



UNIVERSAL LINEAR OPTICS:  
CHARACTERISATION, VERIFICATION AND  
COMPUTATION

JACQUES CAROLAN

Department of Physics

A thesis submitted to the University of Bristol in accordance with the requirements for  
the degree of Doctor of Philosophy in the Faculty of Science, Department of Physics.

August 2015



# Abstract

Photonic approaches to quantum information science and technology promise new scientific discoveries and new applications. Linear optics underpins all of these protocols, and the advent of integrated quantum photonics has brought with it a step change in complexity and control over quantum photonic systems. As systems scale up, near-term nonclassical computational possibilities emerge, as does the prospect of practical quantum technologies.

In this work we present a series of linear optical processors comprising the union of a multi-photon source, active and passive waveguide devices, and a single-photon detection system; and use these systems to explore a multitude of quantum information processing protocols. We propose and implement efficient and robust techniques for device level characterisation of linear optical circuitry, where full scale tomographic techniques become intractable. We demonstrate machine level verification protocols for systems whose complexity renders them formally unverifiable, demonstrating the efficacy of our protocols on systems of up to five photons in 21 waveguides, generating Hilbert spaces of 50,000 dimensions. Finally we present a fully reconfigurable universal linear optical processor with sufficient control to implement all possible linear optical protocols up to the size of the circuit. We programme this device to implement heralded quantum logic gates and entangling operations, simultaneous bosons sampling and verification protocols and six dimensional complex Hadamard operations. These results and techniques will find application as large scale universal linear optical processors begin to replace existing and future prototype systems.

---

**ABSTRACT**

## Acknowledgements

First I would like to thank Jeremy and Mark; the environment they have created at the CQP is one of freedom and possibility. It has enabled me to travel the world and appreciate the beauty of research. During my time at the CQP I have been fortunate enough to work with some exceptional scientists and now some good friends. The Walkers: Jonathan, Jasmine, Kostas, Alberto. The Reckers: Pete, Enrique, Nick, Nobuyuki, Chris Harrold and Chris Sparrow. Our discussions, confusions and enlightenments, both in the lab and in front of the whiteboard, have shaped my understanding of physics, and I've enjoyed every moment of it. Finally, Anthony: through countless flat whites, a broken leg, the film recommendations, that final figure ‘tweak’ and the addition of a beautiful baby girl into your life. The term ‘supervisor’ doesn’t do justice. You are a dear friend. Since the first HOM dip your guidance and support has made me the scientist I am today.

---

## ACKNOWLEDGEMENTS

*To my mum.*

---

## ACKNOWLEDGEMENTS

## Authors' Declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: .....

DATE: .....

AUTHORS' DECLARATION

## Publications

J. Carolan, C. Harrold, C. Sparrow, E. Martín López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing,  
Universal linear optics, *Science* **349**, 711 (2015)

J. Carolan, J. D. A. Meinecke, P. J. Shadbolt, N. J. Russell, N. Ismail, K. Wörhoff, T. Rudolph, M. G. Thompson, J. L. O'Brien, J. C. F. Matthews, and A. Laing,  
On the experimental verification of quantum complexity in linear optics,  
*Nature Photonics* **8**, 621 (2014)

---

PUBLICATIONS

# Presentations

University of Mainz Colloquium, Mainz (2015) *Talk*

University of Bonn Physics Colloquium, Bonn (2015) *Invited*

Quantum Simulation and Quantum Walks, Durban (2014) *Invited*

Photon14, London (2014) *Poster*

CLEO:2014, San Jose (2014) *Talk*

Bristol-Rome Colloquium, Rome (2014) *Talk*

GDR - IQFA Colloquium, Paris (2013) *Talk*

University of Bristol Postgraduate Conference, Bristol (2013) *Talk*

AQUTE Winter School on QIP, Obergurgl (2012) *Poster*

---

PRESENTATIONS

# Contents

<b>Abstract</b>	iii
<b>Acknowledgements</b>	v
<b>Authors' Declaration</b>	ix
<b>Publications</b>	xi
<b>Presentations</b>	xiii
<b>1 Introduction</b>	1
1.1 Thesis Outline . . . . .	4
<b>2 Background</b>	5
2.1 Introduction . . . . .	5
2.2 Quantum Mechanics . . . . .	6
2.2.1 The Paintball gun . . . . .	6
2.2.2 Water waves . . . . .	8
2.2.3 Electrons . . . . .	8
2.2.4 Probability Amplitudes . . . . .	9
2.2.5 Axioms of Quantum Mechanics . . . . .	10
2.3 Quantum Information . . . . .	11
2.3.1 The Qubit . . . . .	12

---

## CONTENTS

2.3.2	Single Qubit Operations . . . . .	13
2.3.3	Multiple qubits . . . . .	14
2.3.4	Entanglement . . . . .	15
2.4	Classical Computing . . . . .	17
2.4.1	The Turing Machine . . . . .	17
2.4.2	Computational Complexity . . . . .	19
2.5	Quantum Computing . . . . .	20
2.5.1	BQP . . . . .	21
2.5.2	Building a quantum computer . . . . .	23
2.5.3	Architectures . . . . .	24
2.6	Photonic Qubits . . . . .	25
2.6.1	Mathematical Framework . . . . .	27
2.6.2	Building Blocks of Linear Optics . . . . .	29
2.6.3	Mach-Zehnder interferometer . . . . .	30
2.6.4	Arbitrary Operations . . . . .	32
2.6.5	Two Qubit Gates . . . . .	34
2.6.6	The HOM-trinity . . . . .	36
2.6.7	HOM Powered Two Qubit Gate . . . . .	40
2.7	Concluding Remarks . . . . .	41
<b>3</b>	<b>Photonic Processing Hardware</b>	<b>43</b>
3.1	Introduction . . . . .	44
3.2	Single Photon Sources . . . . .	44
3.2.1	Spontaneous Parametric Down-Conversion . . . . .	46
3.2.2	Principles of Down-Conversion . . . . .	47
3.2.3	Principles of Multi-photon Production . . . . .	54
3.3	Experimental Multi-photon Source . . . . .	59
3.3.1	Source Performance . . . . .	61
3.4	Integrated Quantum Photonics . . . . .	64
3.4.1	Propagation of Light . . . . .	65

## CONTENTS

---

3.4.2	Coupled modes . . . . .	69
3.4.3	Modulation . . . . .	71
3.5	Experimental Platforms . . . . .	72
3.5.1	Silica . . . . .	73
3.5.2	Silicon Oxynitride . . . . .	74
3.5.3	Silicon Nitride . . . . .	75
3.5.4	Interfacing . . . . .	76
3.6	Single Photon Detection . . . . .	79
3.6.1	Experimental Single Photon Counting . . . . .	80
3.7	Concluding Remarks . . . . .	81
<b>4</b>	<b>Hardware Characterisation</b>	<b>83</b>
4.1	Introduction . . . . .	83
4.2	Super-Stable Tomography . . . . .	85
4.2.1	SST Protocol . . . . .	86
4.2.2	A Worked Example . . . . .	88
4.2.3	Resource Scaling . . . . .	90
4.3	SST implementation . . . . .	90
4.4	Iterative SST . . . . .	93
4.5	iSST Implementation . . . . .	94
4.6	Error propagation . . . . .	96
4.7	Error corrected SST . . . . .	98
4.8	Concluding Remarks . . . . .	99
<b>5</b>	<b>Verifying Quantum Complexity</b>	<b>101</b>
5.1	Introduction . . . . .	102
5.2	Quantum Supremacy . . . . .	103
5.3	Quantum Complexity in Linear Optics . . . . .	105
5.3.1	Boson Sampling . . . . .	106
5.3.2	Photons in modes . . . . .	109
5.3.3	Complexity Proof . . . . .	110

---

## CONTENTS

5.3.4	Related work . . . . .	113
5.4	Verification of Quantum Complexity . . . . .	114
5.4.1	Experimental Verification . . . . .	115
5.5	Uniform Distribution . . . . .	117
5.5.1	Experiment . . . . .	119
5.6	Classical Distribution . . . . .	120
5.6.1	Experiment . . . . .	122
5.7	Predictable Quantum Correlations . . . . .	123
5.7.1	Classical Walks . . . . .	123
5.7.2	Quantum Walks . . . . .	125
5.7.3	Multi-photon Quantum Walks . . . . .	126
5.7.4	Bosonic Clouding . . . . .	127
5.7.5	Efficient Verification . . . . .	130
5.8	Concluding Remarks . . . . .	134
<b>6</b>	<b>Universal Linear Optics</b>	<b>137</b>
6.1	Introduction . . . . .	138
6.2	Universal Circuits . . . . .	139
6.3	Reconfigurable LPU . . . . .	143
6.4	Characterisation . . . . .	145
6.4.1	Phase Shifter Calibration . . . . .	145
6.4.2	Crosstalk . . . . .	148
6.5	Benchmarking . . . . .	149
6.5.1	Classical and Quantum Interference . . . . .	149
6.5.2	Phase accuracy . . . . .	150
6.6	Boson Sampling . . . . .	150
6.7	Verifying Boson Sampling . . . . .	151
6.7.1	Six Photon Verification . . . . .	153
6.8	Complex Hadamard Matrices . . . . .	155
6.9	Concluding Remarks . . . . .	156

## CONTENTS

---

<b>7 Quantum Computation with Universal Linear Optics</b>	<b>159</b>
7.1 Introduction . . . . .	160
7.2 Universal Gate Set . . . . .	160
7.2.1 Universal Classical Gates . . . . .	160
7.2.2 Universal Quantum Gates . . . . .	161
7.3 Heralded Quantum Logic Gates . . . . .	162
7.3.1 Nonlinear Sign Shift . . . . .	164
7.3.2 Heralded CNOT gate . . . . .	165
7.3.3 LPU Implementation . . . . .	166
7.3.4 Results . . . . .	169
7.4 Heralded Entangled States . . . . .	169
7.4.1 Measurement Based Quantum Computation . . . . .	169
7.4.2 Bell State Generator . . . . .	171
7.4.3 Experiment . . . . .	172
7.4.4 Results . . . . .	176
7.5 Quantum Process Tomography . . . . .	176
7.6 Verifying Gate Operation . . . . .	178
7.7 Concluding Remarks . . . . .	179
<b>8 Discussion</b>	<b>181</b>
8.1 Key Results . . . . .	181
8.2 Outlook . . . . .	183
<b>Bibliography</b>	<b>185</b>

---

## CONTENTS

# List of Figures

2.1	The double slit experiment . . . . .	7
2.2	The Bloch sphere . . . . .	13
2.3	The Turing machine . . . . .	18
2.4	Photonic qubits . . . . .	26
2.5	The building blocks of linear optics . . . . .	31
2.6	Quantum interference powered two-qubit gates . . . . .	35
3.1	Birefringence . . . . .	47
3.2	Type I SHG and SPDC phase matching . . . . .	51
3.3	Multi-photon architectures . . . . .	56
3.4	Multi-photon error mechanisms . . . . .	58
3.5	Experimental multi-photon source . . . . .	60
3.6	SHG conversion efficiency . . . . .	61
3.7	HOM-interference dips . . . . .	63
3.8	Waveguide propagation . . . . .	66
3.9	A packaged reconfigurable waveguide device . . . . .	78
4.1	The SST protocol . . . . .	86
4.2	Experimental SST . . . . .	91
4.3	Iterative SST for continuously coupled waveguides . . . . .	94
4.4	SST error analysis . . . . .	97

---

## LIST OF FIGURES

---

4.5	Error corrected SST . . . . .	98
5.1	Quantum and classical integer factorisation . . . . .	104
5.2	Matrix permanents and perfect matching . . . . .	109
5.3	Boson sampling flow chart . . . . .	112
5.4	LPU for experimental verification . . . . .	117
5.5	Verification against the uniform distribution . . . . .	118
5.6	Verification against the classical distribution . . . . .	121
5.7	Continuous time quantum walks . . . . .	127
5.8	Three-photon correlation cubes . . . . .	128
5.9	Bosonic clouding metric . . . . .	131
5.10	Four photon sifting . . . . .	132
5.11	Experimental clouding results . . . . .	135
6.1	Building a universal circuit . . . . .	140
6.2	Reconfigurable waveguide geometry . . . . .	143
6.3	Universal linear optical processor . . . . .	146
6.4	Automated LPU characterisation . . . . .	147
6.5	Universal LPU boson sampling . . . . .	152
6.6	Universal LPU verification . . . . .	154
6.7	Complex Hadamard matrices . . . . .	155
7.1	Heralded linear optical gates . . . . .	164
7.2	Universal LPU labelling . . . . .	167
7.3	LPU heralded-CNOT . . . . .	168
7.4	LPU heralded Bell state generator . . . . .	173
7.5	Heralded Bell state generator measurements . . . . .	174
7.6	Quantum process tomography . . . . .	177

## List of Tables

2.1	CNOT truth table . . . . .	14
2.2	Pauli preparation and measurement settings . . . . .	34
3.1	Comparison of waveguide platforms . . . . .	76
4.1	Comparison of resources for SST and iSST . . . . .	95
4.2	Numerical SST results . . . . .	100
4.3	Numerical SST errors . . . . .	100
7.1	Classical logic gates . . . . .	161
7.2	Quantum logic gates . . . . .	162
7.3	Heralded CNOT results . . . . .	170
7.4	Heralded Bell state generator results . . . . .	175



# 1

## Introduction

The purpose of a scientific theory is to explain observations within a coherent framework, in turn giving rise to falsifiable predictions that via the scientific method can be tested, thus corroborating or contradicting that theory. By this criteria there can be no greater scientific theory than that of understanding and explaining precisely how nature works at her most fundamental level. Quantum mechanics describes physical phenomena at the atomic, and sub-atomic scale. Arguably, it is our most well tested scientific theory, and has resulted in measurements of 1 part in  $10^{14}$  for the magnetic moment of a single electron [1] and 1 part in  $10^{20}$  for the radius of a proton [2].

Whilst the pursuit of scientific knowledge is largely driven by a demand for new technology, developing a deeper understanding of nature at the fundamental level is interesting in and of itself. By illuminating as of yet unseen corners of reality

## 1. INTRODUCTION

---

we open ourselves up to anomalous results which ultimately drive paradigm shifts in human understanding [3]. However, there is a second virtue to exploring the depths; the lessons we learn, the techniques we develop, the hurdles we overcome may find application in wholly disparate corners of humanity. Let us consider two examples from the 20th century. Bardeen, Shockley and Brattain's discovery of the transistor at Bell Labs, and Berners-Lee's invention of the World Wide Web at CERN. Is it likely these scientists could have foresaw the changes to society that the fundamental research into semi-conductors or particle physics might have had? Quantum technologies follow in precisely the same vein; utilising the laws of nature at her most fundamental level to build new machines, with intrinsic advantage in precision or computational power, over their classical counterparts.

Historically photons have played a central role in the development of quantum mechanics: from Einstein's postulate of the quantised nature of light [4] to early demonstrations of Bell nonlocality [5–8]; the photon is both an invaluable conceptual and practical tool. More recently, due to their ease of manipulation, low noise properties and light speed propagation, photons have emerged as exceptional carriers of quantum information [9].

It had been known for some time that photons in linear optical circuits are in principle an efficient platform for quantum information processing and quantum computation [10]; yet it wasn't until the development of *integrated quantum photonics* [11, 12] that this platform became practical. Using the same CMOS compatible fabrication processes that are used in the microelectronics industry, micron scale silicon-based waveguides are fabricated, allowing the manipulation of single photons on-chip [11–19]. This has opened up a new regime, not only for scalability, but also for the monolithic integration of on-chip photon sources [20] and detectors [21].

Integration enables greater scalability for photonic quantum information processing, yet there remain significant hurdles for the construction of a universal linear optical quantum computer (LOQC). Significantly, because photons effectively do not interact with one another — one property that contributes to their

---

effectiveness as quantum bits — realising the qubit-qubit interactions required for large scale quantum information processing is challenging. Overcoming this challenge seems possible but places a large overhead on the resources required for LOQC.

Whilst the ultimate aim of the field remains a universal LOQC, a recent theoretical breakthrough [22] has shown that even in the absence of logic gates and entangling operations, linear optics is still a platform intractable to classical simulation, requiring much fewer resources. The realisation of such a *non-universal* LOQC is both of fundamental interest and practical application. Whilst it would demonstrate that linear optics can be harnessed for nonclassical computational capabilities, it would also be a stepping stone towards universal quantum computation; further driving interest in integrated quantum photonics [23–26]. The major goal of this nascent field is therefore to scale these systems up, to the regime where classical computers fail. As we near this goal we are met with a number of significant challenges: How can the correct operation and quantum complexity of these devices be *verified* if they cannot be simulated or checked with classical computers? Since full tomography of large quantum systems is intractable, how can these new devices be meaningfully *characterised*? Addressing these related challenges has been a major part of this thesis.

Finally we address a major outstanding goal of the field. It has been known for 30 years that it is theoretically possible to construct a single device with sufficient versatility so as to implement *any possible* linear optical operation up to the specified number of modes [27]. Such a *universal* linear optical device, would replace a multitude of current and future prototype systems, and would represent a step change in the development of new quantum protocols. Realising this scheme requires high fidelity fabrication and operation of many reconfigurable waveguide elements, which up until now has not been possible. In this thesis we present a fully reconfigurable universal linear optical processor across six photonic modes and programme it to implement a variety of protocols at the forefront of quantum information science and technology.

### 1.1 THESIS OUTLINE

Throughout this thesis we describe a series of novel concepts and techniques for quantum information science with photons, alongside the development and application of integrated photonics. Specifically we demonstrate how the generation, manipulation and detection of single photon states can be brought together in a single machine — a linear optical processor — capable of performing a multitude of quantum information processing tasks. This work is structured as follows:

Chapter 2 introduces the theoretical framework for the experiments presented within this thesis — drawing on concepts from mathematics, computer science and physics — and explores in detail the platform of photons in linear optical circuits. Chapter 3 introduces the photonic hardware used to realise the photonic processors presented: a multi-photon source, active and passive waveguide devices and a single photon detection system, alongside the underlying physics which governs their operation. Chapter 4 presents a toolbox of hardware level characterisation techniques for efficiently determining the description of a linear optical circuit and demonstrates the efficacy of these techniques via both experimental and numerical analysis. Chapter 5 brings these components together to present fixed, passive linear optical processors. This analogue quantum simulator generates quantum photonic states with up to five photons in optical circuits of 21 waveguides, producing a Hilbert space of up to 50,000 dimensions; motivating the development of new, efficient techniques with which to verify quantum complexity for these class of systems. Chapter 6 presents a fully reconfigurable *universal* linear optical processor, with sufficient versatility to implement all possible linear optical protocols up to the size of that circuit. This added capability is a step change in complexity and control compared with previous demonstrations. Chapter 7 applies this universal device to a variety of quantum information processing protocols, from new entanglement generation schemes to the first integrated implementation of heralded quantum logic gates. Finally, Chapter 8 summarises these results and provides an outlook for future research.

*I was in a sort of ecstasy... Absorbed in the contemplation of sublime beauty... I reached the point where one encounters celestial sensations... Everything spoke so vividly to my soul. Ah, if I could only forget. I had palpitations of the heart... Life was drained from me. I walked with the fear of falling.*

Stendhal (on seeing Giotto's frescoes for the first time)

# 2

## Background

### 2.1 INTRODUCTION

In this chapter we provide a theoretical framework for the experiments presented in this thesis. The mathematics, physics, and computer science material of this chapter reflects the cross-disciplinary nature of quantum information science. The physics of the photonic hardware relevant to this thesis is discussed in the following chapter; here we concentrate on the more general scenario of linear optical quantum computing (LOQC) and the mathematical formalism which underpins it.

The purpose of this chapter is three-fold: to *define* the relations that will be used throughout; to *elucidate* the concepts from the authors own personal perspective; and to *direct* the reader to the relevant texts and research which both found and advance the field.

In Section 2.2 and 2.3 we introduce basic concepts from quantum mechanics and discuss quantum systems as information carriers. We then present the relevant foundations of classical computing and computational complexity in Section 2.4, and introduce the related concepts from quantum complexity and quantum computing in Section 2.5. Finally in Section 2.6, we explore in detail the platform of photons in linear optical circuits; the theoretical framework which will underpin the forthcoming experiments in linear optical quantum information processing. In addition to standard texts which are referenced within, this chapter draws on material from the theses of N. K. Langford, A. Politi, J. C. F. Matthews, A. Laing and P. J. Shadbolt.

## 2.2 QUANTUM MECHANICS

Quantum mechanics is the set of rules which typically governs phenomena at the atomic and subatomic scale. Whilst it defies our intuition, and much of 20th century physics has been spent trying to test it, much of the important mathematics is beautifully simple. At its heart quantum mechanics deals with *probability amplitudes*, and to see this we don't need years of training and university degrees, rather, a simple thought experiment will suffice: the double slit experiment. To do this we follow the elegant formulation of Feynman who notes

*“We choose to examine a phenomena, which is impossible, absolutely impossible, to explain in a classical way, and which has in it the heart of quantum mechanics. In reality, it contains the only mystery.”*

R. P. Feynman [28]

### 2.2.1 THE PAINTBALL GUN

Consider a wall with two nearby holes in. Behind the wall is a second wall covered in white paint. We get a paintball gun and start firing, randomly, at the two holes;

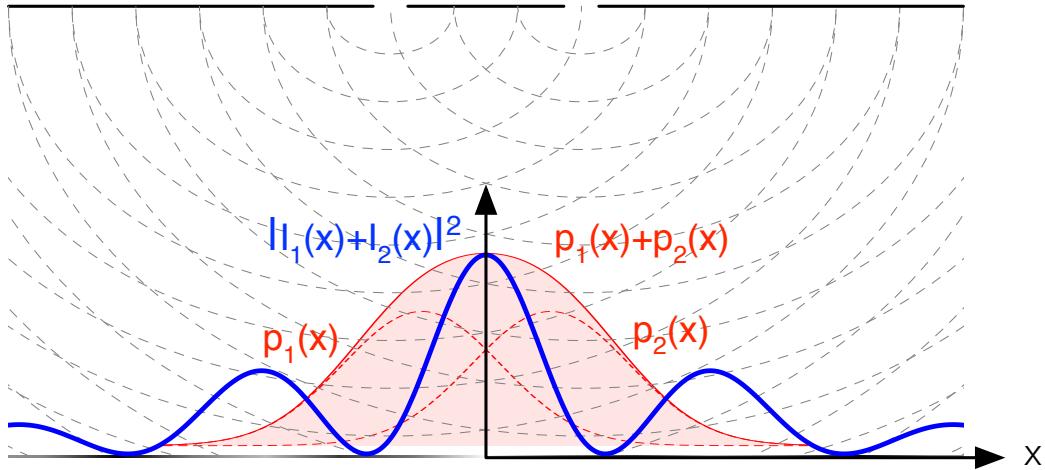


Figure 2.1: **The double slit experiment.** Dashed red lines represent the individual distributions when a single hole is open for both particles and waves. Red solid line shows the combined distribution due to particles  $P_{12}(x) = P_1(x) + P_2(x)$  whilst the blue solid line due to waves  $I_{12}(x) = |I_1(x) + I_2(x)|^2$ .

where, on average, does the paint end up? Let us assume for convenience that whenever a paintball lands in one of the holes, it has insufficient force to burst and bounces towards the white wall, in some unpredictable direction. Because paintballs are discrete lumps, that shoot one at a time (never two at a time), we can treat each possibility separately: either it goes through the first hole or second. If we were to fire just at the first hole most of the paint would be directly in front of that hole with a bit less as the distance increases. Let us call the distribution of paint due to the first hole as  $P_1(x)$ , and similarly for the second as  $P_2(x)$ . The resulting distribution of paint is simply the sum of these distributions

$$P_{12}(x) = P_1(x) + P_2(x), \quad (2.1)$$

telling us paintballs do not interfere with one another.

### 2.2.2 WATER WAVES

Now let us play the same game with water waves on a still pond. To do this we splash circular waves behind two holes set into the water, and behind the holes is another wall which measures the intensity  $I(x)$  of the impinging waves<sup>1</sup>, what is the resulting intensity? As the circular wavefront simultaneously hits both holes, it is as if we had two wave sources. For each individual source the intensity distribution is the same as for the paintballs, but when both holes are open we get a radically different pattern due to interference;  $I_{12}(x) \neq I_1(x) + I_2(x)$ . At certain locations along the wall the waves are in-phase and we see a large intensity, and at certain locations they are out of phase and we see a low intensity.

More concretely we describe the water wave due to hole 1 at time  $t$  by a rotating vector  $\vec{h}_1 = h_1 e^{i\omega t}$  on the complex plane such that the intensity is  $I_1 = |\vec{h}_1|^2$ . The total intensity is therefore

$$I_{12} = |\vec{h}_1 + \vec{h}_2|^2 \quad (2.2)$$

$$= I_1 + I_2 + 2\sqrt{I_1 I_2} \cos[\delta(x)] \quad (2.3)$$

where the final term represents the interference and  $\delta(x)$  is the phase difference between the two waves.

### 2.2.3 ELECTRONS

Let us now imagine a final experiment with quantum particles. We fire electrons, one at a time at a double slit<sup>2</sup> and place a detector along the wall which clicks when an electron hits it. What we first notice is that while the clicks are erratic, they are truly full clicks, no half clicks. That is, one and only one electron passes through the holes at a given instant. We can then calculate the probability for an electron to appear at a given position  $P_{12}(x) = n_{12}(x)/N$  by collecting  $n_{12}(x)$  out of a total

---

<sup>1</sup>If the height of the wave is  $h(x, t)$  the intensity at a position  $x$  is the average height  $I(x) = \int h(x, t)^2 dt$ .

<sup>2</sup>This time the holes must be much smaller than before, on the order of the DeBroglie wavelength of the electron.

## 2.2. QUANTUM MECHANICS

---

of  $N$  events. Now, we might expect electrons, because of their discrete nature, to behave like paintballs. Surprisingly, we observe precisely the same interference pattern as for water waves [29]. This phenomena has been observed experimentally for neutrons [30], atoms [31, 32] and molecules [33–36].

*So which hole did the electron pass through?* Let us place a detector at each hole. If the electron is a wave then we should be able to observe both detectors firing simultaneously, however we never see this. Therefore the statement “the electron is either a particle or wave” gives rise to a contradiction:

- If the electron is a particle, we should not see an interference pattern — but we do.
- If the electron is a wave, we should never see just one detector click — but we do.

We arrive at *wave-particle duality*, and the inadequacy of classical language to describe quantum systems. In this single thought experiment we have the essence of quantum mechanics.

### 2.2.4 PROBABILITY AMPLITUDES

Whilst mental gymnastics may be necessary to interpret these results, the mathematics is beautifully simple. Much like water waves, each event (the electron passing though hole 1 or 2) can be described a complex number  $\psi(x)$  called a *probability amplitude*. If we close hole 2 and therefore know the electron passes through hole 1 the probability to find it at a given position is given by  $P_1(x) = |\psi_1(x)|^2$ . If however both holes are open, and there are multiple possible ways an event can occur, we sum these events at the probability amplitude level

$$P(x) = |\psi_1(x) + \psi_2(x)|^2. \quad (2.4)$$

This tells us something deep about quantum mechanics: If you want to calculate the probability of an event occurring in the lab (i.e. a detector clicking or an

atom decaying) but there are multiple ways it could happen and you don't know which — moreover, it is completely impossible to know which — you must *sum the events at the probability amplitude level*. This summing of probability amplitudes is not only at the heart of the rich phenomena observed within this thesis, but all experiments in quantum mechanics.

### 2.2.5 AXIOMS OF QUANTUM MECHANICS

Whilst we have alluded to the peculiarities of quantum states, we can be more precise in our formulation of quantum mechanics. In particular we wish to understand how the mathematical framework of quantum mechanics represents states, observables, measurements and evolution. To this end, and for completeness we now present the axioms of quantum mechanics following Preskill [37].

#### 1. States

A quantum state is a full description of a physical system and is represented by a ray in Hilbert space  $\mathcal{H}^d$ , a finite<sup>3</sup>  $d$ -dimensional complex inner product vector space over  $\mathbb{C}^d$ . A ray is an equivalence class of vectors  $|\psi\rangle$  that differ by multiplication by a nonzero complex scalar, thus states  $|\psi\rangle$  and  $e^{i\phi}|\psi\rangle$  are physically equivalent.

#### 2. Observables

An observable is a property of a system that can be measured and is described by a Hermitian operator  $\hat{A} = \hat{A}^\dagger$ . An operator is a linear map taking vectors to vectors such that

$$\hat{A} : |\psi\rangle \rightarrow \hat{A}|\psi\rangle; \quad \hat{A} : \alpha|\psi\rangle + \beta|\phi\rangle \rightarrow \alpha\hat{A}|\psi\rangle + \beta\hat{A}|\phi\rangle. \quad (2.5)$$

An observable  $\hat{A}$  has a spectral representation such that its eigenstates form a complete orthonormal basis in  $\mathcal{H}^d$

$$\hat{A} = \sum_n a_n \hat{P}_n \quad (2.6)$$

---

<sup>3</sup>Quantum mechanics is equally well defined over an infinite dimensional Hilbert space but for the work presented here finite dimensions suffice.

### 2.3. QUANTUM INFORMATION

---

where  $\hat{P}_n = |a_n\rangle\langle a_n|$  is the projection onto the space of eigenstates  $|a_n\rangle$  with eigenvalue  $a_n$ .

### 3. Measurements

The outcome of a measurement of an observable  $\hat{A}$  is an eigenvalue  $a_n$  such that after the measurement the state  $|\psi\rangle$  is in the measured eigenstate  $|a_n\rangle$ . The probability of an outcome  $a_n$

$$\text{Prob}(a_n) = \langle\psi|\hat{P}_n|\psi\rangle, \quad (2.7)$$

and the state becomes

$$|\psi\rangle \xrightarrow{a_n} \frac{\hat{P}_n|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_n|\psi\rangle}}. \quad (2.8)$$

### 4. Evolution

The time evolution of a closed quantum system is described by the Schrödinger equation

$$i\hbar\frac{d|\psi\rangle}{dt} = \hat{H}|\psi\rangle \quad (2.9)$$

where  $\hat{H}$  is a Hermitian operator known as the Hamiltonian of the system. This time evolution can therefore be described by the unitary operator  $\hat{U}(t) = \exp[-i\hat{H}t/\hbar]$  such that  $|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle$ . Throughout this thesis we will deal in units of  $\hbar = 1$ .

The beauty of quantum mechanics is that while these axioms are straightforward to state, the phenomena they give rise to are anything but. Whilst much of 20th century physics has been concerned with *observing* physical phenomena and testing these axioms, towards the end of that century the focus began to shift towards *using* these phenomena for new applications and technologies.

## 2.3 QUANTUM INFORMATION

In the classical world, physical systems such as the localised magnetic field of a hard disk drive or engravings on a stone tablet, are used to encode information. As

---

## 2. BACKGROUND

Landauer famously asserted “information is physical” [38] — that is, information processing is in some sense incomplete unless the information carrier is considered. In the classical regime, understanding the physics of these information carriers has led both to significant practical advances — with transistors reaching the size of several atoms [39] — and significant conceptual advances — with investigations into the thermodynamics of information carriers telling us something about the fundamental limits to computation [40, 41].

In a dynamic random-access-memory (DRAM) classical bits are encoded in the charge across a capacitor. Typically, the capacitance of these systems is  $\sim 30 \text{ fF}$  [42] which, with a  $\sim 1 \text{ V}$  potential, has a charge of  $Q = C/V \approx 10^{-14} \text{ C}$ . Therefore a single classical bit corresponds to the collective state of  $10^{-14}/10^{-19} \approx 10^5$  electrons. From the perspective of quantum mechanics, a very natural question to ask is: what happens when we no longer have  $10^5$  particles, but rather just a single particle?

### 2.3.1 THE QUBIT

Quantum information is concerned with using the rules of quantum mechanics to process information, in ways that are radically different from classical information processing [43]. In a classical computer the information carrier exists in a well defined binary state 0 or 1. In a quantum computer the information carrier, the qubit, exists in a well defined state in the two dimensional Hilbert space  $\mathcal{H}^2$ , over the basis states  $\{|0\rangle, |1\rangle\}$ . However, much like the electron has a probability amplitude associated with the being in both holes, a qubit can exist in a linear superposition of these basis states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.10)$$

where  $\alpha, \beta$  are complex numbers such that  $|\alpha|^2 + |\beta|^2 = 1$ . It will be convenient to represent the qubit as a vector  $|\psi\rangle = [\alpha, \beta]^\top$ . Recalling the state axiom, up to a typically unimportant global phase the qubit can be rewritten as

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle. \quad (2.11)$$

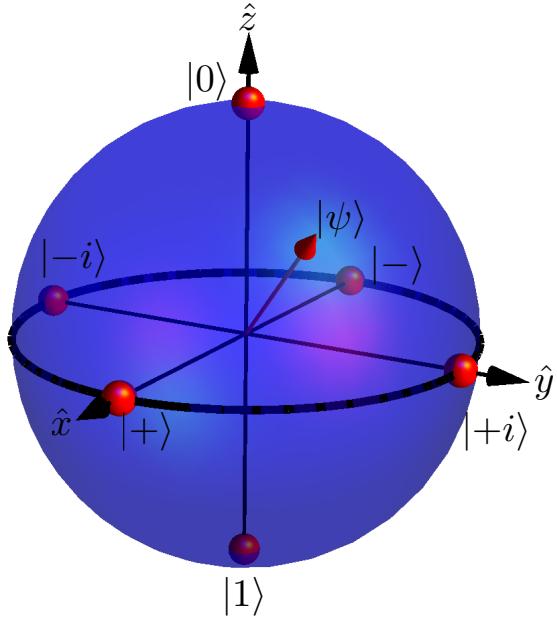


Figure 2.2: **The Bloch sphere representation of a single qubit.** A pure single qubit state  $|\psi\rangle$  can be represented as a point on the surface of the Bloch sphere, with axes representing Pauli eigenstates as shown.

Now  $(\theta, \phi)$  parameterise a point on a unit three-dimensional sphere called the Bloch-sphere, shown in Fig 2.2. This representation will be useful later for visualising the evolution of states. According to the observable axiom we can construct a measurement which projects this state onto the basis  $\{|0\rangle, |1\rangle\}$ , such that with probability  $|\alpha|^2$  we get the outcome  $|0\rangle$  and with probability  $|\beta|^2$  we get  $|1\rangle$ .

### 2.3.2 SINGLE QUBIT OPERATIONS

In analogy to classical computing where NOT takes  $0 \rightarrow 1$  and  $1 \rightarrow 0$ , we can construct single qubit operations provided they obey the evolution postulate and are unitary. Some single qubit operations of interest are

$$\hat{X} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad \hat{Y} \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad \hat{Z} \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \quad \hat{H} \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (2.12)$$

Input	Output
$ 0_C0_T\rangle$	$ 0_C0_T\rangle$
$ 0_C1_T\rangle$	$ 0_C1_T\rangle$
$ 1_C0_T\rangle$	$ 1_C1_T\rangle$
$ 1_C1_T\rangle$	$ 1_C0_T\rangle$

Table 2.1: **CNOT truth table.** Computational state transformations on the control  $C$  and target  $T$  qubits for the CNOT operation.

and act upon qubits via matrix multiplication. For example  $\hat{X}(\alpha|0\rangle + \beta|1\rangle) \rightarrow \beta|0\rangle + \alpha|1\rangle$ , and is the quantum analogue of the NOT gate. Quantum gates can be combined in linear superpositions to create new gates and obey certain identity relationships, for example  $\hat{H} \equiv (\hat{X} + \hat{Z})/\sqrt{2}$ .

### 2.3.3 MULTIPLE QUBITS

The state space of a multi-qubit system is constructed via the *tensor product* of the composite systems. For example the state space of a two qubit system is given by  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ , therefore a two qubit state is a vector in  $\mathcal{H}^4$  described by four parameters  $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ . More generally, an  $n$ -qubit system is described by  $2^n$  parameters.

We can construct multi-qubit gates which conditional on the state of one qubit (the control), operates on the other qubit (the target). Consider the quantum analogue of the XOR, the controlled-NOT (CNOT), which flips the target conditional on the control being  $|1\rangle$ , as shown in Table 2.3.3. This can be represented as a matrix in the computational basis as

$$\hat{U}_{\text{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (2.13)$$

We can act this upon the state  $\hat{H}_C \otimes \hat{I}_T |0_C0_T\rangle$  (where  $\hat{I}$  is the identity operator)

### 2.3. QUANTUM INFORMATION

---

such that

$$\hat{U}_{\text{CNOT}} \left( \hat{H}_C \otimes \hat{I}_T |0_C 0_T\rangle \right) = \hat{U}_{\text{CNOT}} \left( \frac{1}{\sqrt{2}}(|0_C\rangle + |1_C\rangle) |0_T\rangle \right) \quad (2.14)$$

$$= \frac{1}{\sqrt{2}}(|0_C 0_T\rangle + |1_C 1_T\rangle). \quad (2.15)$$

This state cannot be written as the product of two single qubit states. To see this consider the tensor product of two arbitrary single qubit states

$$|\psi_C\rangle \otimes |\psi_T\rangle = (\alpha |0_C\rangle + \beta |1_C\rangle) \otimes (\gamma |0_T\rangle + \delta |1_T\rangle) \quad (2.16)$$

$$= \alpha\gamma |0_C 0_T\rangle + \alpha\delta |0_C 1_T\rangle + \beta\gamma |1_C 0_T\rangle + \beta\delta |1_C 1_T\rangle. \quad (2.17)$$

To remove the  $|0_C 1_T\rangle$  term either  $\alpha$  or  $\delta$  must be zero, if  $\alpha = 0$  then  $|0_C 0_T\rangle = 0$ , if  $\delta = 0$  then  $|1_C 1_T\rangle = 0$ . Generally any state of this form  $|\psi\rangle_{AB} \neq |\phi\rangle_A \otimes |\chi\rangle_B$  is said to be *entangled*.

#### 2.3.4 ENTANGLEMENT

Entanglement provides us with a shocking insight into the nature of reality. Although the idea was first brought to attention by Einstein, Podolsky and Rosen in 1935 [44]; it wasn't until Bell's theorem was formulated in the 1960s [5], and experimentally tested in the 1970s and 1980s [6–8], that the idea was taken seriously as a valid way of understanding nature.

Bell proved that the predictions of quantum theory are incompatible with a seemingly natural notion of locality. *Nature is fundamentally nonlocal*. Following the comprehensive review of Brunner et al. [45] we can see this via a simple game. Consider two players Al and Charlie who each get given a quantum state. They are allowed to make measurements on their state, let us call Al's measurement choice  $x \in \{0, 1\}$  and Charlie's  $y \in \{0, 1\}$ , that have an outcomes  $a \in \{+1, -1\}$  and  $b \in \{+1, -1\}$  respectively. We will be interested in the joint probability of measurement outcomes, that is  $p(ab|xy)$ .

In general

$$p(ab|xy) \neq p(a|x)p(b|y), \quad (2.18)$$

## 2. BACKGROUND

---

and this is no mystery. Even if the measurements are performed in a space-like separated manner, perhaps the particles came from the same source, so they have some pre-assigned values, a set of rules about how to behave. We call these pre-assigned rules ‘hidden variables’  $\lambda$ . Now these rules might be very complicated, perhaps a probability distribution  $q(\lambda)$ , but in principle it should be possible to write down exactly what the set of rules are such that  $p(ab|xy)$  can be made separable

$$p(ab|xy) = \int_{\lambda} d\lambda q(\lambda) p(a|x, \lambda) p(b|y, \lambda), \quad (2.19)$$

and this simply expresses locality; that the outcome of  $a$  only depends on the set of rules  $q(\lambda)$  and the measurement  $x$  — wholly reasonable!

