating, controlling and measuring five single photons is orders of magnitude harder than four photons, mainly due to the statistical nature and low efficiency of PDC as our photon source. Noticing that our function register only encodes two different values, 1 and 4, and that the binary codes for these numbers equal 001 and 100, we realise that no information is encoded to the central bit, which makes it redundant, allowing us to reduce the number of required qubits to four, two in the argument and two in the function. To identify the suitable circuit for the modular exponentiation, we inspect the desired state prior to the QFT and compare it to our input state.

As mentioned previously, the circuit initialisation leaves the argument register in a superposition of all possible values, while the function register is encoding the value 1. Thus our state prior to the modular exponentiation is

$$|\psi\rangle_{in} = (|00\rangle_a + |01\rangle_a + |10\rangle_a + |11\rangle_a)|01\rangle_f, \tag{6.5}$$

where we have omitted the central (qu-)bit and also omitted normalisation as by convention. The state before the QFT should replicate the values of our argument and function register from equations 6.4, and thus should be

$$|\psi\rangle_{out} = |00\rangle_a|01\rangle_f + |01\rangle_a|10\rangle_f + |10\rangle_a|01\rangle_f + |11\rangle_a|10\rangle_f. \tag{6.6}$$

A quick inspection of the input and output state reveals the required logic operations to be two controlled-NOT operations, which are triggered when the second qubit in the argument register assumes the value 1.This converts the function register from the initial $|01\rangle_f$ state to the desired output state $|10\rangle_f$. It now becomes clear that if we had used the three qubit set to encode our function register that the state of the omitted central qubit would not be affected at any stage during the routine, as the final QFT acts solely on the argument register. Similarly the first qubit of the argument register never interacts, except for a swap gate with the second argument register qubit at the end of the circuit. This swap is implemented as a simple relabelling of the respective argument qubits in the circuit diagrams. However, as we generate four photons through the two PDC processes experimentally, we use the fourth photon as a trigger signal for the logic operation. This trigger photon, which never interacts with any other photon can be viewed as the unaltered first qubit of the argument register. practically this trigger photon improves the gate performance as it eliminates multi-photon events where two pairs are created in the direction that contributes two gate inputs.

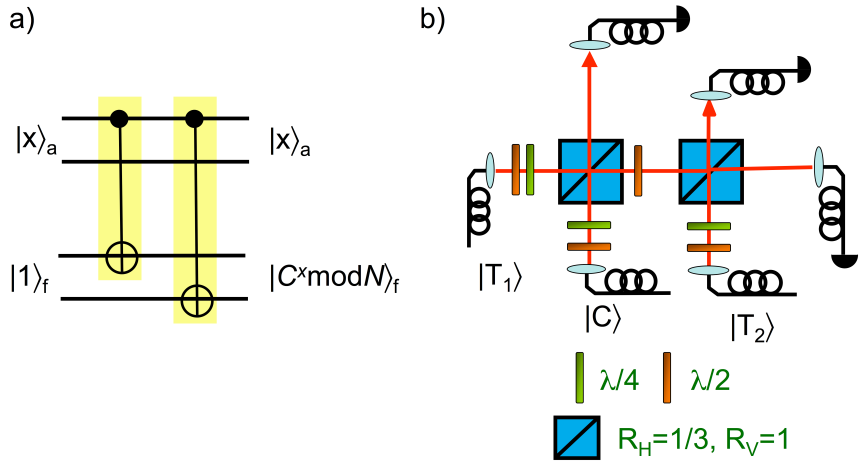


Figure 6.1: a) Required logic circuitry and b) experimental implementation of the modular exponentiation in Shor's algorithm with $C = 4$ and $N = 15$. We have included the swap gate between the argument register qubits, making the upper qubit the second qubit in the equations 6.5,6.6. Only the second (upper) qubit in the argument register triggers logic operations on the function register, namely a controlled-NOT operations on both of the function qubits. Technically the function register consists of three qubits, but as the state of the middle qubit is never affected and thus always zero, it is replaced with a virtual qubit and omitted here. The experimental implementation uses the simplified concatenated gate introduced in chapter 4. The mode labels C and T identify the logic qubits for the CNOT operation, where C is the control, thus the argument qubit, with the two target qubits (T) being the function register. On all outputs we have a complete polarisation analyser (not shown) consisting of a $\lambda/4$ and $\lambda/2$ waveplate and a polarising beamsplitter that allows us to perform full tomographic characterisation of the states.

Without the trigger detection of the second down-conversion direction, this process, that is just as probable as the desired one pair in each direction event, could generate a threefold coincidence event after the gate that could not be differentiated from the desired gate action. Hence the detection of the fourth photon lowers our count rates due to the non unit collection and detection efficiency but improves the gate performance as it allows the discrimination of some undesired multi-photon events. If one wanted to encode all five qubits, the omitted central function register qubit could be implemented by a classical laser beam with fixed polarisation and since it is never interacts will always yield the initial value, which is $|0\rangle$. The required logic gate structure and its physical implementation are shown in figure 6.1 or in the copy of the published paper at the end of this chapter as figure 1d) as part of the more detailed logic evolution to which the reader is also referred to at this point.

6.1.2 Compiling the circuit for $C = 2$

When we chose the co-prime $C = 2$ to factor 15, our function values change likely meaning that we will need a different range for our argument. Thus evaluating the function $y(x) =$

$C^x \mathrm{mod} N$ again until we observe two full periods, we find

$$\begin{aligned} y(0) &= 2^0 \mathrm{mod} 15 = 1, \\ y(1) &= 2^1 \mathrm{mod} 15 = 2, \\ y(2) &= 2^2 \mathrm{mod} 15 = 4, \\ y(3) &= 2^3 \mathrm{mod} 15 = 8, \\ y(4) &= 2^4 \mathrm{mod} 15 = 1, \\ y(5) &= 2^5 \mathrm{mod} 15 = 2, \\ y(6) &= 2^6 \mathrm{mod} 15 = 4, \\ y(7) &= 2^7 \mathrm{mod} 15 = 8. \end{aligned} \tag{6.7}$$

From inspection we see that we need both a larger function and argument register, as we will need to encode up to the values of seven and eight respectively. This would require three and four qubits each—a total of 7 qubits. As discussed earlier in this chapter such a number of photons is unfeasible with current technology. We again inspect the input and output states to identify redundant bits to reduce the number of actually required photons. The input state is thus

$$|\psi\rangle_{in} = (|000\rangle_a + |001\rangle_a + |010\rangle_a + |011\rangle_a + |100\rangle_a + |101\rangle_a + |110\rangle_a + |111\rangle_a)|0001\rangle_f, \tag{6.8}$$

while our desired output state is going to be

$$\begin{aligned} |\psi\rangle_{out} = {} & |000\rangle_a|0001\rangle_f + |001\rangle_a|0010\rangle_f + |010\rangle_a|0100\rangle_f + |011\rangle_a|1000\rangle_f + \\ & |100\rangle_a|0001\rangle_f + |101\rangle_a|0010\rangle_f + |110\rangle_a|0100\rangle_f + |111\rangle_a|1000\rangle_f. \end{aligned} \tag{6.9}$$

This time there are no redundant bits and the required logic also appears to be significantly more difficult due to the extended length of the period. To reduce the resource requirements we realise that instead of evaluating the function $y(x) = C^x \mathrm{mod} N$, we can evaluate $y(x) = \log_C(C^x \mathrm{mod} N)$ As we use the value of the co-prime as the basis for the logarithmic function, this does not alter the periodicity of the function, which is the essential piece of information that is being computed. The required values for this function then become

$$\begin{aligned} y(0) &= \log_2(2^0 \mathrm{mod} 15) = 0, \\ y(1) &= \log_2(2^1 \mathrm{mod} 15) = 1, \\ y(2) &= \log_2(2^2 \mathrm{mod} 15) = 2, \\ y(3) &= \log_2(2^3 \mathrm{mod} 15) = 3, \\ y(4) &= \log_2(2^4 \mathrm{mod} 15) = 0, \\ y(5) &= \log_2(2^5 \mathrm{mod} 15) = 1, \\ y(6) &= \log_2(2^6 \mathrm{mod} 15) = 2, \\ y(7) &= \log_2(2^7 \mathrm{mod} 15) = 3, \end{aligned} \tag{6.10}$$

which reduces our function register size from four down to two bits. We again look at the output state and see that

$$\begin{aligned} |\psi\rangle_{out} = {} & |000\rangle_a|00\rangle_f + |001\rangle_a|01\rangle_f + |010\rangle_a|10\rangle_f + |011\rangle_a|11\rangle_f + \\ & |100\rangle_a|00\rangle_f + |101\rangle_a|01\rangle_f + |110\rangle_a|10\rangle_f + |111\rangle_a|11\rangle_f. \end{aligned} \tag{6.11}$$

Comparing this with the reduced input state (using $|01\rangle_f$ rather than $|0001\rangle_f$) we can see that we need to switch the value of the first qubit in the function register (counting left to right) when the second qubit in the argument register assumes the value 1, and the last qubit in the function register needs to be switched whenever the last qubit in the argument register is of value 0. This is the inverse of the common CNOT logic. We can always flip the value of the last qubit of the function register prior to any gates, which allows us then to use the conventional CNOT logic, flipping the state of the target qubit whenever the control is in the logic 1 state. Either way, we see that the state of the first qubit in the argument register does not alter the required logic and thus does not need to be encoded and measured here. All these measures combined allow us to reduce the required number of qubits from seven down to the much more feasible four. The logic gate is shown schematically in figure 6.2 and in the paper in figure 1g), and the details and results of the experimental implementation are given in the copy of the published paper at the end of this chapter.

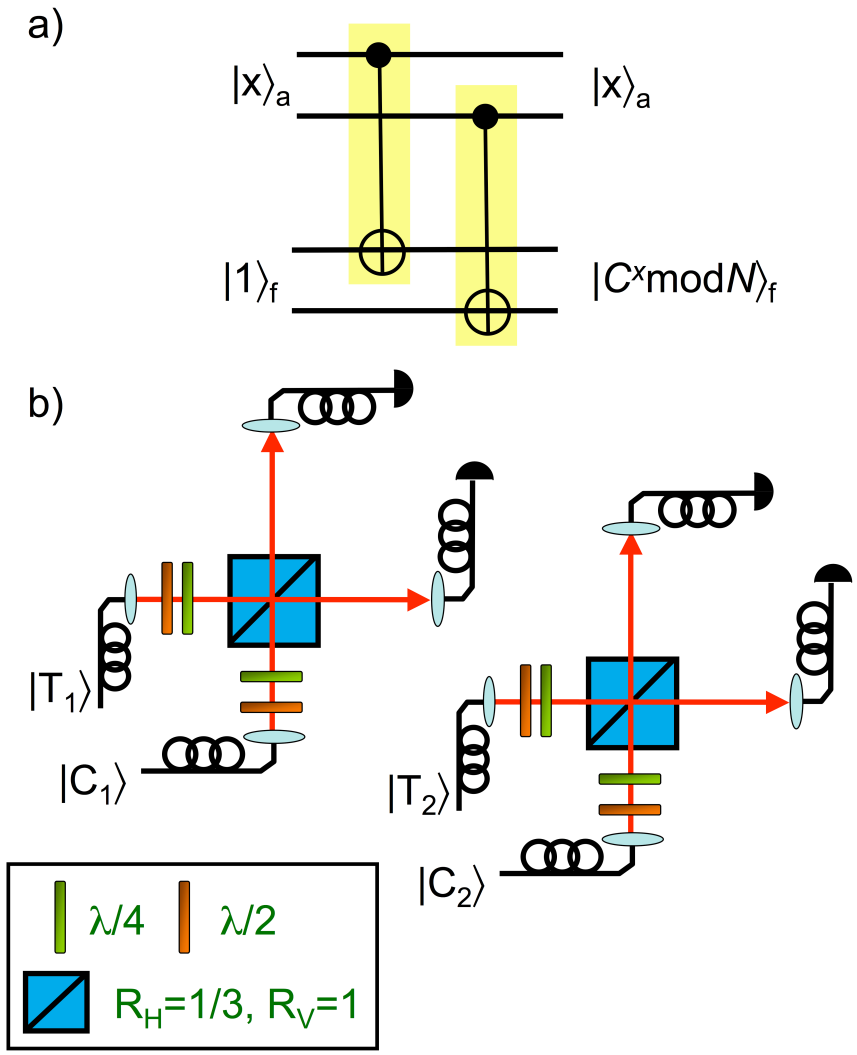


FIGURE 6.2: a) Required logic circuitry and b) experimental implementation for Shor's algorithm with $C = 2$ and $N = 15$ when encoding the function $y(x) = \log_C(C^x \mathrm{mod} N)$. We need two separate CNOT-gates, one between the first argument (C_1) qubit and the first function (T_1) qubit, while the second gate acts between the second qubits of the individual registers. Experimentally, despite this requiring four qubits, we only need non-classical interference between two sets of two qubits. As this can be realised as two CNOT gates between photons from dependent pairs, this is a much easier circuit to achieve high performance in than the $C = 4, N = 15$ case, that required non-classical interference between independently generated photons. All outputs have a complete polarisation analyser (not shown) consisting of a $\lambda/4$ and a $\lambda/2$ waveplate and a polarising beamsplitter allowing full tomographic characterisation of the states.

6.1.3 A note on scalability

The inclined reader will have noticed that the compilation techniques used require the user to know exactly which number he wishes to factor, and then has to devise the appropriate encoding technique and ultimately the appropriate circuit. Hence as it is presented here, this implementation of Shor's algorithm can be seen as an island solution. To be able to build a circuit that can encode all possible numbers in the register, requires many more qubits and many, many more gates than is currently feasible (See the intro of the paper for references). The experiment demonstrated here should be taken as a proof of the functionality of Shor's algorithm and the compilation technique.

6.2 Reprise: Building 3 qubit gates, the right way

Our inspection of the requirements for implementing Shor's algorithm revealed that we will need at least one three qubit gate. As our initial attempt of building such a three qubit gate produced low fidelity results, Shor's Algorithm is going to remain very challenging. The initial failure to produce a high fidelity three-qubit gate led to our investigation of the independent photon gate as a subpart of this gate (Chapter 4). We realised, with assistance from our model, that the main source of gate degradation was the emission of additional pairs of photons into the collected spatio-temporal modes. We also discussed in section 2.1.2 that the efficiency of generating one pair scales linearly with the power, while generating two pairs is quadratic in the pump power. We use equation 4.1 describing parametric down-conversion, but instead of the interaction Hamiltonian given in eq. 4.2 we utilise the interaction Hamiltonian describing only a single down-converter.

$$\mathbf{H} = A_f \mathbf{f1}^\dagger \mathbf{f2}^\dagger \mathbf{p}_f. \tag{6.12}$$

Using the Taylor expansion up to the third order, we find

$$\big|\psi(t)\big\rangle = 1 + \frac{it}{\hbar}\big(A_f \mathbf{f1}^\dagger \mathbf{f2}^\dagger \mathbf{p}_f + A_f^2 \mathbf{f1}^{\dagger 2} \mathbf{f2}^{\dagger 2} \mathbf{p}_f^2/2 + A_f^3 \mathbf{f1}^{\dagger 3} \mathbf{f2}^{\dagger 3} \mathbf{p}_f^3/6 + ...\big)\big|\psi(0)\big\rangle. \tag{6.13}$$

We can see that the ratio between the adjacent orders of simultaneous down-conversion events is proportional to the amplitude A_f of the down conversion, which in turn is proportional to the pump power. We can therefore influence the ratio of single pair emission to multi-pair emission by reducing the pump power. Usually the aim in most multi-photon experiments is to increase and maximise the power with which one pumps the PDC process, in order to maximise the number of available pairs per second, and thereby speed up experiments. However, we realise through these results, that such action leads to degradation of the gate performance due to the increased rate of multi-photon events. In order to reduce the impact of the multi-photon pair emission and thus make our three qubit gate for Shor's algorithm feasible, we reduce the pump power and accept the resulting longer acquisition time.

6.3 Experimental demonstration of Shor's algorithm with quantum entanglement

6.3.1 Unpublished results

Section 6.3.3 provides the paper published in Physics Review Letters and therein contains details and results of the experiment. It is followed by the additional online material which offers a detailed discussion why the QFT can be omitted in the cases we implemented. While not noted above, the circuit for $C = 4$, $N = 15$ can be further compiled by applying the same further encoding of the function as utilised in the $C = 2$ case ($y(x) = \log_C(C^x \mathrm{mod} N)$). This is shown in the paper in figure 1f), but is not discussed there. Analysis of the results leads again to perfect results for the algorithm within the error margin, as this reduces the circuit to a single CNOT gate. Through the reduction of the pump power we managed to achieve a tangle of $90.6 \pm 0.8\%$, which is the highest tangle created through a gate in linear optical quantum computing. The density matrix of the state is shown in figure 6.4, fidelity with the $|\phi^+\rangle$ state, which is the ideal output state is $F = 96.4 \pm 0.2\%$. We repeated this measurement of this specific state while varying the pump power to verify the influence of the multi-photon emission events, and found a clear dependence of all measures of the gate performance (Fidelity with the $|\phi^+\rangle$ state, Tangle, Purity and Linear entropy) on the pump power, and thus the higher order photon emission. These results are shown in figure 6.3 and summarised in Table 6.3.1. It is noteworthy that some measures are far more sensitive than others, and could be used as (more suitable) indicators for the gate performance, however a conclusive investigation of this behaviour is currently still in progress.

P_{pump}	Fidelity %	Tangle %	Purity %	Linear Entropy
500mW	89.9 ± 0.3	72.0 ± 1.2	82.0 ± 0.4	23.6 ± 0.6
300mW	94.2 ± 0.2	83.4 ± 0.9	89.8 ± 0.3	13.6 ± 0.4
150mW	95.7 ± 0.1	89.4 ± 0.5	92.7 ± 0.2	9.8 ± 0.2
75mW	96.4 ± 0.2	90.6 ± 0.8	93.9 ± 0.3	8.2 ± 0.4

Table 6.1: Measures of the state quality obtained with different pump powers while running the reduced encoding of $C = 4$. Clearly all measures improve as we turn down the pump power and thus reduce the ratio of multi-pair to single-pair emission in our PDC-source.

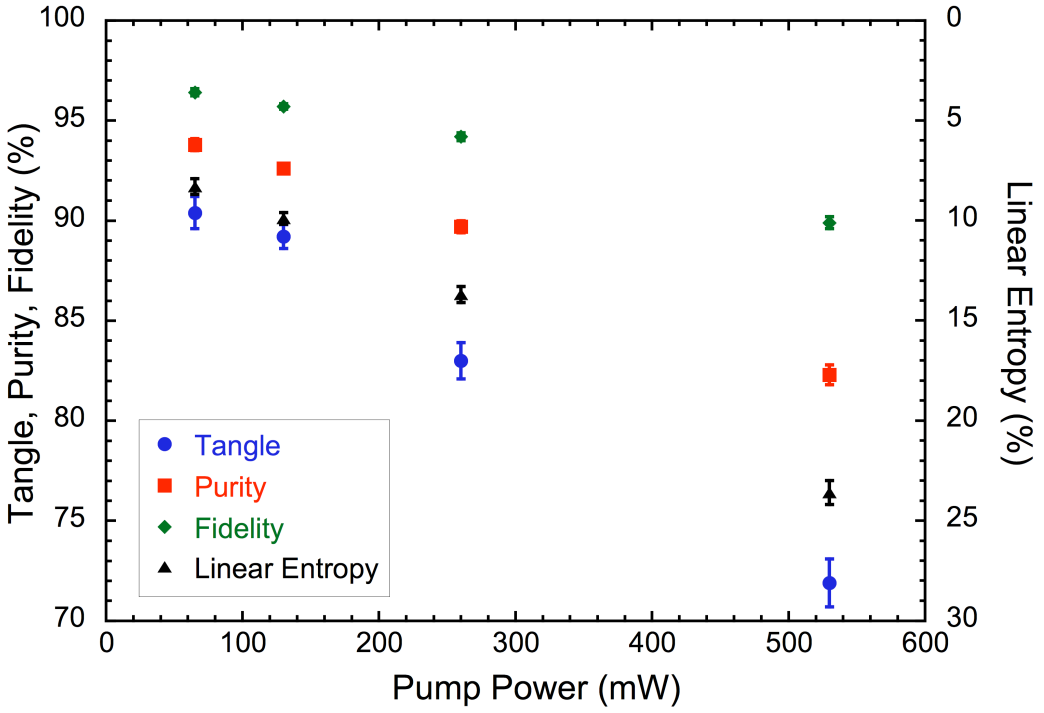


Figure 6.3: Summary of measures of the entangled state from the reduced period 2 encoding of Shor's algorithm for varying pump power. Tangle is the most sensitive of all measures, dropping by 18% when the pump power is decreased from 500mW@410nm to 75mW. The fidelity of the state with the ideal expected output state increases by 6.5% for the same range of pump powers. While these results verify the significance of multi-photon emission as a dominant error source, it also highlights the insensitivity of the fidelity measure to the performance of the gate. Tangle provides a by far more sensitve measure for entangled states. Error bars are derived through Monte Carlo simulations on the state reconstruction, and are smaller than the symbol size where not shown.

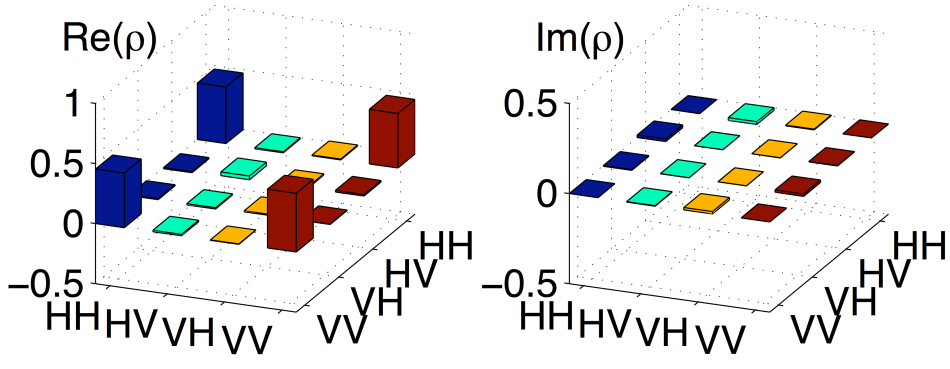


Figure 6.4: Density matrix for the algorithm output for reduced encoding for the $C = 4$ case (qubit 1= argument register, qubit 2= function register). Fidelity with the ideal output state ($|\phi^+\rangle$) is $96.4 \pm 0.2\%$ while the Tangle reaches a record high $90.6 \pm 0.8\%$ for entanglement created in an optical gate.

6.3.2 Conclusions from this experiment

- Full implementation of Shor's algorithm *without* adaptations of the circuit based on the to be factored number N and the chosen co-prime C are still infeasible.
- Use of these known quantities (C, N) for a specific problem leads to several compiling steps which can reduce the circuit complexity.
- Here we demonstrate two different compiled circuits, one for $C = 2$ and one for $C = 4$, both for $N = 15$.
- We find near perfect algorithmic performance, even though the required entangled states are non-ideal (Fidelity with a GHZ-state is as low as 59% in $C = 4, N = 15$ case.
- We verify experimentally the significance of multi-photon emission as a significant source of gate performance degradation.

6.3.3 The paper — Experimental demonstration of Shor's algorithm with quantum entanglement

PRL 99, 250505 (2007) PHYSICAL REVIEW LETTERS week ending 21 DECEMBER 2007

Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement

B. P. Lanyon,[1] T. J. Weinhold,[1] N. K. Langford,[1] M. Barbieri,[1] D. F. V. James,[2] A. Gilchrist,[1] and A. G. White[1]
[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane QLD 4072, Australia*
[2]*Department of Physics and Center for Quantum Information and Quantum Control, University of Toronto, Toronto ON M5S1A7, Canada*
(Received 18 May 2007; published 19 December 2007)

Shor's powerful quantum algorithm for factoring represents a major challenge in quantum computation. Here, we implement a compiled version in a photonic system. For the first time, we demonstrate the core processes, coherent control, and resultant entangled states required in a full-scale implementation. These are necessary steps on the path towards scalable quantum computing. Our results highlight that the algorithm performance is not the same as that of the underlying quantum circuit and stress the importance of developing techniques for characterizing quantum algorithms.