Consider the quantity

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \quad (2.20)$$

where  $\langle a_x b_y \rangle = \sum_{ab} ab p(ab|xy)$  is the expectation value of the joint measurement  $(x, y)$ . By the locality assumption this joint expectation value is a product of individual expectation values  $\langle a_x b_y \rangle = \int d\lambda q(\lambda) \langle a_x \rangle_{\lambda} \langle b_y \rangle_{\lambda}$ , and as  $\langle a_x \rangle, \langle b_y \rangle \in [+1, -1]$ , we arrive at the Clauser-Horne-Shimony-Holt inequality [46]

$$|S| \leq 2. \quad (2.21)$$

Giving Al and Charlie either half of the entangled state  $|\psi\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ , and letting

$$x_0 = \hat{Z}; \quad x_1 = \hat{X}; \quad y_0 = \frac{-\hat{Z} - \hat{X}}{\sqrt{2}}; \quad y_1 = \frac{\hat{Z} - \hat{X}}{\sqrt{2}}, \quad (2.22)$$

yields  $\langle a_0 b_0 \rangle = \langle a_0 b_1 \rangle = \langle a_1 b_0 \rangle = 1/\sqrt{2}$  and  $\langle a_1 b_1 \rangle = -1/\sqrt{2}$ , hence

$$S = 2\sqrt{2} > 2 \quad (2.23)$$

in contradiction with (2.21). Since the seminal experiments of Freedman and Clauser [6] and Aspect et al. [7, 8], this violation has been observed countless times in many different laboratories across the world. This thus tells us the seemingly reasonable assumption of locality — that the state of a particle cannot be

## 2.4. CLASSICAL COMPUTING

---

affected by events outside of its light cone — is incompatible with the predictions of quantum mechanics. Whilst the maximally mixed reduced state for each party makes individual outcomes inherently random (thus preventing faster than light communication); this result does provide us with the tantalising possibility that quantum mechanics somehow offers an advantage for certain tasks. It is this intuition we seek to develop in the forthcoming sections.

## 2.4 CLASSICAL COMPUTING

To understand any potential advantage a computer processing quantum information may offer, we must first understand the limits of classical computers. As laid out by Turing in 1936 [47], the theory of universal computation means we don't have to consider each type of computer on a case-by-case basis to understand how well it processes information. That is, we don't have to understand how an Apple Mac or Playstation or Casio calculator works, we simply have to consider a *universal Turing machine*.

### 2.4.1 THE TURING MACHINE

A Turing machine consists of a device that mechanically operates on a tape according to a set of rules. Specifically, the tape is split into cells, such that the machine reads one, and only one cell at a give instant; and on each cell is a symbol from a finite alphabet  $S_i$  [see Fig. 2.3(a)]. The machine itself has an internal state  $Q_i$  which can be updated. The machine takes as input  $(Q_i, S_i)$  and performs three tasks: writes a new symbol  $S_j$ , updates the internal state  $Q_j$  and moves left or right  $D$ , according to the set of rules (or functions)

$$Q_j = f(Q_i, S_i); \quad S_j = g(Q_i, S_i); \quad D = d(Q_i, S_i). \quad (2.24)$$

The machine is completely determined by this set of functions, which will be some large look up table [see Fig. 2.3(b)], and can be thought of as the programme for the computer. Finally, when the computation is finished, the machine must halt.

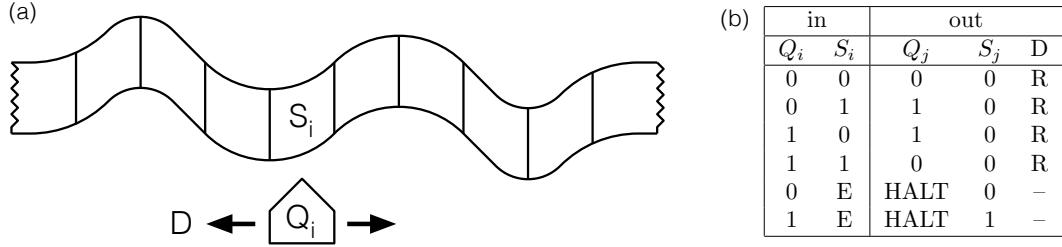


Figure 2.3: **The Turing machine.** (a) A schematic of a Turing machine displaying the internal state of the machine  $Q_i$ , the tape symbol  $S_i$  and the direction  $D$ . (b) A particular rule set (programme) for computing the parity of a binary function taken from Feynman [48].

As an example, you might imagine a programme for multiplying numbers together; the user input will be writing these numbers as symbols onto the tape, and the machine will whirl away, reading and writing symbols until it halts and the answer is written onto the tape.

The main result of Turing was understanding the existence of computable and uncomputable functions. The details of this can be found in Arora and Barak [49], but for our purpose, Turing's important result was the existence of *universal machines*. He showed there exists a universal computing machine (with some specific set of rules) which can simulate any possible computing machine (with any set of rules). The description of the machine to be simulated (i.e. the set of rules and input data) is fed into the universal machine via its input tape. The universal machine then performs this computation and prints an output as if it was the simulated machine.

In his paper Turing laid the foundations for something which seems second nature today: programmable computers. His result means you don't need one machine for playing games, one for internet shopping — a single device can do all this. The theme of universality will play a major role of this thesis.

### 2.4.2 COMPUTATIONAL COMPLEXITY

We can begin to consider the types of problems a computer might be used to solve. It is often convenient to group these problems into *complexity classes*. The types of problems that can be solved in a given complexity class is of fundamental importance to both classical and quantum computing, and to the experiments presented in this thesis. In the following exposition we draw from the entertaining overview of Aaronson [50], and the technical overview of Arora and Barak [49].

Generally, we are interested in the scaling of resources, whether that is time or space (i.e. how long my computer has to run for, or how much memory it requires), that are required to solve a given decision problem as the size of the problem increases. Note, decision problems output a ‘yes’ or ‘no’ answer, as opposed to a numerical answer; e.g. “is the  $n^{\text{th}}$  digit of integers  $a \times b$  a ‘1’?” Formally we say a machine decides a language  $L \subseteq \{0, 1\}^*$  if it computes the function  $f_L : \{0, 1\}^* \rightarrow \{0, 1\}$ , where  $f_L(x) = 1$  when  $x \in L$ . Let us define some common complexity classes:

- **P** is the class of decision problems solvable by a deterministic Turing machine in polynomial time. More formally, a language  $L$  is in **P** if and only if there exists a Turing machine that runs in time  $n^c$ , for some constant  $c > 0$ , and decides  $L$ .
- **BPP** is the class of decision problems solvable by a probabilistic Turing machine (i.e. a Turing machine with access to randomness) in polynomial time with an error probability less than  $1/3$ . Formally, a language  $L$  is in **BPP** if there exists a probabilistic Turing machine  $M$  that runs in polynomial time  $n^c$ , for some constant  $c > 0$ , and for every  $x \in \{0, 1\}^*$ ,  $\Pr[M(x) = L(x)] \geq 2/3$
- **NP** is the class of decision problems for which, if the answer is yes, there exists a polynomial-size proof that lets you verify that answer in polynomial time. Formally a languages  $L$  is in **NP** if there exists a polynomial  $p : \mathbb{N} \rightarrow \mathbb{N}$ ,

and a polynomial-time Turing machine  $M$  (called the *verifier* for  $L$ ) such that for every  $x \in \{0,1\}^*$ , if  $x \in L$  there exists a  $u \in \{0,1\}^{p(|x|)}$  such that  $M(x, u) = 1$ .

- NP-complete is the class of decision problems which are (1) in NP and (2) all problems in NP can be efficiently reduced to it.

Throughout this thesis we will interchangeably use the terms efficient, or tractable for problems that can be solved in polynomial time. Notable problems in P include graph connectivity, 2-SAT and matrix multiplication. Problems in NP are of the form “does there exist an  $n$ -bit string  $x$  such that  $f(x) = 1$ ?” Whilst finding  $x$  may take exponential time, computing  $f(x)$  can be done efficiently. Notable problems in NP that are not known to be in P nor NP-complete are integer factorisation and graph isomorphism. Finally, NP-complete problems can be seen as the hardest problems in NP. If an efficient algorithm exists to solve a single NP-complete problem then all problems in NP can be solved efficiently. Notable problems include the Travelling Salesman problem and the Graph colouring problem.

## 2.5 QUANTUM COMPUTING

*“So now we’ve got this beautiful theory of quantum mechanics, and the possibly-even-more-beautiful theory of computational complexity. Clearly, with two theories this beautiful, you can’t just let them stay single — you have to set them up, see if they hit it off.”*

Scott Aaronson [50]

Deutsch in 1985 [51] realised that implicit in the work of Turing (and in parallel Church [52]) was a statement about physics. The result of Church and Turing can be summarised as the Church-Turing thesis:

## 2.5. QUANTUM COMPUTING

---

*“Every function which would naturally be regarded as computable, can be computed by the universal Turing machine”*

David Deutsch [51]

For something to be “naturally regarded as computable” it must be computed in nature. So the Church-Turing thesis is a claim about a universal Turing machine’s ability to compute anything in nature. To this end Deutsch set about constructing a universal *quantum* machine which used quantum bits to store information and quantum gates to process information, and showed it could solve a black box problem fundamentally quicker than a deterministic Turing machine. This was later generalised by Deutsch and Josza [53] demonstrating exponential speedup.

Whilst this exponential speedup was the first suggestion a quantum machine may offer computational advantage, the black box scenario was somewhat contrived, and offered no speed-up over a *probabilistic* Turing machine. It was later shown by Bernstein and Vazirani [54] that a genuine super-polynomial separation was possible between a quantum computer and a probabilistic computer, and shortly after by Simon [55] that an exponential separation could be achieved for a black-box period finding problem<sup>4</sup>.

### 2.5.1 BQP

For completeness let us explicate the ingredients for a universal quantum computer. We must be able to *initialise* the state of the computer in some polynomial size input  $|x\rangle|0\dots0\rangle$ , where  $x$  encodes the input to the problem. We must be able to *transform* the state via application of a polynomial number of gates from a universal gate set, and finally we must be able to *measure* a qubit which encodes the answer, for example accepting if  $|1\rangle$  and rejecting if  $|0\rangle$ . We can therefore define the complexity class BQP [54]:

---

<sup>4</sup>Only recently experimentally demonstrated [56].

A language  $L$  is in BQP if there exists a family of polynomial-size quantum circuits  $\{C_n\}$  such that  $\forall x \in \{0, 1\}^n$ :

- if  $x \in L$ , then  $C_n$  accepts  $|x\rangle|0\dots0\rangle$  with probability at least  $2/3$ ,
- if  $x \notin L$ , then  $C_n$  accepts  $|x\rangle|0\dots0\rangle$  with probability at most  $1/3$ .

Remarkably little is known about the exact relationship of BQP to other complexity classes. Bernstein and Vazirani showed that  $\text{BPP} \subseteq \text{BQP} \subseteq \text{PP}$ <sup>5</sup>: that is quantum computers are at least as fast as classical computers, and no more than exponentially fast. But it wasn't until Shor's groundbreaking algorithms for integer factorisation and discrete logarithms [58] that strong evidence was provided that  $\text{BPP} \neq \text{BQP}$ .

Shor (directly inspired by Simon) constructed an efficient quantum algorithm, based on the quantum Fourier transform, which is able to give the decomposition of a composite number  $N$  as a product of two primes  $N = p \times q$ ; a problem which is so strongly believed to be in NP that we base our modern cryptographic systems on it [59, 60]. This was the first strong evidence that BQP was able to efficiently solve problems outside of BPP (the corresponding classical complexity class).

Understanding which problems in BQP offer speed-ups over their classical counterparts is a central question for quantum algorithms<sup>6</sup>. Algorithms broadly fall into three categories: First, ones relying (like Shor's) on the quantum Fourier transform to give an exponential speed up (see for example Kitaev's discovery for solving the Abelian stabiliser problem [61]); second, algorithms based on Grover's algorithm for unstructured database search [62] giving a quadratic speedup; third, algorithms based on Hamiltonian simulation giving an in principle exponential speed up<sup>7</sup> [63] (such as the quantum algorithm for linear systems of equations [64], which has recently found application in machine learning tasks [65, 66]).

---

<sup>5</sup>With the upper bound proven by Adleman et al. [57]

<sup>6</sup>For an exhaustive list see <http://math.nist.gov/quantum/zoo/>.

<sup>7</sup>The subtlety is that while the algorithm may run efficiently, encoding or reading out information can often prevent apparent speed up.

### 2.5.2 BUILDING A QUANTUM COMPUTER

While computer scientists are necessarily concerned with developing and understanding quantum algorithms, experimental scientists are necessarily concerned with building apparatus to implement quantum algorithms. At the same time, experimentalists must convince themselves and the wider world that such machines are not in principle unscalable, since we still do not know whether the universe forbids the generation and processing of a computationally significant quantum system. To that end, DiVincenzo formulated the following requirements for the physical implementation of a quantum computer [67]:

1. *A scalable physical system with well characterised qubits.*

The Hamiltonian governing the qubit must be well understood and its coupling to other quantum states well characterised such that it can be considered a genuine two level quantum system. If this is not the case leakage may occur into other quantum states leading to decoherence and loss of quantum information.

2. *The ability to prepare the state of the qubits in an initial fiducial state.*

Reliably preparing the qubits in a low entropy state (that is a pure state as opposed to a maximally mixed state) is essential for reducing errors later in the computation. For atom based architectures where qubits must be cooled to their ground state this can be challenging.

3. *Long decoherence times relative to the gate operation times.*

Decoherence occurs when qubits interact with their environment, resulting in loss of information and computational errors. Decoherence is the mechanism by which classicality emerges, thus a quantum computer with high levels of decoherence begins to resemble a classical machine. If however error levels are below thresholds required for error correcting codes [68] quantum computation can still be achieved.

### 4. A universal set of quantum gates.

A universal gate set is a sufficient set of gates which can be combined together to create *any* gate (see Section 7.2.2 for details). This requires identifying some set of Hamiltonians  $\{\hat{H}_i\}$  which can be applied for time  $t_i$  to give rise to a universal gate set  $\{\hat{U}_i = \exp[-i\hat{H}_i t_i]\}$ . These typically include single qubit operations and two qubit operations, which must be performed quickly and with high fidelity.

### 5. Qubit measurement capability.

Finally the qubit(s) must be measured. This requires coupling the state of a qubit (such as the position of a photon) to the macroscopic state of a detector, which can often lead to inefficiencies.

#### 2.5.3 ARCHITECTURES

Engineering qubits and circuitry which satisfy all of these constraints is recognised as one of the most technologically demanding tasks yet undertaken. For instance, qubits which exhibit strong interactions, such that two qubit gates are feasible, tend to interact with the environment leading to decoherence and loss of information

A variety of quantum systems have been proposed as suitable architectures for a universal quantum computer. An ion trap quantum computer uses the energy levels of electromagnetically trapped charged particles, achieving two body interactions via the Coulomb interaction [69]. Advances in laser science and cooling techniques have allowed the generation of entangled states with up to 15 qubits [70] and high fidelity single qubit gates [71] — yet the prospects for scalability is still an outstanding challenge [72].

Another promising platform is superconducting qubits, which uses the quantised flux or charge around a superconducting circuit coupled to a Josephson junction to realise a two level quantum system [73]. These systems have demonstrated high fidelity single qubit and two qubit gates [74] at the threshold for surface code

## 2.6. PHOTONIC QUBITS

---

error correction [75]. However, advances in material science and large scale fabrication processes must still be made [76]. Other candidate qubits include optically trapped neutral atoms [77], NMR [78] and solid state qubits such as quantum dots and nitrogen vacancy centres [79].

We now move on to the main topic of this chapter, and introduce the platform with which the entire thesis is concerned: *single photons in linear optical circuits*. What we will see is that many of the challenges which plague other architectures are circumvented with photons; they are quick, easy to manipulate, and possess low decoherence properties. However this gain does not come without cost, and many hurdles must be overcome to realise a universal linear optical quantum computer.

## 2.6 PHOTONIC QUBITS

The ease with which single photons can be manipulated, their low decoherence properties and their light-speed propagation has put them at the heart of some of the major advances in experimental quantum physics over the past half century. For example, photons generated from atomic calcium cascades have been used to test the foundations of quantum mechanics [6, 7], whilst spontaneous parametric down-conversion (see Section 3.3) has been used to demonstrate the first teleportation protocols [80, 81]. More recently, photons have enabled the first commercially available quantum technology: quantum cryptographic systems [82]. For a review of quantum photonic technologies see references [9, 12].

Many of the properties of photons which enable quantum cryptographic protocols, are key to their potential as a viable platform for the more technologically ambitious goal of a digital quantum computer. For example, the requirement for a well defined two level system can be met by photons in a number of ways. Since the time of Fresnel, Arago and Young in the early 1800's it was understood that light was a polarised wave that could be manipulated by birefringent materials [83]. Remarkably, the physics that was understood then can be directly mapped to the manipulation of single photonic qubits now.

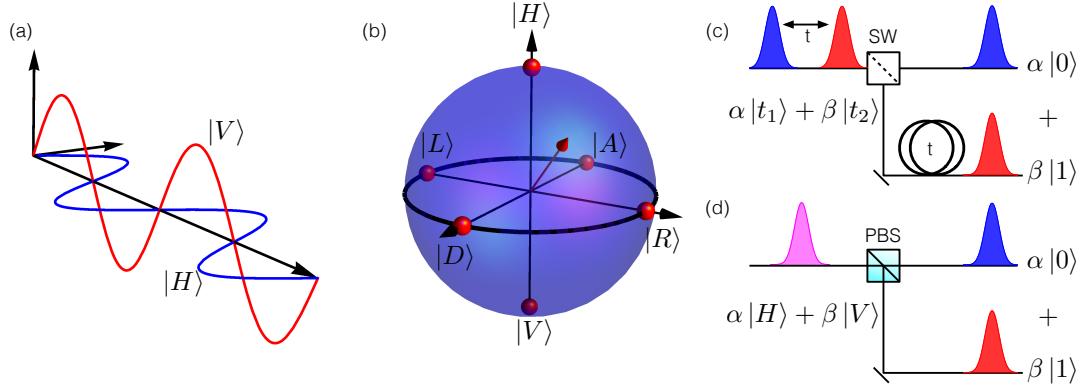


Figure 2.4: **Photonic qubits.** (a) Horizontal  $|H\rangle$  and vertical  $|V\rangle$  polarisation states represent logical  $\{|0\rangle, |1\rangle\}$ . (b) Superpositions of these basis states can be represented on the Poincaré sphere. (c,d) Both time bin and polarisation encoded qubits can be encoded onto path qubits via a clocked switch (SW) and delay line, or a polarising beamsplitter (PBS) respectively.

In the language of qubits we can consider the polarisation of a single photon to be a two state quantum system with the horizontal and vertical polarisation representing the logical basis set  $\{|H\rangle, |V\rangle\} = \{|0\rangle, |1\rangle\}$ , as shown in Fig. 2.4(a), and polarisation superpositions representing different bases

$$|D\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \quad |A\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \quad (2.25)$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle); \quad |L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle), \quad (2.26)$$

see Fig. 2.4(b). Polarisation states can be manipulated with birefringent materials, known as wave-plates, which retard one component of the polarisation with respect to the other thereby introducing a controllable phase shift between any orthogonal polarisation states (see Langford [84]).

Many degrees of freedom exist for photonic qubits, such as polarisation, time-bin or frequency encoding; but in this work we will be entirely concerned with *path degrees of freedom*. We note however, that these can be interconverted, for example using clocked active switching to convert between time-bin and path, or polarisation beamsplitters to convert between polarisation and path [see Fig. 2.4(c,d)].

### 2.6.1 MATHEMATICAL FRAMEWORK

#### STATES

The physics governing a particular encoding of choice is discussed in Chapter 3. Here, we discuss the general picture for photons in optical modes, a mathematical framework which is suitable for any encoding. We begin with the acceptance that a photon is a quantised excitation of the electro-magnetic field [85] and use the mathematical framework of creation  $\hat{a}^\dagger$  and annihilation  $\hat{a}$  operators acting between the vacuum state  $|0\rangle$  and the state of  $n$  photons  $|n\rangle$ , such that

$$\hat{a}|0\rangle = 0; \quad \hat{a}|n\rangle = \sqrt{n}|n-1\rangle; \quad (2.27)$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle; \quad \hat{a}^{\dagger n}|0\rangle = \sqrt{n!}|n\rangle. \quad (2.28)$$

The Fock states form an orthonormal basis in  $\mathcal{H}^n$  such that  $\langle i|j\rangle = \delta_{i,j}$ . This approach can be generalised to multiple modes by considering an  $m$ -mode vacuum state  $|\mathbf{0}\rangle = |0_1, 0_2 \dots 0_m\rangle$  such that

$$\hat{a}_i^{\dagger n}|\mathbf{0}\rangle = \sqrt{n!}|0_1 \dots n_i \dots 0_m\rangle \quad (2.29)$$

where  $|n_i\rangle$  represents  $n$  photons in the  $i^{\text{th}}$  mode. Photons are bosons and therefore obey Bose-Einstein commutation relations

$$[\hat{a}_i, \hat{a}_j] = [\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0; \quad [\hat{a}_i^\dagger, \hat{a}_j] = \delta_{i,j}\mathbb{1}. \quad (2.30)$$

An arbitrary single photon Fock state can be written as a superposition across all modes

$$|\psi\rangle_1 = \sum_{i=1}^m \alpha_i \hat{a}_i^\dagger |\mathbf{0}\rangle = \sum_{i=1}^m \alpha_i |1_i\rangle, \quad (2.31)$$

with  $\sum_i |\alpha_i|^2 = 1$ , such that  $|\psi\rangle_1$  is a vector in the  $m$ -dimensional Hilbert space  $\mathcal{H}^m$  spanned by the basis  $\{|1_i\rangle\}_{i=1}^m$ . A general system of  $p$ -photons in  $m$ -modes can be written as [86]

$$|\psi\rangle_p = \sum_{i \in D_p^m}^{D_p^m} \alpha_i \prod_{j=1}^m \frac{\hat{a}_j^{\dagger n_{ij}}}{\sqrt{n_{ij}!}} |\mathbf{0}\rangle = \sum_{i \in D_p^m}^{D_p^m} \alpha_i |i\rangle \quad (2.32)$$

## 2. BACKGROUND

---

where  $D_p^m$  is the set of basis states  $\{|p_1, 0_2 \dots 0_m\rangle, |p - 1_1, 1_2 \dots 0_m\rangle \dots |0_1, 0_2 \dots p_m\rangle\}$  with dimensionality  $|D_p^m| = \binom{m+p-1}{p}$ , and  $n_{ij}$  is the  $j^{\text{th}}$  element (mode) of the  $i^{\text{th}}$  basis state of  $D_p^m$ . The state  $|\psi\rangle_p$  can therefore be represented by a vector in  $\mathcal{H}^{|D_p^m|}$ . Introducing distinguishability among the  $p$  particles can increase the Hilbert space up to  $m^p$  dimensions, though such a state also becomes classically tractable and not generally useful for quantum computation.

It is worth noting two alternatives notations for describing Fock states. We have presented the *photon number basis*  $|n_1\rangle \otimes |n_2\rangle \dots |n_m\rangle$  where each element in the basis represents a mode, and the entry  $n_i$  is the number of photons in that mode such that  $\sum_i n_i = p$ . An equally valid, and often more compact notation is to represent the state in the *mode number basis*  $|i_1\rangle \otimes |i_2\rangle \dots |i_p\rangle$  where each element represents the  $p^{\text{th}}$  photon and the entry is the location (mode)  $i_p$  of that photon. As an example let us consider the  $p = 2, m = 3$  case. In the photon number basis

$$|n_1\rangle \otimes |n_2\rangle \otimes |n_3\rangle : \{|200\rangle, |110\rangle, |101\rangle, |020\rangle, |011\rangle, |002\rangle\} \quad (2.33)$$

and in the mode number basis

$$|i_1\rangle \otimes |i_2\rangle : \{|11\rangle, |12\rangle, |13\rangle, |22\rangle, |23\rangle, |33\rangle\}, \quad (2.34)$$

where we have enforced ordering from left to right to account for symmetrisation. Both notations will be used in this thesis, the choice of which will be clear from the context.

## TRANSFORMATIONS

Typically, we are interested in how optical elements transform these Fock states. Ideal linear optical operations are described by  $m \times m$  unitary operators  $\hat{U} \in \mathbb{C}^{m \times m}$ , and transform photon states in a linear manner preserving photon number. For example a single photon injected into mode  $j$  transforms

$$\hat{a}_j^\dagger \rightarrow \sum_{i=1}^m u_{i,j} \hat{a}_i^\dagger \quad (2.35)$$

## 2.6. PHOTONIC QUBITS

---

where  $u_{i,j}$  represents the  $i^{\text{th}}$  row and  $j^{\text{th}}$  column element of  $\hat{U}$ , hence  $\sum_i |u_{i,j}|^2 = 1$ . It is often conceptually clearer to think of these transformations as matrix operations on vectors. Moving to the photon number basis

$$|1_j\rangle \xrightarrow{\hat{U}} \hat{U} |1_j\rangle = \quad (2.36)$$

$$\begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,m} \\ \vdots & \vdots & \ddots & \vdots \\ u_{j,1} & u_{j,2} & \cdots & u_{j,m} \\ \vdots & \vdots & \ddots & \vdots \\ u_{m,1} & u_{m,2} & \cdots & u_{m,m} \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} u_{1,j} \\ \vdots \\ u_{j,j} \\ \vdots \\ u_{m,j} \end{bmatrix}, \quad (2.37)$$

in other words, a simple basis transformation.

Throughout this thesis the most interesting phenomena will arise due to *multiple photons*. To understand this transformation we can consider the operation of photons injected into modes  $j$  and  $k$ . By linearity

$$\hat{a}_j^\dagger \hat{a}_l^\dagger \rightarrow \left( \sum_{i=1}^m u_{i,j} \hat{a}_i^\dagger \right) \left( \sum_{k=1}^m u_{k,l} \hat{a}_k^\dagger \right) \quad (2.38)$$

which can be thought of as the tensor product between the vectors described by  $j^{\text{th}}$  and  $k^{\text{th}}$  columns. In the matrix multiplication picture, a more convenient way to describe this  $m \times m$  transformation  $\hat{U}$  is via a homomorphic map  $\varphi$ , which directly transforms the multi-photon mode basis via a  $|D_p^m| \times |D_p^m|$  transformation  $\varphi(\hat{U})$  [22]. This operation can be constructed via the Kronecker product formalism, an example is given in Section 2.6.6.

### 2.6.2 BUILDING BLOCKS OF LINEAR OPTICS

Given the description of states and transformations above let us now consider the building blocks of linear optical circuits. The first operation we consider is a *phase shifter* [Fig. 2.5(a)], which changes the phase of the electromagnetic field by  $\phi$ , such that

$$\hat{a}^\dagger \xrightarrow{\text{PS}} e^{i\phi} \hat{a}^\dagger. \quad (2.39)$$

The second operation is a lossless *beamsplitter* of reflectivity  $\eta$  [Fig. 2.5(b)]. Classically this is a two mode operation which splits the incident power into the two output modes with ratio  $\eta : 1 - \eta$ ; quantum mechanically this operation coherently and unitarily splits the probability amplitudes of the incoming fields across two modes  $\hat{a}_1^\dagger, \hat{a}_2^\dagger$  such that

$$\begin{aligned}\hat{a}_1^\dagger &\xrightarrow{\text{BS}} \sqrt{\eta} \hat{a}_1^\dagger + \sqrt{1-\eta} \hat{a}_2^\dagger \\ \hat{a}_2^\dagger &\xrightarrow{\text{BS}} \sqrt{1-\eta} \hat{a}_1^\dagger - \sqrt{\eta} \hat{a}_2^\dagger.\end{aligned}\quad (2.40)$$

It will be convenient to describe this by a  $2 \times 2$  matrix  $\hat{U}_{\text{BS}}$

$$\hat{U}_{\text{BS}}(\eta) = \begin{bmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{bmatrix} \quad (2.41)$$

where the minus phase shift is necessary to maintain unitarity (see Section 2.2.5) and thus conserving energy [87]. Finally we define an ‘integrated’ beamsplitter, the *directional coupler* [Fig. 2.5(c)], which acts symmetrically such that

$$\hat{a}_1^\dagger \xrightarrow{\text{DC}} \sqrt{\eta} \hat{a}_1^\dagger + i\sqrt{1-\eta} \hat{a}_2^\dagger \quad (2.42)$$

$$\hat{a}_2^\dagger \xrightarrow{\text{DC}} i\sqrt{1-\eta} \hat{a}_1^\dagger \sqrt{\eta} \hat{a}_2^\dagger, \quad (2.43)$$

or in matrix form

$$\hat{U}_{\text{DC}}(\eta) = \begin{bmatrix} \sqrt{\eta} & i\sqrt{1-\eta} \\ i\sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix}. \quad (2.44)$$

All experiments presented in this thesis will use  $\hat{U}_{\text{DC}}$ , but  $\hat{U}_{\text{BS}}$  has pedagogical merit and is often used for simplicity when developing and sketching LO circuitry.

### 2.6.3 MACH-ZEHNDER INTERFEROMETER

From these building blocks we can form larger circuits, such as the canonical two-mode *Mach-Zehnder interferometer* (MZI), which is constructed via a phase shifter sandwiched between two  $\eta = 1/2$  beamsplitters [Fig. 2.5(d)]. Pre-empting the qubit analysis in the forthcoming sections it will be convenient to describe this two mode system via the basis  $\{|0\rangle, |1\rangle\}$ . Let us consider how these building blocks

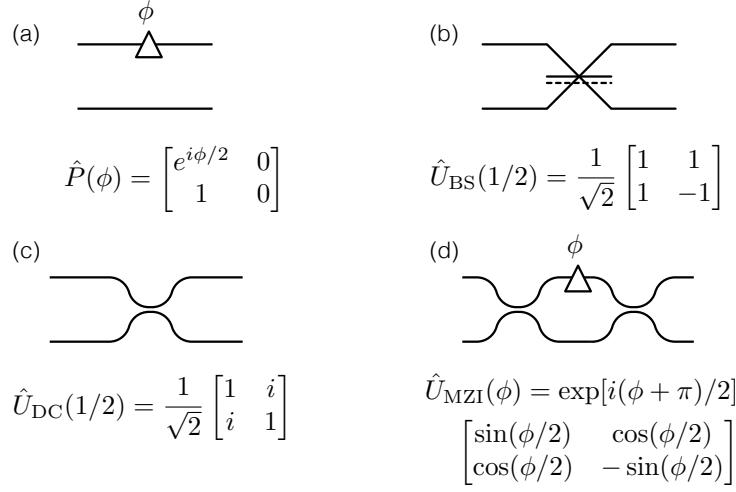


Figure 2.5: **The building blocks of linear optics.** Circuit symbols and matrix description for (a) a phase shifter, (b) a beamsplitter, (c) a directional coupler, and (d) a Mach-Zehnder interferometer.

transform vectors on the Bloch sphere: following the approach of Matthews et al. [15] a relative phase shift  $\phi$  between two optical modes can be modelled via  $\hat{P}(\phi) = \exp[i\phi\hat{Z}/2]$ , that is a rotation around the  $\hat{z}$ -axis of the Bloch sphere

$$\hat{P}(\phi) = e^{i\phi/2} \begin{bmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{bmatrix}. \quad (2.45)$$

Note, we keep track of the global phase which plays an important role later. Now consider the directional coupler with  $\eta = 1/2$

$$\hat{U}_{DC}(1/2) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \quad (2.46)$$

to understand its operation on the Bloch sphere we can see how it transforms basis states. Simple matrix multiplication shows

$$\hat{U}_{DC}|0\rangle = |+i\rangle; \quad \hat{U}_{DC}|1\rangle = e^{i\pi/2}|-i\rangle; \quad (2.47)$$

$$\hat{U}_{DC}|+\rangle = e^{i\pi/4}|+\rangle; \quad \hat{U}_{DC}|-\rangle = e^{-i\pi/4}|-\rangle; \quad (2.48)$$

$$\hat{U}_{DC}|+i\rangle = e^{i\pi/2}|1\rangle; \quad \hat{U}_{DC}|-i\rangle = |0\rangle. \quad (2.49)$$

So up to a global phase  $\hat{U}_{\text{DC}}$  is a  $90^\circ$  clockwise rotation around the  $\hat{x}$ -axis of the Bloch sphere.

We can combine these operations to build an MZI

$$\hat{U}_{\text{MZI}}(\phi) = \hat{U}_{\text{DC}} \hat{P}(\phi) \hat{U}_{\text{DC}} \quad (2.50)$$

$$= \exp[i(\phi + \pi)/2] \begin{bmatrix} \sin(\phi/2) & \cos(\phi/2) \\ \cos(\phi/2) & -\sin(\phi/2) \end{bmatrix}. \quad (2.51)$$

Note, up to a global phase  $\hat{U}_{\text{MZI}}$  resembles the variable reflectivity beamsplitter in (2.41) with  $\eta = \sin^2(\phi/2)$ . Hence, active control of a phase shift is sufficient to realise an arbitrarily reconfigurable beamsplitter, a fact we use in the design of the fully reconfigurable linear optical processing unit (LPU) in Chapter 6.

Injecting bright light of intensity  $I$  into the first mode and measuring the intensity of light in the output modes, gives  $I_0 = I \sin^2(\phi/2)$  and  $I_1 = I \cos^2(\phi/2)$ . This sinusoidal function is referred to as a classical interference fringe and will be used in Chapter 6 to characterise and calibrate the LPU.

#### 2.6.4 ARBITRARY OPERATIONS

Let us now examine how to use these building blocks to prepare arbitrary single qubit states, make single qubit measurements and perform arbitrary operations.

Recall from Section 2.3.1, arbitrary single qubit states can be written as  $|\psi\rangle = \sin(\phi/2)|0\rangle + \exp(i\theta)\cos(\phi/2)|1\rangle$ . Ignoring the global phase, a single photon injected into the first mode of an MZI can be written as

$$\hat{U}_{\text{MZI}}(\phi)|0\rangle = \begin{bmatrix} \sin(\phi/2) & \cos(\phi/2) \\ \cos(\phi/2) & -\sin(\phi/2) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \sin(\phi/2) \\ \cos(\phi/2) \end{bmatrix}. \quad (2.52)$$

Therefore adding a phase shift  $\theta$  to mode 2 after the MZI is sufficient to prepare *any single qubit state*. The task of state preparation is one of finding an operator  $\hat{A}$  such that  $|0\rangle \xrightarrow{\hat{A}} |\psi\rangle$ , hence  $\hat{A} = |\psi\rangle\langle 0| + |\psi^\perp\rangle\langle 1|$  where  $\langle\psi|\psi^\perp\rangle = 0$ .

The task of *measurement* is precisely the reverse. Taking any single qubit state, and deterministically projecting it onto  $|0\rangle$ . In other words an observable which

## 2.6. PHOTONIC QUBITS

---

asks “are you the state  $|\psi\rangle$  or  $|\psi^\perp\rangle$ ?” Placing detectors directly in the modes measures in the basis  $\{|0\rangle, |1\rangle\}$  therefore the relevant measurement operator is  $\hat{A}^\dagger = |0\rangle\langle\psi| + |1\rangle\langle\psi^\perp|$ . Hence a phase shifter followed by a MZI is sufficient to measure in any single qubit basis.

We can generate any two dimensional operation by first noting the Euler decomposition for the generation of any element of SU(2) [88]

$$\hat{U} = R_{\hat{z}}(\alpha)R_{\hat{x}}(\beta)R_{\hat{z}}(\gamma) \quad (2.53)$$

where

$$R_{\hat{n}}(\theta) \equiv \exp(i\theta \hat{n} \cdot \vec{\sigma}/2) \quad (2.54)$$

$$= \cos(\theta/2)\hat{I} + \sin(\theta/2)(n_x\hat{X} + n_y\hat{Y} + n_z\hat{Z}). \quad (2.55)$$

By this definition  $\hat{U}_{\text{MZI}}(\phi)$  is equivalent to  $R_{\hat{x}}(\theta)$  up to input and output phases  $\hat{P}(-\pi/2)$ :

$$R_{\hat{x}}(\phi) = \begin{bmatrix} \cos(\phi/2) & i \sin(\phi/2) \\ i \sin(\phi/2) & \cos(\phi/2) \end{bmatrix} \quad (2.56)$$

$$\hat{P}(-\pi/2)\hat{U}_{\text{MZI}}(\phi + \pi)\hat{P}(-\pi/2) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \cos(\phi/2) & \sin(\phi/2) \\ \sin(\phi/2) & -\cos(\phi/2) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad (2.57)$$

$$= \begin{bmatrix} \cos(\phi/2) & i \sin(\phi/2) \\ i \sin(\phi/2) & \cos(\phi/2) \end{bmatrix} \quad (2.58)$$

Recall,  $\hat{P}(\theta) = \exp(i\theta\hat{Z}/2)$ , therefore an MZI sandwiched between two phase shifters is sufficient to realise any single qubit operation

$$\hat{P}(\alpha')\hat{U}_{\text{MZI}}(\beta')\hat{P}(\gamma') = R_{\hat{z}}(\alpha)R_{\hat{x}}(\beta)R_{\hat{z}}(\gamma) \quad (2.59)$$

with transformations  $\alpha' = \alpha - \pi/2$ ,  $\beta' = \beta + \pi$ ,  $\gamma' = \gamma - \pi/2$ . In Table 2.2 we give phase shifter settings for Pauli preparation and measurements, which will be used for quantum state tomography in Chapter 7.

State	$\phi$	$\theta$	Observable	$\theta$	$\phi$
$ 0\rangle$	$\pi$	0	$\sigma_z$	0	$\pi$
$ 1\rangle$	0	0	$\sigma_x$	0	$\frac{\pi}{2}$
$ +\rangle$	$\frac{\pi}{2}$	0	$\sigma_y$	$\frac{\pi}{2}$	$\frac{3\pi}{2}$
$ -\rangle$	$\frac{\pi}{2}$	$\pi$			
$ +i\rangle$	$\frac{\pi}{2}$	$\frac{3\pi}{2}$			
$ -i\rangle$	$\frac{\pi}{2}$	$\frac{\pi}{2}$			

Table 2.2: **Pauli preparation and measurement settings.** On-chip phase shifter settings to prepare Pauli eigenstates and measure Pauli observables. Here, the global phase has been omitted, but should be accounted for when chaining multiple preparations and measurements together.

### 2.6.5 Two QUBIT GATES

A universal gate set for a quantum computer requires a conditional gate, such as the two-qubit controlled-NOT gate (CNOT) introduced in Section 2.3.3. The CNOT flips the state of the target qubit  $|0_T\rangle \leftrightarrow |1_T\rangle$  if the control qubit is in the logical  $|1_C\rangle$  state, and does nothing otherwise.

To realise this for photonic qubits in linear optics, consider constructing a circuit over four photonic modes (dual rail encoding); two modes for the control, and two modes for the target, such that the mode number basis transforms to the computational basis:

$$\{|13\rangle, |14\rangle, |23\rangle, |24\rangle\} \rightarrow \{|0_C0_T\rangle, |0_C1_T\rangle, |1_C0_T\rangle, |1_C1_T\rangle\}. \quad (2.60)$$

The CNOT can be implemented with an MZI over the target rails [see Fig. 2.6(a)] and a cross nonlinearity between modes  $|1_C\rangle$  and  $|0_T\rangle$ , such that a photon in mode  $|1_C\rangle$  applies a phase shift  $\phi = \pi$  (and the MZI then acts as a swap), whilst the vacuum in this mode results in no phase shift,  $\phi = 0$  (and the MZI then acts as identity).