DOI: 10.1103/PhysRevLett.99.250505 PACS numbers: 03.67.Lx, 03.67.−a, 03.67.Mn, 42.50.Dv

As computing technology rapidly approaches the nanoscale, fundamental quantum effects threaten to introduce an inherent and unavoidable source of noise. An alternative approach embraces quantum effects for computation. Algorithms based on quantum mechanics allow tasks impossible with current computers, notably an exponential speedup in solving problems such as factoring [1]. Many current cryptographic protocols rely on the computational difficulty of finding the prime factors of a large number: a small increase in the size of the number leads to an exponential increase in computational resources. Shor's quantum algorithm for factoring composite numbers faces no such limitation, and its realization represents a major challenge in quantum computation.

To date, there have been demonstrations of entangling quantum-logic gates in a range of physical architectures, ranging from trapped ions [2,3], to superconducting circuits [4], to single photons [5–12]. Photon polarization experiences essentially zero decoherence in free space; uniquely, photonic gates have been fully characterized [6], produced the highest entanglement [8], and are the fastest of any architecture [11]. The combination of long decoherence time and fast gate speeds make photonic architectures a promising approach for quantum computation, where large numbers of gates will need to be executed within the coherence time of the qubits.

Shor's algorithm can factor a k-bit number using $72k^3$ elementary quantum gates; e.g., factoring the smallest meaningful number, 15, requires 4608 gates operating on 21 qubits [13]. Recognizing this is well beyond the reach of current technology, Ref. [13] introduced a compiling technique which exploits properties of the number to be factored, allowing exploration of Shor's algorithm with a vastly reduced number of resources. Although the implementation of these compiled algorithms does not directly imply scalability, it does allow the characterization of core processes required in a full-scale implementation of Shor's algorithm. Demonstration of these processes is a necessary step on the path towards scalable quantum computing. These processes include the ability to generate entanglement between qubits by coherent application of a series of quantum gates. In the only demonstration to date, a compiled set of gate operations were implemented in a liquid NMR architecture [14]. However, since the qubits are at all times in a highly mixed state [15], and the dynamics can be fully modeled classically [16], neither the entanglement nor the coherent control at the core of Shor's algorithm can be implemented or verified.

Here, we implement a compiled version of Shor's algorithm, using photonic quantum-logic gates to realize the necessary processes, and verify the resulting entanglement via quantum state and process tomography [17,18]. We use a linear-optical architecture where the required nonlinearity is induced by measurement; current experiments are not scalable, but there are clear paths to a fully scalable quantum architecture [19,20]. Our gates do not require preexisting entanglement, and we encode our qubits into the polarization of up to four photons. Our results highlight that the performance of a quantum algorithm is not the same as performance of the underlying quantum circuit and stress the importance of developing techniques for characterizing quantum algorithms.

Only one step of Shor's algorithm to find the factors of a number N requires a quantum routine. Given a randomly chosen co-prime C (where $1 < C < N$ and the greatest common divisor of C and N is 1), the quantum routine finds the *order* of C modulo N, defined to be the minimum integer r that satisfies $C^r \bmod N = 1$. It is straightforward to find the factors from the order. Consider $N = 15$: if we choose $C = 2$, the quantum routine finds $r = 4$, and the prime factors are given by the nontrivial greatest common divisor of $C^r/2 \pm 1$ and N, i.e., 3 and 5; similarly, if we choose the next possible co-prime, $C = 4$, we find the order $r = 2$, yielding the same factors.

Figure 1(a) shows a conceptual circuit of the quantum order-finding routine. It consists of three distinct

PRL 99, 250505 (2007) PHYSICAL REVIEW LETTERS week ending 21 DECEMBER 2007

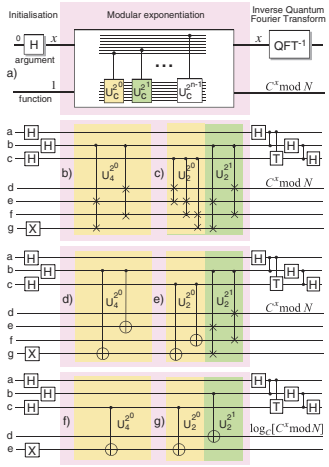


FIG. 1 (color online). (a) Conceptual circuit for the order-finding routine of Shor's algorithm for number N and co-prime C [13]. The argument and function registers are bundles of n and m qubits; the nested order-finding structure uses $U|y\rangle = |Cy \bmod N\rangle$, where the initial function-register state is $|y\rangle = 1$. The algorithm is completed by logical measurement of the argument register, and reversing the order of the argument qubits. (b,c) Implementation of (a) for $N = 15$ and $C = 4$, 2, respectively; the unitaries are decomposed into controlled-swap gates (CSWAP), marked as X; controlled-phase gates are marked by dots; H and T represent Hadamard and $\pi/8$ gates. Many gates are redundant, e.g., the second gate in (b), the first and second gates in (c). (d,e) Partially-compiled circuits of (b,c), replacing CSWAP by controlled-not gates. n.b. (e) is equivalent to the $N = 15$ $C = 7$ circuit in Ref. [14]. (f,g) Fully-compiled circuits of (d,e), by evaluating $\log_C[C^x \bmod N]$ in the function-register.

steps: (i) *register initialization*, $|0\rangle^{\otimes n}|0\rangle^{\otimes m} \rightarrow (|0\rangle + |1\rangle)^{\otimes n}|0\rangle^{\otimes m-1}|1\rangle = \sum_{x=0}^{2^n-1} |x\rangle|0\rangle^{\otimes m-1}|1\rangle$, where the argument-register is prepared in an equal coherent superposition of all possible arguments (normalization omitted by convention); (ii) *modular exponentiation*, which by controlled application of the order-finding function produces the entangled state $\sum_{x=0}^{2^n-1} |x\rangle|C^x \bmod N\rangle$; (iii) the *inverse Quantum Fourier Transform* (QFT) followed by measurement of the argument-register in the logical basis, which with high probability extracts the order r after further classical processing. If the routine is standalone, the inverse QFT can be performed using an approach based on local measurement and feedforward [21]. Note that the inverse QFT in [14] was unnecessary: it is straightforward to show this is true for any order-2^l circuit [22].

Modular exponentiation is the most computationally intensive part of the algorithm [13]. It can be realized by a cascade of controlled unitary operations, U, as shown in the nested inset of Fig. 1(a). It is clear that the registers become highly entangled with each other: since U is a function of C and N, the entangling operation is unique to each problem. Here, we choose to factor 15 with the first two co-primes, $C = 2$ and $C = 4$. In these cases, entire sets of gates are redundant: specifically, $U^{2^n} = I$ when $n > 0$ for $C = 4$, and $U^{2^n} = I$ when $n > 1$ for $C = 2$. Figures 1(b) and 1(c) show the remaining gates for $C = 4$ and $C = 2$, respectively, after decomposition of the unitaries into controlled-swap gates—this level of compiling is equivalent to that introduced in Ref. [14]. Further compilation can always be made since the initial state of the function-register is fixed, allowing the CSWAP gates to be replaced by controlled-not (CNOT) gates as shown in Figs. 1(d) and 1(e) [23].

We implement the order-2-finding circuit, Fig. 1(d). The qubits are realized with simultaneous forward and backward production of photon pairs from parametric down-conversion, Fig. 2(a): the logical states are encoded into the vertical and horizontal polarizations. This circuit requires implementing a recently proposed three-qubit quantum-logic gate, Fig. 2(b), which realizes a cascade of n controlled-z gates with exponentially greater success than chaining n individual gates [24]. The controlled-not gates are realized by combining Hadamards and controlled-z (cz) gates based on partially polarizing beam splitters. The gates are nondeterministic; when fully pre-biased, success probability is 1/4 [8–10]. A run of each routine is flagged by a fourfold event, where a single photon arrives at each output. Dependent photons from the forward pass interfere nonclassically at the first partial polarizer, Fig. 2(d); one photon then interferes with an independent photon from the backward pass at the second partial polarizer. We measure relative nonclassical visibilities, $V_r \equiv V_{\text{meas}}/V_{\text{ideal}}$, of $98 \pm 2\%$ and $85 \pm 6\%$.

Directly encoding the order-4 finding circuit, Fig. 1(e), requires six photons and at least one three-qubit and five

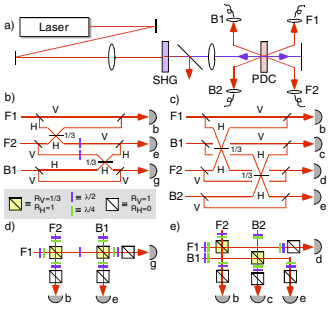


FIG. 2 (color online). Experimental schematic. (a) Forward (F1, F2) and backward (B1,B2) photons pairs are produced via parametric down-conversion [22]. (b,c) Linear-optical circuits for order-2 and order-4 finding algorithms, with inputs from (a) labeled; the letters on the detectors refer to the Fig. 1 qubits. (d,e) Physical optical circuits for (b,c), replacing the classical interferometers with partially polarizing beam splitters.

two-qubit gates. This is currently infeasible: the best six-photon rate to date [12] is 30 mHz, which would be reduced by 6 orders of magnitude using nondeterministic gates. To explore an order-4 routine, and the different processes therein, further compilation is necessary. In particular, we can compile circuits 1(d) and 1(e) by evaluating $\log_C[C^x \mathrm{mod} N]$ in the function-register in place of $C^x \mathrm{mod} N$. This requires $\log_2\{\log_C[N]\}$ function qubits, as opposed to $\log_2[N]$; i.e., for $N = 15$, $C = 2$, the function-register reduces from 4 to 2 qubits. Note that this full compilation maintains all the features of the algorithm as originally proposed in Ref. [13]. Thus, the order-4 circuit, Fig. 1(e), reduces to a pair of CNOTS, allowing us to implement the circuit in Fig. 1(g). We use a pair of compact optical gates [8–10], Fig. 2(c) and 2(e), each operating on a dependent pair of photons, resulting in measured visibilities for both of $V_r = 98 \pm 2\%$.

Figure 3 shows the measured density matrices of the argument-register output for both algorithms, sans the redundant top-rail qubit [25]. Ideally, these are maximally-mixed states [22]: in all cases, we measure near-unity fidelities [26,27]. The output of the routines are the logical state probabilities, i.e., the diagonal elements of the matrices. Combining these with the known state of the redundant qubit, and reversing the argument qubits as required, gives the binary outputs of the algorithm which after classical processing yields the prime factors of N. In the order-2 circuits the binary outputs of the algorithm are 00 or 10: the former represents the expected failure mode of this circuit, the latter a successful determination of $r = 2$; failure and success should have equal probabilities; we measure them to be 50% to within error. Thus, half the time the algorithm yields $r = 2$, which gives the factors, 3 and 5. In the order-4 circuit, the binary outputs are 000, 010, 100, and 110: the second and fourth terms yield the order-4 result, the first is a failure mode, and the third yields trivial factors. We measure output probabilities of 25% to within error, as expected. After classical processing half the time, the algorithm finds $r = 4$, again yielding the factors 3 and 5.

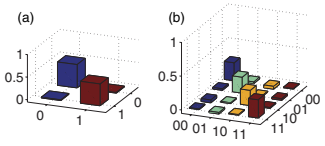


FIG. 3 (color online). Algorithm outputs given by measured argument-register density matrices. The diagonal elements are the logical output probabilities. (a) Order-2 algorithm. The fidelity with the ideal state is $F = 99.9 \pm 0.3\%$, the linear entropy is $S_L = 100 \pm 1\%$ [27]. Combined with the redundant qubit, the logical probabilities are $\{P_{00}, P_{10}\} = \{52, 48\} \pm 3\%$. (b) Order-4 algorithm, $F = 98.5 \pm 0.6\%$ and $S_L = 98.1 \pm 0.8\%$. The logical probabilities are $\{P_{000}, P_{010}, P_{100}, P_{110}\} = \{27, 23, 24, 27\} \pm 2\%$. Real parts shown, imaginary parts are less than 0.6%.

These results show that we have near-ideal algorithm performance, far better than we have any right to expect given the known errors inherent in the logic gates [8,28]. This highlights that the *algorithm* performance is not always an accurate indicator of *circuit* performance since the algorithm produces mixed states. In the absence of the gates, the argument-register qubits would remain pure; as they are mixed, they have become entangled to *something* outside the argument register. From algorithm performance, we cannot distinguish between desired mixture arising from entanglement with the function-register, and undesired mixture due to environmental decoherence. Circuit performance is crucial if it is to be incorporated as a subroutine in a larger algorithm, Fig. 1(a), 1(e), and 1(g). The *joint* state of both registers after modular exponentiation indicates circuit performance; we find entangled states that partially overlap with the expected states, Fig. 4, indicating some environmental decoherence.

Process tomography fully characterizes circuit performance, yielding the χ-matrix, a table of process measurement outcomes and the coherences between them. Measured and ideal χ-matrices can be quantitatively compared using the fidelity [6,27]; we measured process fidelities of $F_p = 85\%$, 89% for the two-qubit gates of the order-4 circuit. It is the easier of the two algorithms to characterize since it consists of two gates acting on inde-

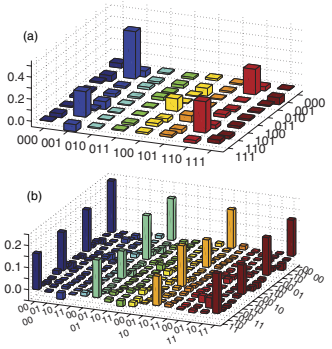


FIG. 4 (color online). Measured density matrices of the state of both registers after modular exponentiation. (a) Order-2 circuit. The ideal state is locally equivalent to a GHZ state: we find $F_{\mathrm{GHZ}} = 59 \pm 4\%$. The state is partially mixed, $S_L = 62\% \pm 4\%$, and entangled, violating the optimal GHZ entanglement witness $W_{\mathrm{GHZ}} = 1/2 - F_{\mathrm{GHZ}} = -9 \pm 4\%$ [31]. (b) Order-4 circuit. Measured fidelity with the ideal state, a tensor product of two Bell-states, is $F = 68 \pm 3\%$. The state is partially mixed, $S_L = 52 \pm 4\%$, and entangled, with tangles of the component Bell-States of $41 \pm 5\%$ and $33 \pm 5\%$. Real parts shown, imaginary parts are, respectively, less than 7% and 4%. The fidelity of the four-qubit state (b) is higher than the three-qubit state (a), chiefly because the latter requires nonclassical interference of photons from independent sources, which suffer higher distinguishability, lowering gate performance [28,32,33].

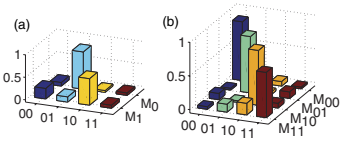


FIG. 5 (color online). Measured function-register probabilities after modular exponentiation, conditioned on logical measurement of the argument-register M_x. There is a high correlation between the registers: (a) Order-2 circuit, $\{P_{01}, P_{10}\} = \{83 \pm 4\%, 59 \pm 5\%\}$; (b) Order-4 circuit, $\{P_{00}, P_{01}, P_{10}, P_{11}\} = \{87 \pm 3\%, 84 \pm 4\%, 82 \pm 5\%, 67 \pm 6\%\}$.

pendent qubit pairs. Consequently, by assuming that only these gates induce error, the order-4 circuit process fidelity is simply the product of the individual gate fidelities [30], $F_p^{bcde} = F_p^{bd} F_p^{ce} = 80\%$. Clearly, this is significantly less than the *algorithm* success rate of 99.7%. The order-2 circuit is harder to characterize, requiring at least 4096 measurements, infeasible with our count rates. Decomposing the three-qubit gate into a pair of two-qubit gates yields process fidelities $F_p = 78\%$, 90% (reflecting differing interferences of independent and dependent photons). There is no simple relation between individual cz gate performances and that of the three-qubit gate. However, a bound can be obtained by chaining the gate errors, $F_p \geq 20\%$ [29]. This is not useful, c.f. the fidelity between an ideal cz and doing nothing at all of $F_p = 25\%$ (The bound only becomes practical as $F_p \to 1$). For larger circuits, full tomographic characterization becomes exponentially impractical. The order-finding routine registers contain $k = n + m$ qubits: state and process tomography of a k-qubit system require at least 2^{2k} and 2^{4k} measurements, respectively.

An alternative is to gauge circuit performance via logical correlations *between* the registers. Modular exponentiation produces the entangled state $\sum_{x=0}^{2^n-1} |x\rangle|y\rangle$ where y is respectively $C^x \mathrm{mod} N$ and $\log_C[C^x \mathrm{mod} N]$ for partial and full compilation. For a correctly functioning circuit, measuring the argument in the state x projects the function into y—requiring at most 2^k measurements to check. Figure 5 shows there is a clear correlation between the argument and function registers, 59 to 83% and 67 to 87% for the order-2 and order-4 circuits, respectively. Again, these indicative values of circuit operation are significantly less than the algorithm success rates.

We have experimentally implemented every stage of a small-scale quantum algorithm. Our experiments demonstrate the feasibility of executing complex, multiple-gate quantum circuits involving coherent multiqubit superpositions of data registers. We present two different implementations of the order-finding routine at the heart of Shor's algorithm, characterizing the algorithmic and circuit performances. Order-finding routines are a specific case of phase-estimation routines, which in turn underpin a wide variety of quantum algorithms, such as those in quantum chemistry [30]. Besides providing a proof of the use of quantum entanglement for arithmetic calculations, this work points to a number of interesting avenues for future research—in particular, the advantages of tailoring algorithm design to specific physical architectures, and the urgent need for efficient diagnostic methods of large quantum information circuits.

We wish to thank M. P. de Almeida and E. DeBenedictis for stimulating discussions. This work was supported by the Australian Research Council, Federation Fellow and DEST Endeavour Europe programs, the IARPA-funded U.S. Army Research Office Contract No. W911NF-05-0397, and the Canadian NSERC.

Note added in proof.—By better spectral filtering, we improved the GHZ state to $F = 67 \pm 3\%$, $S_L = 58 \pm 3\%$, and $W_{GHZ} = -17 \pm 3\%$.

[1] P. Shor, *Proc. 35th Ann. Symp. Found. Comp. Sci.* (IEEE Comp. Soc. Press, Los Alamitos, California, 1994), p. 124.
[2] F. Schmidt-Kaler *et al.*, Nature (London) **422**, 408 (2003).
[3] D. Leibfried *et al.*, Nature (London) **422**, 412 (2003).
[4] M. Steffen *et al.*, Science **313**, 1423 (2006).
[5] J. L. O'Brien *et al.*, Nature (London) **426**, 264 (2003).
[6] J. L. O'Brien *et al.*, Phys. Rev. Lett. **93**, 080502 (2004).
[7] P. Walther *et al.*, Nature (London) **434**, 169 (2005).
[8] N. K. Langford *et al.*, Phys. Rev. Lett. **95**, 210504 (2005).
[9] N. Kiesel *et al.*, Phys. Rev. Lett. **95**, 210505 (2005).
[10] R. Okamoto *et al.*, Phys. Rev. Lett. **95**, 210506 (2005).
[11] R. Prevedel *et al.*, Nature (London) **445**, 65 (2007).
[12] C.-Y. Lu *et al.*, Nature Phys. **3**, 91 (2007).
[13] D. Beckman *et al.*, Phys. Rev. A **54**, 1034 (1996).
[14] L. M. K. Vandersypen *et al.*, Nature (London) **414**, 883 (2001).
[15] S. L. Braunstein *et al.*, Phys. Rev. Lett. **83**, 1054 (1999).
[16] N. C. Menicucci *et al.*, Phys. Rev. Lett. **88**, 167901 (2002).
[17] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
[18] J. F. Poyatos *et al.*, Phys. Rev. Lett. **78**, 390 (1997).
[19] E. Knill *et al.*, Nature (London) **409**, 46 (2001).
[20] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[21] R. B. Griffiths *et al.*, Phys. Rev. Lett. **76**, 3228 (1996).
[22] See EPAPS Document No. E-PRLTAO-99-020750 for supplementary information. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[23] Figure 1(e) is equivalent to the order-4 $C = 7$ circuit in Ref. [14]: CSWAP is equivalent to a Toffoli and CNOTS.
[24] T. C. Ralph, Phys. Rev. A **70**, 012312 (2004).
[25] We use convex optimization tomography [M. De Burgh, A. Doherty, and A. Gilchrist (to be published)] and estimate errors via Monte Carlo simulation [6].
[26] Fidelity is $F(\rho, \sigma) \equiv \mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$; linear entropy is $S_L \equiv d(1 - \mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension [27].
[27] A. G. White *et al.*, J. Opt. Soc. Am. B **24**, 172 (2007).
[28] T. J. Weinhold *et al.* (to be published).
[29] A. Gilchrist *et al.*, Phys. Rev. A **71**, 062310 (2005).
[30] A. Aspuru-Guzik *et al.*, Science **309**, 1704 (2005).
[31] M. Bourennane *et al.*, Phys. Rev. Lett. **92**, 087902 (2004).
[32] J. G. Rarity *et al.*, J. Opt. B **7**, S171 (2005).
[33] R. Kaltenbaek *et al.*, Phys. Rev. Lett. **96**, 240502 (2006).

Experimental demonstration of Shor's algorithm with quantum entanglement: Additional on-line material

B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James*, A. Gilchrist, and A. G. White
Centre for Quantum Computer Technology Department of Physics University of Queensland, Brisbane QLD 4072, Australia
**Department of Physics Center for Quantum Information and Control University of Toronto, Toronto ON M5S1A7, Canada*

For all the circuits Fig. 1b)-g), the consecutive Hadamards in the top qubit of the argument-register cancel each other out (since $\mathrm{H}^2=\mathrm{I}$): consequently both this qubit, and the gate(s) controlled by it, are redundant and need not be implemented experimentally. The remaining argument-register qubits are maximally-entangled to the function-register. Since the function-register output is not measured, these argument qubits are maximally-mixed, and the subsequent gates in the inverse QFT are therefore also redundant. Thus the inverse QFT in Ref. [14] was unnecessary: indeed, it is straightforward to show this is true for any order-2^l circuit. After modular exponentiation, the circuit state is $\sum_{x=0}^{2^n-1}|x\rangle|C^x \mathrm{mod} N\rangle$: for any two values x and y that differ by an integer, k number of orders, i.e. $y-x=k\,2^l$, $C^y \mathrm{mod} N=C^x \mathrm{mod} N$, and the state after modular exponentiation becomes $\sum_{k=0}^{2^{n-l}-1}\sum_{a=0}^{2^l-1}|k2^l+a\rangle|C^a \mathrm{mod} N\rangle$. Note that the first $n-l$ qubits of the argument-register (top to bottom) encode the number k, the remaining l qubits encode 2^l distinct values of a: we divide the argument-register accordingly, $\sum_{k,a}|k\rangle|a\rangle|C^a\rangle$. The $|k\rangle$ qubits do not become entangled to the function-register whereas the $|a\rangle$ qubits are maximally-entangled to it—consequently after tracing out the function-register, the $|a\rangle$ qubits are in a maximally-mixed state and any further gates acting on them are redundant. Application of Hadamard gates in the inverse QFT reset the $|k\rangle$ qubits to 0, inhibiting any gates controlled by them, The final step of the inverse QFT is to swap the first and last qubits of the argument register which can be done after measurement. Thus the inverse QFT can be omitted in all cases $r=2^l$.

7

Expanding the space

In this chapter I report on our work were the emission of multiple photons into one spatio-temporal mode by the parametric down-conversion is no longer treated as a bug, but used as a resource. Due to the bosonic nature of photons, we can not attach any identifying labelling information onto the two overlapping photons, which causes problematic behaviour when viewing them as individual quantum bits. However, we can use this very behaviour and describe their combined polarisation state to represent a three-level quantum system—a qutrit. In the first part of this chapter I will discuss a Fock-state filter which is a device that preferentially transmits states with photon numbers larger than one, while blocking individual photon states. The original experimental work that led to this publication was conducted Kevin Resch, Jeremy O'Brien and myself, while the idea for this device stemmed from Karou Sanaka and Kevin Resch and their original publication of such a Fock-state filter [89]. Later Nathan Langford and Benjamin Lanyon discovered significant rotations caused by the beamsplitters and adapted the measurements to account for these. Further, the temperature stability of lab was significantly improved, remedying the periodic loss of non-classical interference visibility caused by the on/off cycle of the air-conditioning system. This lead to significantly improved results, which were amended to the paper and as supplementary online material and together were published in Physical Review Letters [68].