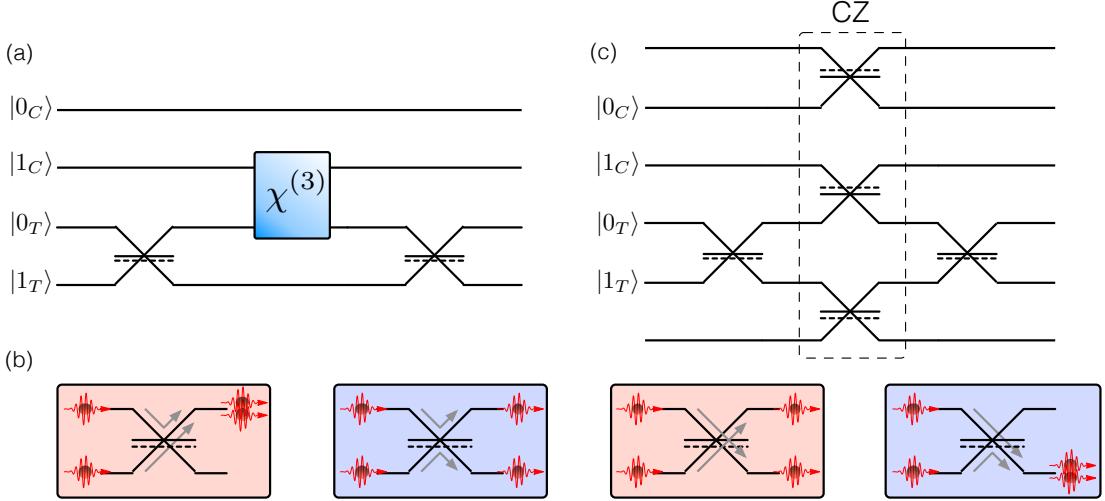


Figure 2.6: **Quantum interference powered two-qubit gates** (a) A two-qubit photonic CNOT gate can be realised with a  $\chi^{(3)}$  nonlinearity which applies a phase to the balanced interferometer conditional on  $|1_C\rangle$ . (b) The four possible outcomes in a Hong-Ou-Mandel interference experiment. A photon reflecting off the dotted face acquires a negative phase shift (shown in blue), and either reflecting off the solid face or transmitting, acquires a positive phase (shown in red). When the photons are indistinguishable, the central two terms destructively interfere and the photons bunch. (c) A quantum interference powered two-qubit CNOT gate can be constructed out of a CZ gate (beamsplitters in dashed box are  $\eta = 1/3$ ) and two  $\eta = 1/2$  beamsplitters.

In the all-photonic setting this phase shift requires an optical nonlinearity<sup>8</sup>: a material whose refractive index is a function of the intensity of light propagating through it. Such optical nonlinearities are incredibly weak as a strong response requires the electromagnetic field of incident light to be comparable to that of the nucleus of atoms within the material (see Section 3.2.2 for a more in-depth discussion). As a result the useful application of such nonlinearities has been limited to high power classical optics such as laser operation. The phase shift due to a single photon in a photonic crystal fibre has been reported by Matsuda et al. [90], but a

<sup>8</sup>Other approaches to inducing single photon nonlinearities exist such as light-matter interactions or engineering photonic structures, see Chang et al. [89] for a recent and comprehensive review.

$\pi$ -phase shift would require  $\mathcal{O}(10^5 \text{km})$  of fibre. Whilst the ultimate feasibility of such a system is an open question [91], it would certainly be a significant challenge.

Up until 2001, this was the status of linear optics. It was seen as a convenient platform for quantum communication or fundamental tests of quantum mechanics, but there were serious doubts as a platform for universal quantum computation. This all changed when Knill, Laflamme and Milburn (KLM) showed that by using the nonlinearity induced by single photon detection, an all optical quantum computer was possible [10]. We leave the details of the scheme to Chapter 7, but note here that a key ingredient is *quantum interference*.

### 2.6.6 THE HOM-TRINITY

At the heart of their proposal is the two photon interference phenomena, the Hong-Ou-Mangal (HOM) effect [92]. In the following we present three mathematically equivalent, yet conceptually distinct approaches to deriving this effect. Each approach will provide its own insight into a phenomena which is at the core of the experiments presented later in this thesis.

The HOM effect asks:

*What happens when you put two completely indistinguishable photons incident on a 50/50 beamsplitter?*

Here ‘completely indistinguishable’ means indistinguishable in all degrees of freedom; polarisation, spatio-temporal structure, frequency etc. As we have seen from Section 2.2.4, because this is a quantum system we must sum the possible outcomes at the probability amplitude level. Let us first examine this through the language of creation operators.

## 2.6. PHOTONIC QUBITS

---

### CREATION OPERATORS

Consider the transformation relations for the beamsplitter<sup>9</sup> in (2.40) with  $\eta = 1/2$ .

$$\begin{aligned}\hat{a}_1^\dagger &\xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}(\hat{a}_1^\dagger + \hat{a}_2^\dagger) \\ \hat{a}_2^\dagger &\xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}(\hat{a}_1^\dagger - \hat{a}_2^\dagger).\end{aligned}\quad (2.61)$$

Injecting a photon into modes 1 and 2 yields

$$\hat{a}_1^\dagger \hat{a}_2^\dagger \xrightarrow{\text{BS}} \frac{1}{2}(\hat{a}_1^\dagger + \hat{a}_2^\dagger)(\hat{a}_1^\dagger - \hat{a}_2^\dagger) \quad (2.62)$$

$$= \frac{1}{2}(\hat{a}_1^{\dagger 2} - \hat{a}_1^\dagger \hat{a}_2^\dagger + \hat{a}_2^\dagger \hat{a}_1^\dagger - \hat{a}_2^{\dagger 2}). \quad (2.63)$$

Examining (2.63) we see precisely what ‘summing at the probability amplitude level’ means. The first term and the last term represent both photons in the same mode, that is one photon transmitting and reflecting through the beamsplitter [see Fig. 2.6(b)]. The middle terms represent one photon per output mode, that is both photons reflecting or transmitting. From (2.30), as these events are indistinguishable (i.e. there is no observable which will tell us *which* photon transmitted), they commute  $[\hat{a}_1^\dagger, \hat{a}_2^\dagger] = 0$  and hence cancel. Therefore

$$\hat{a}_1^\dagger \hat{a}_2^\dagger |0\rangle \xrightarrow{\text{BS}} \frac{1}{2}(\hat{a}_1^{\dagger 2} - \hat{a}_2^{\dagger 2}) |0\rangle \quad (2.64)$$

$$= \frac{1}{\sqrt{2}}(|20\rangle + |02\rangle). \quad (2.65)$$

We arrive at a uniquely quantum mechanical effect: if the photons are indistinguishable they seem to *bunch* together, and you never see one photon per mode. Let us now examine this through the description of the unitary matrix.

### UNITARY DESCRIPTION

The unitary describing this transformation is given in (2.41) as

$$\hat{U}_{\text{BS}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (2.66)$$

---

<sup>9</sup>We consider the beamsplitter for simplicity, but these results can be extended to the directional coupler without loss of generality.

## 2. BACKGROUND

---

Using the Kronecker product formalism we can expand this into multi-photon Hilbert space

$$\hat{U}_{\text{BS}}^{\otimes 2} = \hat{U}_{\text{BS}} \otimes \hat{U}_{\text{BS}} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad (2.67)$$

whose basis in mode number is  $\{|1_1 1_2\rangle, |1_1 2_1\rangle, |2_1 1_2\rangle, |2_1 2_2\rangle\}$ . Following the approach of Popescu [93], inputting a photon in each mode requires symmetrising the initial state such that  $|\psi\rangle = 1/\sqrt{2}(|1_1 2_1\rangle + |2_1 1_2\rangle)$ . The transformation therefore becomes

$$\hat{U}_{\text{BS}}^{\otimes 2} |\psi\rangle = \frac{1}{2\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}, \quad (2.68)$$

recovering the HOM effect. This symmetrisation of the initial state can be thought of as the ‘source’ of entanglement in the HOM-state (2.65). We now present a third approach which will later provide an insight into the *computational complexity* of linear optics.

### PERMANENTS

If a detector is placed in each mode we can calculate the probability of both detectors firing via a matrix function known as the *permanent* [86]. The permanent appears mathematically similar to the determinant, but with the important difference that all terms are positively summed. For an  $n \times n$  square matrix  $A$  it is given by

$$\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i,\sigma(i)} \quad (2.69)$$

## 2.6. PHOTONIC QUBITS

---

where the sum runs over all elements  $\sigma$  of the symmetric subgroup  $S_n$ , that is the  $n!$  permutations of  $(1, 2 \dots n)$ . For example if

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \quad (2.70)$$

$$\text{perm}(A) = a_{1,1}a_{2,2} + a_{1,2}a_{2,1}, \quad (2.71)$$

and so on for larger matrices. We discuss the computational complexity of this function in detail in Chapter 5, but for the moment note that the probability for a coincidence (two-fold) detection event is given by

$$P(\text{2-fold}) = |\text{perm}(\hat{U}_{\text{BS}})|^2 \quad (2.72)$$

$$= |\text{perm} \left( \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)|^2 \quad (2.73)$$

$$= \left| \frac{1}{\sqrt{2}} (1 \times -1 + 1 \times 1) \right|^2 = 0 \quad (2.74)$$

thus recovering the HOM effect. This matrix function approach is simpler from a computational perspective when coding large scale simulations of multi-photon interference. This technique can also be generalised to  $p$ -photons in an  $m$ -mode linear optical circuit. To calculate the probability  $P_{i,o}$  for a given transition from input state  $|\psi_i\rangle = |n_1^i, n_2^i \dots n_m^i\rangle$  to output state  $|\psi_o\rangle = |n_1^o, n_2^o \dots n_m^o\rangle$  we evaluate

$$P_{i,o} = |\langle \psi_o | \hat{U} | \psi_i \rangle|^2 \quad (2.75)$$

$$= \frac{|\text{perm}(\Lambda)|^2}{\prod_j n_j^i! \prod_j n_j^o!}, \quad (2.76)$$

where  $\Lambda$  is a  $p \times p$  submatrix of  $\hat{U}$ , with entries given by the non-zero entries of  $|\psi_i\rangle$  and  $|\psi_o\rangle$ . i.e.  $n_1^i$  copies of the first column,  $n_2^i$  copies of the second column etc. and  $n_1^o$  copies of the first row,  $n_2^o$  of the second row etc. For concreteness consider the  $m = 3$  and  $p = 2$  case with  $|\psi_i\rangle = |101\rangle$  and  $|\psi_o\rangle = |110\rangle$ ,

$$\hat{U} = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} \\ u_{2,1} & u_{2,2} & u_{2,3} \\ u_{3,1} & u_{3,2} & u_{3,3} \end{bmatrix}; \quad \text{hence} \quad \Lambda = \begin{bmatrix} u_{1,1} & u_{1,3} \\ u_{2,1} & u_{2,3} \end{bmatrix}. \quad (2.77)$$

We further note (2.75) refers to the case of completely indistinguishable bosons. If however the bosons are distinguishable the numerator becomes  $\text{perm}(|\Lambda|^2)$  and the denominator runs over  $\prod_j n_j^o!$  only. Methods exist to treat partially distinguishable bosons with immanants [94] or via multidimensional permanents [95]. If the particles are fermions then the determinant  $|\det(\Lambda)|^2$  is used.

### 2.6.7 HOM POWERED TWO QUBIT GATE

Let us now use this interference effect to build an all photonic two-qubit CZ gate. Following the formulations of Ralph et al. [96] and Hofmann and Takeuchi [97] we consider the six-mode circuit shown in the dashed box of Fig. 2.6(c), consisting of three  $\eta = 1/3$  reflectivity beamsplitters, with two dual rail encoded qubits and two *ancilla modes*. We constrain this circuit to post-selected operation; that is we discard events which are outside of our computational subspace  $\{|0_C 0_T\rangle, |0_C 1_T\rangle, |1_C 0_T\rangle, |1_C 1_T\rangle\} \equiv \{|24\rangle, |25\rangle, |34\rangle, |35\rangle\}$ .

From visual inspection we can see  $|0_C 0_T\rangle$  and  $|0_C 1_T\rangle$ , with post-selection, stay as they are up to an overall probability (we discard events such as  $|0_C, 1_C\rangle$ ). The state  $|1_C, 1_T\rangle$ , receives a  $\pi$ -phase shift from the reflection of the control photon, hence  $|1_C, 1_T\rangle \rightarrow -|1_C, 1_T\rangle$ . Finally we can consider the state  $|1_C, 0_T\rangle$  via the evolution of creation operators  $\hat{c}_1^\dagger \hat{t}_0^\dagger$  through  $\hat{U}_{\text{BS}}(1/3)$

$$\hat{c}_1^\dagger \hat{t}_0^\dagger \xrightarrow{\hat{U}_{\text{BS}}(1/3)} \left( -\frac{1}{\sqrt{3}} \hat{c}_1^\dagger + \sqrt{\frac{2}{3}} \hat{t}_0^\dagger \right) \left( \sqrt{\frac{2}{3}} \hat{c}_1^\dagger + \frac{1}{\sqrt{3}} \hat{t}_0^\dagger \right) \quad (2.78)$$

$$= -\frac{\sqrt{2}}{3} \hat{c}_1^{\dagger 2} - \frac{1}{3} \hat{c}_1^\dagger \hat{t}_0^\dagger + \frac{2}{3} \hat{t}_0^\dagger \hat{c}_1^\dagger + \frac{\sqrt{2}}{3} \hat{t}_0^{\dagger 2}. \quad (2.79)$$

Commuting terms and applying post selection yields  $\hat{c}_1^\dagger \hat{t}_0^\dagger / 3$ , that is the state  $|1_C 0_T\rangle$  with probability  $p = 1/9$ , thus realising the full CZ logic.

The qubit basis and the photon number basis are not isomorphic. The Hilbert space dimensionality of two qubits is  $D = 4$ , whilst the dimensionality of two photons in four modes is  $|D_2^4| = 10$ . In the ideal case, quantum interference sets a zero probability for an outcome in some of these extra dimensions, while the successful measurement outcome removes the other extra dimensions. In Chapter

## 2.7. CONCLUDING REMARKS

---

7 we use this measurement induced nonlinearity to construct prototype two qubit gates, that are scalable for LOQC with the addition of fast feedforward capabilities.

## 2.7 CONCLUDING REMARKS

We have seen a variety of the theoretical constructs which underpin linear optical quantum computing — drawing on elements of mathematics, computer science and physics. So far our discussion has been architecture independent, but *a quantum computer is something that must be built in the lab*. In the following chapter we therefore introduce the photonic hardware which will be used for linear optical quantum information processing throughout the course of this thesis.

---

## 2. BACKGROUND

*What goes on inside is just too fast and huge and all interconnected for words to do more than barely sketch the outlines of at most one tiny little part of it at any given instant.*

David Foster Wallace

# 3

## Photonic Processing Hardware

### STATEMENT OF WORK

The multi-photon source was built, characterised and maintained by myself. Waveguide devices were designed and fabricated externally by collaborators and commercial organisations (detailed within), however characterisation, mounting and loss measurements were performed by myself. I built the optical coupling rig for passive waveguide devices, and packaged — in conjunction with C. Harrold and G. Marshall — the active silicon nitride device. Linear optical processor control electronics were designed by J. W. Silverstone, and built by myself. The time correlated single photon counting system was designed and built by P. J. Shadbolt.

## 3.1 INTRODUCTION

Here we present the physical hardware which will enable the photonic systems throughout this thesis. Whilst these systems are demonstrated for many different applications, they share the same basic stages: multi-photon generation; multi-photon manipulation via passive or active linear optical circuitry; and a multi-photon detection stage. Together we term them a ‘linear optical processing unit’ (LPU) — in analog to classical CPU. In our presentation of these basic stages, we include discussions of the core physics underpinning their operation.

In Section 3.2 we discuss single photon sources and the principles governing spontaneous parametric down-conversion; and in Section 3.3 present a multi-photon source based upon down-conversion. We present the theory behind guided propagation of light in Section 3.4 then describe the various material platforms that will be used, along with practical consideration of interfacing for use within the LPU, in Section 3.5. Finally, in Section 3.6, we describe the time-correlated single photon counting system used throughout this thesis.

## 3.2 SINGLE PHOTON SOURCES

Investigation into the quantised nature of light has transformed modern physics. In the late 19th, and early 20th century, anomalous results such as the inability of Maxwell’s equations to account for the photoelectric effect and blackbody radiation, began amounting. This crisis led to a Kuhnian paradigm shift which culminated in 1905 with Einstein postulating that *light itself was quantised*:

*“According to this picture, the energy of a light wave emitted from a point source is not spread continuously over ever larger volumes, but consists of a finite number of energy quanta that are spatially localised at points of space . . . Subsequently, I wish to explain the reasoning and supporting evidence that led me to this picture of light, in the hope that*

### 3.2. SINGLE PHOTON SOURCES

---

*some researchers may find it useful for their experiments.”*

Albert Einstein [4]

From Compton’s initial observation of the momentum of a photon [98], to the use of photons in biological imaging [99]; the photon has become ubiquitous in modern science both as an experimental and conceptual tool. More recent research into the *generation* of photons has been driven by the commercial applications of quantum cryptography [82]. Quantum key distribution systems are now available from companies such as ID Quantique [100] and MagiQ [101], as are off-the-shelf single photon sources [102].

From the perspective of linear optical quantum computing (LOQC) let us recall Section 2.5.2 and DiVincenzo’s second critereon for the physical implementation of a quantum computer:

*“The ability to prepare the state of the qubits in an initial fiducial state.”* [67]

Hence, a LOQC must *reliably* produce on-demand single photons. For our purpose an ideal photon source is one that produces single photons on-demand with unit probability, and multiple photons with zero probability. Multi-qubit gates place a further constraint that these photons must be completely indistinguishable in all degrees of freedom.

Several promising platforms exist for the generation of single photon states [103, 104]. Single emitters relying on the externally controlled excitation and subsequent relaxation of a two-level quantum system are particularly appealing due to their ‘in principle’ deterministic operation. Such systems include nitrogen-vacancy colour centres [105], single optically trapped neutral atoms [106], single trapped ions [107], single molecules [108, 109] and semi-conductor quantum dots [110]. The major outstanding goal for all these platforms is the high efficiency interfacing with optical networks, and the creation of simultaneously addressable, identical, multiple emitters. Due to the nascency of these emitter based technologies we opt for a platform which whilst probabilistic, allows for the reliable generation

---

### 3. PHOTONIC PROCESSING HARDWARE

of high fidelity, high intensity, multi-photon states, via the process spontaneous parametric down-conversion.

#### 3.2.1 SPONTANEOUS PARAMETRIC DOWN-CONVERSION

Spontaneous parametric down-conversion (SPDC) is a process whereby a pump photon incident on a  $\chi^{(2)}$  nonlinear material probabilistically splits into two lower energy daughter photons, conserving energy and momentum. The weak nonlinearities of commonly available materials means this probability is small  $\mathcal{O}(10^{-11})^*$ . However, advances in laser science of the past half century means the absolute rate of photon generation can be made relatively high by pumping the material with a bright, coherent laser beam.

SPDC has been the work horse of quantum optics. Since the first demonstration of correlated photon pairs [112], SPDC has been instrumental in demonstrating quantum interference effects [92, 113, 114], violations of local realism [115–117], proof of principle quantum information processing tasks such as two-qubit quantum gates [118], quantum algorithms [119] and quantum simulations [120], and quantum metrology [121–123]. Further advances in ultra bright entangled sources [124] have enabled quantum teleportation [80], quantum communication [125], quantum cryptography [126–128], and the generation of eight-photon entangled states [129, 130].

More recently, nonlinear effects in waveguide devices such as silicon [20], silica [131], PPLN [132] and PPKTP [133] have demonstrated the feasibility of utilising high fidelity integrated photon sources as a scalable platform for quantum information processing. Moreover, when coupled with fast, low loss switching; such devices can be multiplexed [134] to provide a route towards an all-optical near-deterministic photon source [135–138].

---

\*In Kwiat et al. [111] they estimate a pair photon rate of  $\sim 60,000 \text{ s}^{-1}\text{mW}^{-1}$  of incident power. At 351nm, a single photon has  $E = \hbar c/\lambda = 10^{-19} \text{ J}$  of energy, hence 1mW of laser power contains  $10^{-3}/10^{-19} = 10^{16}$  photons. This therefore gives the probability of creation per photon as  $10^5/10^{16} = 10^{-11}$ .

### 3.2. SINGLE PHOTON SOURCES

---

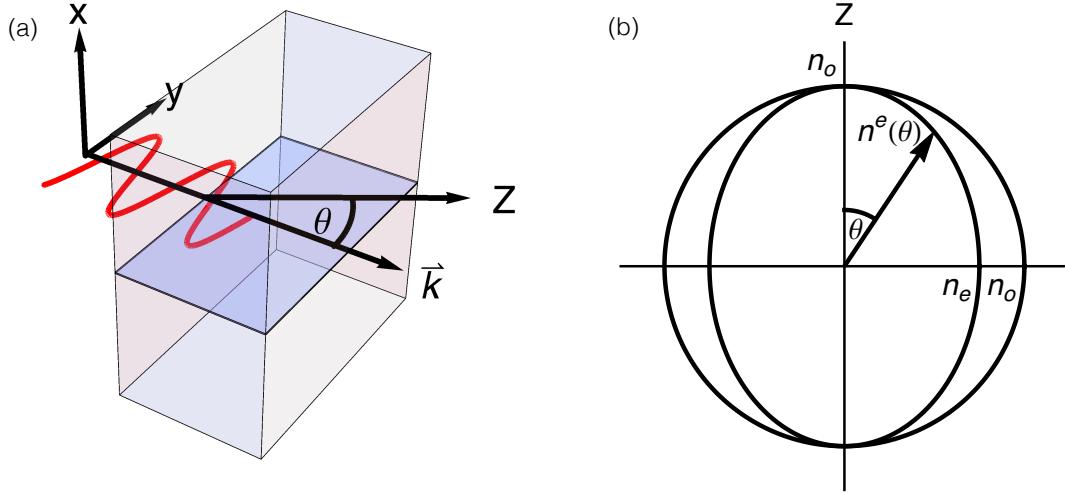


Figure 3.1: **Birefringence.** (a) Extraordinary light with wave vector  $\vec{k}$  is polarised in the principle plane of a birefringent uniaxial crystal, subtending an  $\theta$  with the optic axis  $Z$ . The principle plane is defined as the plane containing  $\vec{k}$  and  $Z$ . (b) Refractive index experienced by an e-beam at an angle  $\theta$  to optic axis for a negative uniaxial crystal ( $n_o > n_e$ ).

#### 3.2.2 PRINCIPLES OF DOWN-CONVERSION

The following discussion of SPDC draws on Dmitriev et al. [139] and the PhD thesis of N. K. Langford [84].

##### BIREFRINGENCE

Birefringence is a property of materials whose refractive index  $n$  is dependent on the polarisation of incident light. The conceptually simplest kind of birefringent material is a *uniaxial crystal* shown in Fig. 3.1(a), which has a single axis of symmetry called the optic axis ( $Z$ ). The principle plane is defined as the plane containing the optic axis and the wave vector  $\vec{k}$  of the light, where

$$|\vec{k}| = \frac{2\pi n}{\lambda}, \quad (3.1)$$

the wavelength of incident light is  $\lambda$ , and the direction is given by the direction of propagation of the light. A beam whose polarisation (i.e. plane in which the elec-

tric field oscillates) is perpendicular to the principle plane is termed the ordinary beam (o-beam), and a beam polarised in the principle plane is termed the extraordinary beam (e-beam). The refractive index of the o-beam  $n_o$  is independent of the direction of propagation, whilst the refractive index of the e-beam  $n^e(\theta)$  depends on the direction. Specifically, if the e-beam is propagating in the direction<sup>2</sup> perpendicular to  $Z$  it experiences a refractive index  $n_e$ , and parallel it experiences  $n_o$ . At a general angle  $\theta$  it sees

$$n^e(\theta) = n_o \sqrt{\frac{1 + \tan^2 \theta}{1 + (n_o/n_e)^2 \tan^2 \theta}}. \quad (3.2)$$

If  $n_o > n_e$  the crystal is described as negative (e.g.  $\beta$ -Barium borate used for second harmonic generation in Section 3.3), if  $n_o < n_e$  it is positive (e.g. quartz wave-plates). The quantity  $n^e(\theta)$  can therefore be represented by an ellipsoid with axes  $n_e$  and  $n_o$ , Fig. 3.1(b).

Finally, we note that crystals are dispersive so the refractive index depends on wavelength according to the Sellmeier equations

$$n(\lambda) = \sqrt{A + \frac{B}{\lambda^2 - C} - D\lambda^2}, \quad (3.3)$$

where  $A, B, C, D$  are empirically derived quantities. In the case of uniaxial crystals there will be two equations governing both the o- and e-beams.

## NONLINEAR OPTICS

The displacement field  $\mathbf{D}$  describes the effect of an electromagnetic field in a dielectric material, and is related to the electric field  $\mathbf{E}$  and the polarisation density of the material  $\mathbf{P}$  via

$$\mathbf{D} = \epsilon_0 \mathbf{E} + \mathbf{P}, \quad (3.4)$$

where  $\epsilon_0$  is the permittivity of free space. When an electric field is applied to a dielectric, positive and negative bound charges can slightly separate creating a

---

<sup>2</sup>There is potential for confusion between the terminology ‘direction of propagation’ and ‘direction of polarisation’. We consider the former, defined as the direction of  $\vec{k}$ .

### 3.2. SINGLE PHOTON SOURCES

---

dipole moment whose field is described by the polarisation density. The overall field must therefore be corrected for and the displacement in (3.4) accounts for this.

This correction can be described with a single term by introducing the electrical susceptibility  $\chi_e$  which for linear materials relates the polarisation and electric field via  $\mathbf{P} = \varepsilon_0 \chi_e \mathbf{E}$ . Rewriting (3.4) as

$$\mathbf{D} = \varepsilon_0(1 + \chi_e)\mathbf{E}, \quad (3.5)$$

gives the displacement solely in terms of electric field. It is convenient to introduce the relative permittivity  $\varepsilon_r = 1 + \chi_e$  so that (3.5) becomes

$$\mathbf{D} = \varepsilon_0 \varepsilon_r \mathbf{E}. \quad (3.6)$$

The relative permittivity can directly be linked to the refractive index by  $n = \sqrt{\varepsilon_r \mu_r}$ , where  $\mu_r$  is the relative permeability which for non-magnetic materials is  $\mu_r = 1$ . In this case the refractive index is given by  $n = \sqrt{\varepsilon_r}$  and is therefore *a measure of how easily dipole moments are induced*. If  $\varepsilon_r$  is large, the dipoles exert a greater retarding force on the incoming electromagnetic field, effectively slowing the phase velocity of the light  $v = c/n$  (where  $c$  is the speed of light in vacuum), thus giving us what we term a ‘large’ refractive index. In Section 3.4.3 we explore this in more detail to account for the thermo-optic effect and dispersion.

From (3.6) we see the displacement field is linear in the electric field, hence the origin of the term *linear* optics. For *nonlinear* materials the displacement field becomes

$$\mathbf{D} = \varepsilon_0 [(1 + \chi^{(1)})\mathbf{E} + \chi^{(2)}\mathbf{E}^2 + \chi^{(3)}\mathbf{E}^3 + \dots], \quad (3.7)$$

where  $\chi^{(2)}, \chi^{(3)} \dots$  represent higher order electric susceptibility terms characterising the nonlinear response of the material. Usually materials are only weakly nonlinear  $\chi^{(1)} \gg \chi^{(2)} \gg \chi^{(3)} \dots$ , and in the work presented here we consider only crystals with  $\chi^{(2)}$  nonlinearity.

From our argument relating refractive index and electric susceptibility, this nonlinear dependence means the refractive index of a material can be a function

### 3. PHOTONIC PROCESSING HARDWARE

---

of the intensity of the incident field. *Light can control light.* In  $\chi^{(2)}$  materials, propagation of two monochromatic beams with frequencies  $\omega_1, \omega_2$  gives rise to new light waves with new frequencies  $\omega_{3,4} = \omega_1 \pm \omega_2$ . In the following we consider two special cases whereby  $\omega_1 = \omega_2$ : *second harmonic generation* (SHG) where two photons create a higher frequency photon, and the reverse process, SPDC, where a single photon splits to two lower energy photons.

#### PHASE MATCHING

First we examine the conceptually simpler SHG process — partly for pedagogic purposes, but partly as it plays the role of the ‘up-convertor’ in the multi-photon source in Section 3.3 — and then we extend this analysis to SPDC.

Typically, nonlinear effects occur when phase matching conditions are satisfied

$$\omega_3 = \omega_2 + \omega_1 \quad (3.8)$$

$$\vec{k}_3 = \vec{k}_2 + \vec{k}_1. \quad (3.9)$$

This is equivalent to saying that energy ( $E = \hbar\omega$ ) and momentum ( $\vec{p} = \hbar\vec{k}$ ) is conserved. In the special case of collinear SHG we define  $k_1$  and  $k_3$  to be the input and output beams respectively [see Fig. 3.2(a)], and the phase matching conditions become  $\omega_3 = 2\omega_1$  and  $k_3 = 2k_1$ . In Type I phase matching a new beam is generated from two beams of the same polarisation, whilst in Type II phase matching a new beam is generated from two beams of orthogonal polarisation. All experiments presented in this thesis rely on Type 1 phase matching, and for SHG we are interested in two e-beams generating an o-beam ( $ee \rightarrow o$ ).

Recall from (3.2) that the refractive index seen by the e-beam  $n^e(\theta)$ , is a function of the direction of propagation with respect to the optic axis. From (3.1),  $\vec{k}$  depends on refractive index, therefore the wave vector of the e-beam  $\vec{k}_e(\theta)$  depends on the angle made with the optic axis.

The aim is to find the phase matching angle  $\theta_{\text{pm}}$  such that

$$\vec{k}_1^e(\theta_{\text{pm}}) + \vec{k}_2^e(\theta_{\text{pm}}) = \vec{k}_3^o, \quad (3.10)$$

### 3.2. SINGLE PHOTON SOURCES

---

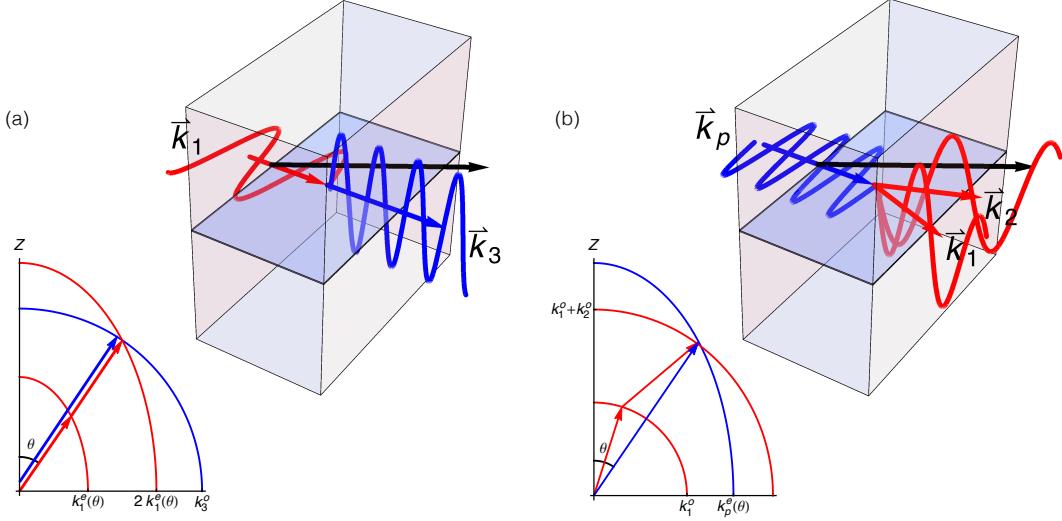


Figure 3.2: **Type I SHG and SPDC phase matching.** (a) Collinear second harmonic generation of  $ee \rightarrow oo$  light with in-coming and outgoing wave vectors shown. Inset, phase matching requires conservation of momentum and energy, and can be visualised as finding the intersection of the ellipse describing the wave vector  $2\vec{k}_1^e(\theta)$  and  $\vec{k}_3^o$ . (b) Non-collinear  $e \rightarrow oo$  spontaneous parametric down-conversion.

which in the case of collinear SHG simplifies to  $2k_1^e(\theta_{\text{pm}}) = k_3^o$ . This can be visualised as finding the intersection between the circle traced by  $k_3^o$  and the ellipse traced by  $2k_1^e(\theta_{\text{pm}})$ , see Fig. 3.2(a) inset. Experimentally, crystals are usually pre-cut for a known  $\theta_{\text{pm}}$ , such that only fine tuning is needed to optimise the conversion efficiency. In the lab, when converting from 800 nm  $\rightarrow$  400 nm this is usually done by aligning the input polarisation in the principle plane, then varying  $\theta$  till an ethereal blue ‘up-converted’ glow is observed. A polarisation analyser (polarising beamsplitter and photodiode) after the SHG can then be used to fine tune  $\theta$  and the principle axis orientation so as to maximise the intensity of  $o$  polarisation.

Let us now consider the reverse SPDC process, whereby a single ‘pump’ photon splits into two lower energy ‘daughter’ photons, Fig. 3.2(b). If the phase matching conditions are carefully met (as in (3.8) and (3.9) with  $\omega_3, \vec{k}_3 \rightarrow \omega_p, \vec{k}_p$ ) the daughter photons should be completely indistinguishable. The subtlety in phase matching SPDC arises when we impose noncollinear generation, so daughter ph-

tons are generated at an ‘opening angle’ to the pump, allowing unwanted laser light to be avoided when collecting single photons. Phase matching conditions must therefore consider perpendicular  $\vec{k}$  components.

Momentum conservation from (3.9) gives  $\vec{k}_p = \vec{k}_1 + \vec{k}_2$ . Breaking this in to components parallel and perpendicular to the pump gives

$$k_p = k_1 \cos \theta_1 + k_2 \cos \theta_2 \quad (3.11)$$

$$0 = k_1 \sin \theta_1 + k_2 \sin \theta_2 \quad (3.12)$$

where  $\theta_1, \theta_2$  are the opening angles of the daughter photons with respect to the pump beam. Note, these conditions are invariant to rotation about the pump, therefore photons are emitted either sides of a *cone*. In the case where  $e \rightarrow oo$  only the pump beam depends on  $\theta$  and it can be shown [84] that

$$\cos \theta_1 = \frac{k_p^2(\theta) - k_2^2 + k_1^2}{2k_1 k_p(\theta)}, \quad (3.13)$$

which given desired frequencies and the optic axis angle  $\theta$ , can be solved to find the opening angle of the emitted photons  $\theta_1$ . Further, dispersion effects must be accounted for using the Sellmeier equations (3.3) and a correction applied due to the refraction of light between the crystal air boundary. Typical opening angles  $\theta_{op} = \theta_1 + \theta_2 \approx 6^\circ$ , with  $\theta_1 = \theta_2$ .

The SPCD process described above occurs in uniaxial crystals such as  $\beta$ -Barium borate (BBO), however the source we present in Section 3.3 uses a relatively new *biaxial* crystal  $\text{BiB}_3\text{O}_6$  (BiBO) with a much higher nonlinearity than that of BBO (2–3 times) [140]. Biaxial crystals have two optic axes, making a single principle plane undefined and the phase matching conditions significantly more complex with three Sellmeier equations  $\{n_x, n_y, n_z\}$  — see reference [139] for a thorough discussion. In practice this does not pose a problem as crystals are cut for a desired wavelength, and photons are emitted at a known opening angle. Once photons are found fine tuning of the phase matching angles can be done *in situ*.

### 3.2. SINGLE PHOTON SOURCES

---

#### THE QUANTUM MECHANICAL PICTURE

In the quantum mechanical picture of creation and annihilation operators (see Section 2.6.1) acting on the pump mode  $\hat{a}_p^\dagger$  and daughter modes  $\hat{a}_{1,2}^\dagger$ , SPDC can be described by the interaction Hamiltonian

$$\hat{H} = g\hat{a}_1^\dagger\hat{a}_2^\dagger a_p + g^*a_1 a_2 \hat{a}_p^\dagger \quad (3.14)$$

where  $g \propto \chi^{(2)}$  is a coupling constant and the second term maintains Hermiticity (physically interpreted as the reverse SHG process).

Typically pump photons are supplied by a bright laser in the form of a coherent state, so we can write the initial state at  $t = 0$  as  $|\psi_{\text{in}}(0)\rangle = |0\rangle_1 |0\rangle_2 |\alpha\rangle_p$ . Following the approach of Ou [141], since the pump field is approximately classical the Hamiltonian can be rewritten as

$$\hat{H} = i\xi\hat{a}_1^\dagger\hat{a}_2^\dagger + i\xi^*a_1 a_2 \quad (3.15)$$

where the properties of the pump and  $g$  are expressed in  $\xi$ . Evolving this Hamiltonian via the unitary operator  $\hat{U}(t) = \exp[-i\hat{H}t]$  for time  $t$  on the vacuum modes  $|0_1 0_2\rangle$  yields

$$|\Psi_{\text{DC}}\rangle = \hat{U}|0_1 0_2\rangle \quad (3.16)$$

$$= \exp[-i(i\xi\hat{a}_1^\dagger\hat{a}_2^\dagger + i\xi^*a_1 a_2)]|0_1 0_2\rangle \quad (3.17)$$

$$\approx \sum_{j=0}^{\infty} \frac{\gamma^j}{j!} \hat{a}_1^{\dagger j} \hat{a}_2^{\dagger j} |0_1 0_2\rangle \quad (3.18)$$

$$= \sum_{j=0}^{\infty} \gamma^j |j_1 j_2\rangle \quad (3.19)$$

$$= |0_1 0_2\rangle + \gamma |1_1 1_2\rangle + \gamma^2 |2_1 2_2\rangle + \dots, \quad (3.20)$$

where  $\gamma = \xi t$  captures the crystal thickness (interaction time), pump properties and nonlinear coupling constant. Between (3.17) and (3.18) we assume that the average photon number of the pump  $|\alpha|^2 \gg 1$ , thus the pump does not ‘lose’ photons  $\hat{a}^\dagger \hat{a} |\alpha\rangle \approx \hat{a} \hat{a}^\dagger |\alpha\rangle \approx |\alpha|^2 |\alpha\rangle$ , and we assume the low gain regime  $|\xi| \ll 1$ .

### 3. PHOTONIC PROCESSING HARDWARE

---

Some remarks: when the pump power is weak  $|\gamma|$  is small and  $|\gamma| \gg |\gamma|^2 \gg |\gamma|^3$ , hence

$$|\Psi_{\text{DC}}\rangle \approx |0_1 0_2\rangle + \gamma |1_1 1_2\rangle. \quad (3.21)$$

Thus, in the idealised lossless case, detecting a single photon in mode one guarantees a single photon in mode two; we say the detection of  $|1\rangle_1$  “heralds” the state  $|1\rangle_2$ .