We further realised that the filter could be used to expand the range of accessible qutrit states. Specifically, we show that the combination of quarter and half waveplates, in addition to the Fock-state filter, suffice to rotate a qutrit state to any other pure qutrit state. Furthermore the operation of the Filter creates entanglement between a qubit and a qutrit, which we prove by measuring the Peres negativity [90, 91]. Again due to the observed rotations the work was repeated with the original implementation being conducted by Kevin Resch, Jeremy O'Brien and myself and the final implementation being conducted by Benjamin Lanyon, Nathan Langford and myself. Alexei Gilchrist assisted in the derivation of required measurement settings and the data analyses was conducted by Kevin Resch, Nathan

Langford, Alexei Gilchrist in myself. This work was published in Physical Review Letters. [92]

7.1 The Fock-State Filter

In section 1.5, the non-classical Hong-Ou-Mandel interference [13] was introduced. This is only a specific case of the non-classical interference of indistinguishable photons at a beamsplitter in general. As used to create the non-deterministic photonic quantum gates, the reflectivity of the beamsplitter could be altered, or as in this chapter, the number of input photons per mode. Again I have chosen to insert the paper [68] to provide the experimental details and only briefly expand the discussion of the Filter behaviour which could not be fitted into the paper due to length constraints. It is briefly discussed in the paper that the probability of detecting a single photon in a specific mode, when n photons are injected into one port of the beamsplitter, and a single photon in the other is given by

$$P(n) = |R^{(n-1)/2}\big(R - n(1-R)\big)|^2, \tag{7.1}$$

where R is the reflectivity of the beamsplitter, and without loss of generality it is assumed, that the single photon is to be observed in the reflected mode with respect to the single photon input. It becomes obvious that for the choice $R = \frac{n}{n+1}$ the probability of observing the single photon in the desired mode is zero. Hong-Ou-Mandel interference is thus only the lowest case of this more general equation, with the choices n=1 and R=1/2. Instead, imagine the case where we have a weak coherent state $|\alpha\rangle$ as input. We can then write this state as the coherent sum of

$$|\alpha\rangle = \sum_{i}^{\infty} a_i |i\rangle, \tag{7.2}$$

where the a_i are the probability of the finding the given photon number in the state. Interacting this state with our single photon input on our Fock-state filter is going to significantly alter the photon number probability distribution of our weak coherent state dependent on the reflectivity of the beamsplitter. Specifically we can see that the Fock-state with photon number n from our reflectivity definition will never be observed.

In our paper, we expand the use of this filter with respect to the original publication of Sanaka et al. [89], by no longer simply acting on photon number Fock states, but by using polarisation superposition states. During this experiment we always inject two horizontally polarised photons in mode a in Figure 1 of the paper, but can alter the state with the subsequent half-waveplate. We also inject two photons from the other fibre launcher, but split one photon off at the first beamsplitter, which is detected as our trigger. The remaining single photon is then horizontally polarised and can interfere with the horizontal components of the two qubit state in mode a on the beamsplitter. To create the photons we use the source discussed in section 2.2.3. Contrary to our previous experiments we now seek the events in which multiple photons are emitted in the same spatio-temporal mode and only operate the source in the forward direction. For our experiment, we chose $R = 1/2$. When we do not rotate the polarisation of the bi-photon state in mode a, this leaves us with two indistinguishable photons in this mode. The interaction with the single photon input from

mode b reduces the probability of observing one photon in mode d and two photons in mode c from 3/8 in the case of distinguishable photons to 1/8 for indistinguishable ones. We thus expect a Hong-Ou-Mandel interference visibility of 2/3, which is shown in Figure 2 of the paper. As the half-waveplate can not act independently on the two photons in mode a, the transformation the photons undergo is given by:

$$\begin{aligned} |2_{\mathrm{H}}, 0_{\mathrm{V}}\rangle_a \quad \rightarrow \quad & \cos^2\theta |2_{\mathrm{H}}, 0_{\mathrm{V}}\rangle_a + \sin^2\theta |0_{\mathrm{H}}, 2_{\mathrm{V}}\rangle_a \\ & + \sqrt{2}\cos\theta\sin\theta |1_{\mathrm{H}}, 1_{\mathrm{V}}\rangle_a, \end{aligned} \tag{7.3}$$

where θ is the relative angle between the optic axis of the waveplate and the plane defined by the horizontally polarised light field. If this state interacts with our single photon in mode b, the $|2_{\mathrm{H}}, 0_{\mathrm{V}}\rangle$ suffer the decrease in count rate due to the non-classical interference as noted above. The $|0_{\mathrm{H}}, 2_{\mathrm{V}}\rangle$ is not affected by the non-classical interference, but conditioning our detection upon the detection of the horizontal photon injected in mode b in the output mode d, coincident with detections of photons on detectors 3 and 4 requires that all 3 photons were reflected, giving us the factor for the amplitude of $\sqrt{R^3}$ which is equal to the attenuation of the horizontal mode. Thus while the two components with equally polarised photons are attenuated equally, the probability of detecting the $|1_{\mathrm{H}}, 1_{\mathrm{V}}\rangle$ in mode c vanishes in the ideal case, as the horizontal photon will always pair with the horizontally polarised photon in mode b. Thus it is impossible to observe a single horizontally polarised photon in output mode d. Whenever the detector in mode d detects horizontally polarised photons (as it is non number resolving, we can not differentiate between one or more photons), this requires that there are two photons. This means in turn, that output mode c is only populated by a single photon, and thus detectors 3 and 4 can not both fire. In other words there is no fourfold signal and subsequently this case does not lead to a valid event. Hence the output state for mode c after the central beamsplitter is

$$\frac{-\cos^2\theta |2_H, 0_V\rangle_c + \sin^2\theta |0_H, 2_V\rangle_c}{(\cos^4\theta + \sin^4\theta)^{1/2}}. \tag{7.4}$$

For $\theta = \pi/4$, this is the lowest order NOON state and thus a path entangled state. To analyse this state, we probabilistically split the path entangled photons at a $50:50$ beamsplitter and subject both paths to a full tomographic polarisation analyses. Measurements of the output state both when the filter is active and when it has been turned off by blocking mode b are shown in Figure 3 of the paper and Figure 1 of the additional online material. Both states have a high fidelity with the ideal state, while the output state when the filter is active also shows high tangle. A more detailed discussion with more complete referencing is given in the paper itself.

7.2 The paper — Entanglement generation by Fock-state filtration

PRL 98, 203602 (2007) PHYSICAL REVIEW LETTERS week ending 18 MAY 2007

Entanglement Generation by Fock-State Filtration

K. J. Resch,[1,2] J. L. O'Brien,[1,3] T. J. Weinhold,[1] K. Sanaka,[4] B. P. Lanyon,[1] N. K. Langford,[1] and A. G. White[1]
[1]*Department of Physics & Centre for Quantum Computer Technology, University of Queensland, Brisbane, QLD 4072, Australia*
[2]*Department of Physics & Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[3]*H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol, BS8 1UB, United Kingdom*
[4]*E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA*
(Received 31 July 2006; published 16 May 2007)

We demonstrate a Fock-state filter which is capable of preferentially blocking single photons over photon pairs. The large conditional nonlinearities are based on higher-order quantum interference, using linear optics, an ancilla photon, and measurement. We demonstrate that the filter acts coherently by using it to convert unentangled photon pairs to a path-entangled state. We quantify the degree of entanglement by transforming the path information to polarization information; applying quantum state tomography we measure a tangle of $T = (20 \pm 9)\%$.

DOI: 10.1103/PhysRevLett.98.203602 PACS numbers: 42.50.Dv, 03.65.Wj, 03.67.Mn, 42.50.Nn

In practice it is extremely difficult to make one photon coherently influence the state of another. The optical nonlinearities required are orders of magnitude beyond those commonly achieved with current technology. Strong effective nonlinearities can be induced in linear optical systems by combining quantum interference and projective measurement [1], opening the possibility of scalable linear-optical quantum computation. Such measurement-induced nonlinearities have had high impact in quantum information, notably in optical quantum logic gate experiments [2,3] and in exotic state production [4,5].

Most schemes achieve an effective nonlinearity via lowest-order nonclassical interference, with one photon per mode input to a beam splitter. Higher-order nonclassical interference, where more than one photon is allowed per mode, enables additional control [1]. An ancilla photon has been used to conditionally control the phase of a two-photon path-entangled state [2], and to conditionally absorb either one- or two-photon states [6]. Applied to superpositions, higher-order interference is predicted to act as a Fock-state filter [7,8], conditionally absorbing only terms with a specified number of photons. In this Letter, we prove that conditional absorption is coherent by applying it to a superposition, and experimentally generating a path-entangled state. We quantify the entanglement by transforming path information to polarization, and applying quantum state tomography [9].

The Fock-state filter uses nonclassical interference at a single, polarization-independent, beam splitter of reflectivity R. Consider the beam splitter in Fig. 1 with $n + 1$ photons incident: n in mode a, and 1 (the ancilla) in mode b. There are $n + 1$ possible ways for there to be one and only one photon in mode d: all the input photons can be reflected, with probability amplitude $\sqrt{R}^{n+1}$, or there are n ways for a photon from each input to be transmitted and the rest reflected, $n(1 - R)\sqrt{R}^{n-1}$. Assuming indistinguishable photons, the probability amplitude for detecting one and only one photon in mode d is $A(n) = R^{(n-1)/2}[R - n(1 - R)]$ [6,7,10]. Note that the probability $P(n) = |A(n)|^2$ can be zero for any single choice of n, when $R = n/(n + 1)$; for all other n, $P > 0$ [6]. Hong-Ou-Mandel interference is the lowest-order case, where $P = 0$ when $n = 1$ and $R = \frac{1}{2}$ [11]: the detector in mode d is never hit by a single photon. If a superposition of number states is input into mode a and a single photon is detected in mode d, then the output state in mode c cannot contain $|1\rangle$.

The Fock-state filter could be tested by creating a number-state superposition, applying the filter, and tomographically measuring the resulting state. In practice, each step of this naïve approach is impractical: creating nonclassical number-state superpositions is onerous [4,12] and they are easily destroyed by loss; the Fock-state filter requires an ancilla photon on demand and a perfect-

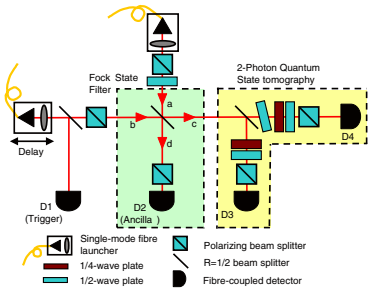


FIG. 1 (color online). The Fock-state filter: a device that blocks the passage of single photons, but allows the coherent passage of photon pairs. As described in the text, a probabilistic Fock-state filter can be created by combining a 50% beam splitter, ancilla photon, quantum interference, and measurement.

PRL 98, 203602 (2007) PHYSICAL REVIEW LETTERS week ending 18 MAY 2007

efficiency number-resolving detector; and tomography needs high-efficiency homodyne measurement.

Our experiment alleviates each difficulty. We use double-pair emission from parametric down conversion to generate a pair of polarized two-photon states in separate spatial modes. Down conversion is often problematic since it emits photon pairs probabilistically, and can emit more than one pair at a time. However, in some cases double-pair emission is beneficial [13], or essential [14]. Double-pair emission provides input two-photon states in mode a and single, ancillary, photons in mode b: we create the superposition in mode a by rotating its polarization,

$$|2_H, 0_V\rangle_a \rightarrow \cos^2\theta|2_H, 0_V\rangle_a + \sin^2\theta|0_H, 2_V\rangle_a + \sqrt{2}\cos\theta\sin\theta|1_H, 1_V\rangle_a, \quad (1)$$

where θ is the polarization angle relative to horizontal. We create a horizontally polarized ancilla photon in mode b by passing the two-photon state through a 50% beam splitter and triggering on detection events from the output mode of the beam splitter, see Fig. 1. The trigger photon is measured in coincidence with the three photons output from the beam splitter: if a photon is lost then it cannot contribute to the fourfold coincidence signal.

The Fock-state filter acts nonlinearly only on light with the same polarization as the ancilla, horizontal in this case. The amplitude given in Eq. (1) determines the transformation on horizontally polarized components of the state, $|n_H\rangle|1_H\rangle \rightarrow A(n_H)|n_H\rangle|1_H\rangle + \ldots$; in contrast, the vertically polarized components are transformed as, $|n_V\rangle|1_H\rangle \rightarrow R^{(n_V+1)/2}|n_V\rangle|1_H\rangle + \ldots$. Measurement of a single horizontally polarized photon in mode d selects only the first terms of these transformations (the latter amplitude represents the only way that a horizontally polarized photon can be detected in mode d). Noting that the conditional transformation is not unitary, and applying this to the terms in Eq. (1) we find, $|2_H, 0_V\rangle_a \rightarrow -|2_H, 0_V\rangle_c/2\sqrt{2}$, $|1_H, 1_V\rangle_a \rightarrow 0$, and $|0_H, 2_V\rangle_a \rightarrow |0_H, 2_V\rangle_c/2\sqrt{2}$, and the state of mode c conditioned on a horizontal photon detected in mode d is,

$$\frac{-\cos^2\theta|2_H, 0_V\rangle_c + \sin^2\theta|0_H, 2_V\rangle_c}{(\cos^4\theta + \sin^4\theta)^{1/2}}. \quad (2)$$

The final state can be tuned between separable and entangled number-path states simply by adjusting the input polarization θ. In the case, $\theta = \pi/4$, this is the lowest-order NOON state [15], $(|2_H, 0_V\rangle - |0_H, 2_V\rangle)/\sqrt{2}$ [16,17].

Note that the vertical polarization is a stable phase reference for the nonlinear sign change of the horizontal components, removing the need for a stable homodyne measurement. The final state is transformed from one to two spatial modes by a 50% beam splitter: mapping the path-entanglement into polarization-entanglement lets us characterize the state with quantum state tomography of the polarization, with all of its attendant advantages [9].

Our down-conversion source was a BBO (β-barium borate) nonlinear crystal cut for noncollinear type-I frequency conversion (410 nm $\rightarrow$ 820 nm), pumped by a frequency-doubled titanium sapphire laser. The down-converted light was coupled into two single-mode optical fibers, which when connected directly to FC-connectorized single-photon counting modules yielded coincidence rates of 30 kHz and singles rates of 220 kHz. Before coupling back into free-space, the polarization of the light was manipulated in-fiber using "bat-ears" to maximize transmission through horizontal polarizers. Light in mode b was split by a 50% beam splitter, where one output mode was coupled directly into a single-mode fiber coupled detector, D1, which acted as a trigger. The remaining light passed through a horizontal polarizer and is combined on a second 50% beam splitter with light from mode a, which is first passed through a horizontal polarizer and half-wave plate to rotate the polarization, as described in Eq. (1). Mode d is directly detected at D2; mode c is split into two modes by a 50% beam splitter, each mode is polarization analyzed using a quarter- and half-wave plate and polarizer. We use D3 and D4 to perform a tomographically complete

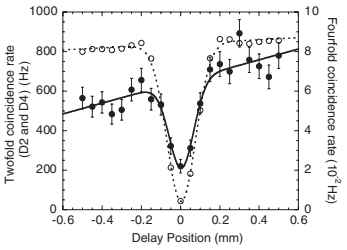


FIG. 2. Quantum interference in two- and fourfold coincidence counts as a function of the longitudinal position of the input fiber coupler for mode b. At zero delay, we see marked preferential absorption of single-photon over two-photon states in mode c, as indicated by the larger dip in two- over fourfold counts. The two- and fourfold raw visibilities are (95.20 $\pm$ 0.02)% and (68 $\pm$ 5)%, respectively; correcting for background as described in the text, the twofold visibility becomes (99.6 $\pm$ 0.1)% (error bars are smaller than the points in the twofold case and are not shown). The visibilities are in excellent agreement with the theoretically expected two- and four-visibilities of 100% and 66.7% [6,11,18]. The input coupler was scanned 1 mm in 630 s: to mitigate drift effects the scan was repeated 63 times, leading to an integration time of 31.5 min per point. The slopes in the data are due to longitudinal-position-dependent coupling to the detectors; the trigger detector was particularly sensitive in this respect, leading to a large slope in the fourfolds; the twofolds show a much smaller slope as the trigger detector plays no role in that data. The visibilities were obtained from curve fits to products of a Gaussian and a linear function.

PRL 98, 203602 (2007) PHYSICAL REVIEW LETTERS week ending 18 MAY 2007

set of two-qubit measurements, $\{H, V, D, R\} \otimes \{H, V, D, R\}$, in coincidence with the trigger and ancilla detectors, D1 and D2. The resulting density matrices are reconstructed using the maximum-likelihood technique [9]. All optical paths between fiber couplers to detectors were made approximately equal (~50 cm) to facilitate high-efficiency single-mode to single-mode fiber coupling. The tilted half-wave plate in the D4 arm, set with its optic axis horizontal, compensated beam splitter birefringence.

Nonclassical interference is the heart of the Fock-state filter. We characterized this by setting the polarization of mode a to horizontal, matching that of mode b, and setting analyzers at D3, D4 to horizontal. Figure 2 shows experimentally measured twofold coincidence counts, in this case between detectors D2 and D4 (open circles), and the fourfold coincidence counts, between D1, D2, D3, and D4 (solid circles), as a function of the longitudinal position of the input fiber coupler for mode b.

As D2 and D4 detect the two outputs of the beam splitter, the twofolds show the standard Hong-Ou-Mandel interference dip [11], with a raw visibility of $V_1 = (95.20 \pm 0.02)\%$. To estimate the performance of the Fock-state filter we must consider the events from double-pair emission. We can estimate these by blocking mode a and b in turn and measuring the twofold coincidences between detectors D2 and D4, 5.8 ± 0.16 Hz and 30.9 ± 0.5 Hz, respectively. Summing these gives an estimate of the number of twofold coincidences due to the two-photon terms in modes a and b, (36.7 ± 0.5) Hz. These coincidences act as a background; subtracting them gives a corrected visibility of $V_1' = (99.6 \pm 0.1)\%$.

The fourfold coincidence counts in Fig. 2 display a higher-order nonclassical interference effect with visibility $V_2 = (68 \pm 5)\%$, which agrees with the expected value of 66.7% [6]. Note that the interference visibility is much larger for the $n = 1$ input state, as measured by the twofold coincidences, than the $n = 2$ input state, as measured by the fourfold coincidences. At the center of the interference dip, single photons are removed from an input state with much higher probability than pairs of photons: this is the action of the Fock-state filter.

The visibilities, V_1' and V_2, set an upper bound to the performance of the Fock-state filter. Ideally, the probability of transmission when the ancilla and n-photon inputs are distinguishable is $Q(n) = R^{n+1} + nR^{n-1}(1 - R)^2$ [6]. The nonlinear absorption probability $P(n)$ is modified by the visibilities as $P'(n) = (1 - V_n)Q(n)$. We estimate the filter's efficiency of blocking single photons, $P'(2)/P'(1) = 60 \pm 20$; at best, it passes two-photon terms at 60 times the rate it passes single-photon terms.

To show the coherent action of the filter, we set the input wave plate in mode a to rotate the linear polarization from horizontal to diagonal, creating the superposition of Eq. (1). We first measure the input state without the action of the Fock-state filter by blocking the ancilla photon in mode b, and performing tomography on mode c using detectors D3 and D4. Counting for 30 s per measurement setting, we measured raw twofold coincidence counts of {86, 68, 156, 61, 89, 77, 195, 61, 200, 170, 328, 131, 98, 102, 175, 71}. The reconstructed density matrix, shown in Fig. 3(c), gives us the initial state of the light and includes the effect of any birefringence in our experiment. The density matrix consists of near equal probabilities, and strong positive coherences between them—characteristic of the expected ideal state $|\psi\rangle = |\mathrm{DD}\rangle$. The fidelity between the ideal and measured state ρ is $\mathcal{F} = \langle\psi|\rho|\psi\rangle = (93 \pm 4)\%$; the linear entropy is $S_L = (11 \pm 8)\%$ [9], indicating the state is near-pure; and the tangle is zero within error, $T = (0.5 \pm 0.8)\%$, indicating that as expected the input state is unentangled.

The Fock-state filter is run by unblocking mode b and setting its coupler to the zero-delay position shown in Fig. 2. We performed tomography on the photon pairs at D3 and D4, but now in coincidence with the trigger and ancilla photon detectors, D1 and D2, counting for 8.25 hours per measurement setting, obtaining the raw counts {62, 10, 45, 25, 10, 59, 49, 49, 53, 40, 36, 45, 37, 50, 46,

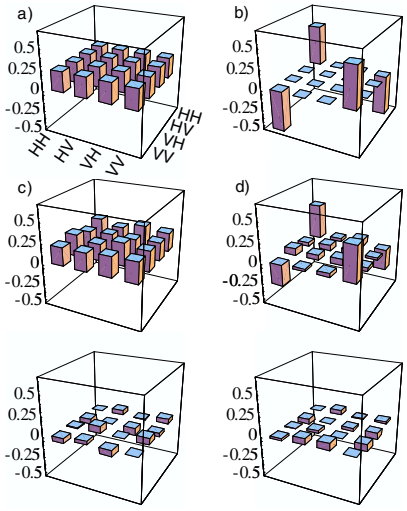


FIG. 3 (color online). Density matrices for the Fock-state filter. Ideal output states from the filter when the filtering is (a) turned off, $|DD\rangle$, and (b) turned on, $(|HH\rangle\text{-}|VV\rangle)/\sqrt{2}$, as described in text. The corresponding experimental tomographic reconstructions, based on raw counts, are shown, respectively, in (c) and (d), the upper (lower) panels are the real (imaginary) components. The fidelity between the ideal and measured states is $93 \pm 4\%$ and $69 \pm 9\%$, respectively. The state measured in (d) is entangled, with tangle $T = 20 \pm 9\%$.

72}. The reconstructed density matrix is shown in Fig. 3(d)]. Consistent with the prediction of Eq. (2) setting $\theta = \pi/4$, there are two striking differences between this and Fig. 3(c)]: (1) the dramatic reduction of the HV and VH populations and coherences; and (2) the sign change of the coherences between the HH and VV populations. The fidelity, between the ideal state, $|\psi\rangle = (|\mathrm{HH}\rangle - |\mathrm{VV}\rangle)/\sqrt{2}$, and the measured state ρ is $\mathcal{F} = (69 \pm 9)\%$. The linear entropy is $S_L = (57 \pm 6)\%$, the increase in entropy indicates that the filter introduces mixture but retains much of the input state's coherence. This is reflected in the output state entanglement, $T = (20 \pm 9)\%$, requiring coherence.

The tomography is based on the fourfold signal, which is particularly susceptible to background, due to low rates and long counting times. We use raw, rather than corrected fourfold counts, as unambiguous measurement of the background is nontrivial due to the manifold combinations of accidental detection events. Thus $(P_{\mathrm{HH}} + P_{\mathrm{VV}})/(P_{\mathrm{HV}} + P_{\mathrm{VH}})$ is a lower bound on the preferential absorption of the filter, 6.0 ± 1.5.

We have constructed a coherent nonlinear absorber—a Fock-state filter—combining measurement with higher-order quantum interference. The filter preferentially absorbed up to 60 times more single photons than photon pairs, and produced an entangled state from a separable state: the output was measured to have a tangle of $T = (20 \pm 9)\%$. By encoding quantum information in both number and polarization, we were able to succinctly demonstrate all the salient features of a Fock-state filter in a single experiment. This is a powerful technique suitable for applications requiring quantum nonlinear optics.

We thank Anton Zeilinger for valuable discussions. This work was supported in part by the DTO-funded U.S. Army Research Office Contract No. W911NF-05-0397, a UQ ECR Grant, and the ARC Discovery program.

Note added in proof.—While correcting the proofs, laboratory temperature stability and source brightness were both improved. Consequently, the Fock-state filter produced a more highly entangled state with tangle of $T = 51 \pm 11\%$, linear entropy of $S_L = 46 \pm 9\%$, and fidelity with the ideal of $\mathcal{F} = 77 \pm 6\%$. See additional online material [19] for details.