If  $|\Psi_{\text{DC}}\rangle$  is injected into a linear optical network and only two detection events are registered, it is as if we had the state  $|\Psi_{\text{DC}}\rangle = |1_1 1_2\rangle$  and we say the two photon state is “postselected”. A particularly useful case will be the Hong-Ou-Mandel (HOM) interference experiment whereby modes one and two are injected into either mode of a  $\eta = 1/2$  beamsplitter. Recall from Section 2.6.6, in the ideal case  $|\Psi_{\text{DC}}\rangle = |1_1 1_2\rangle$  the probability of a coincidence event  $P(\text{2-fold}) = 0$ . If however  $|\Psi_{\text{DC}}\rangle = \sqrt{1-\gamma}|1_1 1_2\rangle + \sqrt{\gamma}|2_1 2_2\rangle$  (perhaps due to an increased pump power), in the presence of non-number-resolving bucket detectors, four photon events will masquerade as two photon events and it is straightforward to show  $P(\text{2-fold}) = \gamma/4 > 0$ , hence quantum interference will be degraded.

As a metric for the quality of this interference we take a HOM-dip, whereby one of the input photons is made distinguishable with respect to the other (usually via a temporal delay  $\Delta\tau$  greater than its coherence length) so that  $P(\text{2-fold}) = 1/2$  and  $N_{\max}$  coincidences are collected. This temporal delay is then tuned such that  $\Delta\tau = 0$  and  $N_{\min}$  coincidences are collected. The visibility  $V = (N_{\max} - N_{\min})/N_{\max}$  is then calculated as a metric for the quality of interference; which in the ideal case  $V = 1$ , and in the fully distinguishable case  $V = 0$ .

#### 3.2.3 PRINCIPLES OF MULTI-PHOTON PRODUCTION

Experiments presented in this thesis require *multi-photon*, multi-mode states of the form  $|1_1 1_2 \dots, 1_p\rangle$  — necessitating multiple down-conversion events. Consider two down-conversion events  $|\Psi_{\text{DC}}^1\rangle$  and  $|\Psi_{\text{DC}}^2\rangle$  occurring simultaneously and identically such that  $\gamma_1 = \gamma_2$ . Each system consists of two modes, so the entire system

### 3.2. SINGLE PHOTON SOURCES

---

is described across four modes. The total output state is given by the tensor products of these two events

$$|\Psi_{\text{DC}}^1\rangle \otimes |\Psi_{\text{DC}}^2\rangle = \sum_{j=0}^{\infty} \gamma^j |j_1 j_2\rangle \otimes \sum_{k=0}^{\infty} \gamma^k |k_3 k_4\rangle \quad (3.22)$$

which expanded up to the four-photon subspace reads

$$|\Psi_{\text{DC}}^1\rangle \otimes |\Psi_{\text{DC}}^2\rangle \approx |0_1 0_2 0_3 0_4\rangle + \quad (3.23)$$

$$\gamma (|0_1 0_2 1_3 1_4\rangle + |1_1 1_2 0_3 0_4\rangle) + \quad (3.24)$$

$$\gamma^2 (|1_1 1_2 1_3 1_4\rangle + |0_1 0_2 2_3 2_4\rangle + |2_1 2_2 0_3 0_4\rangle). \quad (3.25)$$

Some remarks: first, with probability  $|\gamma|^4$  we have a four-photon superposition state. In the idealised lossless case, measuring  $|1_2 1_3\rangle$  guarantees the state  $|1_1 1_4\rangle$ ; in other words *a heralded two-photon state*. Furthermore, measuring  $|1_1\rangle$  and injecting modes  $\{2, 3, 4\}$  into a linear optical circuit then registering three and only three detection events at the output of the circuit, behaves as if we had injected into the circuit  $|1_2 1_3 1_4\rangle$ .

Extending this technique to herald the generation of higher photon numbers results in an exponential fall off in the probability of success. To postselect an  $n$ -photon state requires  $n - 1$  down-conversion events firing simultaneously. If the probability for one crystal to fire is  $p$ , the probability they all fire is  $p^{n-1}$ . Even at a relatively high probability per clock cycle the multi-photon probability rapidly falls off. For example, state of the art experiments report  $p = 0.058$  yet an eight photon rate of just 3 mHz (nine events per hour) [130].

### MULTI-PHOTON ARCHITECTURES

A variety of architectures can be used to realise multiple down-convertors. Perhaps the conceptually simplest is a single pump laser passing through multiple crystals in series (see Fig 3.3(a) and for example [129, 130]). If the laser is continuously pumped both crystals generate photons according to independent Poissonian processes, hence  $|\Psi_{\text{DC}}^1\rangle$  and  $|\Psi_{\text{DC}}^2\rangle$  will not be correlated in time. A *pulsed* laser

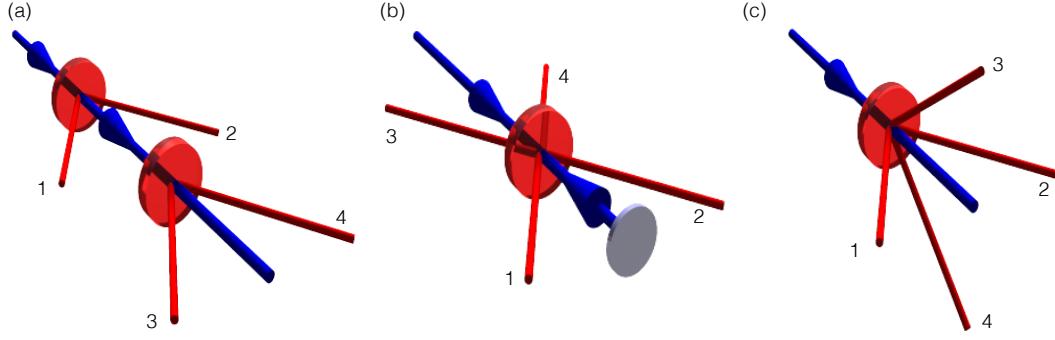


Figure 3.3: **Multi-photon architectures.** A variety of multi-photon source architectures with pump and down-converted photons depicted in blue and red respectively. (a) Multi-crystal architecture, (b) single crystal multi-pass and (c) single-crystal single-pass.

system must therefore be used to ensure correlated photon production. Provided the photon generation takes place in a time frame which is small compared to the coherence length of the photons, the separate generation events can be considered simultaneous. However, as we will see, in an experimentally realistic scenario if this condition is not met the events become distinguishable and quantum interference is degraded. A further advantage of pulsed laser systems is the high peak power, making  $\gamma$  large and the multi-photon production rate appreciable.

Another common architecture is the “double pass”, whereby the same laser pulse is reflected (usually via a dichroic mirror) back through the crystal to generate photons in the reverse direction [Fig 3.3(b)]. This technique was used in some of the earliest multi-photon generation experiments [80], and is still used to this day (see for example [24, 142]).

A final architecture, and the one which we employ, is the single-crystal single-pass technique whereby photons are collected at *multiple points* on the downconversion cone [Fig 3.3(c)]. As we have seen, the phase matching conditions (3.8) and (3.9) are invariant to rotation about the pump, so pairs of photons are generated on either side of a cone. This technique has widely been used in Bristol [143, 144]<sup>3</sup>

---

<sup>3</sup>For a novel method of collecting multiple modes on a downconversion cone see Rossi et al. [145].

### 3.2. SINGLE PHOTON SOURCES

---

and whilst all architectures are effectively equivalent, our choice was primarily based on space constraints. However, in practice, other simplifications arose such as ease of phase matching and filter alignment. Let us now discuss some of the limitations of multi-photon production, noting that the major limiting factors are architecture independent.

#### SOURCES OF ERROR

To understand multi-photon error mechanisms we first define a figure of merit. As in Section 3.2.2 we take the pragmatic approach of measuring quantum interference via HOM dips. In contrast to the two mode case where only a single combination of HOM dips can occur, the multi-mode regime offers a set of HOM patterns. We define “pair dips” as dips between photons from the same creation event (e.g. photons  $\{1, 2\}$  and  $\{3, 4\}$ ), and “off-pair dips” as dips between photons from different creation events (e.g. photons  $\{2, 3\}, \{1, 4\}$ ). For the latter, if modes  $\{2, 3\}$  from (3.25) are directly injected onto a beamsplitter, a maximum visibility of  $V = 1/3$  can only ever be observed. To see this note that only one of the three superposition terms quantum interferes. To see an in principle full visibility dip, the source must be operated in heralded mode: modes  $\{1, 4\}$  are sent into heralding detectors, and modes  $\{2, 3\}$  onto a beamsplitter. In this case the heralding projects (3.25) onto  $|1_2 1_3\rangle$  and an in principle full visibility dip can be observed.

Due to the magnitude of  $\chi^{(2)}$  seeing an appreciable multi-photon rate typically requires larger pump power. In the four photon case that means increasing the pump power such that  $p_4 = |\gamma|^4$  is non negligible. Note however that the ratio of higher order terms grows quadratically  $p_6/p_4 = |\gamma|^2$ , so an increased pump power results in an increased unwanted multi-photon emission probability. This will manifest itself as decrease in both pair and off-pair dip visibilities.

Unwanted multi-photon events can in principle be arbitrarily suppressed by reducing pump power and increasing integration time. Nevertheless, a second source of error is intrinsic to the architecture and cannot be entirely removed: *temporal jitter*. Temporal jitter occurs due to a finite pulse and crystal width, and

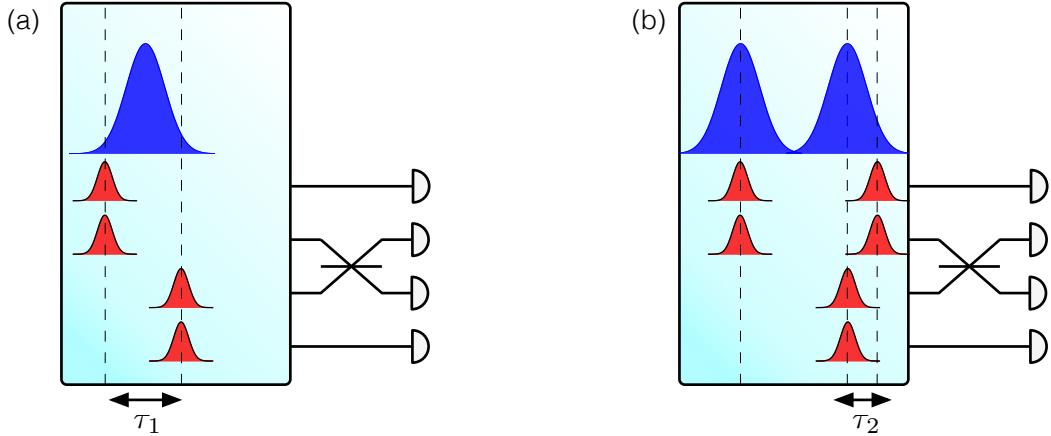


Figure 3.4: **Multi-photon error mechanisms.** (a) Due to finite pulse width (blue) a photon pair (red) can be born at the front of the pulse, and a pair at the back, yielding temporal jitter  $\tau_1$ . (b) Due to group velocity mismatch daughter photons propagate faster than pump photons, causing temporal jitter  $\tau_2$  between photons in different pairs. Adapted from Tanida et al. [146].

is analysed in depth by Tanida et al. [146] — here we describe it qualitatively and discuss methods to minimise it.

Considering the single-crystal single-pass picture Fig. 3.4, there are two sources of temporal jitter: first, due to the finite pump width, a pair of photons may be born near the front of the pulse and a pair near the back of the pulse [see Fig. 3.4(a)], causing temporal distinguishability between pairs as a function of the ratio between pulse width and photon coherence length. This will manifest itself only as a reduction in off-pair dip visibility. Experimentally this effect can be minimised by increasing the coherence length of the photon to be significantly larger than the pulse width; experimentally achieved by passing the down-converted photons through narrow bandwidth filters (width  $\Delta\lambda$ ), thus increasing their coherence length  $L_{coh} = \lambda^2/\Delta\lambda$ .

Second, due to finite crystal width, a pair may be born at the front of the crystal and a pair at the back. If the pump and down-converted photons propagate with same group velocity there would be no temporal mismatch. However crystals

### 3.3. EXPERIMENTAL MULTI-PHOTON SOURCE

---

are dispersive, which means the refractive index, and hence the group velocity is wavelength dependent [see (3.3)]; thus there will be some temporal jitter due to group velocity mismatch [see Fig. 3.4(b)]. This effect can be minimised by reducing the crystal width.

In general both solutions to temporal jitter come at the cost of decreasing the multi-photon rate. Narrower filters throw away more photons, and narrower crystals effectively reduce the Hamiltonian interaction time, thus reducing  $\gamma$ . The necessary hardware for each experiment should therefore be judged on a case-by-case basis, taking into account the need for high fidelity data versus quick data, constrained by factors such as experimental instability and impending conference deadlines.

## 3.3 EXPERIMENTAL MULTI-PHOTON SOURCE

We now describe the multi-photon source which will be used through this thesis. As shown in Figure 3.5, laser light from a tuneable 140 fs pulsed Titanium:Sapphire laser (Coherent Chameleon-Ultra) tuned to 800 nm<sup>4</sup> with 80 MHz repetition rate, is attenuated via a high power half-wave plate (HWP) and Glan-Laser Polariser (PBS) (Edmund Optics NT49-214 and NT47-250), then focused via a thin  $f = 0.15$  m fused silica lens (CVI PLCX-UV) to a  $\sim 40 \mu\text{m}$  waist for second harmonic generation. This waist size is chosen so as to maximise intensity whilst maintaining the plane wave approximation within the Raleigh range of the beam.

Two different Type-I *eeo* SHG crystals were tested: bismuth triborate BiB<sub>3</sub>O<sub>6</sub> (BiBO) and  $\beta$ -barium borate (BBO). Whilst the former has a significantly higher nonlinearity — with conversion efficiencies reported into ultraviolet of 50% [147] — this high conversion efficiency comes at a cost. SHG via BiBO reduces the bandwidth of the UV beam, stretching the pulse and thus increasing the temporal jitter during SPDC [129]. Consequently, a reduction in off-pair dip visibility from

---

<sup>4</sup>We use this source over the wavelengths 780-808 nm dependent on the requirements of waveguide devices, but all components modulo filters and crystals are suitable across this range.

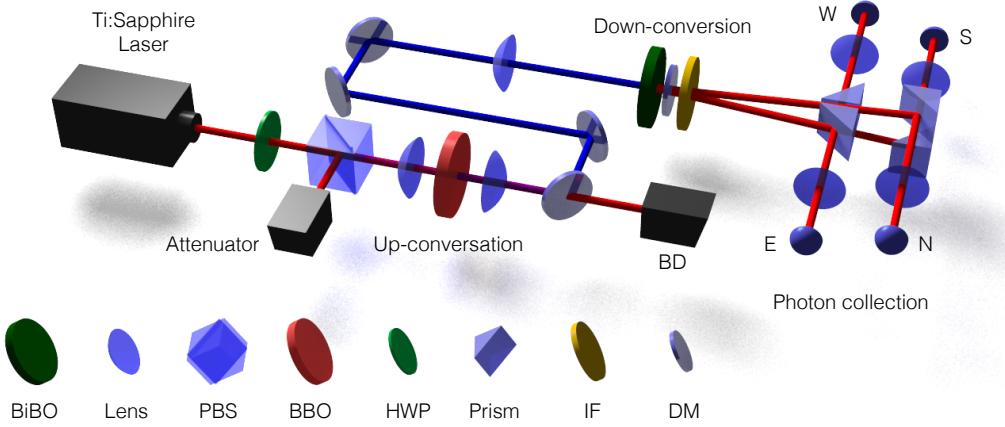


Figure 3.5: **Experimental multi-photon source.** Laser light at 800 nm is first attenuated, then up-converted to 400 nm via second harmonic generation. The up-converted beam is then focused onto a BiBO crystal to seed spontaneous parametric down-conversion. Four points of the down-conversion cone ( $N, S, E, W$  coordinates) are focused onto polarisation maintaining fibres, controlled by high precision fibre collection stages. Full details and abbreviations are given in the main text.

$V = 0.9$  using BBO, to  $V = 0.8$  for BiBO was observed. We therefore opt for the higher fidelity yet lower efficiency 2 mm thick BBO crystal for SHG (Newlight Photonics). In Figure 3.6 we plot a comparison of conversion efficiencies for BBO and BiBO.

Once up-converted to 400 nm, the unwanted 800 nm light is removed via a series of four dichroic mirrors (DM) and a beam dump (BD), then focused via a  $f = 0.2$  m lens to a  $\sim 40 \mu\text{m}$  waist to seed spontaneous parametric down-conversion. As discussed in Section 3.2.2 we opt for a 0.5 mm Type-I BiBO down-converter (Newlight Photonics), designed to emit photons at an opening angle  $\theta_{\text{op}} = 6^\circ$ . Two pairs of 800 nm down-converted photons ( $N, S, E, W$  as labelled in Fig. 3.5) pass through a single  $\Delta\lambda = 3$  nm interference filter (IF) (Semrock Maxline), and are reflected off prisms into four high-precision fibre collections stages (Elliot Martock MDE122). Each collection stage is equipped for XYZ translation, and full rotation control to a precision of 20 nm; along with a  $f = 11$  mm aspheric

### 3.3. EXPERIMENTAL MULTI-PHOTON SOURCE

---

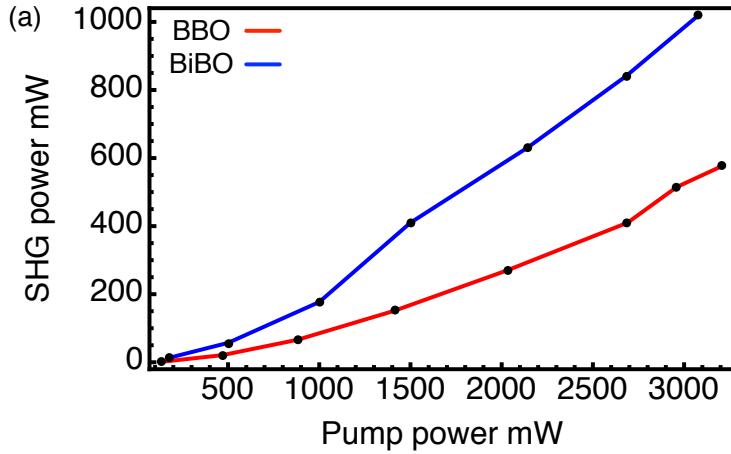


Figure 3.6: **SHG conversion efficiency.** A comparison of second harmonic generation conversion efficiency for both BBO (red) and BiBO (blue) up-conversion crystals.

lens (Thorlabs C220TME-B) to focus the photons into single mode polarisation maintaining fibres (PMF). Two of the four stages are equipped with motorised actuators for automated control of the path length during HOM-interference type experiments.

Down-converted photons are coupled as follows: Visible laser light is launched from the collection stages and focused onto the centre of the SPDC crystal at an angle of  $\sim \theta_{\text{op}}/2$ . Once all four stages are roughly aligned, the fibres are connected to single photon counting, and collection stages are coupled, optimising over coincidence count rates to insure correlated photon events.

#### 3.3.1 SOURCE PERFORMANCE

At maximum pump power we observe a  $p$ -photon count rate  $C_p$  of  $C_1 \approx 5 \times 10^5$  Hz,  $C_2 \approx 1 \times 10^5$  Hz and  $C_4 \approx 1 \times 10^2$  Hz; with a collection efficiency of  $C_2/C_1 \approx 20\%$ . We quote these numbers approximately because they can fluctuate between experiments based on a number of factors: lab conditions (temperature, humidity), laser conditions (wavelength and power fluctuations), crystal degradation. In general, higher quality results are obtained when losses are minimised and the source is as

### 3. PHOTONIC PROCESSING HARDWARE

---

efficient as possible; in this regime pump power can be reduced, limiting the effect of unwanted higher order terms.

Quantum interference is tested via a series HOM-interference experiments. We first test pair-wise interference by injecting photons  $\{E, W\}$  directly onto a fibre pigtailed  $\eta = 1/2$  beamsplitter. The temporal delay  $x$  is then varied and coincidences between output modes  $C_2(x)$  are recorded. These coincidence events are then numerically fitted to the function

$$C_2(x) = (c_1(x - c_2)^2 + c_3) \left[ 1 - V \exp\left(-\frac{(x - x_0)^2}{2\Delta x^2}\right) \operatorname{sinc}(s_1(x - x_0)) \right], \quad (3.26)$$

where  $c_i$  describes the nonlinear decoupling of the collection stage; and  $V, x_0, \Delta x$  the dip visibility, centre and width (i.e. coherence length of the photon) respectively. The sinc function described by  $s_1$  arises due to the Fourier transform of the top-hat spectral profile of the down-conversion crystal; and the function  $C_2(x)$  is related to convolution of this and the Gaussian profile of the filter (see reference [141] for an in-depth analysis). The results are plotted in Figure 3.7(a), where we find a pair dip visibility of  $V = 0.990 \pm 0.008$  (error taken as the error in parameter fit).

We then perform an off-pair dip whereby photons  $\{N, W\}$  are injected into either mode of the beamsplitter, and  $\{E, S\}$  provides the heralding signal. Collecting four-folds and fitting to (3.26) yields  $V = 0.902 \pm 0.01$ . From these fits we estimate the coherence length of the photons to be  $L_{\text{coh}} \approx 140 \mu\text{m}$ , which we note is significantly larger than the pulse width of the pump  $L_{\text{pump}} = c \times 140 \text{ fs} = 0.4 \mu\text{m}$ . Following the various analyses of dip visibility [146, 148] we determine group velocity mismatch and higher order photon number terms to be the major sources of reduction in off-pair dip visibility; with the finite pulse width and mode mismatch each contributing less than  $\sim 1\%$ .

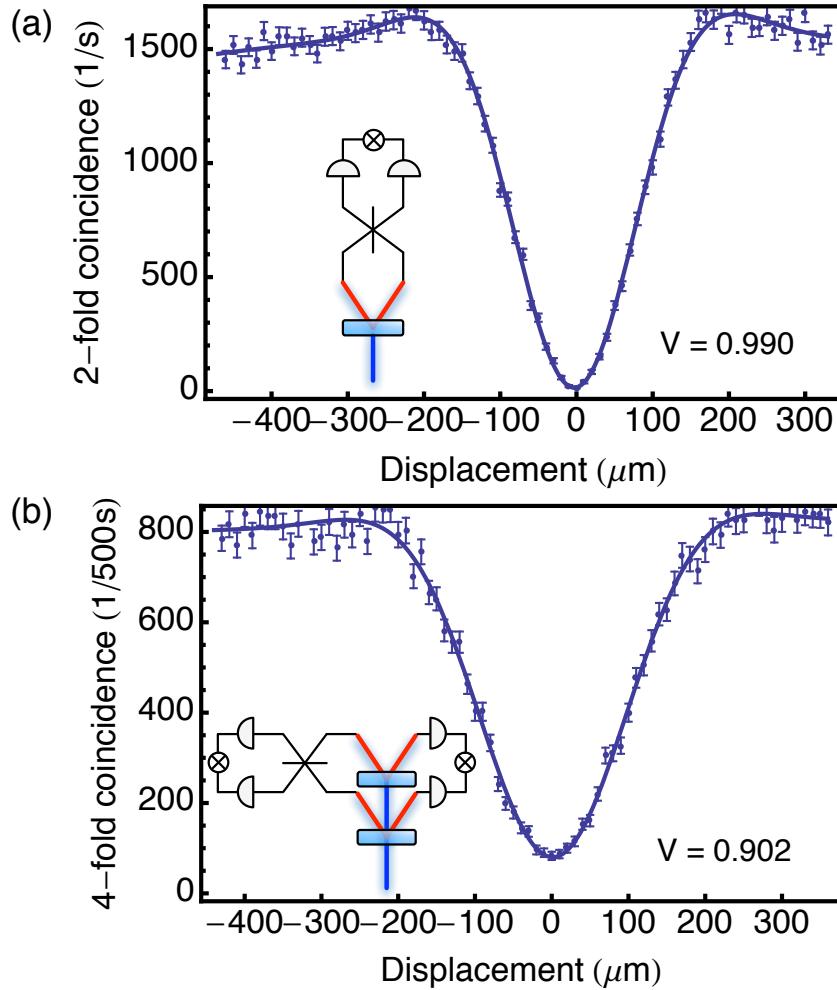


Figure 3.7: **HOM-interference dips.** (a) A pair dip between photons  $\{E, W\}$  (inset), plotting two-fold coincidence rate as a function of temporal distinguishability. (b) An off-pair dip between photons  $\{N, W\}$  whilst heralding on  $\{E, S\}$  (inset). Error bars assume Poissonian counting statistics.

## 3.4 INTEGRATED QUANTUM PHOTONICS

DiVincenzo’s first criterion for the physical implementation of a quantum computer states that any scalable platform for quantum computing must present:

*“A scalable physical system with well characterised qubits.”* [67]

This condition of scalability requires that the numbers of qubits encoded within the platform can be arbitrarily increased to within the error threshold of the chosen error correcting code.

Early demonstrations of LOQC relied upon polarisation encoded qubits due to their ease of manipulation at the single photon level via wave-plates [84]. However scaling this system to larger numbers of qubits requires complex bulk-optical interferometers stable to within the wavelength of light, and often taking up meters in length; limiting demonstrations to just a few qubits [119, 142, 149]. This constraint thus renders bulk optical LOQC unscalable.

A promising route towards scalability is the on-chip manipulation of light via *integrated photonics*. Driven by the microelectronic industries need for ever increased data rates [150], classical states of light are confined in nano-scale silicon-based waveguides [151], and manipulated via fast electro-optic modulators [152]. The silicon platform offers CMOS compatibility, intrinsic nonlinearities for frequency conversion or wavelength division multiplexing [153], and the use of commercial fabrication facilities. However, applying a technology designed for manipulating  $10^6$  photons per bit [154], to manipulating 1 photon per bit comes with a number of challenges; most notably, loss.

Until recently, it was an open question as to whether the tools of integrated photonics could be applied to the quantum regime. However, recent advances — including results presented in this thesis — provide tantalising evidence of the affirmative. Integrated *quantum* photonics has demonstrated high fidelity quantum interference [11, 17], proof of principle demonstrations of Shor’s algorithm [143], entanglement generation and manipulation [155], quantum chemistry simulations

### 3.4. INTEGRATED QUANTUM PHOTONICS

---

[156], quantum metrology [15, 157] and quantum key distribution [158, 159].

In the following we present an overview of the physics governing integrated quantum photonics. Whilst the exposition is in no way intended as an in-depth analysis; a qualitative understanding of the physics governing the platform will aid an understanding of the results presented within this thesis.

#### 3.4.1 PROPAGATION OF LIGHT

In the following we consider two pictures of the propagation of light through waveguide structures. The first, using just ray optics, provides an intuitive understanding of confinement and propagation modes, but provides no tools with which to describe waveguide coupling. The second, using electromagnetic fields, provides a fuller picture, allowing us to describe phenomena such as waveguide coupling; an essential ingredient for integrated quantum photonics. The analysis we present follows the exposition of Lifante [151] and is intended as a pedagogic tool. In practice waveguide structures, including those presented in this thesis, are modelled and designed using commercially available software.

##### RAY OPTICS PICTURE

A waveguide is an optical structure that allows the confinement of light within its boundaries via total internal reflection. Whilst the experiments presented in this thesis use channel waveguides, confining the light in two dimensions, for now we consider the simplified one dimensional picture of a ray propagating via a zig-zag path. In this picture [Fig. 3.8(a)] the waveguide consists of a core with refractive index  $n_1$  surrounded by a lower refractive index cladding  $n_2$ . The critical angle  $\theta_c$  is given by

$$\theta_c = \sin^{-1} \left( \frac{n_2}{n_1} \right), \quad (3.27)$$

and total internal reflection occurs when the angle of incidence  $\theta > \theta_c$ . If this condition is not met and  $\theta < \theta_c$  the light escapes into a radiation mode. Note, as  $n_2/n_1$  decreases  $\theta_c$  increases, thus an increased refractive index contrast allows for

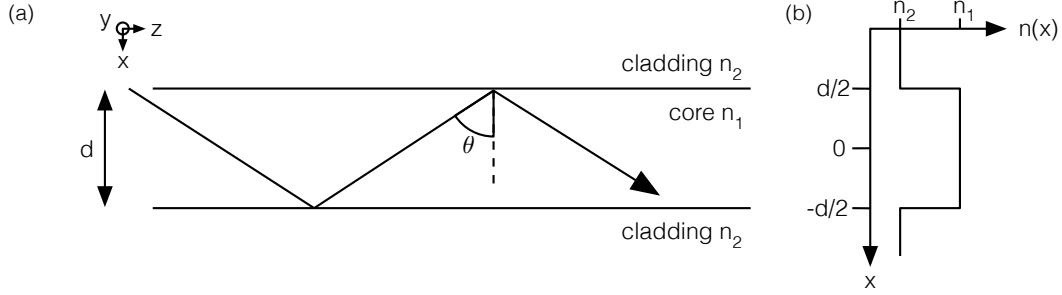


Figure 3.8: **Waveguide propagation.** (a) The ray optics picture of a light ray propagating through a waveguide with core refractive index  $n_1$ , surrounded by a cladding with lower refractive index  $n_2$ . (b) The refractive index profile.

a smaller bend radius and more compact devices.

A second propagation condition must also be met, that the ray *constructively interferes*. In a round trip through the core the light acquires a transversal [i.e.  $x$  direction in Fig. 3.8(a)] phase shift dependent on the core width  $d$ , and phase shifts due to reflection off the boundaries. The total phase shift is given by

$$\phi = 2k_x d - 2\phi_r \quad (3.28)$$

$$= 2k_o n_1 d \cos \theta - 2\phi_r \quad (3.29)$$

where  $k_x$  is the component of the wave vector along the  $x$ -axis and  $\phi_r$  is the phase acquired upon reflection off the core-cladding boundary. Constructive interference requires that the total transversal phase shift in a round trip should be an integer number of  $2\pi$ , hence we arrive at the transversal resonance condition for guided modes

$$2k_o n_1 d \cos \theta - 2\phi_r = 2\pi m \quad (3.30)$$

where  $m$  is the mode number, telling us that light is guided in discretised modes.

The ray optics picture provides the intuition for two important concepts; confinement of light and discretised propagation modes. However, it cannot account

### 3.4. INTEGRATED QUANTUM PHOTONICS

---

for a core functionality of integrated devices — waveguide coupling. To that end we not turn our attention to waveguide propagation in the picture of electromagnetic fields as described by Maxwells equations.

#### ELECTROMAGNETIC FIELDS

Maxwell's equations fully describe the evolution of classical electro-magnetic fields. For light propagating in a dielectric (conductivity  $\sigma = 0$ ) non-magnetic (magnetic permeability  $\mu = \mu_0$ ), isotropic and linear medium ( $\mathbf{D} = \epsilon\mathbf{E}$ ), they are

$$\nabla\mathbf{E} = 0; \quad \nabla \times \mathbf{E} = -\mu_0 \frac{\partial \mathbf{H}}{\partial t}; \quad (3.31)$$

$$\nabla\mathbf{H} = 0; \quad \nabla \times \mathbf{H} = \epsilon_0 n^2 \frac{\partial \mathbf{E}}{\partial t}; \quad (3.32)$$

where  $\mathbf{E}$  and  $\mathbf{H}$  represent the electric and magnetic fields respectively,  $\mu_0$  and  $\epsilon_0$  the permeability and permittivity of free space respectively, and  $n$  the refractive index of the medium. From these equations the following wave equations can be derived:

$$\nabla^2 \mathbf{E} - \epsilon_0 \mu_0 n(\mathbf{r})^2 \frac{\partial^2 \mathbf{E}}{\partial t^2} = 0, \quad (3.33)$$

$$\nabla^2 \mathbf{H} - \epsilon_0 \mu_0 n(\mathbf{r})^2 \frac{\partial^2 \mathbf{H}}{\partial t^2} = 0, \quad (3.34)$$

where  $n(\mathbf{r})$  is the position dependent refractive index profile. Considering the situation Fig 3.8(b), let us take  $n(\mathbf{r}) = n(x)$ ; solutions to (3.33) and (3.34) take the form

$$\mathbf{E}(\mathbf{r}, t) = \mathbf{E}(x) e^{i(\omega t - \beta z)} \quad (3.35)$$

$$\mathbf{H}(\mathbf{r}, t) = \mathbf{H}(x) e^{i(\omega t - \beta z)}, \quad (3.36)$$

where  $\omega$  is the frequency, and  $\beta$  the propagation constant of the wave. The aim is for a given  $n(x)$  to find solutions for the complex field amplitudes  $\mathbf{E}(x)$  and  $\mathbf{B}(x)$  according to Maxwells equations. There are two important regimes to consider: when the propagating light has electric field with only transversal component [i.e.  $y$  direction in Fig 3.8(a)] — the TE mode, and when the magnetic field has transversal component — the TM mode. In the following we consider the former.

### 3. PHOTONIC PROCESSING HARDWARE

---

By definition of the TE mode the only non-zero field components are  $E_y, H_x$  and  $H_z$ , using this fact, and substituting (3.35) and (3.36) into Maxwell's equations (3.31) yields

$$H_x = -\frac{\beta}{\omega\mu_0}E_y; \quad H_z = \frac{i}{\omega\mu_0}\frac{\partial E_y}{\partial x} \quad (3.37)$$

$$i\beta H_x + \frac{\partial H_z}{\partial x} = -i\omega\varepsilon_0 n^2(x)E_y. \quad (3.38)$$

Substituting equations (3.37) into (3.38) and noting the electric field only depends on  $x$  gives

$$\frac{d^2E_y(x)}{dx^2} + (k_0^2 n^2(x) - \beta^2) E_y(x) = 0, \quad (3.39)$$

$k_0$  is the wavenumber of the light in free-space. This differential equation fully describes the electric field amplitude  $E_y(x)$  for TE propagation.

Let us postulate solutions, for the  $j^{\text{th}}$  spatial region, of the form

$$E_j(x) = A_j e^{i\gamma_j x} + B_j e^{-i\gamma_j x} \quad (3.40)$$

where  $A_j, B_j$  will be determined given appropriate boundary conditions and  $\gamma_j = \sqrt{k_0^2 n_j^2 - \beta^2}$ , with  $n_j$  the refractive index of that region. Examining possible solutions we see that two distinct regions apply:

- If  $\beta < k_0 n_j$  then  $\gamma_j$  is real and (3.40) is a sinusoidal function, corresponding to a guiding mode.
- If  $\beta > k_0 n_j$  then  $\gamma_j$  is imaginary and (3.40) is an exponential function, corresponding to a radiative mode that does not guide.

Hence, for a given mode to guide through the waveguide the propagation constant  $\beta$  must fulfil

$$k_0 n_2 < \beta < k_0 n_1. \quad (3.41)$$

Writing wave equations for the core and cladding regions respectively gives

$$\begin{aligned} \frac{d^2E_y(x)}{dx^2} + \kappa^2 E_y(x) &= 0 && \text{if } -d/2 < x < d/2 \\ \frac{d^2E_y(x)}{dx^2} - \gamma^2 E_y(x) &= 0 && \text{if } x \leq -d/2, x \geq d/2 \end{aligned} \quad (3.42)$$

### 3.4. INTEGRATED QUANTUM PHOTONICS

---

where  $\kappa^2 \equiv k_0^2 n_2^2 - \beta^2$  and  $\gamma^2 \equiv \beta^2 - k_0^2 n_1^2$ . From (3.40) this yields solutions of the form

$$E_y = \begin{cases} Ae^{\gamma x} & x \leq -d/2 \\ Be^{i\kappa x} + Ce^{-i\kappa x} & -d/2 < x < d/2 \\ De^{-\gamma x} & x \geq d/2 \end{cases} \quad (3.43)$$

where  $A, B, C$ , are constants dependent upon the waveguide properties and the wavelength of light. This raises an important point not captured by the ray optics picture: Maxwell's equations allow for an exponentially decreasing *evanescent field* outside of the waveguide core, meaning fields can be coupled between waveguides — the governing principle behind directional couplers.

A final point: the waveguide properties  $(n_1, n_2, d)$ , the wavelength  $\lambda$  and the propagation constant  $\beta$  are related via the dispersion relation,

$$\tan(\kappa d) = \frac{2\gamma/\kappa}{1 - \gamma^2/\kappa^2} \quad (3.44)$$

and by noting the periodicity  $\tan(2\kappa d) = \tan(2\kappa d + m\pi)$ , a number of possible solutions satisfy the wave equation. If there is only one solution at  $m = 0$ , that is for a given  $\lambda$  and given waveguide geometry only a single  $\beta$  satisfies (3.44), we say the device is *single mode*. If however there are solutions for  $m > 0$  we say the device is multi-mode. Multiple modes offer extra degrees of freedom which can degrade quantum interference, so all devices presented in this thesis are designed for single-mode operation.

#### 3.4.2 COUPLED MODES

A key component for LOQC is a device which can split optical power between adjacent spatial modes. Using the theory of evanescently propagating waveguides detailed above, we now present a technique for coupling between modes: the *directional coupler*.

The modal coupling equations [151] for two coupled modes with optical field

### 3. PHOTONIC PROCESSING HARDWARE

---

amplitude  $A(z)$  and  $B(z)$  are given by the differential equations

$$\frac{dA(z)}{dz} = -i\kappa_{a,b}B(z)e^{-i(\beta_a-\beta_b)z}; \quad (3.45)$$

$$\frac{dB(z)}{dz} = -i\kappa_{a,b}A(z)e^{+i(\beta_a-\beta_b)z}; \quad (3.46)$$

where  $\kappa_{a,b}$  is the coupling coefficient between the modes  $a$  and  $b$ , and  $\beta$  is the coupling constant for those modes. The final term therefore represents mode-mismatch. Consider the special case whereby the modes are the spatial modes of two single-mode adjacent waveguides; simplifications can therefore be made by letting the propagation constants in modes  $a, b$  be equal ( $\beta_a = \beta_b$ ) and the coupling symmetric  $\kappa_{a,b} = \kappa_{b,a} = \kappa$ . Under these conditions (3.45) and (3.46) reduce to

$$\frac{dA(z)}{dz} = -i\kappa B(z) \quad (3.47)$$

$$\frac{dB(z)}{dz} = -i\kappa A(z). \quad (3.48)$$

It is straightforward to verify the solutions

$$A(z) = A_0 \cos(\kappa z) - iB_0 \sin(\kappa z) \quad (3.49)$$

$$B(z) = B_0 \cos(\kappa z) - iA_0 \sin(\kappa z), \quad (3.50)$$

where  $A_0$  and  $B_0$  are the initial field amplitudes in the respective modes. We consider this in the quantum mechanical picture by labelling modes  $\{A, B\} = \{|0\rangle, |1\rangle\}$ . Injecting a single photon into mode  $A$  (hence setting  $A_0 = 1$  and  $B_0 = 0$ ) yields the evolution  $|0\rangle \rightarrow \cos(\kappa z)|0\rangle - i \sin(\kappa z)|1\rangle$ , and similarly injecting into  $B$  yields  $|1\rangle \rightarrow -i \sin(\kappa z)|0\rangle + |1\rangle \cos(\kappa z)$ . By linearity the unitary operator governing this evolution is

$$\hat{U}(z) = \begin{bmatrix} \cos(\kappa z) & -i \sin(\kappa z) \\ -i \sin(\kappa z) & \cos(\kappa z) \end{bmatrix}, \quad (3.51)$$

which is equivalent to the variable coupler described in Section 2.6.3. In other words, by tuning the coupler length, or equivalently the separation distance, on-chip arbitrary reflectivity beamsplitters can be realised. Once again it is essential these modes are phase matched; imperfections in fabrication processes will lead to the possibility of higher order modes, and imperfect quantum interference.

### 3.4.3 MODULATION

The final functionality we desire is the ability to control, or modulate, light on chip. Fast modulation in silicon is a prerequisite for high speed optical interconnects [152]. Techniques using the Pockels effect or the Kerr effect, rely on the electro-optic properties of materials to induce phase shifts in the presence of an electromagnetic field; but are frustratingly weak in silicon. Other methods relying on plasma-dispersion-effects such as carrier depletion have demonstrated modulation speeds of up to 50 Gb/s [160], but come at the cost of increased loss (for example 7 dB (80%) insertion loss in reference [160]).

In this work — where clock-speeds are limited by multi-photon source rates — we use a much slower, yet lower loss phenomena: the thermo-optic effect. The thermo-optic effect arises from the the *molecular polarisability* of the material. To understand this, recall the argument from Section 3.2.2 where the relative permittivity  $\varepsilon_r$ , which captures the ease at which dipole moments are induced in a material

$$\mathbf{P} = \varepsilon_0(\varepsilon_r - 1)\mathbf{E}, \quad (3.52)$$

is directly linked to the refractive index  $n = \sqrt{\varepsilon_r}$ , and hence the refractive index is a measure of how easily dipole moments are induced.

As Born and Wolf note in their excellent exposition, the molecular polarisability  $\alpha$  provides a “*conceptual bridge which connects Maxwell’s phenomenological theory with the atomistic theory of matter*” [83]. It describes the induced dipole moment due to a single molecule

$$\mathbf{P} = N\varepsilon_0\alpha\mathbf{E}, \quad (3.53)$$

where  $\mathbf{P}$  is the polarisability per unit volume and  $N$  the number of molecules per unit volume. As before, this quantity can be related to the refractive index via the Lorentz–Lorenz equation<sup>5</sup>

$$\frac{n^2 - 1}{n^2 + 2} = \frac{4\pi}{3}N\alpha. \quad (3.54)$$

<sup>5</sup>In a remarkable coincidence, two physicists with almost exactly the same names, independently discovered the same effect at almost exactly the same time.

Now, the molecular polarisability is a function of temperature [161]. Why? Well increasing the temperature increases the energy of the molecule which increases the internuclear distance between the electrons and the nucleus (recall the canonical Leonard-Jones potential). This distance is what determines the dipole moment, and hence the polarisability, therefore *the refractive index is temperature dependent*. A similar argument solving the equations of motion for the orbiting electrons, tells us the internuclear distance is also a function of the frequency of electromagnetic field, giving rise to dispersion [83].

Experimentally, the quantity which captures the magnitude of this temperature dependence is the thermo-optic coefficient  $dn/dT$  which for the universal LPU presented in Chapter 6 is  $1 \times 10^{-5} \text{ }^{\circ}\text{C}^{-1}$ . Finally we note, that whilst the thermo-optic effect is strong in silicon based devices at room temperature, it drops by four order of magnitude at cryogenic temperatures [162]. Thus, if devices are to be used at working temperatures for superconducting detectors (see Section 3.6), alternatives to thermo-optic modulation must be sought.

### 3.5 EXPERIMENTAL PLATFORMS

Many different material systems, waveguide geometries and fabrication techniques exist, each with their relative merits and drawbacks. A decision to adopt a particular platform should be made based on the users requirements<sup>6</sup>. For commercial applications, considerations such as compactness, modulation speed, ease of fabrication and cost play an important role. For our purpose, waveguide circuits will mainly be interfaced with the multi-photon source described in Section 3.3; as the probability of seeing a  $p$ -fold event in the presence of loss  $l$  scales as  $(1 - l)^p$  a key requirement is *low loss circuitry*. Typically, this comes at the cost of compactness [164].

Three material platforms are used within this thesis: silica, silicon oxynitride

---

<sup>6</sup>We note a recent promising proposal whereby multiple materials are monolithically integrated onto a single circuit [137, 163].

### **3.5. EXPERIMENTAL PLATFORMS**

---

and silicon nitride. In the following we introduce these platforms, presenting device details such as waveguide geometries and fabrication methods, along with a discussion of their relative merits and drawbacks — the results of which are collected in Table 3.1. Whilst modelling and fabrication work was mostly done external to Bristol, platform details dictate experimental procedures, and certain limitations of the platform only become apparent when used within the full LPU — so a knowledge of the device is essential to correct and minimise errors.

#### **3.5.1 SILICA**

In Chapter 6 we report an active silica-based fully reconfigurable waveguide device across six modes (labeled Device A in Table 3.1). The chip was conceived in Bristol and designed, fabricated and packaged by collaborators at the Nippon Telegraph and Telephone company (NTT) in Japan. The device was then tested, calibrated and used for quantum information processing in Bristol.

Integrated silica ( $\text{SiO}_2$ ) based components are highly desirable due to their compatibility with commercial fibre optic network systems, and low loss nature. Typical fibre optic cables consist of a silica cladding, with a slightly higher refractive index silica-doped core of about  $8 \mu\text{m}$  in diameter, and can achieve losses of  $0.2 \text{ dB/km}$  at  $1550 \text{ nm}$  [165].

Due to these favourable low loss properties, the first integrated quantum photonic demonstrations were performed on the silica platform; including high fidelity quantum interference with passive quantum gates [11], proof of principle algorithms [143], active Mach-Zehnder interferometers [15] and reconfigurable two qubit gates [155]. Our universal processor represents the natural evolution of this genesis.

Our silica-based planar lightwave circuit (PLC) [166] was fabricated by first depositing a layer of silica, then germanium doped silica ( $\text{SiO}_2\text{-GeO}_2$ ) onto a silicon substrate via flame hydrolysis deposition to give a core cross sectional dimension of  $3.5 \mu\text{m} \times 3.5 \mu\text{m}$ . The substrate and glass layers are then heated to  $1000^\circ\text{C}$

for consolidation, and waveguides are then patterned via photolithographic and reactive ion etching techniques. Finally the silica over-cladding is then deposited and consolidated, and thin-film Tantalum Nitride ( $Ta_2N$ ) thermo-optic heaters fabricated on top of the circuit measuring  $1.5\text{mm} \times 50\mu\text{m}$ . See reference [167] for further fabrication details.

The core-cladding refractive index contrast

$$\Delta = \frac{n_{\text{core}}^2 - n_{\text{cladding}}^2}{2n_{\text{core}}^2} \quad (3.55)$$

was designed to be  $\Delta = 0.45\%$  at our working wavelength (808nm) giving a minimum bend radius of 12 mm. For the purpose of interfacing with the multi-photon source in Section 3.3, a highly desirable property is low insertion and propagation losses. The large core size means the waveguide is well matched to  $4\ \mu\text{m}$  diameter single mode fibres used for in- and out-coupling, giving insertion losses  $0.4\text{dB/facet}$  (9%). Whilst measurements of propagation loss at 800 nm haven't been made, at telecom wavelengths  $0.3\ \text{dB/m}$  has been reported [168]. Directional couplers are designed to have a length of  $500\mu\text{m}$  and a waveguide gap of  $2\mu\text{m}$ , with each directional couplers loss estimated to be less than  $0.1\ \text{dB}$  (2.3%). The mean insertion loss (fibre to fibre) averaged over all modes (including 30 directional couplers) is measured as  $2.4\ \text{dB}$  (42%).

### 3.5.2 SILICON OXYNITRIDE

In Chapter 5 we report a 21-mode array of continuously evanescently coupled waveguides (Device B). The complexity of this system requires a significantly more compact architecture than silica-based devices can offer. Consequently we opt for the core material silicon oxynitride ( $\text{SiO}_x\text{N}_y$ ), whose refractive index can be tuned by carefully varying the ratio of silicon to nitrogen during the plasma-enhanced chemical-vapor-deposition process. The device was fabricated by collaborators at the University of Twente [169, 170].

The waveguide array was fabricated with a silicon oxynitride core surrounded by a silca cladding. The index contrast of  $\Delta = 2.4\%$  enables fabrication of micron

### **3.5. EXPERIMENTAL PLATFORMS**

---

sized single mode waveguides in compact circuit designs with a minimum bend radius of  $560\ \mu\text{m}$ . The waveguides are designed with a constant width of  $2.2\ \mu\text{m}$  and height of  $0.85\ \mu\text{m}$ . They are pitched at  $1.3\ \mu\text{m}$  within the coupling region of length  $700\ \mu\text{m}$  in order to achieve sufficient mode overlap for nearest neighbour coupling. The waveguides bend adiabatically to a pitch of  $127\ \mu\text{m}$  at the input and output facets to match the standard separation of the fibre arrays we butt couple to the chip. The waveguides are tapered to a width  $0.7\ \mu\text{m}$  at the facet to achieve better mode overlap with the fibre modes, this way we obtain an overall fibre to fibre coupling efficiency of  $\sim 30\%$ . Similar silicon oxynitride continuously coupled waveguide devices have been used to demonstrate two photon quantum walks [18], simulate fermion particle statistics [171], and observe the coherent time evolution of walkers [172].

#### **3.5.3 SILICON NITRIDE**

In Chapter 5 we present a passive waveguide device fabricated in stoichiometric silicon nitride  $\text{Si}_2\text{N}_3$  (Device C). The device was conceived in Bristol and designed and fabricated by the company LioniX.

Silicon nitride has a significantly higher refractive index contrast with silica than both silica-doped and silicon oxynitride cores, with  $\Delta \approx 25\%$ . As loss due to sidewall roughness scales as  $\Delta^2$  [164] the high refractive index contrast may limit the interfacing of silicon nitride with bulk-multi photon sources. Techniques have been developed to reduce this effect by employing high aspect ratio waveguide geometries where the width ( $\sim 3\ \mu\text{m}$ ) far exceeds the thickness ( $\sim 90\ \text{nm}$ ), yielding losses of  $3\ \text{dB/m}$  [173]; however this asymmetric core results in heavily birefringent behaviour, and requires low loss spot converters for matching with single mode fibres.

Our silicon nitride system was designed with a refractive index contrast of  $\Delta = 27\%$  at our working wavelength  $780\ \text{nm}$ , with a waveguide width of  $1.5\ \mu\text{m}$ . Outside the interaction region waveguides are separated by  $127\ \mu\text{m}$  and to realise

Device	A	B	C	D
Material	$\text{SiO}_2$	$\text{SiO}_x\text{N}_y$	$\text{Si}_2\text{N}_3$	$\text{Si}_2\text{N}_3$
Circuit	Active	CCWA	Active	Passive
Footprint	$4\text{cm} \times 10\text{cm}$	$2.7\text{mm} \times 75\text{mm}$	$1.0\text{mm} \times 31\text{mm}$	$1.1\text{mm} \times 31\text{mm}$
Core size	$3.5\mu\text{m} \times 3.5\mu\text{m}$	$2.2\mu\text{m} \times 0.85\mu\text{m}$	$1.5\mu\text{m} \times 0.1\mu\text{m}$	$1.5\mu\text{m} \times 0.1\mu\text{m}$
$\lambda$	808nm	780nm	780nm	780nm
$\Delta$	0.45%	2.4%	27%	27%
Bend radius	12mm	$560\mu\text{m}$	$200\mu\text{m}$	$200\mu\text{m}$
DC length	$500\mu\text{m}$	$700\mu\text{m}$	$400\mu\text{m}$	$400\mu\text{m}$
Transmission	58%	30%	7%	5%

Table 3.1: **Comparison of waveguide platforms.** A comparison of different waveguide platforms (labels given in main text) consisting both active and passive waveguide devices, and continuously coupled waveguide arrays (CCWA). Comparison includes core size (given as  $w \times h$ ), operating wavelength  $\lambda$ , refractive index contrast  $\Delta$ , directional coupler (DC) length, and facet-to-facet transmission.

directional couplers waveguides are brought to within  $2.5 \mu\text{m}$  of one another, for an interaction length of  $\sim 400 \mu\text{m}$  (dependent on the desired splitting ratio). The fibre to fibre coupling efficiency was  $\sim 5\%$ .

On the same fabrication run we also received an active waveguide device comprising 24 directional couplers and 19 active phase shifters. During characterisation it became apparent losses were prohibitively high due to an error in the spot size convertor. Whilst we don't present quantum information processing results using this device, we do include it in Table 3.1 for comparison (Device D).

### 3.5.4 INTERFACING

We have so far presented the individual components which comprise LPU's, but we further require they can be efficiently interfaced with one another. To that end, we now describe two methods with which to couple and control single photons

### **3.5. EXPERIMENTAL PLATFORMS**

---

on-chip for both passive and active circuitry.

#### **PASSIVE INTERFACING**

For passive waveguide circuits we are typically interested in having the flexibility in rapidly testing multiple devices, whilst maintaining experimental stability over long data runs. To this end we have designed a stable yet temporary optical coupling rig whereby single-mode polarisation maintaining V-Groove fibre arrays ( $127\ \mu\text{m}$  pitch) are butt-coupled to the waveguide devices via high precision fibre optic launch stages (Elliot Martock MDE122, MDE185) to give full XYZ and roll-pitch-yaw control. The resolution of the coupling rig is  $\sim 20\ \text{nm}$ , well within the range of the  $4\ \mu\text{m}$  fibre core size. Index matching oil with the same refractive index as the silica core is placed between the chip facet and fibre array to enhance coupling. Waveguide devices can be coupled in less than an hour and remain stable for several weeks.

#### **ACTIVE INTERFACING**

The requirements for interfacing thermo-optically controlled active devices is markedly different. Much like in a computer, a single device will be used many times; in that case it will be beneficial to optically and electrically package the device. This process prevents decoupling due to thermal expansion, making the device incredibly stable and robust thus reducing experimental noise.

Both active devices were optically and electrically packaged using essentially the same processes; the silica device was externally packaged at NTT, whilst the silicon nitride device was packaged in-house. Whilst the latter ultimately wasn't used for quantum information processing, we describe the packaging process here to highlight an example of a possible packaging technique.

The silicon nitride device was first mounted onto a copper based printed circuit board (PCB) via a thermally conducting epoxy then wire-bonded for electrical interfacing. Glass based V-Groove fibre arrays were then coupled to the chip using an ultra high precision (1 nm resolution) piezo controlled fibre launch system

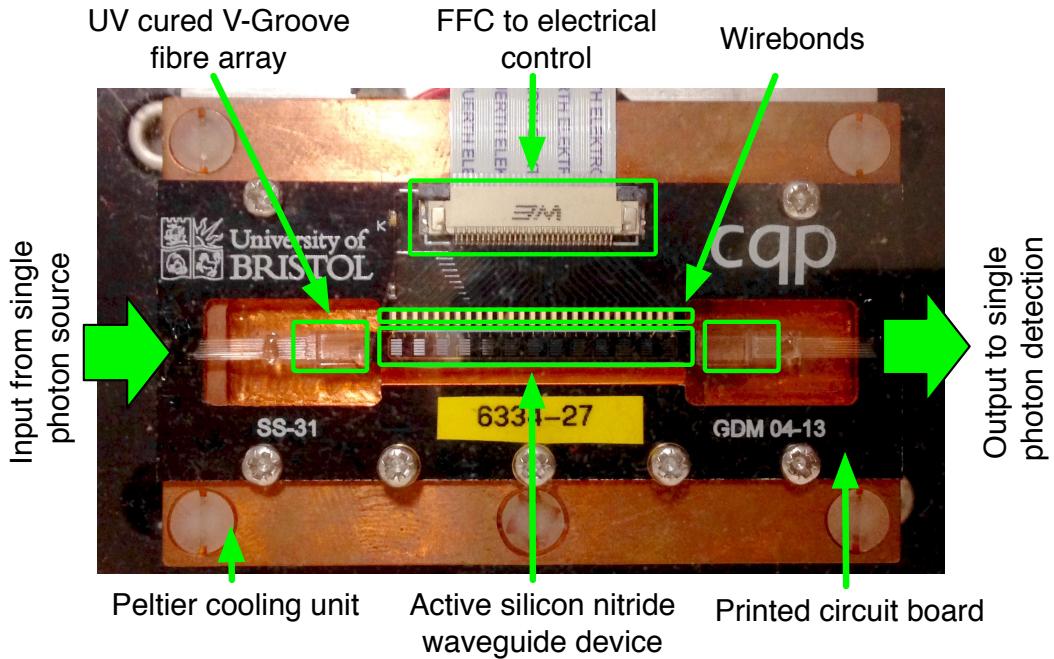


Figure 3.9: **A packaged reconfigurable waveguide device.** Reconfigurable waveguide device, optically and electrically packaged for interfacing with single photon source, single photon counting and electrical control. See main text for details.

(Thorlabs NanoMax), and attached to the chip facet via ultraviolet curing epoxy adhesive. This entire device is then fixed to a Peltier cooling unit which is actively temperature stabilised by a thermoelectric cooler (Arroyo Instruments 5240 TECSource) to ambient lab temperature ( $20^{\circ}\text{C}$ ).

We developed a custom electronic circuit to deliver power to each of the on-chip heaters independently. This circuit consisted of four sets of the following: one micro-controller for communication, arithmetic, and measurement; eight 12-bit digital-to-analogue converters; eight high-power non-inverting drive amplifiers; eight current-measurement amplifiers; and eight 12-bit analogue-to-digital converters for reading out the current sourced to each heater. Each of the 32 drive ports delivered up to 20 V, with 4.9 mV resolution, and could source up to 100 mA of current, with a measurement resolution of 24  $\mu\text{A}$ .

## 3.6 SINGLE PHOTON DETECTION

The detection of single photons has broad application in science; from biological imaging [174], to astronomy [175], to long distance sensing [176]. In the context of LOQC, single photon detection is the means with which the qubit state is readout (see Section 2.5.2 and DiVincenzo’s fifth criterion), so it is crucial we have high fidelity techniques for converting a single quanta of energy  $\sim 10^{-19}$  J to an electrically detectable macroscopic state of  $\sim 10^6$  electrons. In general this requires a high gain, low noise medium.

There are a number of desirable properties for a single photon detector. It should have *high efficiency*, so given that the presence of a single photon, the probability of registering the event is high. It should have *low dark count rates*, whereby the probability of a false detection is small. There should be *low jitter*, where the time uncertainty between absorbing the photon and emitting a signal is small. Finally it should have *quick reset time*. Perhaps unsurprisingly, it is a significant challenge fulfilling all of these criteria.

In particular for LOQC, one of the biggest challenges is computing in the presence of loss. Error correcting techniques have shown loss of up to 50% can be tolerated in the absence of qubit errors [177], whilst loss of 10% can be tolerated with moderate error levels ( $p_{\text{error}} = 0.3\%$ ) [178]. Therefore high efficiency detectors are essential for scalable LOQC. A promising approach are superconducting nanowire single photon detectors (SNSPD’s) which have demonstrated high efficiencies (93%), low dark counts ( $\sim 1$  Hz), low timing jitter ( $\sim 150$  ps), and quick reset time ( $\sim 40$  ns) [179]. Moreover these detectors can readily be integrated [21] making them free of the loss associated with coupling light off chip.

Whilst SNSPD’s are a promising approach, they are still very much a nascent technology, and not available on the scale we require. For our purpose we are interested in accessing large Hilbert spaces, with a view to pushing the limits of what’s simulatable with classical systems. To that end we require many detectors  $n = 16$ , at a relatively low cost, with high efficiency at our working wavelength

---

### 3. PHOTONIC PROCESSING HARDWARE

(800 nm). These conditions are met by commercially available silicon avalanche photodiodes.

#### 3.6.1 EXPERIMENTAL SINGLE PHOTON COUNTING

For experiments presented in this thesis we use an array of 16 silicon avalanche photodiodes (SPADS), with time-correlated single photon counting (TCSPC) capability. The detectors (Perkin Elmer SPCM-AQRH-14) have efficiency of  $\sim 60\%$ , dark count rate of  $\sim 100$  Hz, timing jitter of  $\sim 350$  ps and a reset time of 32 ns.

Using such a large number of detectors in the multi-photon regime presents a number of challenges. First, individual SPAD's can typically have a large variation in electronic delay (up to 10 ns). When looking for *correlated detection events* (i.e. when multiple photons arrive simultaneously at detectors), these delays must be carefully characterised and corrected for. Second, the photon source is clocked at the repetition rate of the pulsed laser (80 MHz), which means we must have full control of the coincidence window — the maximum time between which two detection events are considered a coincidence.

Both these challenges can be overcome in hardware using electrical delays lines and FPGA counting logic, however this is often cumbersome. For this work we have developed a 16-channel TCSPC module, which ‘time-tags’ all possible  $(^{16}_p)$   $p$ -fold coincidence events in realtime. As all events are recorded to within 80 ps accuracy, delays and coincidence windows can be implemented in software. Delays are found using a custom built auto-correlation software, and the coincidence window is set to 3 ns — above the jitter of detectors (so we don’t miss coincidences) and below the 12.5 ns clock rate of the pulsed laser system (so we don’t mistake non-coincidences as coincidences). For a full description of the detection system — the ‘Hilbert space telescope’ — see the thesis of P. J. Shadbolt [180].

## **3.7 CONCLUDING REMARKS**

We have demonstrated key core components for the LPU's presented later in this thesis, along with the underlying physics governing their operation. This deeper understanding is indispensable: First, it provides methods with which to identify and rectify errors. For example, a decrease in multi-photon source performance may give rise to a particular pattern of errors in some quantum information processing task. An intimate knowledge of the source, its limitations (such as experimental instability, crystal degradation etc.) and the manifestation of these errors can allow this problem to be rapidly diagnosed, and ultimately fixed.

Second, the lessons we learn about the limitations of our current systems will feed into the design of next generation LPU's. For example, understanding the particular mechanisms by which a waveguide can introduce distinguishability, and its affect upon computation, will allow this affect to be minimised in future designs. This broad approach of precisely understanding the individual components will be crucial for any quantum technology, not least the ultimate photonic goal of a monolithically integrated LPU.

---

### 3. PHOTONIC PROCESSING HARDWARE

# 4

## Hardware Characterisation

### STATEMENT OF WORK

The original super-stable tomography protocol is due to A. Laing. All proposed extensions, numerical analysis, experimental implementations and subsequent data analysis are due to myself.

#### 4.1 INTRODUCTION

Understanding the real life processes which govern the evolution of quantum systems is a prerequisite for any scalable quantum technology. In principle the omniscient experimentalist who knows all parameters in her setup can use Schrödinger's equation to deterministically predict the evolution of the system. In reality this

is never the case. Experimental devices cannot be made with infinite precision, meaning the experimentalist never has full knowledge about her device.

General protocols for fully characterising an unknown quantum process have been well studied [84, 181] and implemented in a variety of physical systems (for example trapped ions [182], superconducting qubits [183], nitrogen-vacancy centres [184] and linear optics [185]), but due to the exponential number of parameters required to describe a process, rapidly become impractical as systems scale up. A further concern with using methods like quantum process tomography to accurately determine a device error  $\epsilon$ , is that you are ultimately limited by the precision of your preparation and measurement device  $\epsilon'$ . If  $\epsilon < \epsilon'$  (a SPaM error),  $\epsilon$  becomes inaccessible.

A more practical approach — and one which we opt for here — is to characterise a specific quantum device, with known properties. By making well informed assumptions about the system, the size of the characterisation problem can be significantly reduced. This ‘hardware level’ characterisation can detect specific device errors which can either be corrected for *in situ*, fed into future device designs, or be accounted for at an error correcting code level (see for example loss tolerant error correction schemes suitable for linear optical quantum computing (LOQC) [178]).

In this chapter we investigate a hardware characterisation technique designed for LOQC — super-stable tomography (SST) — and propose a series of practical, and experimentally motivated extensions. In Section 4.2 we review the original SST protocol, and in Section 4.3 implement it by characterising a nine-mode waveguide device; noting that such a reconstruction via traditional methods would have been completely infeasible. We then extend this technique in Section 4.4; making it quick, robust and practical, and demonstrate its efficacy on a 21 mode array of continuously coupled waveguides in Section 4.5. Finally, in Section 4.6, a full numerical error analysis of these techniques is performed, and based on these results, in Section 4.7, we propose an error corrected reconstruction protocol, demonstrating a 20% advantage in reconstruction fidelity through numerical experiments.

## 4.2 SUPER-STABLE TOMOGRAPHY

Lossless linear optical circuits are described by  $m \times m$  unitary matrices  $\hat{U} \in \mathbb{C}^{m \times m}$  relating input and output probability amplitudes (see Section 2.6.1). The number of parameters describing this  $m$ -mode system grows as  $\mathcal{O}(m^2)$  and can therefore be efficiently accessed. Protocols exist for determining  $\hat{U}$  using coherent states of light and interferometric measurements [186], yet demands for stability on the scale of the wavelength of light, in-practice, render this method as troublesome. Moreover, waveguides devices are dispersive; that is the refractive index and thus the properties of directional couplers and phase shifters are a function of the wavelength of incident light. Therefore, *the unitary* depends on the wavelength of incident light. Using a light source to characterise a device which does not have precisely the same spectral properties as the photons with which you ultimately hope to compute with, may result in an erroneous reconstruction. We therefore opt for a technique which circumvents both these challenges.

Super-stable tomography (SST) due to Laing and O'Brien [187], uses single photons and two-photon measurements (along with correlated photon detection) to efficiently determine  $\hat{U}$ . The advantages of this approach is that it requires interferometric stability on the order of the coherence length of the photons (which can be increased arbitrarily), such that systematic state preparation and measurement errors are minimised. Additionally, it uses the same resources for both characterisation and operation.

A schematic of the SST protocol is depicted in Fig. 4.1. The key result of SST is the existence a one-to-one (i.e. bijective) mapping between all single photon and a subset of two-photon measurements and the transfer matrix describing the circuit. In other words, a linear optical circuit is uniquely defined by all  $1 \times 1$  and a subset of  $2 \times 2$  permanents. A practical advantage of the scheme is that it reconstructs a unitary description of the circuit independent of input and output losses. This is important as coupling efficiencies in and out of integrated chips and single photon detection efficiencies are the dominant source of loss.

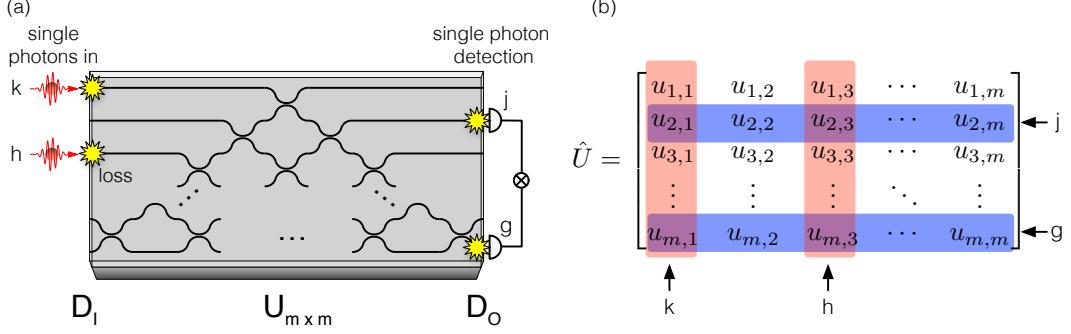


Figure 4.1: **The SST protocol.** (a) Single photons input in modes  $\{k, h\}$  and detected in modes  $\{j, g\}$  can be used to reconstruct the unitary matrix  $\hat{U}$  independent of input and output losses  $\hat{D}_I$  and  $\hat{D}_O$ . (b) Input modes  $\{k, h\}$  select columns of  $\hat{U}$  while output modes  $\{j, g\}$  select rows.

#### 4.2.1 SST PROTOCOL

Here we review the SST protocol. We begin by decomposing the transfer matrix into  $\hat{D}_O \cdot \hat{U} \cdot \hat{D}_I$ , where  $\hat{D}_I$  and  $\hat{D}_O$  are diagonal matrices corresponding to the losses at the inputs and outputs respectively and  $\hat{U} \in \tau_{j,k} e^{i\alpha_{j,k}}$  is the unitary to be determined. To reconstruct the amplitudes  $\tau$ , a series of experiments are performed whereby single photons are input into mode  $k$  and the count rate  $R_{j,k}$  is measured for each output mode  $j$  (see Figure 4.1 for details of the labelling convention).

Using the relation

$$x_{g,h,j,k} = \frac{\tau_{j,k} \tau_{g,h}}{\tau_{j,h} \tau_{g,k}} = \sqrt{\frac{R_{j,k} R_{g,h}}{R_{j,h} R_{g,k}}}, \quad (4.1)$$

so  $x_{g,h,j,k}$  is a value which can be experimentally determined. Then considering

$$\tau_{g,h} = \frac{\tau_{j,h} \tau_{g,k}}{\tau_{j,k}} \times x_{g,h,j,k}, \quad (4.2)$$

and fixing  $j, k = 1$ , each amplitude can be written as a function of the elements on the border of the matrix.

The phases  $\alpha$  are determined using the rates of coincident detection of two photons input in modes  $\{k, h\}$  and detected in modes  $\{j, g\}$  (see Fig 4.1). The visibility of a two photon detection pattern is given by  $V \equiv \frac{C-Q}{C}$  where  $C$  is the

## 4.2. SUPER-STABLE TOMOGRAPHY

---

probability of coincidental detection for distinguishable particles (achieved by deliberately introducing a temporal delay between photons) and  $Q$  is the probability of coincidental detection for indistinguishable particles. Defining

$$y_{g,h,j,k} \equiv x_{g,h,j,k} + x_{g,h,j,k}^{-1}, \quad (4.3)$$

the relation

$$\alpha_{j,k} - \alpha_{j,h} - \alpha_{g,k} + \alpha_{g,h} = \arccos\left(-\frac{1}{2}V_{g,h,j,k} y_{g,h,j,k}\right) \quad (4.4)$$

is used to calculate the magnitude of the phases. Note, for a realistic photon source, quantum interference is typically non-ideal. In this case a correction can be applied to (4.4) by calculating  $V = V_m/V_s$  where  $V_m$  is the measured visibility through the device and  $V_s$  the raw (non-ideal) visibility from the source.

Since input and output phases cannot be detected without further interferometry, all border element phases  $\alpha_{1,k}, \alpha_{j,1} = 0$ . Therefore, by setting  $j, k = 1$  there is only one unknown on the left of (4.4) and the magnitude of all phases is determined. To determine the signs of the phases, first note that since the statistics of the unitary are equivalent up to a global phase,  $\alpha_{2,2}$  can be defined to be positive. Using

$$\cos(\alpha_{j,k} - \alpha_{j,h} - \alpha_{g,k} + \alpha_{g,h}) = -\frac{1}{2}V_{g,h,j,k} y_{g,h,j,k} \quad (4.5)$$

to solve for the sign  $\alpha_{g,h}$ , device ports are judiciously chosen such that the other three phases are known, let us call their sum  $\gamma$ . Further more, the right hand side of (4.5) is also known, let us call it  $X$ . The task is therefore

$$\cos(\gamma \pm |\alpha_{g,h}|) \stackrel{?}{=} X, \quad (4.6)$$

Which can be done by computing

$$\text{sgn}[|\cos(\gamma - \alpha_{g,h}) - X| - |\cos(\gamma + \alpha_{g,h}) - X|]. \quad (4.7)$$

To find the signs of the second column, set  $j = 2, k = 1, h = 2$  and  $g = [3, m]$ . Signs on the second row are found by setting  $j = 1, k = 2, g = 2$  and  $h = [3, m]$ . The remainder are found by setting  $j, k = 2$ . The border amplitudes can now

be found by solving a system of linear equations which enforce orthonormality constraints.

Due to inevitable experimental noise, the reconstructed matrix  $\hat{M}$  will in general not be unitary (note that not all orthonormality constraints were applied). To find the unitary matrix closest to  $\hat{M}$ , a polar decomposition can be performed. Defining

$$\hat{P} = \sqrt{\hat{M}^\dagger \cdot \hat{M}}, \quad (4.8)$$

then the nearest unitary to  $M$  is given by

$$\hat{U} = \hat{M} \cdot \hat{P}^{-1}, \quad (4.9)$$

completing the reconstruction procedure.

### 4.2.2 A WORKED EXAMPLE

For clarity we present a worked example. We first generate an  $m = 4$  mode random unitary

$$\hat{U} = \begin{pmatrix} 0.432 & 0.721 & 0.351 & 0.413 \\ 0.376 & 0.225 - 0.19i & -0.782 + 0.381i & -0.121 + 0.007i \\ 0.245 & -0.473 - 0.151i & -0.159 - 0.147i & 0.704 + 0.389i \\ 0.782 & -0.358 + 0.138i & 0.232 - 0.137i & -0.39 - 0.125i \end{pmatrix}, \quad (4.10)$$

along with the following randomly generated loss matrices

$$\hat{D}_I = \begin{pmatrix} 0.949 & 0. & 0. & 0. \\ 0. & 0.868 & 0. & 0. \\ 0. & 0. & 0.445 & 0. \\ 0. & 0. & 0. & 0.192 \end{pmatrix}; \quad \hat{D}_O = \begin{pmatrix} 0.312 & 0. & 0. & 0. \\ 0. & 0.808 & 0. & 0. \\ 0. & 0. & 0.873 & 0. \\ 0. & 0. & 0. & 0.163 \end{pmatrix}. \quad (4.11)$$

Single photon measurements give a matrix

$$R = \begin{pmatrix} 0.016 & 0.038 & 0.002 & 0.001 \\ 0.083 & 0.043 & 0.098 & 0.0004 \\ 0.041 & 0.142 & 0.007 & 0.018 \\ 0.015 & 0.003 & 0.0004 & 0.0002 \end{pmatrix}, \quad (4.12)$$

## 4.2. SUPER-STABLE TOMOGRAPHY

---

which using (4.1) and (4.2) and setting  $j, k = 1$  gives

$$\Gamma = \begin{pmatrix} \tau_{11} & \tau_{12} & \tau_{13} & \tau_{14} \\ \tau_{21} & \frac{0.470\tau_{12}\tau_{21}}{\tau_{11}} & \frac{2.857\tau_{13}\tau_{21}}{\tau_{11}} & \frac{0.338\tau_{14}\tau_{21}}{\tau_{11}} \\ \tau_{31} & \frac{1.217\tau_{12}\tau_{31}}{\tau_{11}} & \frac{1.09178\tau_{13}\tau_{31}}{\tau_{11}} & \frac{3.436\tau_{14}\tau_{31}}{\tau_{11}} \\ \tau_{41} & \frac{0.295\tau_{12}\tau_{41}}{\tau_{11}} & \frac{0.425\tau_{13}\tau_{41}}{\tau_{11}} & \frac{0.548\tau_{14}\tau_{41}}{\tau_{11}} \end{pmatrix}, \quad (4.13)$$

thus all amplitude elements are functions of unknown boarder elements. Next we solve for phase magnitudes. Defining boarder elements to be 0, making two photon quantum interference measurements with  $j, k = 1$  and using (4.4) yields

$$|\Phi| = \begin{pmatrix} 0. & 0. & 0. & 0. \\ 0. & 0.701 & 2.688 & 3.083 \\ 0. & 2.832 & 2.394 & 0.505 \\ 0. & 2.773 & 0.534 & 2.831 \end{pmatrix}. \quad (4.14)$$

We then solve for phase signs by taking further two photon experiments as prescribed in Section 4.2.1, and computing (4.7) to give a phase matrix

$$\Phi = \begin{pmatrix} 0. & 0. & 0. & 0. \\ 0. & -0.701 & 2.688 & 3.083 \\ 0. & -2.832 & -2.394 & 0.505 \\ 0. & 2.773 & -0.534 & -2.831 \end{pmatrix}. \quad (4.15)$$

Finally we combine these into  $\hat{M} = \Gamma \exp(i\Phi)$  to give

$$\hat{M} = \begin{pmatrix} \tau_{11} & \tau_{12} & \tau_{13} & \tau_{14} \\ \tau_{21} & \frac{(0.359-0.303i)\tau_{12}\tau_{21}}{\tau_{11}} & \frac{(2.568-1.252i)\tau_{13}\tau_{21}}{\tau_{11}} & \frac{(0.338-0.02i)\tau_{14}\tau_{21}}{\tau_{11}} \\ \tau_{31} & \frac{(1.159+0.371i)\tau_{12}\tau_{31}}{\tau_{11}} & \frac{(0.801+0.742i)\tau_{13}\tau_{31}}{\tau_{11}} & \frac{(3.007+1.663i)\tau_{14}\tau_{31}}{\tau_{11}} \\ \tau_{41} & \frac{(0.275-0.106i)\tau_{12}\tau_{41}}{\tau_{11}} & \frac{(0.365-0.216i)\tau_{13}\tau_{41}}{\tau_{11}} & \frac{(0.522+0.167i)\tau_{14}\tau_{41}}{\tau_{11}} \end{pmatrix}. \quad (4.16)$$

Setting  $\tau_{i,1} = \tau_{i,j} = 1$ , and solving the linear equations

$$\hat{M} \cdot [\tau_{11}^2, \tau_{12}^2, \tau_{13}^2, \tau_{14}^2]^\top = [1, 0, 0, 0]^\top \quad (4.17)$$

$$\hat{M}^\dagger \cdot [\tau_{11}^2, \tau_{21}^2, \tau_{31}^2, \tau_{41}^2]^\top = [1, 0, 0, 0]^\top, \quad (4.18)$$

yields

$$[\tau_{11}^2, \tau_{12}^2, \tau_{13}^2, \tau_{14}^2]^\top = [0.187, 0.519, 0.123, 0.171]^\top \quad (4.19)$$

$$[\tau_{11}^2, \tau_{21}^2, \tau_{31}^2, \tau_{41}^2]^\top = [0.187, 0.141, 0.060, 0.612]^\top, \quad (4.20)$$

which substituted into (4.16) gives

$$\hat{M} = \begin{pmatrix} 0.432 & 0.721 & 0.351 & 0.413 \\ 0.376 & 0.225 - 0.19i & -0.782 + 0.381i & -0.121 + 0.007i \\ 0.245 - 0.473 - 0.151i & -0.159 - 0.147i & 0.704 + 0.389i \\ 0.782 - 0.358 + 0.138i & 0.232 - 0.137i & -0.39 - 0.125i \end{pmatrix} \quad (4.21)$$

as required.

#### 4.2.3 RESOURCE SCALING

Determining amplitudes  $R_{j,k}$  requires  $m^2$  single photon measurements, and determining phases (including signs)  $\Phi$  requires  $(m-1)^2 + (m-2)^2 - 1$  two-photon measurements. Note, in the latter case, the number of two-photon measurements is less than total number available  $\binom{m}{2}^2$ . In Section 4.7 we use this redundancy to make the protocol more robust to experimental errors.

### 4.3 SST IMPLEMENTATION

Variants on SST have been used to reconstruct small circuits ( $m \leq 6$ ) [23, 25, 26], but in the following we use SST to reconstruct, to the best of our knowledge, the largest photonic circuit to date: the nine-mode waveguide device presented in Section 3.5.3 [see Fig. 4.2(b)].

To obtain the count matrix  $R_{i,j}$ , heralded 780 nm single photons from the source described in Section 3.3, were injected into modes  $k$  whilst monitoring output modes  $j$ . This totals 81 single photon measurements, but as all output modes are monitored simultaneously the experimentalist effectively makes nine measurements [see Fig. 4.2(b)]. Each measurement was taken for 90s such that the relative error due to Poissonian statistics on each element of  $R$  was  $< 0.5\%$ .