[1] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[2] K. Sanaka, T. Jennewein, J.-W. Pan, K. Resch, and A. Zeilinger, Phys. Rev. Lett. **92**, 017902 (2004).
[3] T. B. Pittman *et al.*, Phys. Rev. A **64**, 062311 (2001); J. L. O'Brien *et al.*, Nature (London) **426**, 264 (2003); S. Gasparoni *et al.*, Phys. Rev. Lett. **93**, 020504 (2004).
[4] K. J. Resch *et al.*, Phys. Rev. Lett. **88**, 113601 (2002); A. I. Lvovsky and J. Mlynek, Phys. Rev. Lett. **88**, 250401 (2002).
[5] J. Wenger *et al.*, Phys. Rev. Lett. **92**, 153601 (2004); A. Zavatta *et al.*, Science **306**, 660 (2004).
[6] K. Sanaka *et al.*, Phys. Rev. Lett. **96**, 083601 (2006).
[7] H. F. Hofmann and S. Takeuchi, quant-ph/0204045; H. F. Hofmann and S. Takeuchi, Phys. Rev. Lett. **88**, 147901 (2002).
[8] B. M. Escher *et al.*, Phys. Rev. A **70**, 025801 (2004); K. J. Resch, Phys. Rev. A **70**, 051803 (2004); K. Sanaka, Phys. Rev. A **71**, 021801 (2005).
[9] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
[10] Singles rate is the rate of single "clicks" from standard detectors and can arise from detection of one or more photons.
[11] C. K. Hong *et al.*, Phys. Rev. Lett. **59**, 2044 (1987).
[12] S. M. Tan *et al.*, Phys. Rev. Lett. **66**, 252 (1991); L. Hardy, Phys. Rev. Lett. **73**, 2279 (1994); D. T. Pegg *et al.*, Phys. Rev. Lett. **81**, 1604 (1998); J. Clausen *et al.*, Appl. Phys. B **72**, 43 (2001).
[13] C. Simon and J.-W. Pan, Phys. Rev. Lett. **89**, 257901 (2002); J.-W. Pan *et al.*, Nature (London) **423**, 417 (2003); P. Walther *et al.*, Phys. Rev. Lett. **94**, 040504 (2005).
[14] D. Bouwmeester *et al.*, Phys. Rev. Lett. **82**, 1345 (1999); A. Lamas-Linares *et al.*, Nature (London) **412**, 887 (2001).
[15] H. Lee *et al.*, *Quantum Imaging and Metrology: Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing*, edited by J. H. Shapiro and O. Hirota (Rinton Press, Princeton, NJ, 2002), pp. 223–229.
[16] Alternatively, this can be seen as transforming a pair of identically polarized photons in the same spatial mode, $|2_D, 0_A\rangle$, to a pair of orthogonally polarized photons $|1_D, 1_A\rangle$, a nonlinear operation impossible with linear optical elements.
[17] $|\{D, A, R\}\rangle = (|0\rangle\{+, -, +i\}|1\rangle)/\sqrt{2}$.
[18] We used the same experiment to simultaneously measure both $n = 1$ and $n = 2$ absorption, unlike Ref. [6]. Our design ensured higher visibilities, $(95.20 \pm 0.02)\%$ and $(68 \pm 5)\%$, c.f. $83 \pm 1\%$ and $(61 \pm 6)\%$ [6], and significantly higher rates.
[19] See EPAPS Document No. E-PRLTAO-98-021711 for supplementary figures and text. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.

Entanglement generation by Fock-state filtration: Additional on-line material

During the type-setting of the paper, the temperature stability of the experiment was dramatically improved by installing a new air-conditioning unit. We also increased the the source brightness by moving from a BBO to BiBO down-conversion crystal. This gave a four-fold coincidence rate of approximately 170 counts per hour. Consequently, the new measured entangled two-qubit state had an improved tangle of T=51±11% and linear entropy of S_L=46±9%. The raw counts were {47, 11, 19, 36, 5, 41, 16, 20, 35, 20, 33, 15, 25, 21, 3, 8} for the measurements {HH, HV, HD, HR, VH, VV, VD, VR, DH, DV, DD, DR, RH, RV, RD, RR} respectively (integration time ∼40 minutes per setting). Instead of using tilted wave plates (as shown in the experimental layout in Figure 1), here we compensated numerically for the unwanted birefringence introduced by the beam splitters by finding the optimal single-qubit unitary rotation. The rotated state is plotted in Fig. **??**. This state has a fidelity with the maximally entangled target state of $F = 77\pm6\%$.

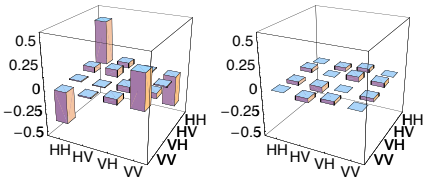


FIG. 1: Real (left) and imaginary (right) components of the density matrix reconstructed as described in text.

7.3 Operations for Qutrits

When two polarisation encoded qubits populated the same spatio-temporal mode, the bi-photonic state can either be thought of as the combination of the individual qubit polarisation states as in the previous section, or we can think of this as a quantum three level system — a qutrit. We choose to encode the bi-photonic qubit polarisations states in such a manner, that

$$\begin{aligned} |H,H\rangle &\rightarrow |0\rangle_3, \\ |H,V\rangle &\rightarrow |1\rangle_3, \\ |V,H\rangle &\rightarrow |1\rangle_3, \\ |V,V\rangle &\rightarrow |2\rangle_3. \end{aligned} \tag{7.5}$$

As we cannot distinguish the two photons unless their polarisation differs, we can not distinguish between the $|H,V\rangle$ and the $|V,H\rangle$ state, leading to them both encoding the logical $|1\rangle$ state. The input into our Fock-state filter, discussed in the previous section, can thus be viewed as a bi-photonic qutrit. Qutrits offer increased security in a range of quantum information protocols, greater channel capacity in communication protocols and novel tests of quantum mechanics[1]. While a method has been demonstrated to create any bi-photonic polarisation encoded qutrit state, the range of operations on a qutrit state is severely limited with linear optics, i.e. as we can see from equation 7.3 we can not use a half-waveplate to arbitrarily coherently shift population between the three logic states of such a qutrit. In the following paper, we present a method based on our previously discussed Fock-state filter that largely extends the range of possible operations on bi-photonic qutrits. In fact it allows transforming any pure qutrit state into any other pure qutrit state with the addition of a QWP and a HWP to the initial state preparation. Furthermore, similar to the Fock-state filter described above, this system is capable of creating entanglement. Specifically it entangles the qutrit with the photon injected in mode b. The output state is comprised of a qubit in mode d and a qutrit in mode c becomes entangled, which we demonstrate by performing state tomography on this system and measuring the Peres negativity [90]. We thereby demonstrate the first experimental entanglement between systems of different dimensions, a scenario, that has not been well investigated. We thus hope that this paper will trigger research into the benefits and behaviour of such systems.

[1]See paper at the end of this chapter for references

7.4 The paper — Manipulating Biphotonic Qutrits

PRL 100, 060504 (2008) PHYSICAL REVIEW LETTERS week ending 15 FEBRUARY 2008

Manipulating Biphotonic Qutrits

B. P. Lanyon,[1] T. J. Weinhold,[1] N. K. Langford,[1] J. L. O'Brien,[2] K. J. Resch,[3] A. Gilchrist,[1] and A. G. White[1]
[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane, Australia*
[2]*Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol, United Kingdom*
[3]*Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, Canada*
(Received 18 July 2007; published 14 February 2008)

Quantum information carriers with higher dimension than the canonical qubit offer significant advantages. However, manipulating such systems is extremely difficult. We show how measurement-induced nonlinearities can dramatically extend the range of possible transforms on biphotonic qutrits—three-level quantum systems formed by the polarization of two photons in the same spatiotemporal mode. We fully characterize the biphoton-photon entanglement that underpins our technique, thereby realizing the first instance of qubit-qutrit entanglement. We discuss an extension of our technique to generate qutrit-qutrit entanglement and to manipulate any bosonic encoding of quantum information.

DOI: 10.1103/PhysRevLett.100.060504 PACS numbers: 03.67.Mn, 03.65.Ud, 03.65.Wj, 42.50.Dv

Higher dimensional systems offer advantages such as increased security in a range of quantum information protocols [1–7], greater channel capacity for quantum communication [8], novel fundamental tests of quantum mechanics [9,10], and more efficient quantum gates [11]. Optically such systems have been realized using polarization [12] and transverse spatial modes [1,13]. However in each case state transformation techniques have proved difficult to realize. In fact, performing such transformations is a significant problem in a range of physical architectures.

The polarization of two photons in the same spatiotemporal mode represents a three-level bosonic quantum system, a biphotonic qutrit, with symmetric logical basis states: $|0_3\rangle \equiv |2_H, 0_V\rangle$, $|1_3\rangle \equiv (|1_H, 1_V\rangle + |1_V, 1_H\rangle)/\sqrt{2}$, and $|2_3\rangle \equiv |0_H, 2_V\rangle$ [14]. The simple optical tools which allow full control over the polarization of a photonic qubit are insufficient for full control over a biphotonic qutrit [15]. Consequently even simple state transformations required in qutrit generation, processing, and measurement are extremely limited. Significant progress has been made in biphoton state generation. For example, complex arbitrary state preparation techniques that employ multiple nonlinear crystals [12] and nonmaximally entangled states [16] have been developed.

Here we present and demonstrate a technique that dramatically extends the range of biphotonic qutrit transforms, for use in all stages of qutrit manipulation. The technique is based on a Fock-state filter which employs a measurement-induced nonlinearity to conditionally remove photon number (Fock) states from superpositions [17–22]. We first demonstrate the action of the filter as a qutrit polarizer, which can conditionally remove a single logical qutrit state from a superposition. We then combine this nonlinear operation with standard wave plate rotations to demonstrate the dramatically increased range of qutrit transforms it enables. Finally we present the first instance and full characterization of a polarization entangled photon-biphoton state, which underpins the power of our technique. Such qubit-qutrit states have been studied extensively [23–29] and we suggest an extension to generate this type of entanglement.

We generate our qutrits through double-pair emission from spontaneous parametric down-conversion (Fig. 1). Fourfold coincidences between detectors D1–D4 select, with high probability, the cases of double-pair emission into inputs 1 and 2. The biphoton state in mode 1 is passed through a horizontal polarizer to prepare the logical qutrit state $|0_3\rangle$. Input 2 is passed through a 50% beam splitter; detection at D1 indicates a single photon in mode b; after a polarizing beam splitter this prepares the ancilla polarization qubit ($|0_2\rangle \equiv |1_H\rangle$, $|1_2\rangle \equiv |1_V\rangle$) in the logical state $|0_2\rangle$. Thus a qubit and qutrit arrive simultaneously at the central 50% beam splitter.

A Fock filter relies on nonclassical interference effects [30]. When two indistinguishable photons are injected into modes a and b (Fig. 1), the probability of detecting a single photon in mode d is zero; if two or more photons are injected into mode a, then this probability is nonzero. By injecting a single photon into mode b and detecting a single photon in mode d, single photon terms can therefore be removed from any photon number superposition states

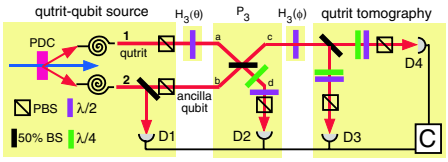


FIG. 1 (color online). Experimental schematic. Emission from a parametric down-conversion (PDC) crystal is coupled into single-mode fiber and injected into modes 1 and 2. Coincident (C) detection of photons at D1–4 selects, with high probability, the cases of double photon-pair emission from the PDC source.

PRL 100, 060504 (2008) PHYSICAL REVIEW LETTERS week ending 15 FEBRUARY 2008

arriving in mode a. By varying the reflectivity of the beam splitter it is possible to conditionally remove any number state from a superposition [21]. This Fock-state filter acts only on light with the same polarization as the ancilla (in our case, horizontal), so by detecting a single horizontal photon in mode d, the logical qutrit state $|1_3\rangle$ is blocked, since it contains a single photon with the same polarization as the ancilla. The remaining logical qutrit states are coherently attenuated.

For a beam splitter of reflectivity 50% the filter acts as a qutrit polarizer described by the operator $\mathbf{P}_3 = |0_3\rangle\langle 0_3| - |2_3\rangle\langle 2_3|$. By varying the polarization of the ancilla, and the reflectivity of the central beam splitter, the operation of our lossy qutrit polarizer can be tuned to preferentially remove the $|0_3\rangle$, $|1_3\rangle$, or $|2_3\rangle$ states. We choose to demonstrate removal of the $|1_3\rangle$ state and include the general operation of the filter for an arbitrary beam splitter reflectivity [31].

The qutrit polarizer offers a powerful tool for transforming between qutrit states. For example, consider the initial qutrit state $|0_3\rangle$ injected into input 1, the red dot of Fig. 2. The black ring shows the limited range of qutrit states, with real coefficients, that are accessible using wave plates [32]. By including the qutrit polarizer the range is dramatically extended to the closed sphere in Fig. 2; the transformation to any real state is possible.

We measure our qutrits by passing mode c through a 50% beam splitter and performing polarization analysis of the two outputs in coincidence, as shown in Fig. 1. This nondeterministically discriminates the logical states $|0_3\rangle$, $|1_3\rangle$, and $|2_3\rangle$ with probabilities $p(0_3) = \frac{1}{2}$, $p(1_3) = \frac{1}{4}$, and $p(2_3) = \frac{1}{2}$. Combining it with single qubit rotations after the beam splitter allows us to perform full qutrit state tomography of mode c. Complete qutrit tomography requires nine independent measurements, which we construct from logical basis states and two-part superpositions [1]. Our method differs from that of Refs. [14,15]. We use convex optimization to reconstruct the qutrit density matrix and Monte Carlo simulations for error analysis [33,34].

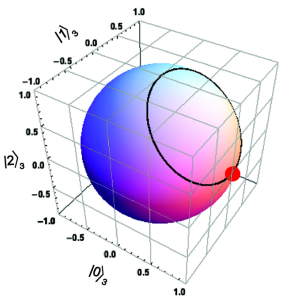


FIG. 2 (color online). Comparison of the range of linearly polarized qutrit states achievable by transforming the state $|0_3\rangle$ (red dot); when using only wave plate operations (black ring); by incorporating our qutrit polarizer, $\mathbf{Q}_3(\alpha)\mathbf{H}_3(\phi)\mathbf{P}_3(\sqrt{0.5})\mathbf{H}_3(\theta)|0_3\rangle$ (sphere) [31,32].

Ideally both the central and tomography beam splitters reflect 50% of both polarizations. In practice, we found that they deviate by a few percent and impart undesired unitary rotations on the optical modes. For the tomography beam splitter, these imperfections modified the nine measured qutrit states; we characterized this effect and incorporated it into the tomographic reconstruction. We found that the effect of the imperfect central beam splitter on the performance of the qutrit polarizer was negligible.

A frequency-doubled mode-locked Ti:Sapphire laser (820 nm $\rightarrow$ 410 nm, $\Delta\tau = 80$ fs at 82 MHz repetition rate) is used to produce photon pairs via parametric down-conversion from a Type I phase-matched 2 mm Bismuth Borate (BiBO) crystal, filtered by blocked interference filters (820 ± 1.5 nm). We collect the down-conversion into single-mode optical fibers. Photons are detected using fiber-coupled single photon counting modules and coincidences measured using a Labview (National Instruments) interfaced quad-logic card (ORTEC CO4020). When directly coupled into detectors the source yielded twofolds at 60 kHz and singles rates at 220 kHz. At the output of the complete circuit we observed fourfold coincidence rates at approximately 1 Hz.

The quality of the nonclassical interference underpinning the qutrit polarizer can be measured directly [21]. Reference [22] relates nonclassical visibilities to a Fock-state filter's ability to block single photon terms. We set all input states and measurement settings to horizontal. Twofold coincidence counts between D2 and D4 show interference between two single photons with visibility $V_{11} = 97 \pm 1\%$. Fourfolds between detectors D1–D4 detect the interference between a photon and a biphoton with visibility $V_{12} = 68 \pm 4\%$. From these visibilities we predict an extinction ratio of $5(\pm 2)$:1 [22]; i.e., our qutrit polarizer will pass the logical $|0_3\rangle$ and $|2_3\rangle$ states at 5 times the rate it passes the logical $|1_3\rangle$ state.

To demonstrate the qutrit polarizer we include a half wave plate in mode a set to $\theta = \frac{\pi}{8}$ to generate the superposition qutrit state [32]:

$$\mathbf{H}_3(\theta)|0_3\rangle = \cos^2 2\theta|0_3\rangle + \sin^2 2\theta|2_3\rangle + \sin 4\theta|1_3\rangle/\sqrt{2}. \quad (1)$$

We measure the output state in mode c without applying the qutrit polarizer. This is achieved by blocking the ancilla photon in mode b and performing qutrit tomography of mode c in twofold coincidence between D3 and D4. The experimentally reconstructed density matrix is shown in Fig. 3(a) and has a near perfect fidelity between the measured and ideal states, $F = 97 \pm 1\%$, and a low linear entropy, $S_L = 6 \pm 7\%$ [35,36]. We then prepare the output state by unblocking the ancilla and, as in all further cases, perform tomography of mode c in fourfold coincidence between D1–D4. The qutrit polarizer is now "on" and we expect the absorption of the logical $|1_3\rangle$ state. The recon-

PRL 100, 060504 (2008) PHYSICAL REVIEW LETTERS week ending 15 FEBRUARY 2008

structed density matrix is shown in Fig. 3(b) and has a lower fidelity with the ideal, $F = 78 \pm 8\%$, and linear entropy $S_L = 47 \pm 14\%$. The relative reduction in the logical $|1_3\rangle$ state probability, when the filter is turned on, yields an extinction ratio of $6.80(\pm 0.07)$:1, consistent with that predicted above.

Measured nonclassical visibilities are significantly limited by higher-order parametric down-conversion photon number terms [37,38]. After removing these effects, as described in Ref. [22], we find a corrected twofold visibility of $V'_{11} = 100 \pm 1\%$, which would be measured given an ideal two-photon source (higher-order effects cannot be distinguished from experimental uncertainty in the fourfold visibility). This corrected visibility can be used to predict the potential performance of our circuit given an ideal source [22]; in this case we predict that the filter would pass the logical $|0_3\rangle$ and $|2_3\rangle$ states at least 24 times the rate it passes the logical $|1_3\rangle$ state. Clearly the performance of our qutrit polarizer is significantly limited by higher-order emissions from our optical source.

Figures 3(c) and 3(d) show experimentally reconstructed density matrices of newly accessible states achieved by incorporating the qutrit polarizer with half wave plate operations applied to the initial state of $|0_3\rangle$; $|1_3\rangle$ and $(|0_3\rangle - |1_3\rangle - |2_3\rangle)/\sqrt{3}$. The fidelities with the ideal are $77 \pm 3\%$ and $83 \pm 7\%$ with linear entropies $51 \pm 7\%$ and $38 \pm 15\%$, respectively. These fidelities exceed the maximum achievable using only linear wave plates (50%) by 9 ± 1 and 5 ± 1 standard deviations, respectively.

The qutrit polarizer employs a measurement-induced nonlinearity whereby the biphoton becomes entangled with the ancilla photon. Instead of detecting the ancilla in a single, fixed polarization state, we can also use tomographic measurements to directly investigate this resultant entangled qubit-qutrit system. Without emphasis to the physical systems involved, such states were first studied by Peres as a special case of his negativity criterion for entanglement; a negativity of 0 (> 0) is conclusive of a

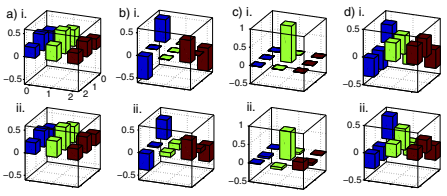


FIG. 3 (color online). Comparison of real parts of (i) ideal and (ii) measured qutrit density matrices. (a) The measured output state with the qutrit polarizer "off" [Eq. (1) for $\theta = \frac{\pi}{8}$]. (b) The output state with the qutrit polarizer "on" showing the removal of the logical $|1_3\rangle$ qutrit state. (c)–(d) Newly accessible qutrit states $|1_3\rangle$ and $(|0_3\rangle - |1_3\rangle - |2_3\rangle)/\sqrt{3}$, respectively. States (b)–(d) all lie on the surface of the sphere of Fig. 2, but not on the ring.

separable (entangled) state [23,39,40]. More recently these states have received a significant amount of attention [23–28] and have been predicted to exhibit novel entanglement sudden death phenomena [29].

On injection of the qutrit state given by Eq. (1) into the Fock filter, we find the following qubit-qutrit joint state of modes c and d:

$$\frac{\cos^2 2\theta |0_2, 0_3\rangle + \sin 4\theta |1_2, 0_3\rangle + \sin^2 2\theta (\sqrt{2}|1_2, 1_3\rangle - |0_2, 2_3\rangle)}{N}, \tag{2}$$

where $N = \sqrt{2 - \cos 4\theta}$. By varying θ we can tune the level of entanglement from zero ($\theta = 0$) to near-maximal ($\theta = \frac{\pi}{4}$), with corresponding negativities of 0 to $\sqrt{8/9} \approx 0.94$, respectively. To perform qubit-qutrit state tomography we use 36 independent measurements constructed from all of the combinations of the aforementioned nine qutrit states and four qubit states (H, V, D, R). Figure 4 shows the measured density matrix for the near-maximally entangled case, which corresponds to the preparation of two vertically polarized photons in mode a. There is a high fidelity of $81 \pm 3\%$ with the ideal state and low linear entropy of $17 \pm 5\%$, and the state is highly entangled with a negativity of 0.77 ± 0.05. We note that a maximally entangled state is predicted for $\theta = \frac{\pi}{4}$ and a central beam splitter reflectivity of $R = \sqrt{2}/(\sqrt{2} + 1) \approx 58.6\%$.

Entangling information carriers to ancilla qubits is an extremely powerful technique [41]: such correlations play a central role in the power of the Fock filter to transform biphotonic qutrits. However, the application of our technique is not limited to extending transforms on single qutrits. We propose that the generation of qubit-qutrit entanglement offers a path to realize multiqutrit operations. For example, a pair of entangled qubit-qutrit states could be used to create qutrit-qutrit entanglement by projecting the qubits into an entangled state using well-known techniques. The much anticipated development of high-brightness single photon sources will make such experiments feasible in the near future. We wish to emphasize that our technique is not limited to manipulating biphotons. The Fock filter can be applied to any system where measurement can induce nonlinear effects, that is, any bosonic encoding of quantum information, including bosonic atoms [42] and time-bin, frequency, and orbital angular momentum encoding of photons.

We have shown that measurement-induced nonlinearities offer significant advantages for the manipulation of higher dimensional bosonic information carriers, specifically biphotonic qutrits. We demonstrated a nonlinear qutrit polarizer, capable of conditionally removing a single logical qutrit state from a superposition and greatly extending the range of possible qutrit transforms. Such tools could find application to quickly generate the mutually unbiased basis states required for optimum security in qutrit quantum-key-distribution protocols [5–7] or as a filtering technique to manipulate entanglement in qutrit-

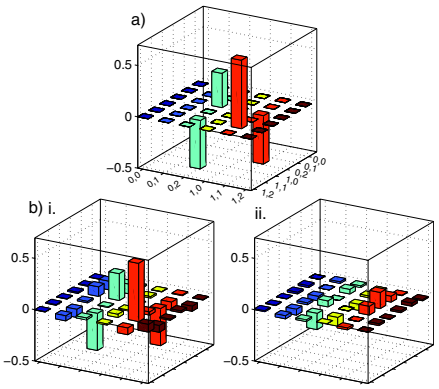


FIG. 4 (color online). Comparison of entangled qubit-qutrit density matrices. (a) Ideal, (b) and (c) measured real and imaginary parts. There is a high fidelity of (81 ± 3%) with the ideal state and low linear entropy (17 ± 5%), and the state is highly entangled with a negativity of 0.77 ± 0.05. The ideal state is given by Eq. (2) for $\theta = \pi/4$. Note the axis label: x,j represents the qubit logical state x and the qutrit logical state j, i.e., $|x_2, j_3\rangle$.

qutrit states. Finally we fully characterized the entangled photon-biphoton state that underpins the power of our technique. This is the first instance of the generation and characterization of entanglement between these distinct physical systems and makes recent theoretical proposals experimentally testable [29]. Besides offering a path to implement novel multiqutrit operations we propose that our technique can be extended to manipulate any bosonic encoding of quantum information.