### 4.3. SST IMPLEMENTATION

---

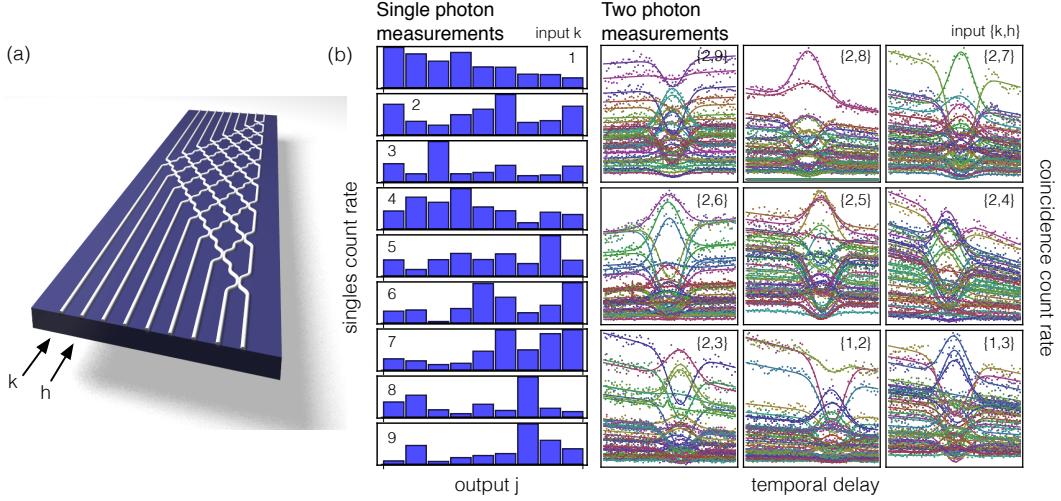


Figure 4.2: **Experimental SST.** (a) Single photons and pair photons probe the nine-mode waveguide device comprising 36 directional couplers and fixed phase shifts in silicon nitride. (b) Raw single photon (left) and two photon measurements (right) are fed into the reconstruction algorithm to output the unitary description of the device.

To obtain the visibility matrix  $V_{g,h,j,k}$  pairs of 780nm photons were injected into modes  $\{k, h\}$  where  $k = [1, 2]$  and  $h = [2, 9]$ , and all  $\binom{9}{2} = 36$  two-fold events were measured simultaneously. The full 64 phases were reconstructed, along with a subset of 15 signs, totalling 79 two-fold measurements, which as all output modes are measured simultaneously, equates to nine two-photon experiments [see Fig. 4.2(b)].

In principle this should be no harder than performing nine Hong-Ou-Mandel interference experiments, however, in practice, various experimental details make it significantly more challenging. Specifically, each fibre connected to the V-Groove array on the input varies in length by up to  $\pm 2\text{mm}$ . A single two-photon experiment involves matching these path lengths to on the order of the coherence length of the photon ( $\sim 140\mu\text{m}$ ). To do this the two photon state  $|11\rangle_{k,h}$  is injected into fibres  $\{k, h\}$  and the path length of one of the input modes is varied by a motorised linear actuator on the collection stage. As the path length is varied two-fold coincidences on the output are monitored till a characteristic ‘dip’ is found, signalling

the path lengths are matched [see Fig. 4.2(b)].

For this particular device high facet loss ( $\sim 95\%$ ) means that the probability of a two-photon event is small  $p = (1 - 0.95)^2$ , which coupled with a two-fold count rate of  $\sim 100\text{kHz}$  split over 36 possible two-fold events give an effective count rate of  $0.05^2 \times 10^5 / 36 \approx 7\text{Hz}$ . To get statistics significant enough to see a dip we move at a rate of  $5\text{s}/\mu\text{m}$  which along with regular restarts to recouple the moving arm of the source, means finding a single dip can take up to half a day. Once found, the source was tuned to a low power to reduce higher order terms thus increasing the maximum dip visibility ( $V_{\max} \approx 0.95$ ), and the linear actuator was scanned over the range  $\pm 400\mu\text{m}$  in  $10\mu\text{m}$  steps for 30 s per point. Two photon count rates were fitted as described in Section 3.3.1. Fitted dips for all input configuration  $\{k, h\} = \{1, 2\}$  are displayed in Fig. 4.2(b). The count-rate matrix  $R_{j,k}$  and visibility matrix  $V_{g,h,j,k}$  (normalised by the known dip visibility) are then fed into the reconstruction algorithm to output a unitary matrix.

To test the reconstruction, the circuit should be probed with a state which was not itself used as part of the procedure, and the results compared with theory based on the reconstruction. Preempting a result in Section 5.7.4, we probe the circuit with ensembles of three photons giving rise to a probability distribution  $p_i$  with 84 elements (see Section 5.7.4 for full details of the calculation). The statistical fidelity  $\mathcal{F}_s = \sum_i \sqrt{p_i^{exp} p_i^{th}}$  between the normalised theoretical  $p_i^{th}$  (based on the reconstruction) and experimental  $p_i^{exp}$  probability distributions is calculated, finding  $\mathcal{F}_s^q = 0.939 \pm 0.010$  and  $\mathcal{F}_s^c = 0.970 \pm 0.007$  for indistinguishable and distinguishable photons respectively. High fidelities imply accurate reconstruction of a large waveguide system. A full reconstruction of the three qudit nine-dimensional process via quantum process tomography (QPT) would require  $(9^{2 \times 3} - 1)^2 \approx 3 \times 10^{11}$  measurements [188]. Leveraging the experimentalists information about a system, namely the nature of the device that gives rise to the process, can significantly reduce the size of the problem.

## 4.4 ITERATIVE SST

Whilst SST is mathematically proven to reconstruct a unique unitary description of the device, in certain settings it can be experimentally impractical. Obtaining an entire visibility matrix can often take days, which if there are unknown changes occurring in the device or source, will manifest itself as errors in the final reconstruction. Moreover, if a large number of devices must be rapidly characterised (as is often the case with new fabrication runs) full SST is out of the question. We have therefore developed a rapid and robust extension of SST which allows the experimentalist to quickly determine partial information about  $\hat{U}$  without the need for two photon measurements. This protocol, iterative SST (iSST), uses single photons (or bright light) and an iterative normalisation procedure to determine the amplitudes  $|\hat{U}|^2$ .

The protocol works by noting that the matrix of single photon count rates  $R_{j,k}$  is given by  $R = D_O^2 |U|^2 D_I^2$ , where  $D_I^2$  and  $D_O^2$  are diagonal matrices and  $|U|^2$  is a doubly stochastic matrix<sup>1</sup>. Sinkhorn's theorem [189] states that any matrix of nonnegative entries can be decomposed into this form using the Sinkhorn-Knopp algorithm [190], thus we obtain  $|U|^2$  from  $R$ . The algorithm proceeds by successively normalising the columns, then rows of  $R$  until convergence and is proven to converge under the condition that  $R$  has total support. Intuitively this procedure works by iteratively constraining the normalisation condition (all rows and columns must be normalised) on the underlying count rate matrix until convergence. We tested the convergence speed with  $m = 10$  numerical simulations, finding that after just 10 iterations the reconstructed amplitudes were  $10^{-6}$  away from the true amplitudes, and after 50 iterations the error was  $10^{-15}$ .

Although the protocol does not recover phase information it is possible that for a limited number of small, sparse or highly structured circuits,  $|U|^2$  is sufficient to determine salient information about the circuit (beamsplitter ratios, phase shifter settings etc).

---

<sup>1</sup>That is, a square matrix of nonnegative real numbers whose rows and columns sum to one.

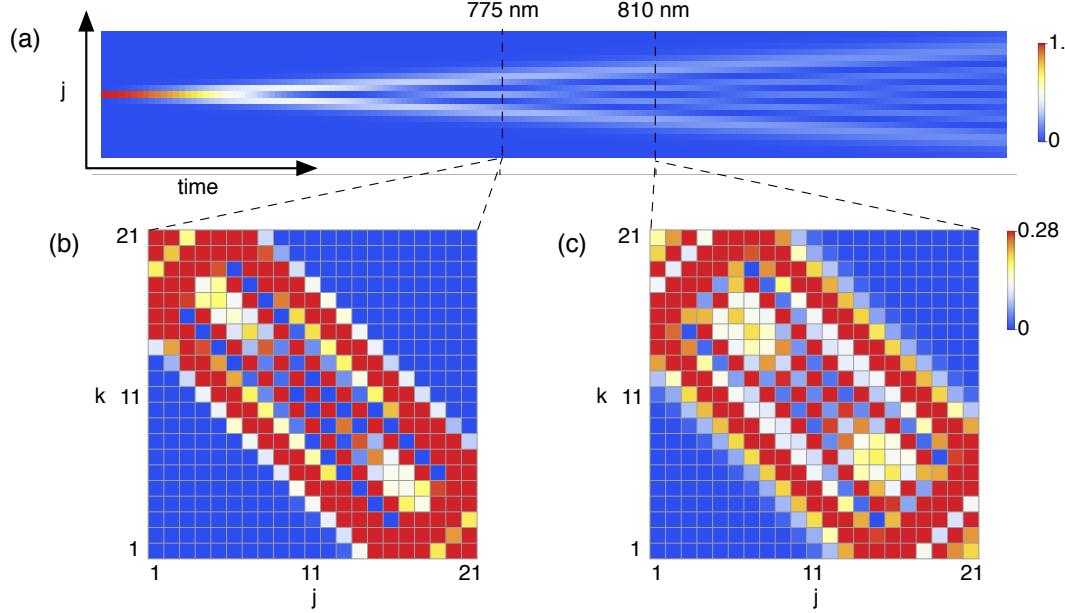


Figure 4.3: **Iterative SST** (a) The time evolution of light injected into the central mode of a CCW. This evolution can be simulated by either varying the optical path length, or varying the wavelength of incident light. (b) Reconstructed  $|\hat{U}(t)|^2$  via iSST at 775 nm and (c) 810 nm shows time evolution. To quantify this a model of the CCW Hamiltonian is optimised with respect to  $|\hat{U}(t)|^2$  to determine  $t$ , the results of which are displayed in (a).

## 4.5 iSST IMPLEMENTATION

Iterative SST was used to reconstruct the 21-mode array of continuously coupled waveguides (CCW) described in Section 3.5.2. To obtain  $R_{j,k}$  bright laser light from a tuneable laser source was injected into modes  $k$  whilst monitoring the output modes  $j$  with kHz response photodiodes. The power matrix was then fed into the iSST protocol to determine  $|\hat{U}|^2$ .

The unitary describing the CCW is generated by a nearest neighbour Hamiltonian, where the effective time evolution  $t$  is proportional to the optical path length  $z$  as shown in Fig. 4.3(a) (see Section 3.4.2 for a derivation of this from the modal coupling equations). As the velocity of light in a medium with refractive index  $n$

#### 4.5. iSST IMPLEMENTATION

---

is given by  $v = c/n$  (where  $c$  is the speed of light in vacuum), the time evolution is  $t = nz/c$ . Whilst  $z$  cannot be varied<sup>2</sup>, due to dispersion effects  $n$  can be tuned the wavelength of incident light. Hence the time evolution of the system can be simulated by varying the wavelength of light.

The speed at which iSST can be implemented allowed the reconstruction of  $|\hat{U}(t)|^2$  for a number of time steps, two of which are shown in Figs. 4.3(b,c) where the time evolution can clearly be seen. A model of the CCW Hamiltonian is then optimised to find  $t$  at different wavelengths, which is also shown on Fig. 4.3. Multiple reconstructions of such a large waveguide system is made possible precisely because of the speed at which iSST can be implemented. Achieving similar results via full SST would require a complete reconstruction of the phases totalling 760 two photons experiments over 39 different inputs. With a single input taking  $\sim 1/2$  day this would take  $\sim 1$  month

In this vein let us compare experimental resources for SST and iSST respectively: SST requires a source of indistinguishable photons (although this can be replaced with coherent light and a randomised phase [191, 192]) and single photon detection (such as single photon avalanche photodiodes), totalling  $\mathcal{O}(\mathcal{L}10^3)$ . In contrast iSST requires coherent laser light and bright-light photodiodes totalling  $\mathcal{O}(\mathcal{L}10)$ . This fact, coupled with the rapid speed at which iSST can be performed, might make it preferable for certain applications — see Table 4.1 for a comparison.

Resource	SST	iSST
Output	$U$	$ U ^2$
Source	Indistinguishable photons	Coherent laser light
Detection	Single photon counting	Photodiode
Cost	$\mathcal{O}(\mathcal{L}10^3)$	$\mathcal{O}(\mathcal{L}10)$
Time	$\mathcal{O}(1 \text{ day})$	$\mathcal{O}(1 \text{ second})$

Table 4.1: Comparison of resources for SST and iSST.

---

<sup>2</sup>Unlike in Meinecke et al. [172] where time evolution is simulated by CCW's of varying length.

## 4.6 ERROR PROPAGATION

A desirable property for any tomographic technique is robustness to experimental errors, so even in the presence of noise an accurate representation of the underlying experiment can still be recovered. To analyse the effect of noise on the reconstruction procedures we perform a Monte Carlo analysis whereby each element of  $R_{j,k}$  and  $V_{g,h,j,k}$  is multiplied by  $(1 + X)$  where  $X \sim \mathcal{N}(0, \delta)$  (i.e. a Gaussian centred on 0 with standard deviation  $\delta$ ) hence  $\delta$  is the noise parameter. We perform 1000 reconstructions for a given  $\delta$  and take the mean *circuit fidelity* defined as the distance  $\mathcal{F}_C = \text{Tr}(|U^\dagger U'|^2)/m$  between the reconstructed unitary  $U'$  and the intended unitary  $U$ . This has the operational meaning as the average output state fidelity for a given process  $U'$  over all possible single photon input states (i.e. the probability of getting a +1 outcome when projecting onto the desired state).

Choosing  $m = 10$  modes we vary the noise  $\delta \in [0, 0.5]$  plotting  $\mathcal{F}_C(\delta)$  for SST and iSST in Fig. 4.4(a). At a noise level of just  $\delta = 10\%$  we observe a circuit fidelity of  $\mathcal{F}_C = 0.788$  and  $0.792$  for SST and iSST respectively, and for  $\delta = 30\%$  observe  $\mathcal{F}_C = 0.527$  and  $0.593$ ; implying our reconstruction methods are highly sensitive to noise (although we note in the extremum,  $\delta > 10\%$ , iSST is more robust).

The natural question is where exactly does this sensitivity comes from? We identify three possible sources of reconstruction error: erroneous amplitudes  $\alpha$ , phases  $\phi$  or signs  $|\phi|$ . To analyse this we define the following metrics for the distance between amplitudes and phases of the the reconstructed unitary  $U' = \tau'_{j,k} \exp[i\phi'_{j,k}]$  and the ideal unitary  $U = \tau_{j,k} \exp[i\phi_{j,k}]$ :

$$D_\alpha = 1/m^2 \sum_{j,k} |\tau_{j,k} - \tau'_{j,k}| / \text{Max}(\tau_{j,k}, \tau'_{j,k}), \quad (4.22)$$

$$D_\phi = 1/m^2 \sum_{j,k} 1/\pi [\text{Max}(\phi_{j,k}, \phi'_{j,k}) - \text{Min}(\phi_{j,k}, \phi'_{j,k})] \mod 2\pi, \quad (4.23)$$

$$D_{|\phi|} = 1/m^2 \sum_{j,k} 1/\pi [\text{Max}(|\phi_{j,k}|, |\phi'_{j,k}|) - \text{Min}(|\phi_{j,k}|, |\phi'_{j,k}|)] \mod 2\pi. \quad (4.24)$$

The amplitude distance  $D_\alpha$  is the mean normalised L1-distance between all

#### 4.6. ERROR PROPAGATION

---

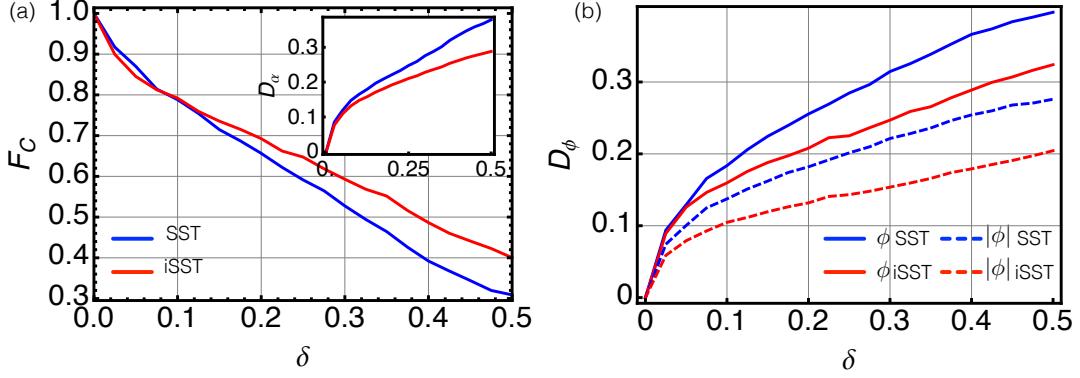


Figure 4.4: **SST error analysis.** (a) A comparison of reconstruction fidelity  $\mathcal{F}_C$  as a function of simulated experimental noise  $\delta$  on a  $m = 10$  mode unitary, for SST (blue) and iSST (red). Each point was generated from 1000 Monte-Carlo experiments. Inset, the mean distance  $D_\alpha$  between reconstructed amplitudes and ideal amplitudes. (b) A comparison of  $D_\phi$  for phases  $\phi$  and signs  $|\phi|$ . Error bars are omitted for clarity, but included in Table 4.3.

amplitudes, and the phase distance  $D_\phi$  is the mean normalised distance between two unit vectors at angles  $\phi$  and  $\phi'$  with a common axis (i.e.  $D_\phi(0, \pi) = 1$ ).

In Figs. 4.4 we plot these distances as a function of noise. There are two points to note: first, from Fig. 4.4(a) inset, iSST amplitude reconstruction is more robust to noise, and as phase reconstruction depends on amplitudes this in turn filters through to an increased accuracy in both phase and overall fidelity. Second, from Fig. 4.4(b), for both reconstruction techniques  $D_\phi > D_{|\phi|}$  implying that the magnitude of the phase is nearer than the total phase. The only way this can occur is due to an *erroneous sign flip*. Due to noise, the sign of a reconstructed phase gets flipped and this error propagates when that phase is used as reference in subsequent reconstructions. We can thus think about mitigating this error propagation by utilising some of the unused entries in  $V_{g,h,j,k}$  to error correct the reconstruction.

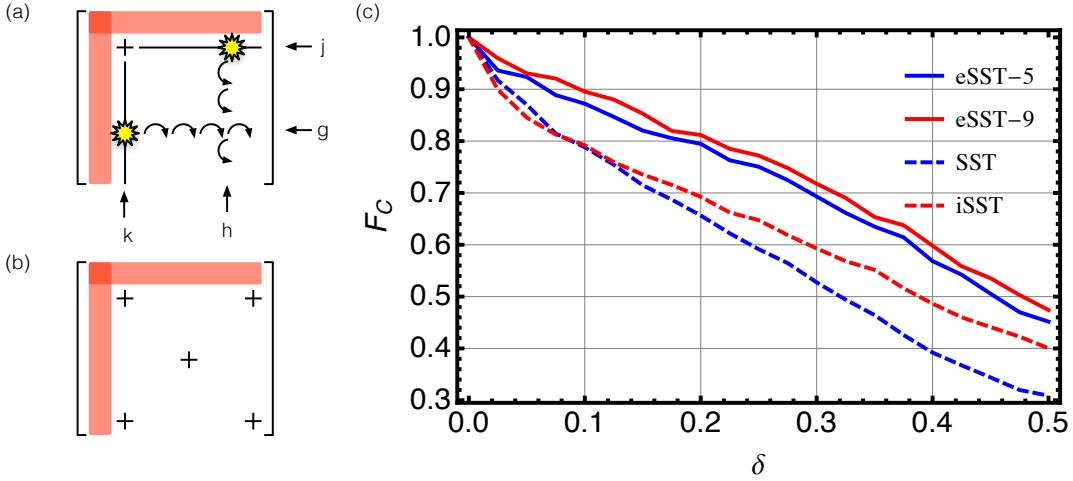


Figure 4.5: **Error corrected SST.** (a) Defining an entry  $\{j, k\}$  to be positive fixes the columns and rows with which all other signs are calculated by. If an erroneous sign flip occurs in one of these reference columns (rows) it will propagate across the entire row (column). (b) Error corrected SST (eSST) defines multiple support entries, and performs majority voting on the multiple reconstructed sign matrices. (c) Numerical results for eSST with five supports, nine supports and SST and iSST for comparison. Each point was generated from 1000 Monte-Carlo experiments and errors are included in Table 4.3.

## 4.7 ERROR CORRECTED SST

We introduce the error corrected SST formalism (eSST) by noting that the key step in the reconstruction of phases is in defining a single reference phase to be positive. This defines the columns and rows with which all other phases are determined by, thus if an error occurs in one of these entries it will propagate to multiple entries [see Figure 4.5(a)]. Note however this choice of reference phase is arbitrary, so other reference phases (we term ‘supports’) can be used to corroborate the reconstructed signs.

In particular for the  $m = 10$  mode case we define a cross of five support phases so as to minimise the possible distance between entries [see Figure 4.5(b)]. We then build a matrix of reconstructed signs for each of these five support phases then

## 4.8. CONCLUDING REMARKS

---

perform a majority voting on each entry to determine the final signs. During this process we also reconstruct five phase matrices so therefore take the final phase to be the mean of these for added robustness.

We find at  $\delta = 10\%$  and  $30\%$  a circuit fidelity of  $\mathcal{F}_C = 0.872$  and  $0.693$  [see Fig. 4.5(c)], which is a maximum of  $17\%$  increase in reconstruction fidelity over SST and a  $10\%$  over iSST. As a final test we increase the number of supports to nine, but observe only a small increase ( $< 3\%$ ) suggesting that for this size matrix we are near the limit of what we can error correct using redundancies. A numerical comparison of all results and errors is given in Table 4.2 and Table 4.3.

An  $n$  column error correction protocol requires  $(m - 1)^2 + n(m - 2)^2 - n$  two-photon measurements, so is efficient in  $n$ . The error model presented thus far is completely general, assuming nothing about the experimental apparatus. An interesting research line is understanding the limitations of this error model, and if a more appropriate error model exists, whether error correction protocols can be constructed to make use of this knowledge.

## 4.8 CONCLUDING REMARKS

In this chapter we have presented a series of efficient characterisation techniques, which designed for linear optics, uses knowledge about the device to significantly reduce the size of the characterisation problem. Each technique is tailor made to suit the experimentalists needs, be it for rapid partial characterisation or accurate full characterisation; in the lab the experimentalist must make a judgement about which is more appropriate.

For any quantum technology to have a hope of scaling, efficient ‘hardware level’ characterisation techniques are essential for feeding into next generation device designs. Other platforms have spent significant resources in precisely understanding device level errors [76] and LOQC must deliver similar analysis. Our results form a small part of this picture, and other techniques will be necessary for machine level characterisation of integrated single photon sources [193] and single photon detectors [21].

#### 4. HARDWARE CHARACTERISATION

---

Noise $\delta$	SST	iSST	eSST-5	eSST-9
0.	1.	1.	1.	1.
0.05	0.87	0.845	0.924	0.931
0.1	0.788	0.792	0.872	0.896
0.15	0.715	0.735	0.82	0.853
0.2	0.656	0.693	0.795	0.812
0.25	0.591	0.648	0.751	0.772
0.3	0.527	0.593	0.693	0.718
0.35	0.464	0.552	0.635	0.653
0.4	0.392	0.486	0.568	0.598
0.45	0.344	0.441	0.506	0.535
0.5	0.309	0.4	0.452	0.474

Table 4.2: Numerical results for SST reconstruction circuit fidelities, generated from 1000 Monte Carlo experiments with applied noise  $\delta$ .

Noise $\delta$	$1\sigma$ SST	$1\sigma$ iSST	$1\sigma$ eSST-5	$1\sigma$ eSST-9
0.	0.	0.	0.	0.
0.05	0.168	0.222	0.169	0.165
0.1	0.175	0.212	0.194	0.181
0.15	0.181	0.215	0.213	0.194
0.2	0.182	0.203	0.195	0.202
0.25	0.172	0.194	0.207	0.206
0.3	0.151	0.184	0.206	0.205
0.35	0.139	0.169	0.188	0.198
0.4	0.111	0.148	0.174	0.182
0.45	0.092	0.129	0.153	0.161
0.5	0.077	0.111	0.132	0.141

Table 4.3: One standard deviation of numerical results presented above.

# 5

## Verifying Quantum Complexity

### STATEMENT OF WORK

The work presented in this chapter was published in Carolan et al. *Nat. Photon.* **8** 621 (2014) [194]. The project proposal for using special-case classically tractable but non-trivial photon statistics as a verifier for boson sampling came from A. Laing, who supervised the project. I developed these ideas and analysed experimental data along with A. Laing, P. Shadbolt, J Meinecke, N.Russell, and J. Matthews. I performed the experimental implementation of these ideas and the additional idea to use bunching statistics to determine the distinguishability of photons (based on Spagnolo et al. [195] but proposed independently by myself). I developed the state-sifting proposal with A.Laing, which I also implemented experimentally. The quantum walk device was fabricated by collaborators

at the University of Twente, and the random unitary device was fabricated by the commercial organisation LioniX. Finally, this project took place after a two-year period that began with building the multi-photon source and included a series of tests for devices that were found to operate below performance threshold. These tests (supervised by A. Laing) were performed largely by myself but served as an effective preparation stage for the verification work that followed.

### 5.1 INTRODUCTION

In the previous chapter we introduced the necessary photonic components for linear optical quantum computing (LOQC), but here we bring this hardware together and present a *linear optical processor* (LPU). The combination of high efficiency photon source, complex waveguide structures and multi-channel single photon detection, results in the generation of large scale quantum photonic states which could provide a near-term route to outperforming classical machines.

With up to five photons in 21 modes we generate states with Hilbert spaces of up to 50,000 dimensions. The comparatively low number of events we observe in this state space is indicative of the task of verification as quantum simulators scale in size. In general these quantum machines won't be performing clear computational tasks which can be efficiently verified, so alternative techniques must be developed to assess the performance of the machine. In this chapter we review the computational complexity of rudimentary linear optical systems, and develop a toolbox of experimentally motivated *in situ* verification protocols; for a particular class of linear optical simulator, a ‘boson sampler’. Whilst formally unverifiable, these techniques leverage the experimentalists knowledge of the system to achieve efficient assessment

## 5.2 QUANTUM SUPREMACY

If the goal of quantum computer science, as is often claimed, is to outperform a classical computer, to achieve *quantum supremacy* [196]; in moments of quiet introspection the honest quantum computer scientist should ask herself two questions:

1. *Why are we doing this?* The super-polynomial advantage a quantum computer would offer has the potential to change many aspects of human understanding; from studying phase transitions in quantum many body systems [197], to calculating quantities in quantum field theory [198, 199], to providing us with *fundamentally new physics*. Yet there is a deeper reason we strive for quantum supremacy. A quantum machine that outperforms a classical machine tells us something fundamental about nature. It makes clear, perhaps even defines, the gap between the quantum and classical world.
2. *How near are we?* This is crucial in driving both financial investment (and hence experimental resources) and focusing theoretical efforts. Consider this in the context of integer factorisation (Section 2.5). The factoring world record is RSA-768 [200]: A 768-bit (232 decimal digit) number, which took a cluster of a few hundred PC's running the fastest known classical factoring algorithm — number field sieve [60, 201] — approximately 2 years (1500 CPU-years). How long would a quantum computer running Shor's algorithm take? In Fig. 5.1 the computational run times for both a classical computer running number field sieve and a quantum computer running Shor's algorithm are plotted on a log-log scale; the respective exponential and polynomial scaling lines can clearly be seen.

Using the modular exponentiation routine of Beckman et al. [203] factoring an  $N$ -bit number requires  $73N^3$  quantum gates and  $5N + 1$  qubits. For  $N = 768$ , the overhead is 33 billion gates and 4000 logical qubits, *not* including error correction<sup>1</sup>. Which, with an optimistic clock speed of GHz, gives a run time of  $\sim 30$  s. However, the record number of qubits to date is 14 [204]. This thus raises the question *what*

---

<sup>1</sup>Include error correction, these numbers get multiplied by  $\sim 10^3$  [75].

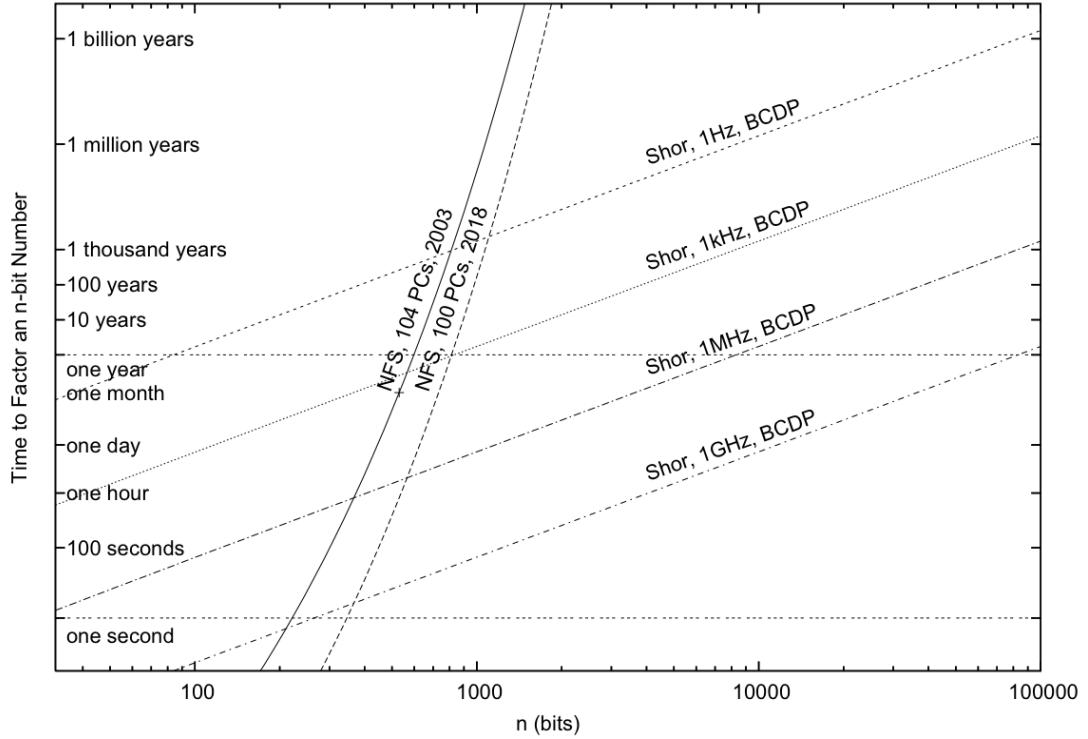


Figure 5.1: **Quantum and classical integer factorisation.** A comparison of the run times for a quantum computer running Shors factoring algorithm (solid lines) versus a cluster of computers running the best known classical factoring algorithm (dashed lines). Note the importance of clock speed; a kHz quantum computer provides no advantage over current classical computers for problems with less than a year run time. Taken from the thesis of Rodney Van Meter [202].

*can we do with todays or tomorrows resources and technologies to outperform a classical computer?*

This resource counting exercise becomes all the more pertinent in the context of photonics. A single silicon wafer can contain billions of transistors<sup>2</sup>, implying on-chip linear optical elements have the potential to be relatively cheap. The bottle neck, however, occurs with single photon sources; the record number of photonic qubits is eight [129, 130], owing to the difficulty of inducing photon-photon interactions. This problem affects linear optical quantum computing (LOQC) two-fold:

---

<sup>2</sup>Intel's Broadwell-U processor contains 1.9 billion transistors in a  $133 \text{ mm}^2$  area using 14 nm transistor technology [205]. The smallest known virus is 17 nm in diameter.

### 5.3. QUANTUM COMPLEXITY IN LINEAR OPTICS

---

first in the generation of photons (see Section 3.2.1), and second in implementing two qubit gates (see Section 2.6.5).

If the major experimental challenges for LOQC are single photon sources and entangling gates, is there anything we can do in the near term to achieve quantum supremacy which relaxes these constraints? In the following we review a classically intractable algorithm, native to linear optics, which does precisely that.

## 5.3 QUANTUM COMPLEXITY IN LINEAR OPTICS

Following in the vein of Deutsch (Section 2.5) let us formally express the notion of quantum supremacy by extending the Church-Turing thesis to a statement about physics:

*“All computational problems that are efficiently solvable by realistic physical devices, are efficiently solvable by a probabilistic Turing machine.”*

Scott Aaronson [22]

The extended Church-Turing thesis (ECT) is a statement about what is efficiently computable within the laws of physics. If there existed physical systems which solved problems that *could not* be efficiently solved on a probabilistic Turing machine, the ECT would be false. Couched in these terms it seems a universal quantum computer, running for example Shor’s algorithm, unequivocally sinks the ECT, but the issue is more subtle than that.

Whilst we strongly believe there to be no efficient classical algorithm for factoring, the existence of one would not cause significant disruption to our understanding of computational complexity. Moreover, breakthroughs in number theory during the early 1990’s have lead to remarkable sub-exponential ‘sieve’ algorithms for factoring [60, 201]; and it is not yet proven we won’t see further breakthroughs. A final point: the ECT is a statement about what we can physically build. We

need to go into the lab and demonstrate a large scale, classically un-simulatable machine. Whilst error correcting codes tell us this is in principle possible, there is no guarantee that as of yet undiscovered physics prevents the construction of large scale quantum systems.

### 5.3.1 BOSON SAMPLING

*“... proving a quantum systems computational power by having it factor integers encoded in binary is a bit like proving a dolphin’s intelligence by teaching it to solve arithmetic problems. Yes, with heroic effort, we can probably do this, and perhaps we have good reasons to. However, if we just watched the dolphin in its natural habitat, then we might see it display equal intelligence with no special training at all.”*

Aaronson and Arkhipov [22]

Designed for linear optics, with no requirement for quantum logic gates, qubit entangling operations, or number resolved photon detection, *boson sampling* [22] is a quantum protocol that has been developed as a rapid route to challenge the ECT and demonstrate that quantum physics can be harnessed to provide fundamentally new and non-classical computational capabilities.

Based on the foundations of computer science, boson sampling is a mathematical proof (using plausible conjectures) that a many-boson state, when acted on by a large random linear optical circuit, will give rise to a probability distribution that cannot be efficiently sampled by a classical algorithm. At the heart of this proof is the fact that many photon quantum interference is governed by a classically intractable matrix function — the permanent.

#### THE PERMANENT

The permanent is similar in nature to the determinant, but with each negative term in the expansion taken as positive. Recalling from Section 2.6.6, the permanent

for a  $n \times n$  square matrix  $A$  is given by

$$\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i,\sigma(i)} \quad (5.1)$$

where the sum runs over all elements  $\sigma$  of the symmetric subgroup  $S_n$ , that is the  $n!$  permutations of  $(1, 2 \dots n)$ . For example if

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \quad (5.2)$$

$$\text{perm}(A) = a_{1,1}a_{2,2} + a_{1,2}a_{2,1}, \quad (5.3)$$

and so on for larger matrices. Whilst *prima facie* analogous to the determinant, it has radically different computational properties. The determinant, although when naively defined has  $n!$  terms, can be calculated in time  $\mathcal{O}(n^3)$  via certain decompositions of  $A$  (such as LU, or QR). Such decompositions, in general, do not exist for permanent calculations.

Whilst the permanent had been discussed at least a century before [206, 207], it was in 1979 that Valiant's seminal work [208] showed calculating the permanent of a  $(0,1)$ -matrix (that is  $a_{i,j} \in \{0, 1\}$ ) is  $\#P$ -complete.  $\#P$  is the class of counting problems in  $NP$ , and asks the number of accepting paths for a Turing machine running in polynomial time. Formally:

A function  $f : \{0, 1\}^* \rightarrow \mathbb{N}$  is in  $\#P$  if there exists a polynomial  $p : \mathbb{N} \rightarrow \mathbb{N}$  and a polynomial-time Turing machine  $M$  such that for every  $x \in \{0, 1\}^*$ ,  $f(x) = |\{y \in \{0, 1\}^{p(|x|)} : M(x, y) = 1\}|$  [49]

Take a prototypical problem from  $NP$ : the travelling salesman problem. The  $NP$  problem asks “are there any Hamiltonian paths with cost less than 50” while the corresponding  $\#P$  problem asks “*how many* Hamiltonian paths have cost less than 50”. Immediately  $\#P$  is at least as hard as  $NP$  (if you can count how many paths accept, you can certainly find a single accepting path), but to understand how much harder we must first generalise  $P$  and  $NP$  into the *polynomial hierarchy* ( $PH$ ).

If problems in  $\text{NP}$  have the form “does there exist an  $n$ -bit string  $x$  such that  $f(x) = 1$ ?” (where  $f$  is a polynomial time computable function), we can include another quantifier “does there exist an  $x$  such that for all  $y$   $f(x, y) = 1$ ?” to define  $\text{NP}^{\text{NP}}$ , that is is an  $\text{NP}$  machine with an  $\text{NP}$  oracle.  $\text{NP} = \Sigma_1\text{P}$  is the first level of  $\text{PH}$  and  $\text{NP}^{\text{NP}} = \Sigma_2\text{P}$  is the second;  $\text{PH}$  is the union  $\Sigma_k\text{P}$  over all integers  $k$ . Maintaining the structure of  $\text{PH}$  is of fundamental importance to theoretical computer science and results which lead to a collapse of these levels are seen as highly improbable. Toda’s theorem shows  $\text{PH} \subseteq \text{P}^{\#\text{P}}$  [209]. That is the entire polynomial hierarchy can be solved by a polynomial time Turing machine with a single call to a  $\#\text{P}$  oracle. This is all the more surprising as certain  $\#\text{P}$  problems correspond to counting problems in  $\text{P}$ .

To see this, consider Valiant’s example from above. Notice the permanent of a  $(0,1)$ -matrix  $A$  is equivalent to calculating the number of perfect matchings (i.e. the number of ways to connect two vertices such that no two edges share a connection) for a bipartite graph  $\mathcal{G}$ , described by an adjacency matrix  $A$ ; such that the set of vertices  $\{x_1, x_2 \dots x_n\}$  and  $\{y_1, y_2 \dots y_n\}$  share an edge between  $x_i$  and  $y_j$  iff  $a_{i,j} = 1$ . The clearest non trivial example is an  $n = 3$  matrix, as shown in Fig. 5.2. Surprisingly, efficient algorithms exist for finding perfect matchings [210]. So it is *easy to find* a perfect matching, but incredibly hard to calculate *how many*. Intuitively this is because there are  $\mathcal{O}(n!)$  matches to count.

Even if we can’t efficiently and exactly calculate the permanent of a  $(0,1)$ -matrix, can we do better than the naive  $\mathcal{O}(n!)$ ? The fastest known exact algorithm for calculating permanents is due to Ryser [211] who in 1963 gave an  $\mathcal{O}(2^n n)$  algorithm. In 2004 Jerrum, Sinclair and Vigoda [212] showed that if the elements of  $A$  are nonnegative real (which includes a  $(0,1)$ -matrix) then a polynomial time algorithm exists to approximate  $\text{perm}(A)$  to within multiplicative error. Finally in 2005 Gurvits [213] gave a polynomial time algorithm to approximate the permanent of a matrix with complex entries up to additive error.

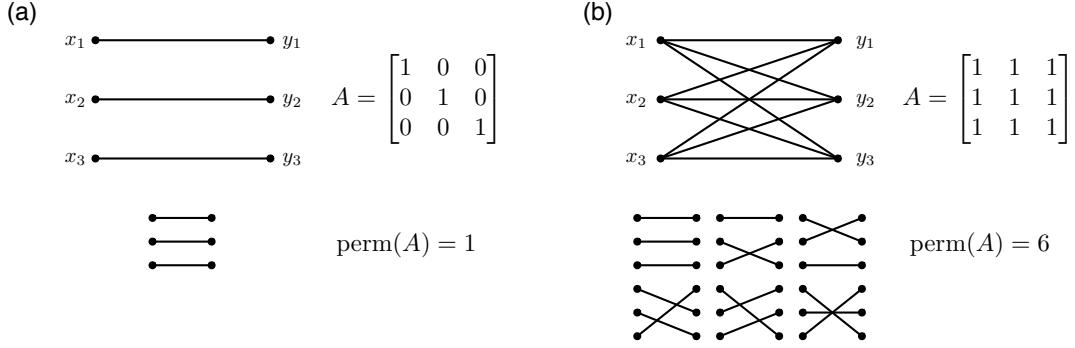


Figure 5.2: **Matrix permanents and perfect matching.** The number of perfect matchings for a bipartite graph is equal to the permanent of its adjacency matrix  $A$ . (a) When  $A = I$ , there is only one perfect matching, and when (b)  $A$  is a block matrix of ones there are six.

### 5.3.2 PHOTONS IN MODES

Recall from Section 2.6.6, the transition probability for photons propagating through a linear optical circuit  $\hat{U}$  is given by  $|\text{perm}(\Lambda)|^2$ , where  $\Lambda$  is a sub-matrix of  $\hat{U}$  defined by the input and output modes. Whilst the first mention of bosons and permanents dates back to the 1950's [214], the first mention of it in the context of linear optics is more recent and due to Scheel [86].

The collision free subspace of  $p$ -photons in  $m$ -modes is a Hilbert space in  $d_p^m$  — which in the photon number basis reads  $\{|n_1, \dots, n_m\rangle\}$  with  $n_1 + \dots + n_m = p$  and  $n_i \leq 1 \forall i$  — with dimension  $|d_p^m| = \binom{m}{p}$ . This means a rudimentary LOQC defines a probability distribution  $\mathcal{B}$ , with  $|d_p^m|$  elements each given by the absolute square of a unique matrix permanent.

If we fix  $m = p^2$  then  $|d_p^{p^2}|$  grows exponentially in  $p$  [22]. So evaluating  $\mathcal{B}$  requires calculating exponentially many, exponentially hard unique matrix functions; hence a classical computer can never efficiently reproduce this entire distribution. Crucially *neither can a rudimentary LOQC*. There are exponentially many elements in  $\mathcal{B}$  so a LOQC would require exponential time to saturate this distribution. However, Aaronson and Arkhipov (AA) showed that a rudimentary

LOQC can efficiently *sample* from this distribution which cannot be done classically. Their proof relies on plausible complexity conjectures which we will now look at in detail.

### 5.3.3 COMPLEXITY PROOF

We formalise the boson sampling problem. The input to the problem is a  $m \times p$  matrix  $A$ , where  $A$  is taken from first  $p$  columns of a unitary drawn uniformly from the Haar measure<sup>3</sup>. Given  $A$ , with a basis state  $S \in d_p^m$ , let  $A_S$  be the  $p \times p$  sub-matrix obtained by taking  $s_i$  copies of the  $i^{\text{th}}$  row for all  $i \in [m]$ . Then  $\mathcal{B}$  is the probability distribution over  $d_p^m$  defined as

$$\Pr_{d_p^m}(S) = \frac{|\text{perm}(A_S)|^2}{s_1! \cdots s_m!} \quad (5.4)$$

The goal of boson sampling is to sample from  $\mathcal{B}$  given  $A$  as input.

In theoretical computer science proofs often take the form of *modus tollens*: “if A is true, then B is true. We strongly believe B to be false, hence A is false”. The proof for boson sampling runs similar whereby AA show that a classical machine which could efficiently (even approximately) sample from  $\mathcal{B}$  would have severe consequences for theoretical computer science.

AA’s proof has a number of conceptual steps (summarised in Figure 5.3) and it is worth familiarising ourselves with them. Their main result is:

*Suppose there exists a classical computer that takes as input  $A$  and error bound  $\varepsilon$ , and that samples from the probability distribution  $\mathcal{B}'$  such that  $||\mathcal{B}' - \mathcal{B}|| \leq \varepsilon$  in  $\text{poly}(|A|, 1/\varepsilon)$ . Then the  $|\text{GPE}|_{\pm}^2$  problem is solvable in  $\text{BPP}^{\text{NP}}$ .*

Here  $|\text{GPE}|_{\pm}^2$  is the problem of calculating to within additive error  $|\text{perm}(X)|^2 \pm \varepsilon \cdot n!$  for a Gaussian matrix  $X \sim \mathcal{N}(0, 1)^{n \times n}_{\mathbb{C}}$  in  $\text{poly}(n, 1/\varepsilon, 1/\delta)$  time. The reliance

---

<sup>3</sup>The Haar measure samples uniformly from the space of all unitaries. To generate a  $m \times m$  Haar random unitary, first generate a Gaussian matrix  $A \sim \mathcal{N}(0, 1)^{m \times m}_{\mathbb{C}}$ , then orthogonalise  $A$  via the GramSchmidt process.

### 5.3. QUANTUM COMPLEXITY IN LINEAR OPTICS

---

of Gaussian matrices is important. If submatrices are not Gaussian — perhaps certain sub-matrices have larger entries — they could be identified by inspecting  $A$ . Gurvit's algorithm could then be used to evaluate these submatrices, but because the permanents would be large, the relative additive error would be small, and  $\mathcal{B}$  could be efficiently sampled from. The requirement for Gaussian submatrices prevents this.

The proof so far deals with  $|\text{perm}(X)|^2$  (the transition probabilities of photons) but for reduction purposes it is more convenient to deal with  $\text{perm}(X)$ , which is described by the analogous  $\text{GPE}_\times$  problem (with multiplicative error). To that end AA construct the (highly plausible) permanent anti-concentration conjecture which if true gives a polynomial time equivalence between  $|\text{GPE}|_\pm^2$  and  $\text{GPE}_\times$ <sup>4</sup>. This means a classical boson sampling machine would imply  $\text{GPE}_\times$  is solvable in  $\text{BPP}^{\text{NP}}$ .

Finally, they conjecture that calculating  $\text{GPE}_\times$  is  $\#P$ -hard. In fact this is the biggest open question in their proof, and they give strong, but not conclusive, evidence in favour of it. As  $\#P$  is a counting problem it needs to be couched in terms of a decision problem which can be done with the class  $P^{\#P}$  — a classical machine with a  $\#P$  oracle. From their main theorem a polynomial time classical algorithm for approximate boson sampling would imply  $P^{\#P} = \text{BPP}^{\text{NP}}$  which from Toda's theorem (above), collapses the polynomial hierarchy to the third level. This is seen as incredibly unlikely as, therefore, is the existence of a classical boson sampling machine. A summary of the steps and assumptions in their proof is shown in Fig. 5.3.

Photons in linear optical circuits by their very nature sample from  $\mathcal{B}$ . So the existence of a rudimentary LOQC provides incredibly strong evidence for the fallacy of the ECT. Much stronger than a universal computer running Shor's algorithm; a polynomial time factoring algorithm would only change the complexity class for

---

<sup>4</sup>An equivalent conjecture has recently been proven for the IQP non-universal model of quantum computing [215], providing strong evidence for the validity of the permanent anti-concentration conjecture.

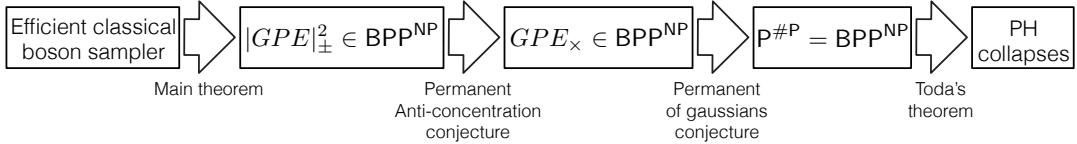


Figure 5.3: **Boson sampling flow chart.** A summary of the assumptions necessary to prove Aaronson and Arkhipov’s hardness results. Adapted from reference [22].

a single problem, which from a complexity theoretic perspective is nowhere near as strong as a collapse of the polynomial hierarchy.

It is precisely because boson sampling does not require measurement and feedforward that significantly fewer resources are required to achieve quantum supremacy. The exact number of photons and modes which are intractable to classical calculation is an open question, but  $\sim 20$  photons in  $\sim 400$  modes<sup>5</sup> is often cited which is significantly less than the  $10^6$  error corrected logical qubits needed to beat a classical machine at factoring. Consider evaluating  $\mathcal{B}$  for  $p = 20$ ,  $m = 400$ . Ryser’s algorithm uses about  $2^{(p+1)}p^2$  floating point operations to calculate a  $p \times p$  permanent, so that is  $10^8$  floating point operations per permanent. For a modern supercomputer such as the University of Bristol’s ‘Blue Crystal’ which runs at 200 TFlops<sup>6</sup> this takes a fraction of a second ( $10^{-6}$  s); however, it is  $|d_p^m|$  which provides the significant overhead. In this instance  $|d_{20}^{400}| = 10^{33}$  and therefore takes  $10^{20}$  years to evaluate. In reality an optimised algorithm wouldn’t calculate all  $|d_p^m|$  elements, but rather use some sampling method such as rejection sampling; however this back of the envelope calculation provides a heuristic for the magnitude of the task.

Boson sampling solves a sampling problem rather than a decision problem, as such it is unclear if can be used for practical computation. However it does tell us something fundamentally interesting about linear optics which may lead to further, more practical advances. It was known since KLM [10] that linear optics, with

<sup>5</sup>AA’s proof requires  $m = p^5$ , but they conjecture  $m = p^2$  suffices.

<sup>6</sup>Flop = floating point operations per second.

### 5.3. QUANTUM COMPLEXITY IN LINEAR OPTICS

---

the addition of measurement and active feedforward, could solve classically hard problems in BQP. Yet Aaronson and Arkhipov show us that linear optics, *without* the highly nonlinear operations of measurement and feedforward, still provides non-classical computational capabilities. This leaves us with the tantalising question regarding the intermediate regime: namely, if we only have a small amount of measurement induced nonlinearity (pre KLM) can we still solve useful problems that a classical computer cannot?

Some final remarks regarding the role of experiments. The task of the experimentalist isn't to try to overturn the Church-Turing thesis. This is a statement about asymptotic behaviour and AA have already shown that *given the existence* of a LOQC which samples from  $\mathcal{B}$ , the ECT is false. The task of the experimentalist is *prove the existence* of such a device, and show that photons are truly governed by matrix permanents as  $p$  becomes large. Perhaps nature conspires against us to build such systems. Perhaps some as of yet undiscovered theory of quantum gravity prevents large scale bosonic interference. The only way we can ever know, is to get in the lab and build it.

#### 5.3.4 RELATED WORK

Aaronson and Arkhipov's initial proposal in 2010 ignited a flurry of experimental efforts, with groups from Oxford [23], Brisbane [24], Vienna [25] and Rome [26] performing small-scale ( $p = 3, 4$ ,  $m = 5, 6$ ) boson sampling experiments, demonstrating non-interacting bosonic transition probabilities are in fact governed by matrix permanents. Crucially these realisations are made possible by the advances in integrated photonic technology (see Section 3.4).

Proposals have suggested [216] and experimentally demonstrated [217] using Gaussian input states to overcome probabilistic sources, or multiplexed schemes using time-bin encoded photons in a fibre loop to reduce source and circuit overheads [218] (although resilience to loss remains an open question). There have been proposals to use dispersive optics to access a high dimensional unitary [219]

or even non-interacting bosonic architectures other than photons, such as the local transverse phonon modes of trapped ions [220, 221]. Even though the original proof deals with the approximate case, a series of papers have looked at the effect of errors in boson sampling experiments; from the effect of loss and mode mismatch [222] to the presence of circuit imperfections [223].

With the rapid advance in both experimental and theoretical work, it is not optimistic to predict an experiment that within the next five years can start to challenge classical machines. As we strive to reach this goal we are faced with an immediate question: *how will we know when we get there?*

### 5.4 VERIFICATION OF QUANTUM COMPLEXITY

You've just ordered the newest and tastiest 'Norwegian Jarlsberg' from the cheese shop. It's sold as the butteriest, richest Jarlsberg on the market and when it arrives you want to verify the cheese shop did in fact send you the Jarlsberg you ordered. Now, there are tests you can do *before you even eat it*. You can check the colour of the cheese, inspect the texture, you can smell the nutty flavours. The aggregate of all these tests give you confidence this was in fact the cheese you ordered, and based on this you eat it.

The problem is the same in computing: if a machine purports to run an algorithm, under certain conditions it suffices to check the output to that algorithm (i.e. eat the cheese), namely, by definition, when the problem is in **NP**. If however the problem is outside of **NP**, the output cannot be efficiently verified (i.e. you can't fit the cheese in your mouth) and other techniques must be used to give circumstantial evidence: pulling the hard disk out, checking the motherboard, running test computations you know the answer to.

In the context of quantum computation, that means a quantum computer running Shor's factoring algorithm, can also be efficiently verified by checking the solution. We can also think about this in terms of the output distribution that is generated; Shor's algorithm creates an exponentially large probability distribution

## 5.4. VERIFICATION OF QUANTUM COMPLEXITY

---

with individual peaks at highly regular intervals that facilitate the solution to the factoring problem.

In contrast, because boson sampling relates to  $\#P$ , it is not clear that similarly useful structure exists in  $\mathcal{B}$ , with formal verification likely to be impossible. In short: how do you verify the output to a counting problem unless you go ahead and count the accepting paths for yourself?

The correct operation of Shor’s algorithm is verified independently of the physical platform of the universal quantum computer on which it is run. However, boson sampling is native to linear optical experiments, allowing us to exploit experimental methods and fundamental properties of linear optics to develop procedures that provide strong evidence that the system is functioning properly.

In the following we present a series of experimentally motivated *machine level* verification techniques that make use of the physical phenomena themselves. Whilst formal verification is believed to be impossible, we propose techniques that provide circumstantial evidence of computational complexity, by availing the experimentalists information about the system.

### 5.4.1 EXPERIMENTAL VERIFICATION

We present two broad approaches to efficient verification. Firstly, we demonstrate techniques which rule out various known tractable distributions which when summed provide counterfactual evidence for correct operation. Specifically we look at a proposal by Aaronson and Arkhipov [224] which rules out sampling a computationally trivial distribution [225]. Whilst this tells us we are not doing something trivial, we determine a more experimentally motivated route to incorrect operation is the unwanted introduction of distinguishability between photons, which destroys quantum interference [92]. We therefore propose and demonstrate a protocol which rules out the distribution of distinguishable photons.

Secondly, we propose the method of finding configurations of optical circuits that engender large-scale, ordered, photonic quantum interference, to produce an

efficiently predictable structure in the probability distribution of possible detection events. With large scale single-photon and multi-photon interference verified with predictable multimode correlations, the system is then reconfigured to implement a random unitary operation as required for the algorithm. The only assumption made is that quantum mechanics holds and the system maintains correct operation as the circuit is continuously reconfigured.

In these latter experiments, we observe and exploit a regular structure in the quantum probability distribution generated by a circuit of continuously coupled waveguides, which arises from a phenomenon related to boson bunching, which we term *bosonic clouding*. This describes the increased tendency of indistinguishable photons to cluster in different but nearby modes, in a superposition around two separate locations, when compared to distinguishable photons. Our observation of this basic behaviour of particles is of fundamental interest, moreover the emergence of bosonic clouds provides a way to predict multimode correlations in the transition from the classical to the quantum regime without having to calculate the matrix permanents.

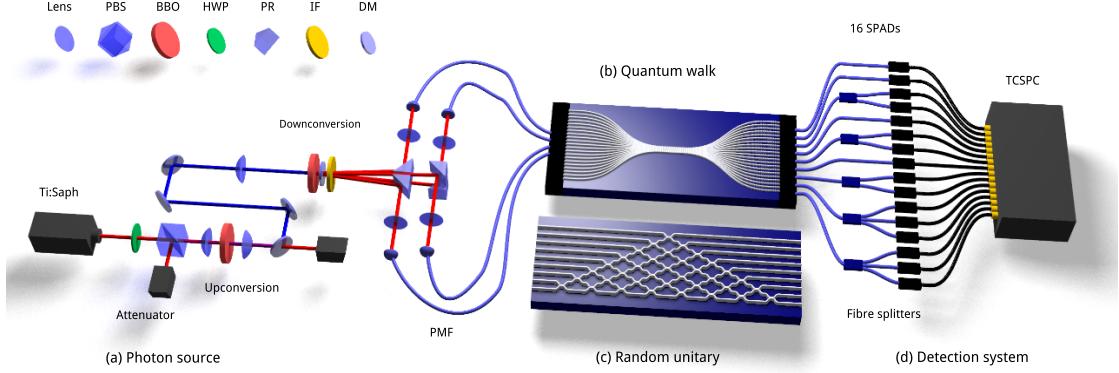
We experimentally implement our verification methods with 3, 4, and 5 photon ensembles propagating in arrays of up to 21 waveguides. We demonstrate that with relatively few events, quantum complexity can be verified in  $> 50,000$  dimensional Hilbert spaces, exemplifying the enormity of the challenge faced by verification techniques as experiments grow in size and complexity

### EXPERIMENTAL RESOURCES

All experiments presented use the hardware shown in Fig. 5.4. We use the multi-photon source described in detail in Section 3.3, and two waveguide circuits which we label as RU and QW. The RU chip is the passive nine-mode silicon nitride linear optical processor described in Section 3.5.3, comprising directional couplers and fixed phase shifts fabricated to realise a random unitary. The QW chip is the planar array of 21 evanescently coupled single mode waveguides fabricated in silicon oxynitride and described in Section 3.5.2.

## 5.5. UNIFORM DISTRIBUTION

---



**Figure 5.4: LPU for experimental verification.** Experimental setup to generate (a), interfere (b,c) and detect (d) single photons. (a) Two pairs of 780 nm photons are generated from a multi-photon source and injected into either (b) the QW chip, or (c) the RU chip. Outgoing photons are coupled from the chip either directly to 16 single photon avalanche diodes (SPADs) (d), or via a network of fibre splitters. Detection events are time-correlated and counted using a 16-channel time-correlated single photon counting system (TCSPC). A full description of hardware is given in Chapter 3.

## 5.5 UNIFORM DISTRIBUTION

The task of verification in linear optics was first brought to light by Gogolin et al. [225] who proved that in the black box setting, boson sampling with an optical network described by a random unitary matrix is operationally indistinguishable from the case where detection events are drawn from an unbiased or flat probability distribution  $\mathcal{F}$  (i.e. uniformly from the basis  $d_p^m$ ); with discrimination between the two only becoming possible after an exponential number of trials.

Their proof captures the essence of verification whereby an experimentalist with no information about a system requires exponential time to verify its quantum nature. Simply put: a black box claiming to be performing boson sampling (that is a quantum optics setup costing  $\mathcal{O}(\mathcal{L}100,000)$  and requiring  $\mathcal{O}(\text{months})$  of experimental effort) cannot be distinguished from the single line of Mathematica code:

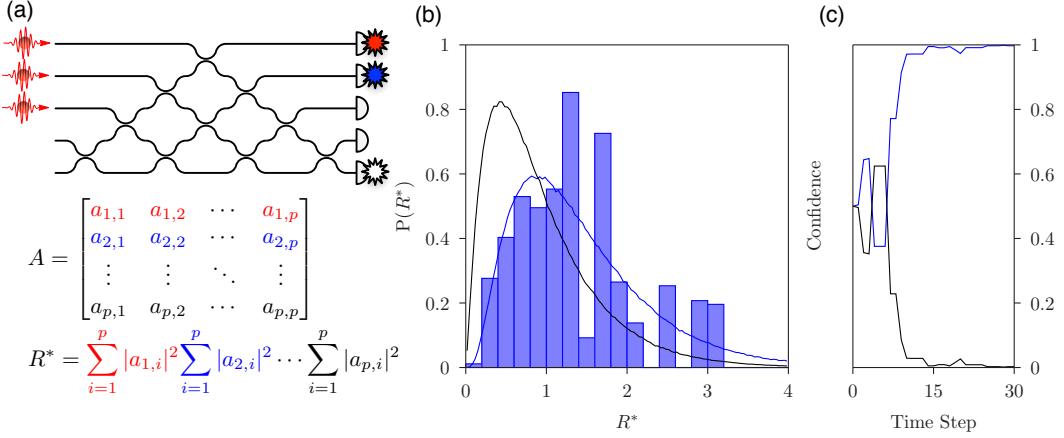


Figure 5.5: **Verification against the uniform distribution.** (a) For each event a value of  $R^*$  is recorded from the detection sub-matrix  $A$ . (b) The expected probability density function for values of  $R^*$  averaged over the Haar measure, with sub-matrices chosen from  $\mathcal{B}$  (blue line), and the uniform distribution (black line). The bars show a histogram of  $R^*$  values from experimental three photon data using the RU chip. (c) Dynamic updating using Bayesian model comparison for confidence in sampling from boson sampling distribution, rather than the uniform distribution.

```
RandomVariate[DiscreteUniformDistribution[1,Binomial[m,p]]].
```

If however, as AA show [224], the experimentalist has some information about the system — namely the unitary description of the device — efficient verification can be achieved. Note from Chapter 4, even if a priori unknown,  $\hat{U}$  can be efficiently accessed and is therefore a reasonable piece of information. Their approach is to construct a discriminator which, whilst efficiently accessible, yields different results when sampled from  $\mathcal{B}$  and  $\mathcal{F}$ . Specifically, the discriminator  $R^*$  is the product of squared row 2-norms of the  $p \times p$  sub-matrix  $A$  that describes the transformation of  $p$  photons through the circuit.

Concretely, for every detection event we write down the submatrix consisting of the  $p$  input columns and  $p$  output rows to give a matrix  $A \in \mathbb{C}^{p \times p}$ , then for each row calculate  $R_i = |a_{i,1}|^2 + |a_{i,2}|^2 + \cdots + |a_{i,p}|^2$  and take the product  $R^* = \prod_i^p R_i$ , normalising such that  $E[R^*] = 1$  [shown in Fig 5.5(a)]. Aaronson and Arkhipov

## 5.5. UNIFORM DISTRIBUTION

---

prove that for  $m \geq p^{5.1}/\delta$  with sufficiently large  $p$ , and with probability  $1 - \mathcal{O}(\delta)$

$$\Pr[R^* \geq 1 | \mathcal{B}] - \Pr[R^* \geq 1 | \mathcal{F}] \geq \frac{1}{9}. \quad (5.5)$$

In other words, with high probability  $\mathcal{F}$  and  $\mathcal{B}$  have constant variation distance, thus on average  $R^*$  will be larger when sampled from  $\mathcal{B}$  than  $\mathcal{F}$  (see Fig 5.5(b), solid lines). The intuition being that larger  $|\text{perm}(A)|^2$  values are more probable (by definition), and  $R^*$  is sufficiently correlated with  $|\text{perm}(A)|^2$ , but efficiently computable in  $\mathcal{O}(p^2)$ .

### 5.5.1 EXPERIMENT

We demonstrated this protocol using the three photon postselected state  $|111\rangle$  injected into modes  $\{1, 2, 3\}$  of the  $m = 9$  mode RU chip whose unitary description was reconstructed in Section 4.3. Over a period of five days we collected 434 three-fold detections events, and hence 434 values of  $R^*$ , a histogram of which is shown in Fig. 5.5(b) together with numerical plots of expected bosonic ( $\mathcal{B}$ ) and flat ( $\mathcal{F}$ ) distributions obtained by averaging over  $10^5$  Haar random unitaries. From this we can see that our results are at least consistent with sampling from  $\mathcal{B}$ .

To quantify this performance, we use Bayesian model comparison to update in real time our relative confidence that the samples were drawn from  $\mathcal{B}$  rather than  $\mathcal{F}$ . The choice of a Bayesian approach is motivated by the ability to perform real-time analysis. Since the computational cost of the experiment is mostly determined by the number of detection events, we want to be able to make the most of each event.

We have determined numerically (by averaging over  $10^5$  Haar random unitaries) that for the case of  $p = 3$  photons and  $m = 9$  modes:

$$\begin{aligned} P((R^* > 1) | \mathcal{B}) &= 0.631, \\ P((R^* < 1) | \mathcal{B}) &= 0.369, \\ P((R^* > 1) | \mathcal{F}) &= 0.355, \\ P((R^* < 1) | \mathcal{F}) &= 0.645. \end{aligned}$$

Given these probabilities we can use the value of  $R^*$  computed from a detection event to update our confidence that the device is sampling from  $\mathcal{B}$  rather than  $\mathcal{F}$  according to Bayes' theorem

$$P(\mathcal{H}|R^*) = \frac{P(R^*|\mathcal{H}) P(\mathcal{H})}{P(R^*)},$$

where for  $\mathcal{H}$  we substitute either  $\mathcal{B}$  or  $\mathcal{F}$ . Our prior is  $P(\mathcal{B}) = P(\mathcal{F}) = 0.5$ .

Figure 5.5(c) plots confidence that we are sampling from  $\mathcal{B}$  not  $\mathcal{F}$ . After only 12 three-fold detection events a confidence level of 90% that sampling is not from  $\mathcal{F}$  is achieved, which rises to  $1 - 10^{-35}$  by the end of the experiment. This rapid speed at which confidence is achieved demonstrates the power of Bayesian model comparison, a technique we put to use for six photon verification in Section 6.7.1.

These results demonstrate experimental events depend non-trivially on the circuit configuration. However, in reality this is rarely a concern. In the following we construct a protocol to verify against a more experimentally relevant distribution.

## 5.6 CLASSICAL DISTRIBUTION

A more physically relevant probability distribution to rule out which is classically simulatable, is that which is generated when photons become distinguishable, which we label as  $\mathcal{C}$ . This distribution can be efficiently simulated in a number ways: either by noting from Section 5.3.2 that the matrix has entirely real values so the permanent can be efficiently evaluated by the algorithm of Jerrum, Sinclair and Vigoda [212]. Or more simply, by noting that a sample can be taken by  $p$  separate single photon experiments (since they photons do not interfere), which takes time  $\mathcal{O}(p)$ .

While  $R^*$  discriminates between  $\mathcal{B}$  and  $\mathcal{F}$ , it does not discriminate between  $\mathcal{B}$  and  $\mathcal{C}$ . Indistinguishability among photons may be verified at source [92], yet the circuit may introduce distinguishability through decoherence, dispersion and other extra unwanted degrees of freedom such as polarisation. We therefore implement a scalable method to verify that photon indistinguishability is maintained during

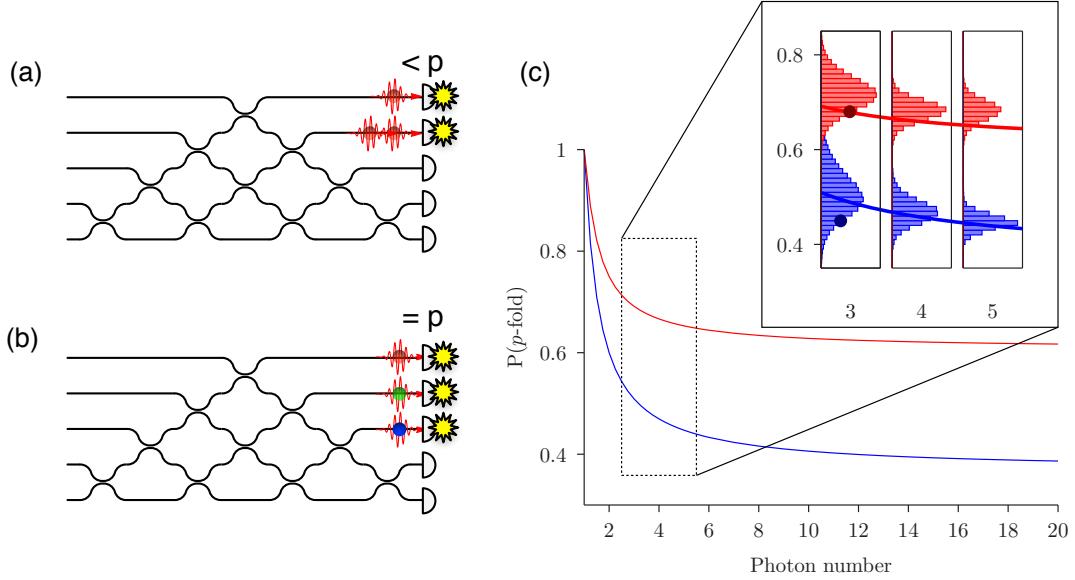


Figure 5.6: **Verification against the classical distribution.** (a) Indistinguishable photons (b) Distinguishable photons, (c) Probability of finding  $p$  photons at  $p$  detectors (that is, no bunching) for quantum (blue) and classical (red) particles. Lines are theoretical asymptotic values with the constraint  $m = p^2$ , and histograms (inset) are for theoretically simulated data for up to five photons in 25 modes. Values calculated from our experimental data are shown by the circles in the histograms for three photons in nine modes.

propagation through the circuit, based upon the question:

*Given a  $p$ -photon input state in  $p$  modes (one photon per mode) what is the probability  $P(p\text{-fold})$  of observing a  $p$ -fold detection event (i.e. finding  $p$  photons at  $p$  detectors)?*

The intuition is that  $p$ -fold detection is *less* likely for *indistinguishable* photons due to bosonic bunching [Fig. 5.6(a,b)]. This is formalised by Arkhipov and Kuiperberg [226] whereby a simple counting argument shows that for  $p$  indistinguishable photons in  $m$  modes, when averaged over the Haar measure,  $P^Q(p\text{-fold}) = |d_p^m|/|D_p^m| = \binom{m}{p} / \binom{m+p-1}{p}$ . To extend their result we use a similar argument to show that in the case of distinguishable photons  $P^C(p\text{-fold}) = \binom{m}{p} p! / m^p$ , as in the classical *birthday paradox*.

The bosonic birthday ‘paradox’ occurs when  $m \gg p^2$  and  $P^C(p\text{-fold}) \approx P^Q(p\text{-fold})$  [195]. If however  $m = p^2$  then  $P^C(p\text{-fold}) > P^Q(p\text{-fold})$ , as can be seen in Fig. 5.6(c). In the limit of large  $p$ ,  $P^Q(p\text{-fold}) = 1/e$  and  $P^C(p\text{-fold}) = 1/\sqrt{e}$ . The protocol requires  $N$  trials of  $p$ -photon input states, which gives rise to  $M$   $p$ -fold detections, allowing the comparison  $M/N$  to the analytic values of  $P^Q(p\text{-fold})$  and  $P^C(p\text{-fold})$ . Clearly as  $P(p\text{-fold})$  does not vanish, this test is scalable.

### 5.6.1 EXPERIMENT

The non-deterministic nature of the down-conversion process, along with circuit loss, makes directly knowing the number of input trails  $N$ , and hence  $P(p\text{-fold})$  problematic; however the method of Spagnolo et al. [195] allows it to be estimated. Firstly, by delaying two arms of the down-conversion source via motor controlled actuators at the collection stage we can introduce temporal distinguishability between the photons to collect  $M^C$  classical events. Next, we maximise the indistinguishability and for the same amount of time collect  $M^Q$  quantum events. Assuming the number of events that entered the device were the same in both cases (confirmed by the total number of single photon events in both experiments) we can estimate the ratio  $M^Q/M^C = P^Q(p\text{-fold})/P^C(p\text{-fold})$ . By using single photon experiments to calculate  $P^C(p\text{-fold})$  we can then estimate  $P^Q(p\text{-fold})$ .

We found  $P^Q(p\text{-fold}) = 0.450 \pm 0.028$  (error calculated assuming Poissonian counting statistics) compared to an expected value 0.509, while the deliberate introduction of (temporal) distinguishability among photons gave  $P^C(p\text{-fold}) = 0.680 \pm 0.0002$  compared to an expected value of 0.691. Using the numerically determined probability density functions shown in Fig. 5.6(c), we estimate the probability (over Haar-random unitaries) that quantum data is the result of distinguishable particles to be  $3 \times 10^{-3}$ , while the probability that classical data is the result of indistinguishable particles is  $2 \times 10^{-2}$ .

## 5.7 PREDICTABLE QUANTUM CORRELATIONS

Taken together, the tests in Fig. 5.5 and 5.6 provide circumstantial evidence that a boson sampling machine is operating according to the laws of quantum mechanics, with non-trivial dependence on circuit parameters, and exhibiting quantum interference. However, we now present a method that gives even stronger evidence for correct operation. Consider implementing a highly structured unitary that promotes all of the essential physical features of boson sampling, including single photon and large-scale multimode multi-photon interference, but where significantly large parts of the probability distribution of  $p$ -fold detections can be determined efficiently, classically, without calculating matrix permanents. After experimentally confirming correct multimode correlations, the optical circuit is continuously tuned to realise a unitary operation, such as a Haar random unitary, with classically intractable matrix permanents that produce classically unpredictable multimode correlations. The reasonable assumption is that correct operation is maintained during the tuning. Such a protocol could be realised by highly reconfigurable circuitry (see Chapter 6). In this proof of principle experimental demonstration — at the classically tractable scale where correct sampling from both probability distributions can be verified — we physically swap between circuits. The structured unitary operation we choose is the QW chip of continuously coupled waveguides [192] which exhibits *bosonic clouding*.

### 5.7.1 CLASSICAL WALKS

The classical random walk can be most intuitively understood by considering a so-called walker evolving on a  $D$  vertex one-dimensional graph via a discrete Markovian process. The walker starts in the middle of this graph then flips a coin. If it lands heads she moves right, tails she moves left. If she repeats this  $N$  times the probability to be at a given position  $d$  is given by

$$P(d) = \frac{1}{2^N} \binom{N}{\frac{N+d}{2}}, \quad (5.6)$$

which after many flips, can be approximated as a Gaussian with standard deviation  $\sigma_C \propto \sqrt{N}$ . Random walks have been used to describe phenomena in a variety of fields; from physics (Brownian motion, the motion of gas molecules during a diffusion process, thermal noise phenomena) to genetics and economics [227, 228].

For our purpose it will be beneficial to extend this analysis to the case of continuous time classical Markov chains, where we follow the approach of Farhi and Guttman [229]. Here the walk takes place without a coin, entirely in the position space over some  $D$ -dimensional vertex set  $V$ . With the walker in some initial state  $\vec{p} = (p_1, p_2, \dots, p_{|D|})$ , a classical probability distribution over  $V$ , she evolves according to a matrix  $M$  with elements  $M_{i,j}$  that describe the probability to transition from vertex  $i$  to  $j$  in a given time step. After the first time step the probability the walker is at the  $i^{\text{th}}$  vertex is given by

$$p_i^{t+1} = \sum_j M_{i,j} p_j^t \quad (5.7)$$

thus the entire state of the walker becomes

$$\vec{p}_{t+1} = M\vec{p}_t. \quad (5.8)$$

To make this process continuous we allow transitions to occur at any time, and replace  $M$  by the generator  $H$ , which describes the probability per unit time  $\gamma_{i,j}$  of hopping from vertex  $i \rightarrow j$  such that

$$H_{i,j} = \begin{cases} -\gamma_{i,j} & \text{if } i \neq j \text{ and } i \text{ and } j \text{ connected} \\ 0 & \text{if } i \neq j \text{ and } i \text{ and } j \text{ not connected} \\ d_i \gamma_i & \text{if } i = j \end{cases}$$

where  $d_i$  is the connectivity of vertex  $i$ . To describe the evolution of our walker note that in analogy to (5.7)

$$\frac{dp_i(t)}{dt} = \sum_j H_{i,j} p_j(t) \quad (5.9)$$

which has the solution  $\vec{p}(t) = \exp(-Ht)\vec{p}(0)$ .

### 5.7.2 QUANTUM WALKS

Farhi and Guttman's insight was to replace the classical probabilities  $\vec{p}$  with quantum probability amplitudes  $|\psi\rangle = \sum_i \alpha_i |i\rangle$  over the orthonormal basis of vertices  $|i\rangle$ , the generator  $H$  with a Hamiltonian  $\hat{H}$  and the classical Markov process with the unitary evolution  $\hat{U}(t) = \exp(-i\hat{H}t)$ . In this 'quantum walk' scenario they find examples of graphs which are traversed exponentially quicker than their classical counterpart. This observation of computational advantage has since ignited fields from computer science [230–232], to biology [233, 234]; and motivated experimental realisations in a variety of physical platforms including: trapped ions [235, 236], optically trapped neutral atoms [237], NMR qubits [238] and proposals with superconducting systems [239, 240].

Photons, due to their low decoherence properties and ease of manipulation are particularly amenable to the implementation of non-interacting quantum walks. Quantum walks have been realised in bulk optics using beamsplitters [241], beam displacers [242], and fibre loops [243, 244]; but perhaps the most natural route to achieve large scale complexity is via integrated optics. The inherent phase stability of integrated optics has been used to realise quantum walks with directional couplers [19], but a more robust fabrication method and one which directly maps to our above analysis is via continuously coupled waveguides [245].

If we consider the case where  $\hat{H}$  is a nearest neighbour Hamiltonian describing the one dimensional graph

$$H_{i,j} = \begin{cases} -\gamma_{i,j} & \text{if } i = j \pm 1 \\ d_i \gamma & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

then the evolution on a single site is governed by

$$-i \frac{\partial |i\rangle}{\partial t} = d_i \gamma |i\rangle - \gamma_{i,i+1} |i+1\rangle - \gamma_{i,i-1} |i-1\rangle. \quad (5.10)$$

In comparison light evolving through weakly coupled nearest neighbour single

mode waveguides obey [245]

$$-i\frac{n}{c}\frac{\partial \hat{a}_i^\dagger}{\partial t} = \beta_i \hat{a}_i^\dagger - C_{i,i+1} \hat{a}_{i+1}^\dagger - C_{i,i-1} \hat{a}_{i-1}^\dagger, \quad (5.11)$$

where  $\beta_i$  is the propagation constant for waveguide  $i$ ,  $C_{i,j}$  is the coupling constant between adjacent cites  $i$  and  $j$  and  $\hat{a}_i^\dagger$  is the bosonic creation operator acting on mode  $i$ . Note the similarity between equations (5.10) and (5.11) is reminiscent of Feynman's quantum simulator [246]; if we can engineer a system of continuously coupled waveguides we can simulate a continuous time quantum walk [see Fig. 5.7(a)].

Evolving the single particle state via  $\hat{H}$  gives rise to the archetypal quantum walk ballistic propagation (Fig. 5.7(b), blue). However this can be entirely described via wave mechanics, and hence simulated on a classical computer [247]. To see true dynamics which cannot be efficiently simulated classically we need to introduce *multiple walkers*.

### 5.7.3 MULTI-PHOTON QUANTUM WALKS

Multi-photon quantum walks propagate multiple photons and measure correlated detection events at the output [192]. This added complexity gives rise to a much richer set of dynamics, and effectively simulates a single walker on a higher dimensional graph [18, 248]. Multi-photon quantum walks have been used to observe fermionic evolution [19, 171], phenomena such as Anderson localisation [249] and the coherent time evolution of walkers [172].

Much like in boson sampling these transition probabilities are given by matrix permanents of sub-matrices of  $\hat{U}$ . Due to a generalisation of the HOM effect, when the photons are indistinguishable a highly structured probability distribution is observed. Specifically, as shown by Peruzzo et al. [18], photons at the output are found to cluster in nearby locations, a bunching effect<sup>7</sup>, see Fig. 5.7(c). It is this structure in the output distribution we wish to use as a verifier.