This work was supported by the Australian Research Council, ARC Discovery Federation, DEST Endeavour Europe programs, and the IARPA-funded U.S. Army Research Office Contract No. W911NF-05-0397.

Note added.—Recently several proposals were presented to which our technique is directly relevant [43–45].

[1] N. K. Langford *et al.*, Phys. Rev. Lett. **93**, 053601 (2004).
[2] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).
[3] G. Molina-Terriza *et al.*, Phys. Rev. Lett. **92**, 167903 (2004).
[4] S. Gröblacher *et al.*, New J. Phys. **8**, 75 (2006).
[5] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[6] N. J. Cerf *et al.*, Phys. Rev. Lett. **88**, 127902 (2002).
[7] T. Durt *et al.*, Phys. Rev. A **67**, 012311 (2003).
[8] M. Fujiwara *et al.*, Phys. Rev. Lett. **90**, 167906 (2003).
[9] D. Collins *et al.*, Phys. Rev. Lett. **88**, 040404 (2002).
[10] D. Kaszlikowski *et al.*, Phys. Rev. A **65**, 032118 (2002).
[11] T. C. Ralph, K. Resch, A. Gilchrist, Phys. Rev. A **75**, 022313 (2007).
[12] Y. I. Bogdanov *et al.*, Phys. Rev. Lett. **93**, 230503 (2004).
[13] A. Mair *et al.*, Nature (London) **412**, 313 (2001).
[14] Y. Bogdanov *et al.*, arXiv:quant-ph/0411192v1.
[15] Y. I. Bogdanov *et al.*, Phys. Rev. A **70**, 042303 (2004).
[16] G. Vallone *et al.*, Phys. Rev. A **76**, 012319 (2007).
[17] A. Grudka and A. Wojcik, Phys. Rev. A **66**, 064303 (2002).
[18] H. F. Hofmann and S. Takeuchi, Phys. Rev. Lett. **88**, 147901 (2002).
[19] X. Zou, K. Pahlke, and W. Mathis, Phys. Rev. A **66**, 064302 (2002).
[20] K. Sanaka *et al.*, Phys. Rev. Lett. **92**, 017902 (2004).
[21] K. Sanaka, K. J. Resch, and A. Zeilinger, Phys. Rev. Lett. **96**, 083601 (2006).
[22] K. J. Resch *et al.*, Phys. Rev. Lett. **98**, 203602 (2007).
[23] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[24] P. B. Slater, Phys. Rev. A **71**, 052319 (2005).
[25] A. Cabello, A. Feito, and A. Lamas-Linares, Phys. Rev. A **72**, 052112 (2005).
[26] O. Osenda and G. A. Raggio, Phys. Rev. A **72**, 064102 (2005).
[27] S. Jami andM. Sarbishei, arXiv:quant-ph/0606039.
[28] P. B. Slater, arXiv:quant-ph/0702134.
[29] K. Ann and G. Jaeger, arXiv:quant-ph/0707.4485.
[30] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[31] For our Fock filter with reflectivity $R = r^2$,
$$\mathbf{P}_3(r) = \begin{bmatrix} r(2-3r^2 & 0 & 0 \\ 0 & r(1-2r^2) & 0 \\ 0 & 0 & -r^3 \end{bmatrix}.$$
[32] From Ref. [15], the wave plate action on a qutrit is
$$\begin{bmatrix} t^2 & \sqrt{2}tr & r^2 \\ -\sqrt{2}tr^* & |t|^2 - |r|^2 & \sqrt{2}t^*r \\ r^{*2} & -\sqrt{2}t^*r^* & t^{*2} \end{bmatrix},$$
where $t = \cos\delta + i\sin\delta\cos2\theta$, $r = i\sin\delta\sin2\theta$, and θ is the wave plate angle. For a half wave plate, $\mathbf{H}_3(\theta)$, $\delta = \pi/2$; for a quarter-wave plate, $\mathbf{Q}_3(\theta)$, $\delta = \pi/4$.
[33] A. Doherty and A. Gilchrist (to be published).
[34] J. L. O'Brien *et al.*, Phys. Rev. Lett. **93**, 080502 (2004).
[35] Fidelity is $F(\rho,\sigma) \equiv \{\mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]\}^2$; linear entropy is $S_L \equiv d(1 - \mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension.
[36] A. G. White *et al.*, J. Opt. Soc. Am. B **24**, 172 (2007).
[37] J. Fulconis *et al.*, Phys. Rev. Lett. **99**, 120501 (2007).
[38] T. J. Weinhold *et al.*, (to be published).
[39] T. Wei *et al.*, Phys. Rev. A **67**, 022110 (2003).
[40] We define negativity, following [39], as $N = \max\{0, -2 * \sum_i \lambda_i\}$, where λ_i are the negative eigenvalues of the partial transpose of the target density matrix.
[41] E. Knill *et al.*, Nature (London) **409**, 46 (2001).
[42] S. Popescu, Phys. Rev. Lett. **99**, 130503 (2007).
[43] I. Bregman *et al.*, arXiv:quant-ph/0709.3804.
[44] C. Bishop and M. S. Byrd, arXiv:quant-ph/0709.0021.
[45] M. Ali *et al.*, arXiv:0710.2238.

8

Conclusion and whereto from here

Linear optical quantum computing has under gone a remarkable turn around since the realisation, in the KLM paper [12] that measurement induced non-linearities, ancilla photons and fast feed-forward can suffice to produce scalable gates. A further boost was the adaptation of the one-way quantum computing idea [7] to optics [8, 9] leading to a wide spread investigation into generation of optical cluster states.

In this thesis, I have described the development of a pulsed parametric down-conversion source cable of generating up to 4 photons simultaneously. In chapter 3, I discuss the application of this source to the development and characterisation of a novel two-photon gate for optical quantum computing. By employing partially polarising beamsplitters, this gate no longer requires classical interferometers to perform the CZ or CNOT logic operations. Hence the alignment difficulty is largely reduced, while the stability is increased and equal performance is achieved. In chapter 4, I continue the investigation in to the behaviour of theses gates, by operating them with independently generated PDC photons. I complete the first full characterisation of an entangling gate between independently generated qubits. The worse than expected gate performance leads me to develop a comprehensive model of this gate. This model, which is in very good agreement with the experimentally measured gate performance, and allows us to derive the first comprehensive and complete error model for any quantum computing architecture. The model allows us to pinpoint the main sources of gate performance degradation. Surprisingly this is not mode matching as expected, but the probabilistic emission of multiple photon pairs in the same spatio-temporal mode.

While experiments have routinely performed gate characterisations and measuring the overlap of the performed gate operation with the intended, no path was known to correlate the experimental gate performance to the error per gate thresholds derived theoretically for fault tolerant quantum computing. We bridge this gap, by developing the first methods that allow benchmarking of experimental gate performance measures with respect to the theoretically derived fault-tolerance thresholds. Using these techniques, we can now find bounds

for the error probability per gate of experimentally characterised gates. Together with the model of the gate, this benchmarking allows the estimation of advances and improvements required to reach the fault-tolerant regime with linear optical quantum computing.

Having identified the main error source in our gate as multi-photon emission, we proceed to implement a quantum logic gate with three qubits and a pair of two qubit gates. Both allow the implement a compiled version of Shor's algorithm [2] to factor the number 15 into its prime factors. We find near perfect algorithmic fidelity despite the non-ideal gate operation, raising the open question of how exactly the individual errors affect the algorithmic performance.

In the final experiments described in this thesis, we work on the expanded Hilbert space of qutrits. We demonstrate a non-linear filter that attenuates states with lower photon number stronger than those with higher photon number. Additionally we employ this filter to entangle a qubit and a qutrit for the first time and show that the filter combined with ordinary waveplates suffices to generate and rotate between all pure qutrit states.

The work demonstrated in this thesis should give rise to a pinpointed approach to minimise the noise sources in linear optical quantum computing. Utilising the demonstrated modelling technique novel sources, gates and detectors could easily be tested for their suitability and the offered improvements for linear optical quantum computing. The benchmarking technique should be able to clearly identify if and when the technological advances theoretically allow fault-tolerant quantum computing. Experimentally this crossover-point will be shifted to lower tolerable error probabilities per gate due to the extensive encoding overhead near the thresholds. That said, the issue of post-selective detection and non-determinism will also need to be addressed. Nevertheless I believe that the tools developed in this thesis can be extended and optimised for identification of error sources in experimental gates and could become useful tools for the characterisation and optimisation of larger quantum logic circuits. Even without reaching the fault-tolerant regime a probabilistic quantum computer with possibly a few tens of qubits could be optimised with such tools and could be a test beds for the first significant quantum calculations, possibly even surpassing classical supercomputers.

An extension of the available and controllable qubit number should also see the rise of the first proof-of-principle implementations of quantum error-correction protocols. Again careful analyses of the performance of these codes similar to the analyses of the gate operation here, could reveal important insights in the required conditions to operate larger scale error correction codes and should thereby assist in prying open the door to linear optical quantum computing a little bit further. Just as I hope that this thesis has succeeded in offering stepping stones between the experimental gates of today and the desired full scale fault tolerant linear optical quantum computation of the future.

A

The independent photon CZ-gate model

The following is a single state run of the model developed to simulate the independent photon gate with the parameters set to model the gate with realistic values for all error sources. As the mathematica code was developed for the numerical solution and not with the idea of reprinting it in my thesis, it has some test functions embedded that are not strictly necessary as well as it makes use of some definitions which are loaded in and are not shown explicitly here. The reason for the reprint here is to merely offer some guidance in the methodology of the model, should anyone wish to recreate a similar model.

I would also like to note, that a model for the case where three qubits interact in two subsequent gates as described in Chapter 6, to study the impact of the noise sources when more photons can potentially interact and especially higher order photon terms can contribute in many additional ways. It turned out though, that the model was to complex to be solved in mathematica for the higher order photon cases. The utilised structure is by no means optimised and an improvement in the memory handling might lead to some results here, but the lack of both time and knowledge have prevented this from occurring so far. Hence I present with out further ado the code for the DD input state which of course means two pre-biased photons are injected so that they would give (individually) balanced diagonally polarised output states.

```
In[1]:= Off[General::spell1]
        Off[General::spell]

In[3]:= Clear[PDC, Loss, ach, acv, adh, adv, af1, af2, ab1, ab2, ab, af, η, ξ, α,
         β, γ, δ, ν, kc, kd, kf2, kb2, asd, zxc, Gate, NoCoinc, NoCoinc1, NoCoinc2,
         NoCoinc3, NoCoinc4, Coinc3Phot, Photon2, Photon3, NoCoinc3, Coinc3Phot,
         b, f, aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4, time1, time2]

In[4]:= << "/Users/till/Documents/MATHEMATICA/LOQC.m"


In[5]:= time1 = AbsoluteTime[];

In[6]:= schrocoeff[coeff_, ind_] := coeff (Times @@ Map[Sqrt[#!] &, ind - 1]) ket[ind - 1];
        ToKets[expr_, modes_, sum_: True] := (tmp = CoefficientList[expr, modes];
          tmp = Flatten[MapIndexed[schrocoeff, tmp, {Length[Dimensions[tmp]]}]];
          If[sum, Plus @@ tmp, tmp])

In[8]:= (* This is the source equation,
         givng the probabilitys of creating 2 photon pairs (1 forward,1 backward)
          and 3 Photon Pairs with at least one in each direction. Other
          terms and orders are ignored.Removed additional factor of 1/2
          that was added with Andrew and Kevin to compensate Bose factors,
         as these are taken care of by the factorials in the fractions.*)

        PDC = (1 / (2 !)) * 2 ab1 ab2 af1 af2 b f +
           (1 / (3 !)) * (3 ab1 ab2 af1^2 af2^2 b (f^2) + 3 ab1^2 ab2^2 af1 af2 (b^2) f);

In[9]:= (*Expand[PDC]*)

In[10]:= (* This section  polarises the modes that are fed into the gate. α,β,γ,
          δ are the input populations for the desired stateloss needs to introduce
           a new mode and relables the modes that go directly to the detectors*)

         Polarise =
           ReplaceAll [PDC, {af1 → (α * aah + β * aav), ab1 → (γ * abh + δ * abv), ab2 → a4, af2 → a3}];

In[11]:= (*Expand[Polarise]/.{aav→aav/Sqrt[3],abv→abv/Sqrt[3]}*)

In[12]:= (* this describes the actions of the gate  with
           reflectivitiy η for h polarised modes and ξ for V Polarisation,
          the input modes are a and b, c and d being the output modes.*)

         Gate = ReplaceAll[Polarise,
            {aah → (-Sqrt[η] * ach + Sqrt[1 - η] * adh), abh → (Sqrt[η] * adh + Sqrt[1 - η] * ach),
             aav → (-Sqrt[ξ] * acv + Sqrt[1 - ξ] * adv), abv → (Sqrt[ξ] * adv + Sqrt[1 - ξ] * acv)}];

In[13]:= (*This section acts as loss for the individual modes just before detection. The
           individual modes are the four spatial modes and two polarisation modes for each
           spatial mode in the actual gate. Make sure all loss modes are distinguishable*)

         Loss = ReplaceAll[Gate, {ach → ach * Sqrt[kc] + aloss1h * Sqrt[(1 - kc)],
             acv → acv * Sqrt[kc] + aloss1v * Sqrt[(1 - kc)],
             adh → adh * Sqrt[kd] + aloss2h * Sqrt[(1 - kd)], adv →
              adv * Sqrt[kd] + aloss2v * Sqrt[(1 - kd)], a3 → a3 * Sqrt[kf2] + aloss3 * Sqrt[(1 - kf2)]
             a4 → a4 * Sqrt[kb2] + aloss4 * Sqrt[(1 - kb2)]}];

In[14]:= (* This gives the final contributions for 2 PDC Pairs*)
         Photon2 = Coefficient[Loss, {b * f}] * b * f;
```

```
In[15]:= (*Sanity check of gate output*)
         (*Expand[(Photon2)/(a3 a4 b f) /. {kc→1,kd→1,kf2→1,kb2→1,
             η→1/3,ξ→1,α→Sqrt[3]/2,β→1/2,γ→Sqrt[3]/2,δ→1/2 }]*)

In[16]:= (* This section collects the terms that
           don't give coincidences for the two pair input*)

         NoCoinc1 = Coefficient[Photon2, {ach^2}] * ach^2;
         NoCoinc2 = Coefficient[Photon2, {acv^2}] * acv^2;
         NoCoinc3 = Coefficient[Photon2, {adh^2}] * adh^2;
         NoCoinc4 = Coefficient[Photon2, {adv^2}] * adv^2;
         NoCoinc5 = Coefficient[Photon2, {ach * acv}] * ach * acv;
         NoCoinc6 = Coefficient[Photon2, {adh * adv}] * adh * adv;
         NoCoinc = NoCoinc1 + NoCoinc2 + NoCoinc3 + NoCoinc4 + NoCoinc5 + NoCoinc6;


In[23]:= (*Check here which terms are removed
           by cycling through the different NoCoinc terms.*)
         (*Expand[NoCoinc6/(a3 a4 b f) /. {kc→1,ks→1,kf2→1,kb2→1,
             η→1/3,ξ→1,α→Sqrt[3]/2,β→1/2,γ→Sqrt[3]/2,δ→1/2 }]*)

In[24]:= (* This section returns only those modes
           that create coincidences for the two pair input *)

         Coinc2Photon = Photon2 - NoCoinc;

In[25]:= (* This selects the output state generated from the three pair-creation cases *)
         Photon3 = Expand[
            (Coefficient[Loss, (b^2) * f] * (b^2) * f) + (Coefficient[Loss, (f^2) * b] * (f^2) * b)];

In[26]:= (*Sanity check of gate output*)
         (*Expand[(Photon3)/(a3 a4 b f) /. {kc→1,kd→1,kf2→1,
             kb2→1,η→1/3,ξ→1,α→Sqrt[3]/2,β→1/2,γ→Sqrt[3]/2,δ→1/2 }]*)

In[27]:= (*And again collect all terms that don't yield actual fourfoulds or
           more percisely coniceidences in the gate, but for the three pair case*)
          NoCoinc3 = Expand[Coefficient[Photon3, {ach^2 * acv}] * ach^2 * acv +
             Coefficient[Photon3, {acv^2 * ach}] * acv^2 * ach +
             Coefficient[Photon3, {adh^2 * adv}] * adh^2 * adv +
             Coefficient[Photon3, {adv^2 * adh}] * adv^2 * adh +
             Coefficient[Photon3, {ach^3}] * ach^3 +
             Coefficient[Photon3, {acv^3}] * acv^3 +
             Coefficient[Photon3, {adh^3}] * adh^3 +
             Coefficient[Photon3, {adv^3}] * adv^3];

In[28]:= (* The collection of all contributing terms for the three pair case*)
         Chop[Coinc3Photon = Photon3 - NoCoinc3, 10^-6];

In[29]:= ClearAll[α, β, γ, δ, η, ξ, kc, kd, kb2, kf2, b,
          f, aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4]

In[30]:= (*Expand[Gate]/.{η→1/3,ξ→1,β→β/Sqrt[3],δ→δ/Sqrt[3] }*)
```

```
In[31]:=
(*Now lets set some values for the variables.*)
η = 0.35; (*Reflection coeff for H*)
ξ = 0.99; (*Reflection coeff for V*)

kf2 = 0.09597;
kb2 = 0.08883;
(* Photon-Survival or Detector-Coupling Probability for trigger photons*)

kc = 0.04675;
kd = 0.02964;
(* Photon-Survival or Detector-Coupling Probability for gate photons*)
(*kc=kd=kf2=kb2=1;(*ideal detection*)*)

α = Sqrt[3] / 2; (* H-Component of a-mode*)
β = 1 / 2; (* V Component of a-mode*)
γ = Sqrt[3] / 2; (* H-Component of b-mode*)
δ = 1 / 2; (* V Component of b-mode*)

b = 2 * Sqrt[0.01085824673785808` / (2 - kb2)](* backward emission amplitude*)
f = 2 * Sqrt[0.004675078456577784` / (2 - kf2)] (*forward emission amplitude*)

Out[38]= 0.150751

Out[39]= 0.0991032

In[40]:= (*Set the path and file name to which the output file is writen*)
SetDirectory["/Users/till/Documents/MATHEMATICA/
    ContainingData/IPGTheory/NewSourceEquation/FullGate"];
FileOutName = "DD.csv";

In[42]:= (*Normalisation check for polarisation modes*)

In[43]:= Abs[α] ^ 2 + Abs[β] ^ 2 == 1
Abs[γ] ^ 2 + Abs[δ] ^ 2 == 1

Out[43]= True

Out[44]= True

In[45]:= (*Addition of dummy variable kkk to the two photon
  term to simplify the use of the PostSelect search routine*)
Expand[Coinc2Photon];
Coinc2Phot = Expand[Coinc2Photon] + kkk;

In[47]:= ClearAll[outHH, outHH1, outHV, outHV1, outVH, outVH1, outVV, outVV1];
```

```
In[48]:= (*The HV-HV POVM*)
         outHH = PostSelect[MatchQ[#, ach * adh * a3 * a4 * _] &] ** Coinc2Phot;
         outHH1 = ToKets[outHH, {ach, acv, adh, adv, a3, a4}];
         HH = Re[(outHH1 /. ket[_] → 1) * Conjugate[(outHH1 /. ket[_] → 1)]]

         outHV = PostSelect[MatchQ[#, ach * adv * a3 * a4 * _] &] ** Coinc2Phot;
         outHV1 = ToKets[outHV, {ach, acv, adh, adv, a3, a4}];
         HV = Re[(outHV1 /. ket[_] → 1) * Conjugate[(outHV1 /. ket[_] → 1)]]

         outVH = PostSelect[MatchQ[#, acv * adh * a3 * a4 * _] &] ** Coinc2Phot;
         outVH1 = ToKets[outVH, {ach, acv, adh, adv, a3, a4}];
         VH = Re[(outVH1 /. ket[_] → 1) * Conjugate[(outVH1 /. ket[_] → 1)]]

         outVV = PostSelect[MatchQ[#, acv * adv * a3 * a4 * _] &] ** Coinc2Phot;
         outVV1 = ToKets[outVV, {ach, acv, adh, adv, a3, a4}];
         VV = Re[(outVV1 /. ket[_] → 1) * Conjugate[(outVV1 /. ket[_] → 1)]]

Out[50]= 1.3348 × 10^-10

Out[53]= 1.27589 × 10^-10

Out[56]= 1.27589 × 10^-10

Out[59]= 1.58264 × 10^-10

In[60]:= (* The HV-PlusMinus POVM *)
         adh = (adpl + admi) / Sqrt[2];
         adv = (adpl - admi) / Sqrt[2];

         outHPl = PostSelect[MatchQ[#, ach * adpl * a3 * a4 * _] &] ** Coinc2Phot;
         outHPl1 = ToKets[outHPl, {ach, acv, adpl, admi, a3, a4}];
         HPl = Re[(outHPl1 /. ket[_] → 1) * Conjugate[(outHPl1 /. ket[_] → 1)]]

         outHMi = PostSelect[MatchQ[#, ach * admi * a3 * a4 * _] &] ** Coinc2Phot;
         outHMi1 = ToKets[outHMi, {ach, acv, adpl, admi, a3, a4}];
         HMi = Re[(outHMi1 /. ket[_] → 1) * Conjugate[(outHMi1 /. ket[_] → 1)]]

         outVPl = PostSelect[MatchQ[#, acv * adpl * a3 * a4 * _] &] ** Coinc2Phot;
         outVPl1 = ToKets[outVPl, {ach, acv, adpl, admi, a3, a4}];
         VPl = Re[(outVPl1 /. ket[_] → 1) * Conjugate[(outVPl1 /. ket[_] → 1)]]

         outVMi = PostSelect[MatchQ[#, acv * admi * a3 * a4 * _] &] ** Coinc2Phot;
         outVMi1 = ToKets[outVMi, {ach, acv, adpl, admi, a3, a4}];
         VMi = Re[(outVMi1 /. ket[_] → 1) * Conjugate[(outVMi1 /. ket[_] → 1)]]

         Clear[adh, adv];

Out[64]= 3.32343 × 10^-14

Out[67]= 2.61036 × 10^-10

Out[70]= 2.85028 × 10^-10

Out[73]= 8.25329 × 10^-13
```

```
In[75]:= (* The HV-RightLeft POVM *)
         adh = (adri + adle) / Sqrt[2];
         adv = -i * (adri - adle) / Sqrt[2];

         outHri = PostSelect[MatchQ[#, ach * adri * a3 * a4 * _] &] ** Coinc2Phot;
         outHri1 = ToKets[outHri, {ach, acv, adri, adle, a3, a4}];
         HRe = Re[(outHri1 /. ket[_] → 1) * Conjugate[(outHri1 /. ket[_] → 1)]]


         outHle = PostSelect[MatchQ[#, ach * adle * a3 * a4 * _] &] ** Coinc2Phot;
         outHle1 = ToKets[outHle, {ach, acv, adri, adle, a3, a4}];
         HLe = Re[(outHle1 /. ket[_] → 1) * Conjugate[(outHle1 /. ket[_] → 1)]]

         outVri = PostSelect[MatchQ[#, acv * adri * a3 * a4 * _] &] ** Coinc2Phot;
         outVri1 = ToKets[outVri, {ach, acv, adri, adle, a3, a4}];
         VRe = Re[(outVri1 /. ket[_] → 1) * Conjugate[(outVri1 /. ket[_] → 1)]]

         outVle = PostSelect[MatchQ[#, acv * adle * a3 * a4 * _] &] ** Coinc2Phot;
         outVle1 = ToKets[outVle, {ach, acv, adri, adle, a3, a4}];
         VLe = Re[(outVle1 /. ket[_] → 1) * Conjugate[(outVle1 /. ket[_] → 1)]]

         Clear[adh, adv];

Out[79]= 1.30534 × 10^-10

Out[82]= 1.30534 × 10^-10

Out[85]= 1.42927 × 10^-10

Out[88]= 1.42927 × 10^-10

In[90]:= (* The PlusMinus-HV POVM *)
         ach = (acpl + acmi) / Sqrt[2];
         acv = (acpl - acmi) / Sqrt[2];

         outPlH = PostSelect[MatchQ[#, acpl * adh * a3 * a4 * _] &] ** Coinc2Phot;
         outPlH1 = ToKets[outPlH, {acpl, acmi, adh, adv, a3, a4}];
         PlH = Re[(outPlH1 /. ket[_] → 1) * Conjugate[(outPlH1 /. ket[_] → 1)]]

         outPlV = PostSelect[MatchQ[#, acpl * adv * a3 * a4 * _] &] ** Coinc2Phot;
         outPlV1 = ToKets[outPlV, {acpl, acmi, adh, adv, a3, a4}];
         PlV = Re[(outPlV1 /. ket[_] → 1) * Conjugate[(outPlV1 /. ket[_] → 1)]]

         outMiH = PostSelect[MatchQ[#, acmi * adh * a3 * a4 * _] &] ** Coinc2Phot;
         outMiH1 = ToKets[outMiH, {acpl, acmi, adh, adv, a3, a4}];
         MiH = Re[(outMiH1 /. ket[_] → 1) * Conjugate[(outMiH1 /. ket[_] → 1)]]

         outMiV = PostSelect[MatchQ[#, acmi * adv * a3 * a4 * _] &] ** Coinc2Phot;
         outMiV1 = ToKets[outMiV, {acpl, acmi, adh, adv, a3, a4}];
         MiV = Re[(outMiV1 /. ket[_] → 1) * Conjugate[(outMiV1 /. ket[_] → 1)]]

         Clear[ach, acv];

Out[94]= 3.32343 × 10^-14

Out[97]= 2.85028 × 10^-10

Out[100]=
       2.61036 × 10^-10

Out[103]=
       8.25329 × 10^-13
```

In[105]:=

```
(*The PlusMinus-PlusMinus POVM*)

ach = (acpl + acmi) / Sqrt[2];
acv = (acpl - acmi) / Sqrt[2];
adh = (adpl + admi) / Sqrt[2];
adv = (adpl - admi) / Sqrt[2];

outPlPl = PostSelect[MatchQ[#, acpl * adpl * a3 * a4 * _] &] ** Coinc2Phot;
outPlPl1 = ToKets[outPlPl, {acpl, acmi, adpl, admi, a3, a4}];
PlPl = Re[(outPlPl1 /. ket[_] → 1) * Conjugate[(outPlPl1 /. ket[_] → 1)]]

outPlMi = PostSelect[MatchQ[#, acpl * admi * a3 * a4 * _] &] ** Coinc2Phot;
outPlMi1 = ToKets[outPlMi, {acpl, acmi, adpl, admi, a3, a4}];
PlMi = Re[(outPlMi1 /. ket[_] → 1) * Conjugate[(outPlMi1 /. ket[_] → 1)]]

outMiPl = PostSelect[MatchQ[#, acmi * adpl * a3 * a4 * _] &] ** Coinc2Phot;
outMiPl1 = ToKets[outMiPl, {acpl, acmi, adpl, admi, a3, a4}];
MiPl = Re[(outMiPl1 /. ket[_] → 1) * Conjugate[(outMiPl1 /. ket[_] → 1)]]

outMiMi = PostSelect[MatchQ[#, acmi * admi * a3 * a4 * _] &] ** Coinc2Phot;
outMiMi1 = ToKets[outMiMi, {acpl, acmi, adpl, admi, a3, a4}];
MiMi = Re[(outMiMi1 /. ket[_] → 1) * Conjugate[(outMiMi1 /. ket[_] → 1)]]

Clear[ach, acv, adh, adv];
```

Out[111]=

$$1.39453 \times 10^{-10}$$

Out[114]=

$$1.45608 \times 10^{-10}$$

Out[117]=

$$1.45608 \times 10^{-10}$$

Out[120]=

$$1.16253 \times 10^{-10}$$

In[122]:=

```
(*The PlusMinus-RightLeft POVM*)

ach = (acpl + acmi) / Sqrt[2];
acv = (acpl - acmi) / Sqrt[2];
adh = (adre + adle) / Sqrt[2];
adv = -i * (adre - adle) / Sqrt[2];

outPlRe = PostSelect[MatchQ[#, acpl * adre * a3 * a4 * _] &] ** Coinc2Phot;
outPlRe1 = ToKets[outPlRe, {acpl, acmi, adre, adle, a3, a4}];
PlRe = Re[(outPlRe1 /. ket[_] → 1) * Conjugate[(outPlRe1 /. ket[_] → 1)]]

outPlLe = PostSelect[MatchQ[#, acpl * adle * a3 * a4 * _] &] ** Coinc2Phot;
outPlLe1 = ToKets[outPlLe, {acpl, acmi, adre, adle, a3, a4}];
PlLe = Re[(outPlLe1 /. ket[_] → 1) * Conjugate[(outPlLe1 /. ket[_] → 1)]]

outMiRe = PostSelect[MatchQ[#, acmi * adre * a3 * a4 * _] &] ** Coinc2Phot;
outMiRe1 = ToKets[outMiRe, {acpl, acmi, adre, adle, a3, a4}];
MiRe = Re[(outMiRe1 /. ket[_] → 1) * Conjugate[(outMiRe1 /. ket[_] → 1)]]

outMiLe = PostSelect[MatchQ[#, acmi * adle * a3 * a4 * _] &] ** Coinc2Phot;
outMiLe1 = ToKets[outMiLe, {acpl, acmi, adre, adle, a3, a4}];
MiLe = Re[(outMiLe1 /. ket[_] → 1) * Conjugate[(outMiLe1 /. ket[_] → 1)]]

Clear[ach, acv, adh, adv];
```

Out[128]=

$$1.42531 \times 10^{-10}$$

Out[131]=

$$1.42531 \times 10^{-10}$$

Out[134]=

$$1.3093 \times 10^{-10}$$

Out[137]=

$$1.3093 \times 10^{-10}$$

In[139]:=

```
(*The RightLeft-HV POVM*)

ach = (acre + acle) / Sqrt[2];
acv = -i * (acre - acle) / Sqrt[2];

outReH = PostSelect[MatchQ[#, acre * adh * a3 * a4 * _] &] ** Coinc2Phot;
outReH1 = ToKets[outReH, {acre, acle, adh, adv, a3, a4}];
ReH = Re[(outReH1 /. ket[_] → 1) * Conjugate[(outReH1 /. ket[_] → 1)]]

outReV = PostSelect[MatchQ[#, acre * adv * a3 * a4 * _] &] ** Coinc2Phot;
outReV1 = ToKets[outReV, {acre, acle, adh, adv, a3, a4}];
ReV = Re[(outReV1 /. ket[_] → 1) * Conjugate[(outReV1 /. ket[_] → 1)]]

outLeH = PostSelect[MatchQ[#, acle * adh * a3 * a4 * _] &] ** Coinc2Phot;
outLeH1 = ToKets[outLeH, {acre, acle, adh, adv, a3, a4}];
LeH = Re[(outLeH1 /. ket[_] → 1) * Conjugate[(outLeH1 /. ket[_] → 1)]]

outLeV = PostSelect[MatchQ[#, acle * adv * a3 * a4 * _] &] ** Coinc2Phot;
outLeV1 = ToKets[outLeV, {acre, acle, adh, adv, a3, a4}];
LeV = Re[(outLeV1 /. ket[_] → 1) * Conjugate[(outLeV1 /. ket[_] → 1)]]

Clear[ach, acv];
```

Out[143]=

$$1.30534 \times 10^{-10}$$

Out[146]=

$$1.42927 \times 10^{-10}$$

Out[149]=

$$1.30534 \times 10^{-10}$$

Out[152]=

$$1.42927 \times 10^{-10}$$

In[154]:=

In[155]:=

```
(*The RightLeft-PlusMinus POVM*)

ach = (acre + acle) / Sqrt[2];
acv = -i * (acre - acle) / Sqrt[2];
adh = (adpl + admi) / Sqrt[2];
adv = (adpl - admi) / Sqrt[2];

outRepl = PostSelect[MatchQ[#, acre * adpl * a3 * a4 * _] &] ** Coinc2Phot;
outRepl1 = ToKets[outRepl, {acre, acle, adpl, admi, a3, a4}];
RePl = Re[(outRepl1 /. ket[_] → 1) * Conjugate[(outRepl1 /. ket[_] → 1)]]

outRemi = PostSelect[MatchQ[#, acre * admi * a3 * a4 * _] &] ** Coinc2Phot;
outRemi1 = ToKets[outRemi, {acre, acle, adpl, admi, a3, a4}];
ReMi = Re[(outRemi1 /. ket[_] → 1) * Conjugate[(outRemi1 /. ket[_] → 1)]]

outLepl = PostSelect[MatchQ[#, acle * adpl * a3 * a4 * _] &] ** Coinc2Phot;
outLepl1 = ToKets[outLepl, {acre, acle, adpl, admi, a3, a4}];
LePl = Re[(outLepl1 /. ket[_] → 1) * Conjugate[(outLepl1 /. ket[_] → 1)]]

outLemi = PostSelect[MatchQ[#, acle * admi * a3 * a4 * _] &] ** Coinc2Phot;
outLemi1 = ToKets[outLemi, {acre, acle, adpl, admi, a3, a4}];
LeMi = Re[(outLemi1 /. ket[_] → 1) * Conjugate[(outLemi1 /. ket[_] → 1)]]

Clear[ach, acv, adh, adv];
```

Out[161]=

$$1.42531 \times 10^{-10}$$

Out[164]=

$$1.3093 \times 10^{-10}$$

Out[167]=

$$1.42531 \times 10^{-10}$$

Out[170]=

$$1.3093 \times 10^{-10}$$

In[172]:=
```
(*The RightLeft-RightLeft POVM*)

ach = (acre + acle) / Sqrt[2];
acv = -i (acre - acle) / Sqrt[2];
adh = (adre + adle) / Sqrt[2];
adv = -i * (adre - adle) / Sqrt[2];

outReRe = PostSelect[MatchQ[#, acre * adre * a3 * a4 * _] &] ** Coinc2Phot;
outReRe1 = ToKets[outReRe, {acre, acle, adre, adle, a3, a4}];
ReRe = Re[(outReRe1 /. ket[_] → 1) * Conjugate[(outReRe1 /. ket[_] → 1)]]

outReLe = PostSelect[MatchQ[#, acre * adle * a3 * a4 * _] &] ** Coinc2Phot;
outReLe1 = ToKets[outReLe, {acre, acle, adre, adle, a3, a4}];
ReLe = Re[(outReLe1 /. ket[_] → 1) * Conjugate[(outReLe1 /. ket[_] → 1)]]

outLere = PostSelect[MatchQ[#, acle * adre * a3 * a4 * _] &] ** Coinc2Phot;
outLere1 = ToKets[outLere, {acre, acle, adre, adle, a3, a4}];
LeRe = Re[(outLere1 /. ket[_] → 1) * Conjugate[(outLere1 /. ket[_] → 1)]]

outLele = PostSelect[MatchQ[#, acle * adle * a3 * a4 * _] &] ** Coinc2Phot;
outLele1 = ToKets[outLele, {acre, acle, adre, adle, a3, a4}];
LeLe = Re[(outLele1 /. ket[_] → 1) * Conjugate[(outLele1 /. ket[_] → 1)]]

Clear[ach, acv, adh, adv];
```

Out[178]=
$$2.73197 \times 10^{-10}$$

Out[181]=
$$2.63664 \times 10^{-13}$$

Out[184]=
$$2.63664 \times 10^{-13}$$

Out[187]=
$$2.73197 \times 10^{-10}$$

In[189]:=
```
MeasuredCounts = Re[{HH, HV, HPl, HMi, HRe, HLe, VH, VV, VPl, VMi, VRe,
    VLe, PlH, PlV, PlPl, PlMi, PlRe, PlLe, MiH, MiV, MiPl, MiMi, MiRe, MiLe,
    ReH, ReV, RePl, ReMi, ReRe, ReLe, LeH, LeV, LePl, LeMi, LeRe, LeLe}];
```

In[190]:=
```
(*Here is the tensor product definition*)
kron[u_ /; MatrixQ[u], v_ /; MatrixQ[v]] := Module[{w}, w = Outer[Times, u, v];
   Partition[Flatten[Transpose[w, {1, 3, 2, 4}]],
    Dimensions[w][[2]] Dimensions[w][[4]]]];
SetAttributes[kron, OneIdentity];
kron[u_, v_, w__] := Fold[kron, u, {v, w}];
CircleTimes = kron;
<< Graphics`Graphics3D`
```

In[195]:=

```
(*This is the matrix from Daniel' s paper*)
pM = {{t1, 0, 0, 0}, {t5 + I * t6, t2, 0, 0},
   {t7 + I * t8, t9 + I * t10, t3, 0}, {t11 + I * t12, t13 + I * t14, t15 + I * t16, t4}};
pMd = {{t1, t5 - I * t6, t7 - I * t8, t11 - I * t12}, {0, t2, t9 - I * t10, t13 - I * t14},
   {0, 0, t3, t15 - I * t16}, {0, 0, 0, t4}};
(*pM//MatrixForm*)
(*The product of pM and pMd makes the
  parametrized density matrix guaranteed to be a physical state*)
GeneralDM = Simplify[pMd.pM];
Prediction[DM_, State_] := Conjugate[Flatten[State]].DM.Flatten[State];
(*GeneralDM//MatrixForm*)
```

In[199]:=

```
(*Define the single qubit measurements*)
H = {{1}, {0}};
V = {{0}, {1}};
Pl = {{1 / Sqrt[2]}, {1 / Sqrt[2]}};
Mi = {{1 / Sqrt[2]}, {-1 / Sqrt[2]}};
Ri = {{1 / Sqrt[2]}, {I / Sqrt[2]}};
Le = {{1 / Sqrt[2]}, {-I / Sqrt[2]}};
```

In[205]:=

```
MeasuredStates =
  {kron[H, H], kron[H, V], kron[H, Pl], kron[H, Mi], kron[H, Ri], kron[H, Le],
   kron[V, H], kron[V, V], kron[V, Pl], kron[V, Mi], kron[V, Ri], kron[V, Le],
   kron[Pl, H], kron[Pl, V], kron[Pl, Pl], kron[Pl, Mi], kron[Pl, Ri], kron[Pl, Le],
   kron[Mi, H], kron[Mi, V], kron[Mi, Pl], kron[Mi, Mi], kron[Mi, Ri], kron[Mi, Le],
   kron[Ri, H], kron[Ri, V], kron[Ri, Pl], kron[Ri, Mi], kron[Ri, Ri], kron[Ri, Le],
   kron[Le, H], kron[Le, V], kron[Le, Pl], kron[Le, Mi], kron[Le, Ri], kron[Le, Le]};
```

In[206]:=

```
MaxLikError[DM_] :=
 Sum[Simplify[(Prediction[DM, MeasuredStates[[i]]] - MeasuredCounts[[i]]) ^ 2],
  {i, Length[MeasuredStates]}]
BadnessPolynomial = MaxLikError[GeneralDM];
MinimizeOutput = NMinimize[BadnessPolynomial, {t1, t2, t3, t4, t5, t6,
    t7, t8, t9, t10, t11, t12, t13, t14, t15, t16}, MaxIterations → 1000];
UnnormalizedDensityMatrix = GeneralDM /. MinimizeOutput[[2]];
DensityMatrix =
  UnnormalizedDensityMatrix / Sum[UnnormalizedDensityMatrix[[i, i]], {i, 4}];
```

In[211]:=

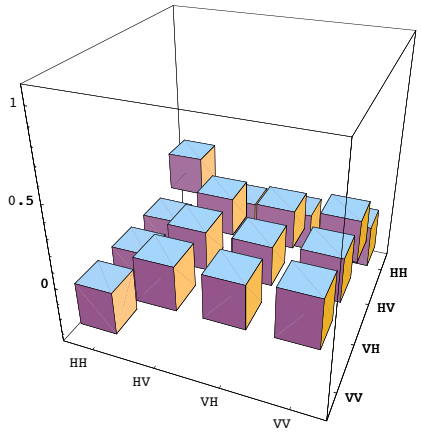
```
Chop[DensityMatrix] // MatrixForm
```

Out[211]//MatrixForm=

$$\begin{pmatrix} 0.244056 & -0.23861 + 3.16228 \times 10^{-9}\, i & -0.23861 - 1.0873 \times 10^{-9}\, i & -0.26575 \\ -0.23861 - 3.16228 \times 10^{-9}\, i & 0.233286 & 0.233286 + 1.10301 \times 10^{-9}\, i & 0.25982 \\ -0.23861 + 1.0873 \times 10^{-9}\, i & 0.233286 - 1.10301 \times 10^{-9}\, i & 0.233286 & 0.25982 \\ -0.26575 & 0.25982 & 0.25982 & 0.289373 \end{pmatrix}$$

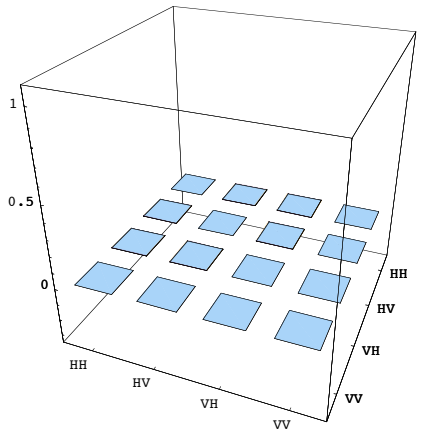
In[212]:=

```
BarChart3D[Re[DensityMatrix], XSpacing → 0.4,
 YSpacing → 0.4, PlotRange → {{0.5, 4.5}, {0.5, 4.5}, {-0.35, 1.1}},
 Ticks -> {{{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}},
   {{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}}, Automatic}, ViewPoint → {2, 0.8, 1.2}]
BarChart3D[Im[DensityMatrix], XSpacing → 0.4, YSpacing → 0.4,
 PlotRange → {{0.5, 4.5}, {0.5, 4.5}, {-0.35, 1.1}},
 Ticks -> {{{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}},
   {{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}}, Automatic}, ViewPoint → {2, 0.8, 1.2}]
```



Out[212]=

- Graphics3D -



Out[213]=

- Graphics3D -

In[214]:=

```
(* And now for the 3 Photons in the gate terms. Again use kkk as a dummy variable*)

Chop[Coinc3Phot = Coinc3Photon + kkk];
```

In[215]:=

```
(*The HV-HV POVM*)
outHH2 = PostSelect[MatchQ[#, ach- * adh * _ | ach * adh- * _ | ach * adh * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outHH = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] ** (outHH2 + ppp + lll);
HHx = ToKets[outHH,
   {ach, acv, adh, adv, a3, a4, aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[HHx[[0]] == Times], outHH1 = HHx * Conjugate[HHx],
  outHH1 = Sum[HHx[[i]] * Conjugate[HHx[[i]]], {i, 1, Length[HHx]}]];
HH1 = Re[(outHH1 /. ket[_] → 1)]

outHV2 = PostSelect[MatchQ[#, ach- * adv * _ | ach * adv- * _ | ach * adv * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outHV = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] ** (outHV2 + ppp + lll);
HVx = ToKets[outHV,
   {ach, acv, adh, adv, a3, a4, aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[HVx[[0]] == Times], outHV1 = HVx * Conjugate[HVx],
  outHV1 = Sum[HVx[[i]] * Conjugate[HVx[[i]]], {i, 1, Length[HVx]}]];
HV1 = Re[(outHV1 /. ket[_] → 1)]

outVH2 = PostSelect[MatchQ[#, acv- * adh * _ | acv * adh- * _ | acv * adh * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outVH = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] ** (outVH2 + ppp + lll);
VHx = ToKets[outVH,
   {ach, acv, adh, adv, a3, a4, aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[VHx[[0]] == Times], outVH1 = VHx * Conjugate[VHx],
  outVH1 = Sum[VHx[[i]] * Conjugate[VHx[[i]]], {i, 1, Length[VHx]}]];
VH1 = Re[(outVH1 /. ket[_] → 1)]

outVV2 = PostSelect[MatchQ[#, acv- * adv * _ | acv * adv- * _ | acv * adv * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outVV = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] ** (outVV2 + ppp + lll);
VVx = ToKets[outVV,
   {ach, acv, adh, adv, a3, a4, aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[VVx[[0]] == Times], outVV1 = VVx * Conjugate[VVx],
  outVV1 = Sum[VVx[[i]] * Conjugate[VVx[[i]]], {i, 1, Length[VVx]}]];
VV1 = Re[(outVV1 /. ket[_] → 1)]
```

Out[219]=

$$5.77514 \times 10^{-11}$$

Out[224]=

$$4.29153 \times 10^{-11}$$

Out[229]=

$$2.76898 \times 10^{-11}$$

Out[234]=

$$1.97826 \times 10^{-11}$$

In[235]:=

```
(* The HV-PlusMinus POVM *)
adh = (adpl + admi) / Sqrt[2];
adv = (adpl - admi) / Sqrt[2];

outHPl2 = PostSelect[MatchQ[#, ach- * adpl * _ | ach * adpl- * _ | ach * adpl * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outHPl = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outHPl2 + ppp + lll);
HPlx = ToKets[outHPl, {ach, acv, adpl, admi, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[HPlx[[0]] == Times], outHPl1 = HPlx * Conjugate[HPlx],
  outHPl1 = Sum[HPlx[[i]] * Conjugate[HPlx[[i]]], {i, 1, Length[HPlx]}]];
HPl1 = Re[(outHPl1 /. ket[_] → 1)]

outHMi2 = PostSelect[MatchQ[#, ach- * admi * _ | ach * admi- * _ | ach * admi * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outHMi = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outHMi2 + ppp + lll);
HMix = ToKets[outHMi, {ach, acv, adpl, admi, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[HMix[[0]] == Times], outHMi1 = HMix * Conjugate[HMix],
  outHMi1 = Sum[HMix[[i]] * Conjugate[HMix[[i]]], {i, 1, Length[HMix]}]];
HMi1 = Re[(outHMi1 /. ket[_] → 1)]

outVPl2 = PostSelect[MatchQ[#, acv- * adpl * _ | acv * adpl- * _ | acv * adpl * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outVPl = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outVPl2 + ppp + lll);
VPlx = ToKets[outVPl, {ach, acv, adpl, admi, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[VPlx[[0]] == Times], outVPl1 = VPlx * Conjugate[VPlx],
  outVPl1 = Sum[VPlx[[i]] * Conjugate[VPlx[[i]]], {i, 1, Length[VPlx]}]];
VPl1 = Re[(outVPl1 /. ket[_] → 1)]

outVMi2 = PostSelect[MatchQ[#, acv- * admi * _ | acv * admi- * _ | acv * admi * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outVMi = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outVMi2 + ppp + lll);
VMix = ToKets[outVMi, {ach, acv, adpl, admi, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[VMi[[0]] == Times], outVMi1 = VMix * Conjugate[VMix],
  outVMi1 = Sum[VMix[[i]] * Conjugate[VMix[[i]]], {i, 1, Length[VMix]}]];
VMi1 = Re[(outVMi1 /. ket[_] → 1)]

Clear[adh, adv];
```

Out[241]=

$$6.34599 \times 10^{-11}$$

Out[246]=

$$3.73657 \times 10^{-11}$$

Out[251]=

$$4.2135 \times 10^{-11}$$

Out[256]=

$$5.22917 \times 10^{-12}$$

In[258]:=

```
(* The HV-RightLeft POVM *)
adh = (adri + adle) / Sqrt[2];
adv = -i * (adri - adle) / Sqrt[2];

outHRe2 = PostSelect[MatchQ[#, ach- * adri * _ | ach * adri- * _ | ach * adri * _] &] **
   Expand[Chop[Coinc3Phot, 10^(-20)]];
outHRe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outHRe2 + ppp + lll);
HRex = ToKets[outHRe, {ach, acv, adri, adle, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[HRex[[0]] == Times], outHRe1 = HRex * Conjugate[HRex],
  outHRe1 = Sum[HRex[[i]] * Conjugate[HRex[[i]]], {i, 1, Length[HRex]}]];
HRe1 = Re[(outHRe1 /. ket[_] → 1)]

outHLe2 = PostSelect[MatchQ[#, ach- * adle * _ | ach * adle- * _ | ach * adle * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outHLe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outHLe2 + ppp + lll);
HLex = ToKets[outHLe, {ach, acv, adri, adle, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[HLex[[0]] == Times], outHLe1 = HLex * Conjugate[HLex],
  outHLe1 = Sum[HLex[[i]] * Conjugate[HLex[[i]]], {i, 1, Length[HLex]}]];
HLe1 = Re[(outHLe1 /. ket[_] → 1)]

outVRe2 = PostSelect[MatchQ[#, acv- * adri * _ | acv * adri- * _ | acv * adri * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outVRe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outVRe2 + ppp + lll);
VRex = ToKets[outVRe, {ach, acv, adri, adle, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[VRex[[0]] == Times], outVRe1 = VRex * Conjugate[VRex],
  outVRe1 = Sum[VRex[[i]] * Conjugate[VRex[[i]]], {i, 1, Length[VRex]}]];
VRe1 = Re[(outVRe1 /. ket[_] → 1)]

outVLe2 = PostSelect[MatchQ[#, acv- * adle * _ | acv * adle- * _ | acv * adle * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outVLe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outVLe2 + ppp + lll);
VLex = ToKets[outVLe, {ach, acv, adri, adle, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[VLex[[0]] == Times], outVLe1 = VLex * Conjugate[VLex],
  outVLe1 = Sum[VLex[[i]] * Conjugate[VLex[[i]]], {i, 1, Length[VLex]}]];
VLe1 = Re[(outVLe1 /. ket[_] → 1)]

Clear[adh, adv];
```

Out[264]=

$$5.02997 \times 10^{-11}$$

Out[269]=

$$5.02997 \times 10^{-11}$$

Out[274]=

$$2.37328 \times 10^{-11}$$

Out[279]=

$$2.37328 \times 10^{-11}$$

In[281]:=

```
(* The PlusMinus-HV POVM *)
ach = (acpl + acmi) / Sqrt[2];
acv = (acpl - acmi) / Sqrt[2];


outPlH2 = PostSelect[MatchQ[#, acpl- * adh * _ | acpl * adh- * _ | acpl * adh * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outPlH = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outPlH2 + ppp + lll);
PlHx = ToKets[outPlH, {acpl, acmi, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[PlHx[[0]] == Times], outPlH1 = PlHx * Conjugate[PlHx],
  outPlH1 = Sum[PlHx[[i]] * Conjugate[PlHx[[i]]], {i, 1, Length[PlHx]}]];
PlH1 = Re[(outPlH1 /. ket[_] → 1)]

outPlV2 = PostSelect[MatchQ[#, acpl- * adv * _ | acpl * adv- * _ | acpl * adv * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outPlV = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outPlV2 + ppp + lll);
PlVx = ToKets[outPlV, {acpl, acmi, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[PlVx[[0]] == Times], outPlV1 = PlVx * Conjugate[PlVx],
  outPlV1 = Sum[PlVx[[i]] * Conjugate[PlVx[[i]]], {i, 1, Length[PlVx]}]];
PlV1 = Re[(outPlV1 /. ket[_] → 1)]

outMiH2 = PostSelect[MatchQ[#, acmi- * adh * _ | acmi * adh- * _ | acmi * adh * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outMiH = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outMiH2 + ppp + lll);
MiHx = ToKets[outMiH, {acpl, acmi, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[MiHx[[0]] == Times], outMiH1 = MiHx * Conjugate[MiHx],
  outMiH1 = Sum[MiHx[[i]] * Conjugate[MiHx[[i]]], {i, 1, Length[MiHx]}]];
MiH1 = Re[(outMiH1 /. ket[_] → 1)]

outMiV2 = PostSelect[MatchQ[#, acmi- * adv * _ | acmi * adv- * _ | acmi * adv * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outMiV = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outMiV2 + ppp + lll);
MiVx = ToKets[outMiV, {acpl, acmi, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[MiVx[[0]] == Times], outMiV1 = MiVx * Conjugate[MiVx],
  outMiV1 = Sum[MiVx[[i]] * Conjugate[MiVx[[i]]], {i, 1, Length[MiVx]}]];
MiV1 = Re[(outMiV1 /. ket[_] → 1)]

Clear[ach, acv];
```

Out[287]=

$$4.07672 \times 10^{-11}$$

Out[292]=

$$5.0525 \times 10^{-11}$$

Out[297]=

$$4.45395 \times 10^{-11}$$

Out[302]=

$$1.20101 \times 10^{-11}$$

In[304]:=

```
(*The PlusMinus-PlusMinus POVM*)

ach = (acpl + acmi) / Sqrt[2];
acv = (acpl - acmi) / Sqrt[2];
adh = (adpl + admi) / Sqrt[2];
adv = (adpl - admi) / Sqrt[2];

outPlPl2 = PostSelect[MatchQ[#, acpl^- * adpl * _ | acpl * adpl^- * _ | acpl * adpl * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outPlPl = PostSelect[MatchQ[#, a3^- * a4 * _ | a3 * a4^- * _ | a3 * a4 * _] &] **
   (outPlPl2 + ppp + lll);
PlPlx = ToKets[outPlPl, {acpl, acmi, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[PlPlx[[0]] == Times], outPlPl1 = PlPlx * Conjugate[PlPlx],
  outPlPl1 = Sum[PlPlx[[i]] * Conjugate[PlPlx[[i]]], {i, 1, Length[PlPlx]}]];
PlPl1 = Re[(outPlPl1 /. ket[_] → 1)]

outPlMi2 = PostSelect[MatchQ[#, acpl^- * admi * _ | acpl * admi^- * _ | acpl * admi * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outPlMi = PostSelect[MatchQ[#, a3^- * a4 * _ | a3 * a4^- * _ | a3 * a4 * _] &] **
   (outPlMi2 + ppp + lll);
PlMix = ToKets[outPlMi, {acpl, acmi, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[PlMix[[0]] == Times], outPlMi1 = PlMix * Conjugate[PlMix],
  outPlMi1 = Sum[PlMix[[i]] * Conjugate[PlMix[[i]]], {i, 1, Length[PlMix]}]];
PlMi1 = Re[(outPlMi1 /. ket[_] → 1)]

outMiPl2 = PostSelect[MatchQ[#, acmi^- * adpl * _ | acmi * adpl^- * _ | acmi * adpl * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outMiPl = PostSelect[MatchQ[#, a3^- * a4 * _ | a3 * a4^- * _ | a3 * a4 * _] &] **
   (outMiPl2 + ppp + lll);
MiPlx = ToKets[outMiPl, {acpl, acmi, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[MiPlx[[0]] == Times], outMiPl1 = MiPlx * Conjugate[MiPlx],
  outMiPl1 = Sum[MiPlx[[i]] * Conjugate[MiPlx[[i]]], {i, 1, Length[MiPlx]}]];
MiPl1 = Re[(outMiPl1 /. ket[_] → 1)]

outMiMi2 = PostSelect[MatchQ[#, acmi^- * admi * _ | acmi * admi^- * _ | acmi * admi * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outMiMi = PostSelect[MatchQ[#, a3^- * a4 * _ | a3 * a4^- * _ | a3 * a4 * _] &] **
   (outMiMi2 + ppp + lll);
MiMix = ToKets[outMiMi, {acpl, acmi, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[MiMix[[0]] == Times], outMiMi1 = MiMix * Conjugate[MiMix],
  outMiMi1 = Sum[MiMix[[i]] * Conjugate[MiMix[[i]]], {i, 1, Length[MiMix]}]];
MiMi1 = Re[(outMiMi1 /. ket[_] → 1)]

Clear[ach, acv, adh, adv];
```

Out[312]=

$$6.30406 \times 10^{-11}$$

Out[317]=

$$2.83034 \times 10^{-11}$$

Out[322]=

$$4.21579 \times 10^{-11}$$

Out[327]=

$$1.43907 \times 10^{-11}$$

In[329]:=

```
(*The PlusMinus-RightLeft POVM*)

ach = (acpl + acmi) / Sqrt[2];
acv = (acpl - acmi) / Sqrt[2];
adh = (adre + adle) / Sqrt[2];
adv = -i * (adre - adle) / Sqrt[2];

outPlRe2 = PostSelect[MatchQ[#, acpl- * adre * _ | acpl * adre- * _ | acpl * adre * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outPlRe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outPlRe2 + ppp + lll);
PlRex = ToKets[outPlRe, {acpl, acmi, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[PlRex[[0]] == Times], outPlRe1 = PlRex * Conjugate[PlRex],
  outPlRe1 = Sum[PlRex[[i]] * Conjugate[PlRex[[i]]], {i, 1, Length[PlRex]}]];
PlRe1 = Re[(outPlRe1 /. ket[_] → 1)]

outPlLe2 = PostSelect[MatchQ[#, acpl- * adle * _ | acpl * adle- * _ | acpl * adle * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outPlLe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outPlLe2 + ppp + lll);
PlLex = ToKets[outPlLe, {acpl, acmi, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[PlLex[[0]] == Times], outPlLe1 = PlLex * Conjugate[PlLex],
  outPlLe1 = Sum[PlLex[[i]] * Conjugate[PlLex[[i]]], {i, 1, Length[PlLex]}]];
PlLe1 = Re[(outPlLe1 /. ket[_] → 1)]

outMiRe2 = PostSelect[MatchQ[#, acmi- * adre * _ | acmi * adre- * _ | acmi * adre * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outMiRe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outMiRe2 + ppp + lll);
MiRex = ToKets[outMiRe, {acpl, acmi, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[MiRex[[0]] == Times], outMiRe1 = MiRex * Conjugate[MiRex],
  outMiRe1 = Sum[MiRex[[i]] * Conjugate[MiRex[[i]]], {i, 1, Length[MiRex]}]];
MiRe1 = Re[(outMiRe1 /. ket[_] → 1)]

outMiLe2 = PostSelect[MatchQ[#, acmi- * adle * _ | acmi * adle- * _ | acmi * adle * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outMiLe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outMiLe2 + ppp + lll);
MiLex = ToKets[outMiLe, {acpl, acmi, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[MiLex[[0]] == Times], outMiLe1 = MiLex * Conjugate[MiLex],
  outMiLe1 = Sum[MiLex[[i]] * Conjugate[MiLex[[i]]], {i, 1, Length[MiLex]}]];
MiLe1 = Re[(outMiLe1 /. ket[_] → 1)]

Clear[ach, acv, adh, adv];
```

Out[337]=

$$4.55871 \times 10^{-11}$$

Out[342]=

$$4.55871 \times 10^{-11}$$

Out[347]=

$$2.82968 \times 10^{-11}$$

Out[352]=

$$2.82968 \times 10^{-11}$$

In[354]:=

```
(*The RightLeft-HV POVM*)

ach = (acre + acle) / Sqrt[2];
acv = -i * (acre - acle) / Sqrt[2];

outReH2 = PostSelect[MatchQ[#, acre- * adh * _ | acre * adh- * _ | acre * adh * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outReH = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outReH2 + ppp + lll);
ReHx = ToKets[outReH, {acre, acle, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[ReHx[[0]] == Times], outReH1 = ReHx * Conjugate[ReHx],
  outReH1 = Sum[ReHx[[i]] * Conjugate[ReHx[[i]]], {i, 1, Length[ReHx]}]];
ReH1 = Re[(outReH1 /. ket[_] → 1)]

outReV2 = PostSelect[MatchQ[#, acre- * adv * _ | acre * adv- * _ | acre * adv * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outReV = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outReV2 + ppp + lll);
ReVx = ToKets[outReV, {acre, acle, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[ReVx[[0]] == Times], outReV1 = ReVx * Conjugate[ReVx],
  outReV1 = Sum[ReVx[[i]] * Conjugate[ReVx[[i]]], {i, 1, Length[ReVx]}]];
ReV1 = Re[(outReV1 /. ket[_] → 1)]

outLeH2 = PostSelect[MatchQ[#, acle- * adh * _ | acle * adh- * _ | acle * adh * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outLeH = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outLeH2 + ppp + lll);
LeHx = ToKets[outLeH, {acre, acle, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[LeHx[[0]] == Times], outLeH1 = LeHx * Conjugate[LeHx],
  outLeH1 = Sum[LeHx[[i]] * Conjugate[LeHx[[i]]], {i, 1, Length[LeHx]}]];
LeH1 = Re[(outLeH1 /. ket[_] → 1)]

outLeV2 = PostSelect[MatchQ[#, acle- * adv * _ | acle * adv- * _ | acle * adv * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outLeV = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outLeV2 + ppp + lll);
LeVx = ToKets[outLeV, {acre, acle, adh, adv, a3, a4, aloss1h,
    aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[LeVx[[0]] == Times], outLeV1 = LeVx * Conjugate[LeVx],
  outLeV1 = Sum[LeVx[[i]] * Conjugate[LeVx[[i]]], {i, 1, Length[LeVx]}]];
LeV1 = Re[(outLeV1 /. ket[_] → 1)]

Clear[ach, acv];
```

Out[360]=

$$4.25792 \times 10^{-11}$$

Out[365]=

$$3.13377 \times 10^{-11}$$

Out[370]=

$$4.25792 \times 10^{-11}$$

Out[375]=

$$3.13377 \times 10^{-11}$$

In[377]:=

```
(*The RightLeft-PlusMinus POVM*)

ach = (acre + acle) / Sqrt[2];
acv = -i * (acre - acle) / Sqrt[2];
adh = (adpl + admi) / Sqrt[2];
adv = (adpl - admi) / Sqrt[2];


outRePl2 = PostSelect[MatchQ[#, acre- * adpl * _ | acre * adpl- * _ | acre * adpl * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outRePl = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outRePl2 + ppp + lll);
RePlx = ToKets[outRePl, {acre, acle, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[RePlx[[0]] == Times], outRePl1 = RePlx * Conjugate[RePlx],
  outRePl1 = Sum[RePlx[[i]] * Conjugate[RePlx[[i]]], {i, 1, Length[RePlx]}]];
RePl1 = Re[(outRePl1 /. ket[_] → 1)]

outReMi2 = PostSelect[MatchQ[#, acre- * admi * _ | acre * admi- * _ | acre * admi * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outReMi = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outReMi2 + ppp + lll);
ReMix = ToKets[outReMi, {acre, acle, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[ReMix[[0]] == Times], outReMi1 = ReMix * Conjugate[ReMix],
  outReMi1 = Sum[ReMix[[i]] * Conjugate[ReMix[[i]]], {i, 1, Length[ReMix]}]];
ReMi1 = Re[(outReMi1 /. ket[_] → 1)]

outLePl2 = PostSelect[MatchQ[#, acle- * adpl * _ | acle * adpl- * _ | acle * adpl * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outLePl = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outLePl2 + ppp + lll);
LePlx = ToKets[outLePl, {acre, acle, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[LePlx[[0]] == Times], outLePl1 = LePlx * Conjugate[LePlx],
  outLePl1 = Sum[LePlx[[i]] * Conjugate[LePlx[[i]]], {i, 1, Length[LePlx]}]];
LePl1 = Re[(outLePl1 /. ket[_] → 1)]

outLeMi2 = PostSelect[MatchQ[#, acle- * admi * _ | acle * admi- * _ | acle * admi * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outLeMi = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outLeMi2 + ppp + lll);
LeMix = ToKets[outLeMi, {acre, acle, adpl, admi, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[LeMix[[0]] == Times], outLeMi1 = LeMix * Conjugate[LeMix],
  outLeMi1 = Sum[LeMix[[i]] * Conjugate[LeMix[[i]]], {i, 1, Length[LeMix]}]];
LeMi1 = Re[(outLeMi1 /. ket[_] → 1)]

Clear[ach, acv, adh, adv];
```

Out[385]=

$$5.25793 \times 10^{-11}$$

Out[390]=

$$2.13629 \times 10^{-11}$$

Out[395]=

$$5.25793 \times 10^{-11}$$

Out[400]=

$$2.13629 \times 10^{-11}$$

In[402]:=

```
(*The RightLeft-RightLeft POVM*)

ach = (acre + acle) / Sqrt[2];
acv = -i (acre - acle) / Sqrt[2];
adh = (adre + adle) / Sqrt[2];
adv = -i * (adre - adle) / Sqrt[2];

outReRe2 = PostSelect[MatchQ[#, acre- * adre * _ | acre * adre- * _ | acre * adre * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outReRe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outReRe2 + ppp + lll);
ReRex = ToKets[outReRe, {acre, acle, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[ReRex[[0]] == Times], outReRe1 = ReRex * Conjugate[ReRex],
  outReRe1 = Sum[ReRex[[i]] * Conjugate[ReRex[[i]]], {i, 1, Length[ReRex]}]];
ReRe1 = Re[(outReRe1 /. ket[_] → 1)]

outReLe2 = PostSelect[MatchQ[#, acre- * adle * _ | acre * adle- * _ | acre * adle * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outReLe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outReLe2 + ppp + lll);
ReLex = ToKets[outReLe, {acre, acle, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[ReLex[[0]] == Times], outReLe1 = ReLex * Conjugate[ReLex],
  outReLe1 = Sum[ReLex[[i]] * Conjugate[ReLex[[i]]], {i, 1, Length[ReLex]}]];
ReLe1 = Re[(outReLe1 /. ket[_] → 1)]

outLeRe2 = PostSelect[MatchQ[#, acle- * adre * _ | acle * adre- * _ | acle * adre * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outLeRe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outLeRe2 + ppp + lll);
LeRex = ToKets[outLeRe, {acre, acle, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[LeRex[[0]] == Times], outLeRe1 = LeRex * Conjugate[LeRex],
  outLeRe1 = Sum[LeRex[[i]] * Conjugate[LeRex[[i]]], {i, 1, Length[LeRex]}],];
LeRe1 = Re[(outLeRe1 /. ket[_] → 1 )]

outLeLe2 = PostSelect[MatchQ[#, acle- * adle * _ | acle * adle- * _ | acle * adle * _] &] **
   Chop[Coinc3Phot, 10^(-20)];
outLeLe = PostSelect[MatchQ[#, a3- * a4 * _ | a3 * a4- * _ | a3 * a4 * _] &] **
   (outLeLe2 + ppp + lll);
LeLex = ToKets[outLeLe, {acre, acle, adre, adle, a3, a4,
    aloss1h, aloss1v, aloss2h, aloss2v, aloss3, aloss4}];
If[TrueQ[LeLex[[0]] == Times], outLeLe1 = LeLex * Conjugate[LeLex],
  outLeLe1 = Sum[LeLex[[i]] * Conjugate[LeLex[[i]]], {i, 1, Length[LeLex]}]];
LeLe1 = Re[(outLeLe1 /. ket[_] → 1)]

Clear[ach, acv, adh, adv];
```

Out[410]=

$$5.35749 \times 10^{-11}$$

Out[415]=

$$2.03049 \times 10^{-11}$$

Out[420]=

$$2.03049 \times 10^{-11}$$

Out[425]=

$$5.35749 \times 10^{-11}$$

In[427]:=

```
N[MeasuredCounts1 =
   Re[{HH1, HV1, HPl1, HMi1, HRe1, HLe1, VH1, VV1, VPl1, VMi1, VRe1, VLe1, PlH1, PlV1,
     PlPl1, PlMi1, PlRe1, PlLe1, MiH1, MiV1, MiPl1, MiMi1, MiRe1, MiLe1, ReH1,
     ReV1, RePl1, ReMi1, ReRe1, ReLe1, LeH1, LeV1, LePl1, LeMi1, LeRe1, LeLe1}]];
```

In[428]:=

```
MaxLikError1[DM_] :=
 Sum[Simplify[(Prediction[DM, MeasuredStates[[i]]] - MeasuredCounts1[[i]])^2],
  {i, Length[MeasuredStates]}]
BadnessPolynomial1 = MaxLikError1[GeneralDM];
MinimizeOutput1 = NMinimize[BadnessPolynomial1, {t1, t2, t3, t4, t5, t6,
    t7, t8, t9, t10, t11, t12, t13, t14, t15, t16}, MaxIterations → 1000];
UnnormalizedDensityMatrix1 = GeneralDM /. MinimizeOutput1[[2]];
DensityMatrix1 =
  UnnormalizedDensityMatrix1 / Sum[UnnormalizedDensityMatrix1[[i, i]], {i, 4}];
Chop[DensityMatrix1] // MatrixForm
```

Out[433]//MatrixForm=

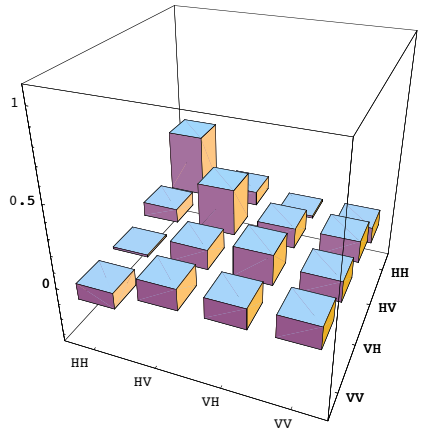
$$\begin{pmatrix} 0.390029 & 0.0875988 & -0.0128117 & -0.100672 \\ 0.0875988 & 0.289999 & 0.124231 & 0.130117 \\ -0.0128117 & 0.124231 & 0.186582 & 0.124142 \\ -0.100672 & 0.130117 & 0.124142 & 0.133391 \end{pmatrix}$$

In[434]:=

```
(*Eigensystem[DensityMatrix1]//Chop*)
```

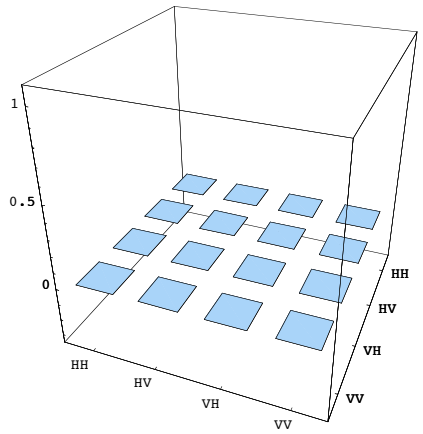
In[435]:=

```
BarChart3D[Re[DensityMatrix1], XSpacing → 0.4,
 YSpacing → 0.4, PlotRange → {{0.5, 4.5}, {0.5, 4.5}, {-0.35, 1.1}},
 Ticks -> {{{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}},
   {{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}}, Automatic}, ViewPoint → {2, 0.8, 1.2}]
BarChart3D[Im[DensityMatrix1], XSpacing → 0.4, YSpacing → 0.4,
 PlotRange → {{0.5, 4.5}, {0.5, 4.5}, {-0.35, 1.1}},
 Ticks -> {{{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}},
   {{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}}, Automatic}, ViewPoint → {2, 0.8, 1.2}]
```



Out[435]=

- Graphics3D -



Out[436]=

- Graphics3D -

In[437]:=

```
(*Comparison of the Individual Probailities of the two-pair,
 the three pair and the combined case.*)
N[MeasuredCounts]
N[MeasuredCounts1]
N[MeasuredCounts2 = MeasuredCounts + MeasuredCounts1]
```

Out[437]=

$$\{1.3348\times10^{-10}, 1.27589\times10^{-10}, 3.32343\times10^{-14}, 2.61036\times10^{-10},$$
$$1.30534\times10^{-10}, 1.30534\times10^{-10}, 1.27589\times10^{-10}, 1.58264\times10^{-10},$$
$$2.85028\times10^{-10}, 8.25329\times10^{-13}, 1.42927\times10^{-10}, 1.42927\times10^{-10},$$
$$3.32343\times10^{-14}, 2.85028\times10^{-10}, 1.39453\times10^{-10}, 1.45608\times10^{-10},$$
$$1.42531\times10^{-10}, 1.42531\times10^{-10}, 2.61036\times10^{-10}, 8.25329\times10^{-13}, 1.45608\times10^{-10},$$
$$1.16253\times10^{-10}, 1.3093\times10^{-10}, 1.3093\times10^{-10}, 1.30534\times10^{-10}, 1.42927\times10^{-10},$$
$$1.42531\times10^{-10}, 1.3093\times10^{-10}, 2.73197\times10^{-10}, 2.63664\times10^{-13}, 1.30534\times10^{-10},$$
$$1.42927\times10^{-10}, 1.42531\times10^{-10}, 1.3093\times10^{-10}, 2.63664\times10^{-13}, 2.73197\times10^{-10}\}$$

Out[438]=

$$\{5.77514\times10^{-11}, 4.29153\times10^{-11}, 6.34599\times10^{-11}, 3.73657\times10^{-11},$$
$$5.02997\times10^{-11}, 5.02997\times10^{-11}, 2.76898\times10^{-11}, 1.97826\times10^{-11},$$
$$4.2135\times10^{-11}, 5.22917\times10^{-12}, 2.37328\times10^{-11}, 2.37328\times10^{-11}, 4.07672\times10^{-11},$$
$$5.0525\times10^{-11}, 6.30406\times10^{-11}, 2.83034\times10^{-11}, 4.55871\times10^{-11}, 4.55871\times10^{-11},$$
$$4.45395\times10^{-11}, 1.20101\times10^{-11}, 4.21579\times10^{-11}, 1.43907\times10^{-11},$$
$$2.82968\times10^{-11}, 2.82968\times10^{-11}, 4.25792\times10^{-11}, 3.13377\times10^{-11},$$
$$5.25793\times10^{-11}, 2.13629\times10^{-11}, 5.35749\times10^{-11}, 2.03049\times10^{-11}, 4.25792\times10^{-11},$$
$$3.13377\times10^{-11}, 5.25793\times10^{-11}, 2.13629\times10^{-11}, 2.03049\times10^{-11}, 5.35749\times10^{-11}\}$$

Out[439]=

$$\{1.91231\times10^{-10}, 1.70504\times10^{-10}, 6.34931\times10^{-11}, 2.98401\times10^{-10},$$
$$1.80834\times10^{-10}, 1.80834\times10^{-10}, 1.55279\times10^{-10}, 1.78047\times10^{-10},$$
$$3.27163\times10^{-10}, 6.0545\times10^{-12}, 1.66659\times10^{-10}, 1.66659\times10^{-10}, 4.08005\times10^{-11},$$
$$3.35553\times10^{-10}, 2.02493\times10^{-10}, 1.73912\times10^{-10}, 1.88118\times10^{-10},$$
$$1.88118\times10^{-10}, 3.05575\times10^{-10}, 1.28355\times10^{-11}, 1.87766\times10^{-10},$$
$$1.30643\times10^{-10}, 1.59227\times10^{-10}, 1.59227\times10^{-10}, 1.73114\times10^{-10}, 1.74264\times10^{-10},$$
$$1.9511\times10^{-10}, 1.52293\times10^{-10}, 3.26772\times10^{-10}, 2.05686\times10^{-11}, 1.73114\times10^{-10},$$
$$1.74264\times10^{-10}, 1.9511\times10^{-10}, 1.52293\times10^{-10}, 2.05686\times10^{-11}, 3.26772\times10^{-10}\}$$

In[440]:=

```
MaxLikError2[DM_] :=
 Sum[Simplify[(Prediction[DM, MeasuredStates[[i]]] - MeasuredCounts2[[i]])^2],
   {i, Length[MeasuredStates]}]
BadnessPolynomial2 = MaxLikError2[GeneralDM];
MinimizeOutput2 = NMinimize[BadnessPolynomial2, {t1, t2, t3, t4, t5, t6,
    t7, t8, t9, t10, t11, t12, t13, t14, t15, t16}, MaxIterations → 1000];
UnnormalizedDensityMatrix2 = GeneralDM /. MinimizeOutput2[[2]];
DensityMatrix2 =
  UnnormalizedDensityMatrix2 / Sum[UnnormalizedDensityMatrix2[[i, i]], {i, 4}];
```

In[445]:=

```
(*Comparison of Density Matrices for the "ideal" two
  pair case and the combined case*)Chop[DensityMatrix] // MatrixForm
Chop[DensityMatrix1] // MatrixForm
Chop[DensityMatrix2] // MatrixForm
```

Out[445]//MatrixForm=

$$\begin{pmatrix} 0.244056 & -0.23861 + 3.16228 \times 10^{-9}\, i & -0.23861 - 1.0873 \times 10^{-9}\, i & -0.26575 \\ -0.23861 - 3.16228 \times 10^{-9}\, i & 0.233286 & 0.233286 + 1.10301 \times 10^{-9}\, i & 0.25982 \\ -0.23861 + 1.0873 \times 10^{-9}\, i & 0.233286 - 1.10301 \times 10^{-9}\, i & 0.233286 & 0.25982 \\ -0.26575 & 0.25982 & 0.25982 & 0.289373 \end{pmatrix}$$

Out[446]//MatrixForm=

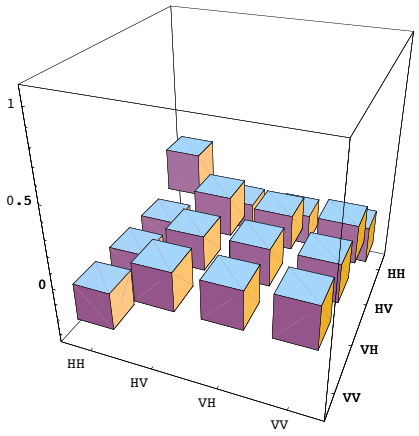
$$\begin{pmatrix} 0.390029 & 0.0875988 & -0.0128117 & -0.100672 \\ 0.0875988 & 0.289999 & 0.124231 & 0.130117 \\ -0.0128117 & 0.124231 & 0.186582 & 0.124142 \\ -0.100672 & 0.130117 & 0.124142 & 0.133391 \end{pmatrix}$$

Out[447]//MatrixForm=

$$\begin{pmatrix} 0.275133 & -0.169162 & -0.190539 & -0.230606 \\ -0.169162 & 0.24536 & 0.210068 & 0.232207 \\ -0.190539 & 0.210068 & 0.223343 & 0.230935 \\ -0.230606 & 0.232207 & 0.230935 & 0.256165 \end{pmatrix}$$

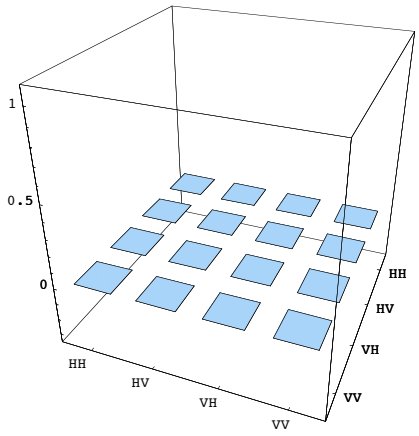
In[448]:=

```
(* Plot of the combined case*)
BarChart3D[Re[DensityMatrix2], XSpacing → 0.4,
 YSpacing → 0.4, PlotRange → {{0.5, 4.5}, {0.5, 4.5}, {-0.35, 1.1}},
 Ticks -> {{{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}},
   {{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}}, Automatic}, ViewPoint → {2, 0.8, 1.2}]
BarChart3D[Im[DensityMatrix2], XSpacing → 0.4, YSpacing → 0.4,
 PlotRange → {{0.5, 4.5}, {0.5, 4.5}, {-0.35, 1.1}},
 Ticks -> {{{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}},
   {{1, "HH"}, {2, "HV"}, {3, "VH"}, {4, "VV"}}, Automatic}, ViewPoint → {2, 0.8, 1.2}]
```



Out[448]=

- Graphics3D -



Out[449]=

- Graphics3D -

In[450]:=

```
(*Gate with ideal beamsplitters*)

Output2x = {{-(1 / 3) * α * γ}, {Sqrt[(1 / 3)] α * δ}, {Sqrt[(1 / 3)] β * γ}, {β * δ}};
ExpectDM2x = Output2x.Conjugate[Transpose[Output2x]];
idealDM = N[ExpectDM2x / Tr[ExpectDM2x]];
idealDM // MatrixForm
```

Out[453]//MatrixForm=

$$\begin{pmatrix} 0.25 & -0.25 & -0.25 & -0.25 \\ -0.25 & 0.25 & 0.25 & 0.25 \\ -0.25 & 0.25 & 0.25 & 0.25 \\ -0.25 & 0.25 & 0.25 & 0.25 \end{pmatrix}$$

In[454]:=

```
theo1 = DensityMatrix;
theo = DensityMatrix2;
```

In[456]:=

```
(*Fiedelity Ideal-Modell with ideal source*)
Fidideallinput = Re[Chop[Tr[MatrixPower[
       MatrixPower[theo1, 1 / 2].idealDM.MatrixPower[theo1, 1 / 2], 1 / 2]]^2]];
(*Fiedelity Ideal-Modell*)
Fid = Re[Chop[
    Tr[MatrixPower[MatrixPower[theo, 1 / 2].idealDM.MatrixPower[theo, 1 / 2], 1 / 2]]^2]]
```

In[458]:=

```
Print["The fidelity of the theoretical prediction with an ideal source
   for the realistic gate and loss with the ideal is ", Fididealinput, ".

 The fidelity of the theoretical Prediction
   of the entire realistic gate with the ideal is ", Fid]
```

```
The fidelity of the theoretical prediction with
   an ideal source for the realistic gate and loss with the ideal is
 0.997948.   The fidelity of the theoretical Prediction of the
   entire realistic gate with the ideal is 0.881759
```

In[459]:=

```
(*Normalisation step before creating the output file
  for the Tomography reconstruction*)POVMHH = MeasuredCounts2[[1]] +
     MeasuredCounts2[[2]] + MeasuredCounts2[[7]] + MeasuredCounts2[[8]];
POVMHD = MeasuredCounts2[[3]] + MeasuredCounts2[[4]] +
     MeasuredCounts2[[9]] + MeasuredCounts2[[10]];
POVMHR = MeasuredCounts2[[5]] + MeasuredCounts2[[6]] +
     MeasuredCounts2[[11]] + MeasuredCounts2[[12]];
POVMDH = MeasuredCounts2[[13]] + MeasuredCounts2[[14]] +
     MeasuredCounts2[[19]] + MeasuredCounts2[[20]];
POVMDD = MeasuredCounts2[[15]] + MeasuredCounts2[[16]] +
     MeasuredCounts2[[21]] + MeasuredCounts2[[22]];
POVMDR = MeasuredCounts2[[17]] + MeasuredCounts2[[18]] +
     MeasuredCounts2[[23]] + MeasuredCounts2[[24]];
POVMRH = MeasuredCounts2[[25]] + MeasuredCounts2[[26]] +
     MeasuredCounts2[[31]] + MeasuredCounts2[[32]];
POVMRD = MeasuredCounts2[[27]] + MeasuredCounts2[[28]] +
     MeasuredCounts2[[33]] + MeasuredCounts2[[34]];
POVMRR = MeasuredCounts2[[29]] + MeasuredCounts2[[30]] +
```

```
MeasuredCounts2[[35]] + MeasuredCounts2[[36]];
```

```
Normalise = ( POVMHH
              POVMHH
              POVMHD
              POVMHD
              POVMHR
              POVMHR
              POVMHH
              POVMHH
              POVMHD
              POVMHD
              POVMHR
              POVMHR
              POVMDH
              POVMDH
              POVMDD
              POVMDD
              POVMDR
              POVMDR
              POVMDH
              POVMDH
              POVMDD
              POVMDD
              POVMDR
              POVMDR
              POVMRH
              POVMRH
              POVMRD
              POVMRD
              POVMRR
              POVMRR
              POVMRH
              POVMRH
              POVMRD
              POVMRD
              POVMRR
              POVMRR );
```

```
Done = Chop[N[MeasuredCounts2 / Normalise]];
```

In[460]:=
```
Export[FileOutName, Done];
```

In[461]:=
```
time2 = AbsoluteTime[];
```

In[462]:=
```
duration = time2 - time1;
```

In[463]:=

```
Print["The total eveluation time for the notebook is ", duration]
```

```
The total eveluation time for the notebook is 136.348559
```

References

[1] R. Feynman. Int. J. of theor. Phys. **21**, 467 (1982).

[2] P. W. Shor. Proc. 35th Annu. Symp. Foundations of Computer Science, IEEE Computer Society, Los Alamitos, CA, pp. 124–134 (1994). Ed. S. Goldwasser.

[3] J. I. Cirac and P. Zoller. *Quantum computation with cold trapped ions.* Phys. Rev. Lett. **74**, 4091 (1995).

[4] R. Rivest, A. Shamir, and L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM **21**, 120 (1978).

[5] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon. *Simulated Quantum Computation of Molecular Energies.* Science **309**, 1704 (2005).

[6] D. P. DiVincenzo. *The physical implementation of quantum computation* (2000). URL `quant-ph/0002077`.

[7] R. Raussendorf and H. J. Briegel. *A one-way quantum computer.* Phys. Rev. Lett. **86**, 5188 (2001).

[8] M. A. Nielsen. *Optical quantum computation using cluster states.* Phys. Rev. Lett. **93**, 040503 (2004).

[9] D. E. Brown and T. Rudolph. *Resource-efficient linear optical quantum computation.* Phys. Rev. Lett. **95**, 010501 (2004).

[10] N. K. Langford. *Encoding, manipulating and measuring quantum information in optics.* The University of Queensland PhD thesis (2007).

[11] R. Menzel. *Photonics* (Springer-Verlag, Berlin, 2001).

[12] E. Knill, R. Laflamme, and G. J. Milburn. *A scheme for efficient quantum computation with linear optics.* Nature **409**, 46 (2001).

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

[14] R. Prevedel, P. Walther, F. Tiefenbacher, P. Bohi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. *High-speed linear optics quantum computing using active feed-forward.* Nature **445**, 65 (2007).

[15] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, and M. Fürst. *Entanglement-based quantum communication over 144 km.* Nature Physics **3**, 481 (2007).

[16] *A quantum information science and technology roadmap* (2004). URL `http://qist.lanl.gov/qcomp_map.shtml`.

[17] M. A. Nielsen. *Optical quantum computation using cluster states* (2004). URL `arXiv.org:quant-ph/0402005`.

[18] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto. *Triggered single photons from a quantum dot.* Phys. Rev. Lett. **86**, 1502 (2001).

[19] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter. *Stable solid-state source of single photons.* Phys. Rev. Lett. **85**, 290 (2000).

[20] A. Kuhn, M. Hennrich, and G. Rempe. *Deterministic single-photon source for distributed quantum networking.* Phys. Rev. Lett. **89**, 067901 (2002).

[21] A. J. Miller, S. W. Nam, J. M. Martinis, and A. V. Sergienko. *Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination.* APL **83**(4), 791 (2003).

[22] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[23] M. Barbieri. *Hyperentangled two photon states for quantum information and nonlocality tests.* University of Rome PhD thesis (2006).

[24] G. G. Stokes. Trans. Cambridge Philos. Soc. **9**, 399 (1852).

[25] J. Fiurášek and Z. c. v. Hradil. *Maximum-likelihood estimation of quantum processes.* PRA **63**, 020101 (2001).

[26] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White. *Measurement of qubits.* Phys. Rev. A **64**, 052312 (2001).

[27] I. Chuang and M. Nielsen. *Prescribtion for experimental determination of the dynamics of a quantum black box.* J. Mod. Opt **44**, 2455 (1996).

[28] J. Poyatos, J. Cirac, and P. Zoller. *Complete characterization of a quantum process: The two-bit quantum gate.* Phys. Rev. Lett. **78**, 390 (1996).

[29] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White. *Quantum process tomography of a controlled-not gate.* Phys. Rev. Lett. **93**, 080502 (2004).

[30] A. Gilchrist, N. Langford, and M. Nielsen. *Distance measures to compare real and ideal quantum processes.* Phys. Rev. A **71**, 062310 (2005).

[31] A. G. White, A. Gilchrist, G. J. Pryde, J. L. O'Brien, M. J. Bremner, and N. K. Langford. *Measuring two-qubit gates.* J. Opt. Soc. Am. B **24**, 172 (2007).

[32] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. *Measurement of conditional phase shifts for quantum logic.* Phys. Rev. Lett. **75**, 4710 (1995).

[33] K. Nemoto and W. J. Munro. *Nearly deterministic linear optical controlled-not gate.* Phys. Rev. Lett. **93**, 250502 (2004).

[34] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn. *Simple scheme for efficient linear optics quantum gates.* Phys. Rev. A **65**, 012314 (2001).

[35] G. J. Pryde, J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph. *Measuring a photonic qubit without destroying it.* Phys. Rev. Lett. **92**, 190402 (2004).

[36] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels.* Phys. Rev. Lett. **70**, 1895 (1993).

[37] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. *Experimental quantum teleportation.* Nature **390**, 575 (1997).

[38] M. A. Nielsen, E. Knill, and R. Laflamme. *Complete quantum teleportation using nuclear magnetic resonance.* Nature **396**, 52 (1998).

[39] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. F. H. J. Kimble, and E. S. Polzik. *Unconditional quantum teleportation.* Nature **282**, 706 (1998).

[40] R. M. Stevenson, R. J. Young, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields. *A semiconductor source of triggered entangled photon pairs.* Nature **439**, 179 (2006).

[41] A. Gilchrist, K. Resch, and A. White. *Quantum information: Source of triggered entangled photon pairs?* Nature **445**, E4 (2007).

[42] M. Stevenson, R. Young, P. Atkinson, K. Cooper, D. Ritchie, and A. Shields. *Quantum information: Source of triggered entangled photon pairs? (reply).* Nature **445**, E5 (2007).

[43] See special issue:. *Focus on single photons on demand.* New Journal of Physics **6** (2004).

[44] D. Klysko. Sov. Phys. JETP **28**, 522 (1969).

[45] D. Burnham and D. Weinberg. *Observation of simultaneity in parametric production of optical photon pairs.* Phys. Rev. Lett. **25**, 84 (1970).

[46] Amnon.Yariv. *Quantum Electronics, 3rd Edition* (John Wiley & Sons Inc, New York, 1988).

[47] K. J. Resch. *Making photonstalk to each other - nonlinear optics in the quantum domain.* University of Toronto (2003).

[48] M. Atatüre, A. V. Sergienko, B. M. Jost, B. E. A. Saleh, and M. C. Teich. *Partial distinguishability in femtosecond optical spontaneous parametric down-conversion.* Phys. Rev. Lett. **83**, 1323 (1999).

[49] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter. *High-efficiency entangled photon pair collection in type-II parametric fluorescence.* Phys. Rev. A **64**, 023802 (2001).

[50] R. Wehner and R. Menzel. *Homing in the ant cataglyphis bicolor.* Science **164**, 192 (1969).

[51] M. Lagunas-Solar. *Method of controlling insects and mites with pulsed ultraviolet light.* Tech. rep. (March,4 1997). United States Patent 5607711.

[52] G. Di Giuseppe, L. Haiberger, F. De Martini, and A. V. Sergienko. *Quantum interference and indistinguishability with femtosecond pulses.* Phys. Rev. A **56**, R21 (1997).

[53] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White. *Demonstration of a simple entangling optical gate and its use in bell-state analysis.* Physical Review Letters **95**, 210504 (2005).

[54] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter. *Linear optics controlled-phase gate made simple.* Physical Review Letters **95**, 210505 (2005).

[55] R. Okamoto, H. F. Hofmann, S. Takeuchi, and K. Sasaki. *Demonstration of an optical quantum controlled-not gate without path interference.* Physical Review Letters **95**, 210506 (2005).

[56] 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).

[57] T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson. *Experimental controlled-not logic gate for single photons in the coincidence basis.* Phys. Rev. A **68**, 032316 (2003).

[58] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger. *Realization of a photonic controlled-not gate sufficient for quantum computation.* Phys. Rev. Lett. **93**, 020504 (2004).

[59] K. Sanaka, T. Jennewein, J.-W. Pan, K. Resch, and A. Zeilinger. *Experimental nonlinear sign shift for linear optics quantum computation.* Phys. Rev. Lett. **92**, 017902 (2004).

[60] T. C. Ralph. *Scaling of multiple postselected quantum gates in optics.* Phys. Rev. A **70**, 012312 (2004).

[61] T. Pittman and J. Franson. *Violation of bell's inequality with photons from independent sources.* Phys. Rev. Lett. **90**, 240401 (2003).

[62] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg. *Super-resolving phase measurement with a multiphoton entangled state.* Nature **429**, 161 (2004).

[63] J. Rarity, P. Tapster, and R. Loudon. *Non-classical interference between independent sources.* arXiv.org:quant-ph/9702032 (1997).

[64] R. Kaltenbaek, B. Blauensteiner, M. Żukowski, M. Aspelmeyer, and A. Zeilinger. *Experimental interference of independent photons.* Phys. Rev. Lett. **96**, 240502 (2006).

[65] Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J.-F. Du, T. Yang, and J.-W. Pan. *Experimental demonstration of a nondestructive controlled-not quantum gate for two independent photon qubits.* Physical Review Letters **94**, 030501 (2005).

[66] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White. *Linear optical controlled-NOT gate in the coincidence basis.* Phys. Rev. A **65**, 062324 (2001).

[67] H. F. Hofmann and S. Takeuchi. *Quantum phase gate for photonic qubits using only beam splitters and postselection.* Phys. Rev. A **66**, 024308 (2001).

[68] K. J. Resch, J. L. O'Brien, T. J. Weinhold, K. Sanaka, B. P. Lanyon, N. K. Langford, and A. G. White. *Entanglement generation by fock-state filtration.* Phys. Rev. Lett. **98**, 203602 (2007).

[69] D. Gottesman. *Fault-tolerant quantum computation* (2007). URL `arXiv.org:quant-ph/0701112`.

[70] P. W. Shor. *Scheme for reducing decoherence in quantum computer memory.* Phys. Rev. A **52**, R2493 (1995).

[71] A. M. Steane. *Error correcting codes in quantum theory.* Phys. Rev. Lett. **77**, 793 (1996).

[72] G. Gilbert, M. Hamrick, and Y. S. Weinstein. *Reliable final computational results from faulty quantum computation* (2007). URL `arXiv.org:quant-ph/0707.0008`.

[73] D. Gottesman. *An introduction to quantum error correction* (2002). URL `arXiv.org:quant-ph/0004072`.

[74] J. Preskill. *Reliable quantum computers.* Proc. R. Soc. London, Ser. A **454**, 385 (1998).

[75] E. Knill. *Quantum computing with realistically noisy devices.* Nature **434**, 39 (2005).

[76] D. Leibfried, B. DeMarco, V. Meyer, D. Lucas, M. Barrett, J. Britton, W. M. Itano, B. Jelenkovi, C. Langer, T. Rosenband, and D. J. Wineland. *Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate.* Nature **422**, 412 (2003).

[77] C. F. Roos, G. P. T. Lancaster, M. Riebe, H. Haffner, W. Hansel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, and R. Blatt. *Bell states of atoms with ultralong lifetimes and their tomographic state analysis.* Phys. Rev. Lett. **92**, 220402 (2004).

[78] P. Aliferis, D. Gottesman, and J. Preskill. *Quantum accuracy threshold for concatenated distance-3 codes.* Quant. Inf. Comput. **6**, 97 (2006).

[79] P. Aliferis and J. Preskill. *Fault-tolerant quantum computation against biased noise* (2007). URL `arXiv.org:quant-ph/0710.1301`.

[80] S. Boyd and L. Vandenberghe. *Convex Optimization* (Cambridge University Press, Cambridge, 2004).

[81] R. Blume-Kohout and P. Hayden. *Accurate quantum state estimation via "keeping the experimentalist honest"* (2006). URL `arXiv.org:quant-ph/0603116`.

[82] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan. *Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits.* Physical Review Letters **99**, 250504 (2007).

[83] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. *Efficient networks for quantum factoring.* Phys. Rev. A **54**, 1034 (1996).

[84] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt. *Scalable multiparticle entanglement of trapped ions.* Nature **438**, 643 (2005).

[85] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. *Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance.* Nature **414**, 883 (2001).

[86] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. *Separability of very noisy mixed states and implications for nmr quantum computing.* Phys. Rev. Lett. **83**, 1054 (1999).

[87] N. C. Menicucci and C. M. Caves. *Local realistic model for the dynamics of bulk-ensemble nmr information processing.* Phys. Rev. Lett. **88**, 167901 (2002).

[88] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W. bo Gao, J. Zhang, Z. sheng Yuan, A. Goebel, T. Yang, and J.-W. Pan. *Experimental entanglement of six photons in graph states.* Nature Physics **3**, 91 (2007).

[89] K. Sanaka, K. J. Resch, and A. Zeilinger. *Filtering out photonic fock states.* Physical Review Letters **96**, 083601 (2006).

[90] A. Peres. *Separability criterion for density matrices.* Phys. Rev. Lett. **77**, 1413 (1996).

[91] T.-C. Wei, K. Nemoto, P. M. Goldbart, P. G. Kwiat, W. J. Munro, and F. Verstraete. *Maximal entanglement versus entropy for mixed quantum states.* Phys. Rev. A **67**, 022110 (2003).

[92] B. P. Lanyon, T. J. Weinhold, N. K. Langford, J. L. O'Brien, K. J. Resch, A. Gilchrist, and A. G. White. *Manipulating biphotonic qutrits.* Phys. Rev. Lett. **100**, 060504 (2008).