---

<sup>7</sup>A beautiful experiment is reported by Rom et al. [250], whereby the opposite *fermionic anti-bunching* effect is observed for a fermionic gas released from an optical lattice.

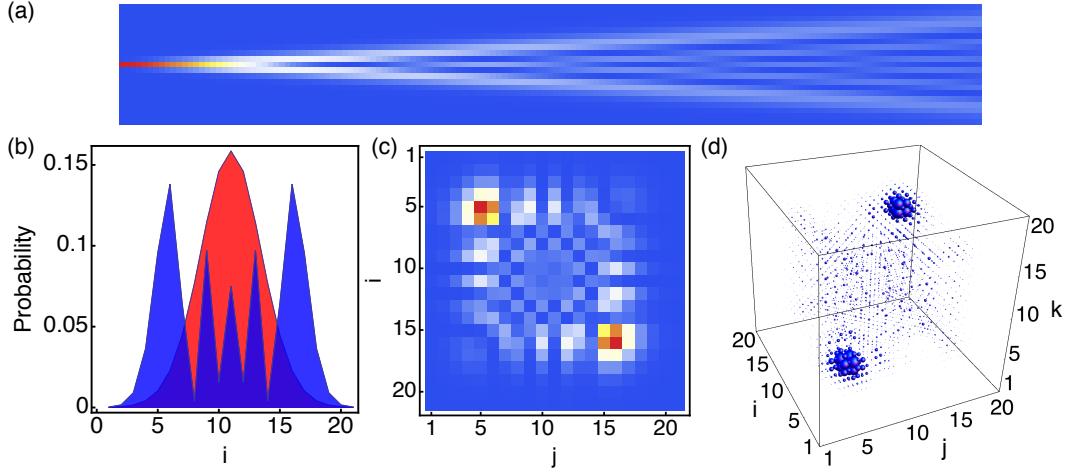
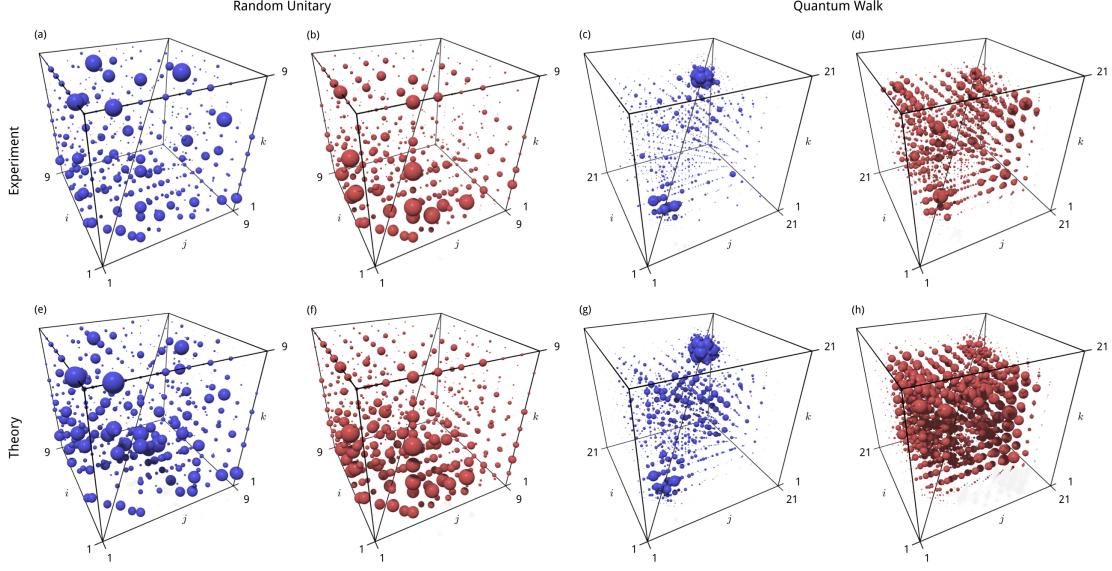


Figure 5.7: **Continuous time quantum walks.** (a) Photons propagating through an array of continuously coupled waveguides simulate a continuous time quantum walk. (b) Theoretical simulations of the single photon quantum (blue) and classical walk (red), measuring the probability to find a photon at waveguide  $i$ . (c) The two-photon case measures the *correlated* detection probability for photons in waveguides  $i$  and  $j$ . (d) Similarly, the three-photon quantum walk gives the probability (proportional to the radius of sphere) for photons in waveguides  $i, j$  and  $k$ . In (c,d) the bosonic clouding effect can clearly be seen.

#### 5.7.4 BOSONIC CLOUDING

*Bosonic clouding* describes an increased tendency for multimode correlations with indistinguishable particles clustering, in superposition, around two separate local groups of modes, when compared with distinguishable particles. To use this phenomena as a verifier we first wish to observe this effect for the three-particle case.

We inject three photons into modes  $\{10, 11, 12\}$  of the 21 mode QW chip. This larger circuit makes detecting the entire  $|D_3^{21}| = 1771$  possible three-photon detection events (including cases with more than one photon at a single detector) challenging. To detect a large proportion of this space we use fibre splitters and multiple detectors to achieve nondeterministic number resolved photon detection.



**Figure 5.8: The absence and emergence of multimode correlations in the form of bosonic clouds in three-photon correlation cubes for a 21 mode quantum walk.** The radii of spheres centred at coordinates  $(i, j, k)$  are proportional to the probability of finding three photons in output modes  $i$ ,  $j$  and  $k$  respectively. We tune between indistinguishable (blue) and distinguishable (red) photons by introducing a time delay between them. These data are: (a), Experimental nine mode random unitary with indistinguishable and (b) distinguishable photons. (c), Bosonic clouds from experimental 21 mode quantum walk unitary with indistinguishable and (d) distinguishable photons. (e), Theoretical nine mode random unitary with indistinguishable and (f) distinguishable photons. (g), Theoretical bosonic clouds from 21 mode quantum walk unitary with indistinguishable and (h) distinguishable photons. The experimental data (top row) has been corrected for detector efficiencies and the theory has been filtered to show only events that were experimentally measured, which is the main reason for the apparent asymmetry between the pair of boson clouds.

## 5.7. PREDICTABLE QUANTUM CORRELATIONS

---

Which along with multiple measurements in different configurations allow us to access 524/1771 possible events.

We use eight separate measurements, corresponding to different configurations of the detection apparatus. Writing the number of detectors  $d$  connected to an output port  $i$  as  $d_i$ , these detection configurations can be described as:

$$\begin{aligned} M_1 &= \{3_1 3_2 3_3 3_4 3_5\}; M_2 = \{3_6 3_7 3_8 3_9 3_{10}\}; M_3 = \{3_{11} 3_{12} 3_{13} 3_{14}\}; M_4 = \{3_{15} 3_{16} 3_{17} 3_{18}\}; \\ M_5 &= \{1_1 2_3 1_5 2_7 1_9 2_{11} 1_{13} 2_{15} 1_{17} 2_{19}\}; M_6 = \{2_1 1_3 2_5 1_7 2_9 1_{11} 2_{13} 1_{15} 2_{17} 1_{19}\}; \\ M_7 &= \{1_2 2_4 1_6 2_8 1_{10} 2_{12} 1_{14} 2_{16} 1_{18} 2_{20}\}; M_8 = \{2_{14} 2_6 1_8 2_{10} 1_{12} 2_{14} 1_{16} 2_{18} 1_{20}\}. \end{aligned}$$

Where  $M_1-M_4$  address the main diagonal of the correlation matrix  $i = j = k$ . The probability distribution is reconstructed by summing count rates over all measurement settings, and then compensating for detection efficiency based on a model of the measurement apparatus.

For the case of indistinguishable photons we collect 3870 three-photon detection events which is sufficient to saturate and reproduce the QW chip probability distribution, shown in Fig. 5.8(c). We then repeat this for distinguishable photons by temporally delaying two of the three photons and collect 5588 events, shown in Fig. 5.8(d) We found a statistical fidelity  $\mathcal{F}_s = \sum_i \sqrt{p_i^{exp} p_i^{th}}$  between the normalised theoretical  $p_i^{th}$  and experimental  $p_i^{exp}$  probability distributions of  $\mathcal{F}_s^q = 0.930 \pm 0.003$  and  $\mathcal{F}_s^c = 0.961 \pm 0.002$  for the indistinguishable and distinguishable case respectively. Error bars are calculated by propagating Poissonian count rate errors. The deviation from unit fidelity can be attributed to unwanted temporal distinguishability among photons and higher order terms (see Section 3.3).

Bosonic clouding behaviour can be clearly seen for indistinguishable photons in Fig. 5.8(c). That is, photons cluster around the main diagonal line of the correlation cube, where probabilities exactly on this line correspond to full bunching of all three photons in the same mode. Two clouds have formed at separate locations in the cube centred on modes 6 and 16. If one photon is detected in the locality of mode 16 (for example), the remaining two photons have a higher probability of being correlated to this event and also detected around mode 16. In contrast,

when temporal distinguishability is introduced between all photons [Fig. 5.8(d)], quantum interference is destroyed and the clouds dissipate: there is now a higher probability that the two remaining photons will be found away from the modes local to mode 16.

For further comparison, we have also presented all possible 84 (non-bunched) three-photon correlated detection probabilities in the RU chip in Fig. 5.8(a,b,e,f). We note that the clouds observed in Fig. 5.8(c) are absent in the RU chip for both indistinguishable [Fig. 5.8(a)] and distinguishable photons [Fig. 5.8(b)]; the correlation cubes do not reveal any discernible structure. Here, we found a fidelity between our experiment and theoretical model of  $\mathcal{F}_s^q = 0.939 \pm 0.010$  and  $\mathcal{F}_s^c = 0.970 \pm 0.007$ , for indistinguishable and distinguishable photons, respectively.

### 5.7.5 EFFICIENT VERIFICATION

Let us formalise this notion of clouding and construct an efficient metric with which we can verify and quantify multimode correlations in quantum walk experiments. The metric works by assigning a value  $-1 \leq c \leq +1$  to each trial:  $+1$  is awarded when all  $p$  photons are found in either the upper or the lower half of the chip [Fig 5.9(a)];  $-1$  is awarded if exactly  $p/2$  photons are found at both sides of the chip [Fig 5.9(b)]; and intermediate values are linearly interpolated for approximate clouding [Fig 5.9(c)]. More precisely, with  $t$  and  $b$  the number of photons found, respectively, in the top and bottom half of the chip,  $c_i = 2|(t - b)/(t + b)| - 1$  for the  $i^{th}$  trial and the clouding metric  $C = 1/n \sum_i c_i$  is calculated as the average over all  $n$  trials. To make our metric suitable to standard detectors that do not give information on the number of photons received, here  $C$  does not include bunching terms (when more than one photon arrives at a single detector) which we expect would enhance the clouding metric.

Exact numerical simulations for up to  $p = 7$  photons in  $p^2$  modes confirm that  $C$  efficiently reveals clouding, discriminating between indistinguishable and distinguishable photons. Approximate Monte Carlo numerical simulations support

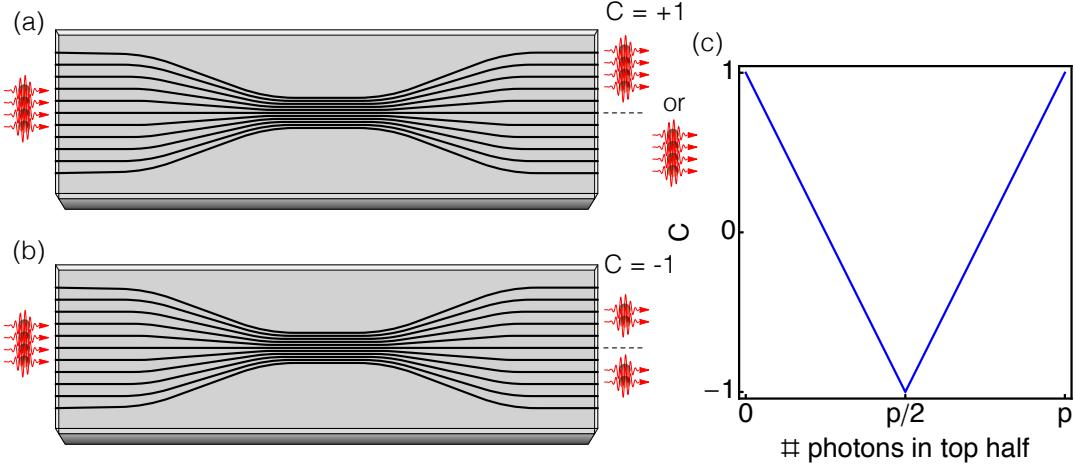


Figure 5.9: **Bosonic clouding metric.** (a) If all photons are maximally clouded and in the same half  $C = +1$  is awarded and if (b) photons are not clouded and equally distributed  $C = -1$  is awarded. (c) This function is continuous allowing for approximate clouding.

the efficiency of the clouding metric  $C$  for up to  $p = 14$  photons in  $p^2$  modes.

#### FOUR PHOTON SIFT

We evaluated this metric with three, four and five photons. In the four photon case we inject one photon per mode into the central  $\{9, 10, 11, 12\}$  waveguides. As discussed in Section 3.2.3, unlike the three photon case an efficient postselection technique to isolate  $|1111\rangle$  does not exist with just two down-convertors. However, we have developed a technique to effectively sift this state from the entire four mode down-conversion state. To see this recall the (unnormalised) four mode down-conversion state in the four photon subspace is

$$|\Psi_{4DC}\rangle = |\Psi_{DC}^1\rangle \otimes |\Psi_{DC}^2\rangle \quad (5.12)$$

$$\begin{aligned} &= e^{i(\phi_1+\phi_2+\phi_3+\phi_4)} |1111\rangle \\ &+ e^{2i(\phi_3+\phi_4)} |0022\rangle + e^{2i(\phi_1+\phi_2)} |2200\rangle, \end{aligned} \quad (5.13)$$

where  $\phi_i$  is an unknown phase on mode  $i$  due to the path length difference from crystal to chip. The density matrix for this state is

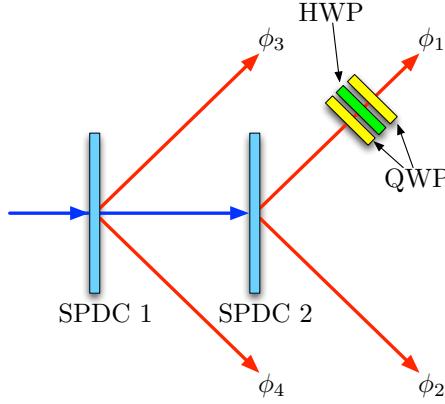


Figure 5.10: **Four photon sifting.** Half and quarter wave plates are placed in one arm of the four mode down-conversion source, and data summed, to force the maximally mixed input state  $\rho_{\text{mix}}$ .

$$\rho_{\text{DC}} = |\Psi_{4\text{DC}}\rangle \langle \Psi_{4\text{DC}}| \quad (5.14)$$

$$= \begin{bmatrix} 1 & e^{i(\phi_1+\phi_2-\phi_3-\phi_4)} & e^{-i(\phi_1+\phi_2-\phi_3-\phi_4)} \\ e^{-i(\phi_1+\phi_2-\phi_3-\phi_4)} & 1 & e^{-2i(\phi_1+\phi_2-\phi_3-\phi_4)} \\ e^{i(\phi_1+\phi_2-\phi_3-\phi_4)} & e^{2i(\phi_1+\phi_2-\phi_3-\phi_4)} & 1 \end{bmatrix}. \quad (5.15)$$

Consider applying a phase  $\theta$  to mode 1 so the entire phase on that arm is now  $\theta + \phi_1$  [see Fig. 5.10], we represent this state as  $\rho_{\text{DC}}(\theta)$ . This can be achieved by inserting half (H) and quarter (Q) wave plates in that mode in the configuration  $Q(\pi/4)H(\theta/4 + \pi/4)Q(\pi/4)$ . It is straightforward to verify that

$$\rho_{\text{mix}} = \rho(0) + \rho(\pi/2) + \rho(\pi) + \rho(3\pi/2) \quad (5.16)$$

$$= |1111\rangle \langle 1111| + |0022\rangle \langle 0022| + |2200\rangle \langle 0022|, \quad (5.17)$$

hence summing data at  $\theta = \{0, \pi/2, \pi, 3\pi/2\}$  yields the same results as a maximally mixed state. We then separately input the two-mode state on modes  $\{1,2\}$  and  $\{3,4\}$ , yielding data for  $\rho_{2200} = |2200\rangle \langle 2200|$  and  $\rho_{0022} = |0022\rangle \langle 0022|$ , which can be subtracted from the  $\rho_{\text{mix}}$  data to give  $|1111\rangle$ . A few remarks: First, this method does not scale efficiently in photon number, and second neither would we want to; the coherences are postselected, and not useful for any kind of processing further down the line. However, for our purpose, it serves to test our clouding metric

## 5.7. PREDICTABLE QUANTUM CORRELATIONS

---

with added complexity. Finally, we note the phases  $\phi_i$  in general are a function of time. However, our scheme yields statistics for the  $\rho_{\text{mix}}$  independent of the speed of phase fluctuation, provided  $\phi_i$  is not correlated with the phase  $\theta$ .

## RESULTS

The mean values of  $C$  for the three-, four- and five-photon experiments are shown in Fig. 5.11(c-f), for indistinguishable and distinguishable photons, alongside ideal theoretical distributions, given the same number of events. Experimental imperfections result in non-ideal values of  $C$ , so we calculate the *change* in clouding between distinguishable and indistinguishable photons,  $\Delta C = C_Q - C_C$ , as a witness for the emergence of clouds.

For  $p = 3$  photons we find  $\Delta C = 0.138 \pm 0.014$ , compared to a numerically determined value of  $0.169 \pm 0.014$ , see Fig. 5.11(c). For  $p = 4$  photons we measure 1016 out of a possible 10626 four-fold, registering 50,000 events over a period of  $\sim 1$  week, as shown in Fig. 5.11(a,b). The fidelity between experimental and theoretical probability distributions, for both indistinguishable and distinguishable photons, was found to be  $F_Q = 0.971 \pm 0.001$  and  $F_C = 0.978 \pm 0.0004$ . We evaluated the clouding to be  $\Delta C = 0.137 \pm 0.008$  compared to a numerically determined value of  $0.145 \pm 0.008$ , as shown in Fig. 5.11(d). The deviation from theory is primarily due to the complexity of the sifting procedure (experimental fluctuations over long data runs), but the emergence of bosonic clouding can clearly be seen.

During the course of this data run our detection system registered 217 five-fold detection events, originating from a six-photon down-conversion event and a lost photon (so the state was partially mixed). For  $p = 5$  photons in  $m = 21$  modes the Hilbert space dimension is  $|D_5^{21}| = 53,130$ . Due to this vast Hilbert space size, and small number of detection events, no single event was recorded more than once exemplifying the challenge of verification as quantum systems grow. In this case, full probability distributions are meaningless and fidelities cannot be evaluated. However our metric still found a statistically significant separation of  $\Delta C = 0.137 \pm 0.041$  compared to a numerically determined value of

$\Delta C = 0.106 \pm 0.041$ , shown in Fig 5.11(e).

Finally clouding for  $p = 3$  photons in the random unitary is shown for comparison in Fig. 5.11(f), with  $\Delta C = -0.014 \pm 0.029$  compared to a numerical value of  $0.044 \pm 0.028$ , which is consistent with the absence of clouding.

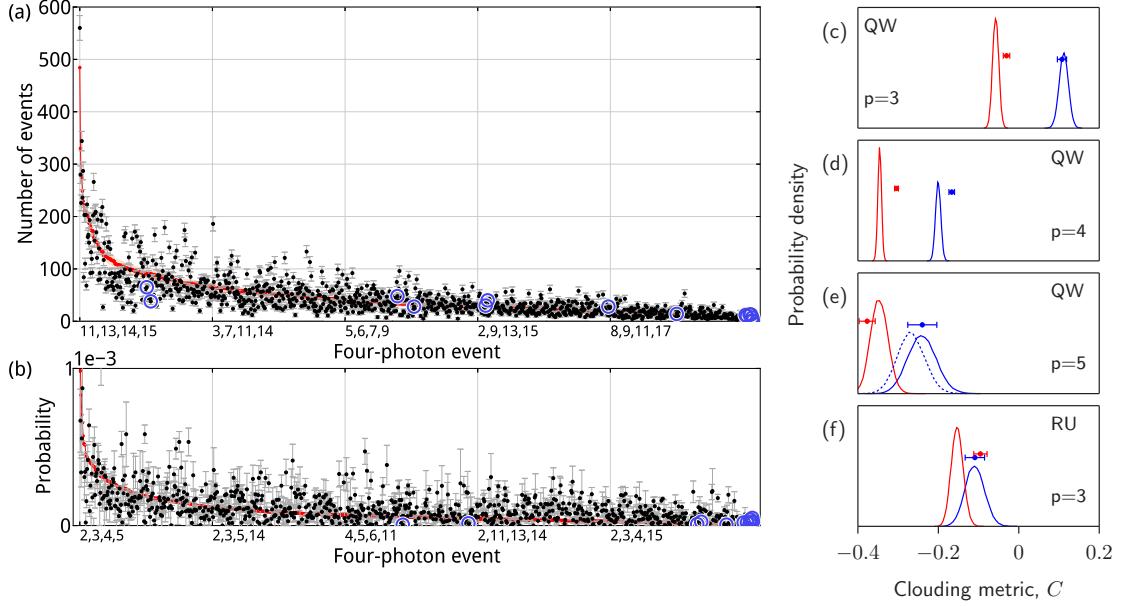
## 5.8 CONCLUDING REMARKS

We have shown how to exploit the intrinsic physical properties of a quantum system, configured to a verifiable mode of operation, to assess its level of performance. If the experimentalist possess no information about this system, this cannot be done efficiently. If however the experimentalist possess some knowledge about the system; such as the circuit describing the operation (in the case of verifying against a uniform distribution), the class of particles (in the case of verifying against a classical distribution) or an expected probability distribution (in the case of verifying a multi-photon quantum walk), efficient verification can be achieved. Positive assessment is then cited as evidence that the system is performing correctly when configured to an unverifiable mode of operation, such as the implementation of a quantum algorithm that is mathematically unverifiable.

As experiments grow in complexity, it is likely new error sources will emerge which can rise to classical tractability. We therefore expect new machine level verification protocols to appear. One such example, for which there are solid analytical results, is the predictable probability distribution due to quantum interference in a Fourier transforms [251]. We examine this protocol in the following chapter. Whilst we have demonstrated the efficacy of this approach in the context of boson sampling, machine level verification techniques like these are likely to find application in other analogue quantum simulators which exhibit their own physical traits, such as large scale quantum annealing machines [252, 253], ion traps with hundreds of spins [254], and fermionic gasses which exhibit anti-bunching [250].

## 5.8. CONCLUDING REMARKS

---



**Figure 5.11: Experimental clouding results.** (a) Experimental data for four indistinguishable photons into QW, with black points showing 1016 of the possible 10626 detection patterns, ordered by descending theoretical probability (red points). Data circled in blue identify cases of partial or full bunching, which are not included in the clouding metrics here. Error bars are calculated from Poissonian statistics. Here, the input state includes unwanted terms with more than one photon per mode. (b) Unwanted parts of the input state are sifted out, so that it approximates to one photon per mode. In (c-e) we show the results from evaluating our clouding metric  $C$  for  $p = 3, 4, 5$  photons. Experimental points with horizontal error bars are shown in blue for indistinguishable photons, in red for distinguishable photons, and theoretically reconstructed distributions from the same number of samples are shown as solid lines. For 3 and 4 photons, the increase in  $C$  is statistically significant. The separation is reduced for the partially mixed state of 5 indistinguishable photons across four modes, yet still observable with only 217 counts. (e) Theoretically predicted fall in clouding (blue dotted line) when one of the 5 photons becomes distinguishable. In (f) we show results from the same test for 3 photons in a 9-mode random unitary and observe no significant levels of clouding as expected, showing that our test is sensitive to the implemented unitary.

---

## 5. VERIFYING QUANTUM COMPLEXITY

*Computers can do lots of things. They can add millions of numbers together in the twinkling of an eye. They can outwit chess grandmasters. They can guide weapons to their targets. They can book you onto a plane between a guitar-strumming nun and a non-smoking physics professor. Some can even play the bongos. Thats quite a variety!*

Richard Feynman

# 6

## Universal Linear Optics

### STATEMENT OF WORK

The work presented in this chapter was published in Carolan et al. *Science* **349**, 711 (2015) [255]. The universal linear optical device was conceived by A. Laing who supervised the project, and designed and fabricated by N. Matsuda and colleagues at Nippon Telegraph and Telecom Corporation. The majority of experimental work (characterisation, calibration, data taking) was due to myself, C. Harrold and N. Matsuda. The characterisation protocol was proposed by myself and N. Russell. The phase accuracy benchmarking protocol was proposed and analysed by myself, as were the boson sampling procedures. The complex Hadamard matrices were proposed and developed by E. Martín-Lopez and A. Laing, and analysed by myself. The six photon verification experiment was proposed by myself and A.

Laing and analysed by N. Russell. Preceding the device presented here, myself and C. Harold packaged and tested a universal silicon nitride device (not presented) which was judged to be below performance threshold.

### 6.1 INTRODUCTION

From smart phones to swiss army knives, multifunctional technologies have had profound impact on society. Since the time of Turing, universal machines have enabled both conceptual and practical advances: for the former, the concept of universality has provided us with a deep understanding of the relationships between algorithms, allowing the discovery of new protocols and applications. For the latter, programmable machines place ultimate power in the hands of the programmer. They liberate. It is almost inconceivable to imagine society, industry or science without programmable computers; and there are very few technologies with which we can make such bold claims.

We have so far seen how a linear optical processor (LPU) equipped with passive waveguide technology, can be harnessed to explore the boundaries of quantum complexity. In this chapter we show that with the addition of active reconfigurability we can significantly increase capabilities of LPU's. Specifically we demonstrate a single reprogrammable optical circuit that is sufficient to implement all possible linear optical protocols up to the size of that circuit. Our six-mode universal system consists of a cascade of 15 Mach-Zehnder interferometers with 30 thermo-optic phase shifters integrated into a single photonic chip that is electrically and optically interfaced for arbitrary setting of all phase shifters, input of up to six photons, and their measurement with a 12-single-photon detector system. We term this system a ‘universal LPU’. The versatility such a system affords, and the fidelity with which it operates, allows us to achieve orders of magnitude increase in quantum control and complexity compared with previous demonstrations.

We describe the key technological developments which has made possible such a device in Section 6.3, and in Section 6.4 and 6.5 propose and demonstrate full

characterisation and benchmarking procedures. We perform one hundred different boson sampling experiments in Section 6.6, and extend our analysis of verification techniques by implementing newly proposed verification protocols on up to six photons in Section 6.7. Crucially these protocols are all implemented on the same device pointing the way towards a truly verifiable analogue quantum simulator. Finally, in Section 6.8 we use multi-particle quantum interference to distinguish six-dimensional complex Hadamard operations, including newly discovered examples, where full classification remains an open mathematical problem. The results presented required reconfiguration of this single device to implement  $\sim 500$  experiments.

## 6.2 UNIVERSAL CIRCUITS

We've seen throughout this thesis that linear optical circuits are described by unitary operators. Here we ask: *what class of circuits give rise to unitary operators?* Does each gate, algorithm or unitary we wish to implement require distinct circuitry? The answer to this question is emphatically *no*. A single photonic device, configured in such a way is sufficient to realise all possible linear optical unitaries up to the size of the circuit. The original proof was given in 1994 by Reck et al. [27], but here we give a physically intuitive proof of this theorem. Not only is this of fundamental interest, but it will also be the method with which we programme circuits onto our device.

To find the circuit for an arbitrary  $m \times m$  unitary  $\hat{U}$ , we can imagine the  $m$ -mode linear optical box implementing  $\hat{U}$ . The aim is to build a new circuit  $\hat{U}'$  such that  $\hat{U}'\hat{U} = \hat{I}$ , and hence  $\hat{U}^\dagger = \hat{U}'$ . In other words, *if we can build  $\hat{U}'$  we've found the circuit for  $\hat{U}$* <sup>1</sup>.

To do this consider injecting single photons into the first mode of the linear optical box, this generates an  $m$ -dimensional output vector  $\hat{U}|1\rangle = |\psi_1\rangle$ , which

---

<sup>1</sup>Technically, the circuit for  $\hat{U}^\dagger$  has been found, but this is easily fixed by taking the conjugate transpose of  $\hat{U}$  in the first instance.

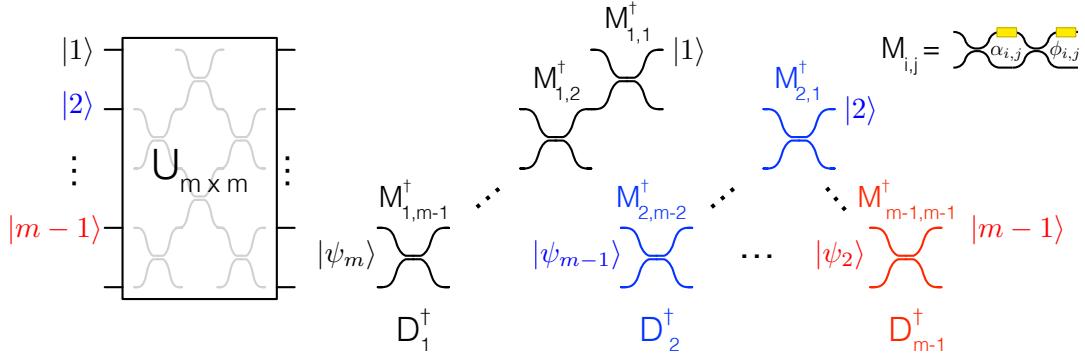


Figure 6.1: **Building a universal circuit.** To find the circuit for any  $m \times m$  unitary  $\hat{U}$ , photons are injected into the first mode of the unitary, generating a state  $|\psi_m\rangle$ , and a diagonal array  $\hat{D}_m^\dagger$  of MZI-shifters  $M_{1,i}^\dagger$  is configured to output the state  $|1\rangle$ . This is repeated for photons injected into the second mode (blue), up until the  $m - 1^{\text{th}}$  mode (red). The final unitary is implemented by  $\hat{D}_1\hat{D}_2 \cdots \hat{D}_{m-1}$ .

corresponds to the first column of  $\hat{U}$ . Let us examine  $|\psi_1\rangle$ : first, it has  $m - 1$  amplitude and  $m - 1$  phase components (due to normalisation and a global phase) hence

$$|\psi_1\rangle = a_{1,1}e^{i\varphi_{1,1}}|1\rangle + a_{1,2}e^{i\varphi_{1,2}}|2\rangle + \cdots + (1 - \sum_{i=1}^{m-1} a_{1,i}^2)|m\rangle. \quad (6.1)$$

So what type of circuit can give rise to  $|\psi_1\rangle$ ? Simply, a diagonal array of MZI's and phase shifters where each element of the diagonal is described by

$$\hat{M}(\phi, \alpha) = \hat{P}(\phi)\hat{U}_{\text{MZI}}(\alpha). \quad (6.2)$$

For clarity we recall equations (2.45) and (2.50):

$$\hat{P}(\phi) = e^{i\phi/2} \begin{bmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{bmatrix}; \quad \hat{U}_{\text{MZI}}(\alpha) = e^{i(\alpha+\pi)/2} \begin{bmatrix} \sin(\alpha/2) & \cos(\alpha/2) \\ \cos(\alpha/2) & -\sin(\alpha/2) \end{bmatrix}, \quad (6.3)$$

hence

$$\hat{M}(\phi, \alpha) = e^{i(\alpha+\pi)/2} \begin{bmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \sin(\alpha/2) & \cos(\alpha/2) \\ \cos(\alpha/2) & -\sin(\alpha/2) \end{bmatrix} \quad (6.4)$$

$$= e^{i(\alpha+\pi)/2} \begin{bmatrix} e^{i\phi} \sin(\alpha/2) & e^{i\phi} \cos(\alpha/2) \\ \cos(\alpha/2) & -\sin(\alpha/2) \end{bmatrix} \quad (6.5)$$

To generate  $|\psi_1\rangle$ , the first MZI-shifter  $\hat{M}_{1,1}(\phi_{1,1}, \alpha_{1,1})$  is configured to send  $|a_{1,1}|^2$  of power into the first mode then apply a phase  $\varphi_{1,1}$  to that mode. In the parameterisation of (6.2) we set

$$\alpha_{1,1} = 2 \sin^{-1}(a_{1,1}); \quad \phi_{1,1} = \varphi_{1,1} - (\alpha_{1,1} + \pi)/2 \quad (6.6)$$

Next, we repeat this process for  $\hat{M}_{1,2}$  such that  $|a_{1,2}|^2$  of the remaining  $1 - |a_{1,1}|^2$  power is directed into the second mode, along with a phase shift  $\varphi_{1,2}$ . Specifically we set

$$\alpha_{1,2} = 2 \sin^{-1}(a_{1,2}/(1 - a_{1,1})); \quad \phi_{1,2} = \varphi_{1,2} - (\alpha_{1,1} + \alpha_{1,2} + 2\pi)/2 \quad (6.7)$$

and repeat this process until

$$\hat{M}_{1,m-1} \hat{M}_{1,m-2} \cdots \hat{M}_{1,1} |1\rangle = |\psi_1\rangle. \quad (6.8)$$

There is a subtlety here when using directional couplers, whereby the phase on the final mode  $|m\rangle$  is non-zero, depending in some non-trivial way on the phases  $\{\alpha_{1,i}\}$ . To correct for this *all* phases  $\{\phi_{1,i}\}$  are shifted relative to this final mode. Specifically, defining the erroneous phase to be  $\varphi'_1$  the corrected phases become  $\{\phi_{1,i}^c\} = \{\phi_{1,i}^c + \varphi'_1\}$ . We note this is a technicality when using directional couplers (and not intrinsic to the proof) but is important, in practice, when finding circuits.

The diagonal array in (6.8) is also described by an  $m \times m$  unitary matrix

$$\hat{D}_1 = \hat{M}_{1,m-1} \hat{M}_{1,m-2} \cdots \hat{M}_{1,1}. \quad (6.9)$$

such that

$$\hat{D}_1 |1\rangle = |\psi_1\rangle. \quad (6.10)$$

Take this new unitary, do the conjugate transpose, and place it after  $\hat{U}$  so the entire system becomes  $\hat{D}_1^\dagger \hat{U}$  [Fig. 6.1, black]. Conveniently, this has the structure of an  $m \times m$  unitary with the top left element equal to 1, and all other elements in the corresponding row and column equal to zero. To see this note a photon input into the top mode *must* only output from the top mode

$$\hat{D}_1^\dagger \hat{U} |1\rangle = \hat{D}_1^\dagger |\psi_1\rangle \quad (6.11)$$

$$= |1\rangle \quad (6.12)$$

where the last line uses (6.10). So

$$\hat{D}_1^\dagger \hat{U} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \boxed{\hat{U}_{m-1}} \\ \vdots & & & \\ 0 & & & \end{bmatrix} \quad (6.13)$$

and we repeat this process, but this time with  $\hat{D}_1^\dagger \hat{U}$ :

1. Inject photons into the second mode
2. Generate  $m - 1$  dimensional vector  $\hat{D}_1^\dagger \hat{U} |2\rangle = |\psi_2\rangle$
3. Build the diagonal array  $\hat{D}_2$  such that  $\hat{D}_2 |2\rangle = |\psi_2\rangle$
4. Repeat with the new unitary  $\hat{D}_2 \hat{D}_1^\dagger \hat{U}$

After  $m - 1$  iterations we are left with  $\hat{D}_{m-1}^\dagger \hat{D}_{m-2}^\dagger \cdots \hat{D}_1^\dagger \hat{U} = \hat{I}$  and therefore

$$\hat{U} = \hat{D}_1 \hat{D}_2 \cdots \hat{D}_{m-1}. \quad (6.14)$$

Up to undetected output phases, this means that an  $m$ -mode circuit as per Fig. 6.3(a) with  $1/2(m^2 - m)$  MZI-shifters and full control over all  $m^2 - m$  phase shifters, is sufficient to realise *all* possible linear optical protocols up to the size of the circuit.

We say this circuit is *universal* for linear optics.

### 6.3. RECONFIGURABLE LPU

---

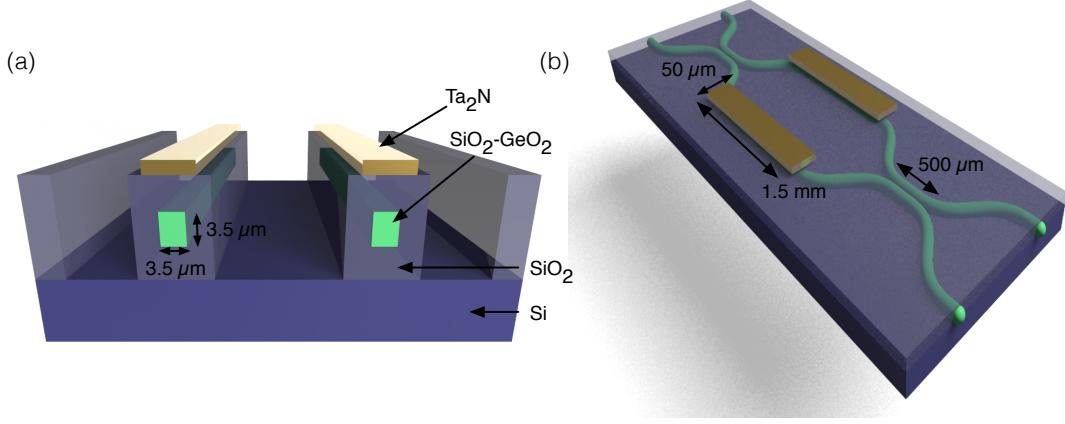


Figure 6.2: **Reconfigurable waveguide geometry.** (a) A germanium doped silica core is fabricated with a silica cladding onto a silicon substrate, and thin film tantalum nitride thermo-optic heaters are deposited on top. Heat isolation grooves are fabricated to reduce thermal cross talk and power consumption. (b) MZI geometry. See Section 3.5.1 for further details.

## 6.3 RECONFIGURABLE LPU

Realising such a scheme requires sub-wavelength stability and high fidelity components to support both classical and quantum interference — possibilities opened up by integrated quantum photonics [11–19]. The platform with which we realise this scheme is silica-on-silicon, whose waveguide geometry is shown in Figure 6.2. The circuit itself is made with planar lightwave circuit (PLC) technology [166, 256, 257], and comprises an array of 30 silica-on-silicon waveguide directional couplers with 30 electronically controlled thermo-optic phase shifters, to form a cascade of 15 MZIs across six modes. The advantage of interfacing silica based devices with a multi-photon source is the low insertion and propagation losses; we measure the mean insertion loss (fibre to fibre) averaged over all modes to be 2.4 dB (42%) — significantly lower than the 13 dB (95%) reported for the passive LPU.

The key step in realising a fully reconfigurable LPU is having a robust and accurate modulation technique. We achieve this via 30 thin-film tantalum nitride

(Ta<sub>2</sub>N) thermo-optic heaters fabricated on top of the circuit measuring 1.5mm × 50μm. To calculate the temperature change for a 2π phase shift we use the fact that the phase shift  $\Delta\phi = \Delta n \times k_0 \times L$  hence  $\Delta n = 2\pi/(2\pi/808\text{nm} \times 1.5\text{mm}) = 5.4 \times 10^{-4}$ . The thermal coefficient of Silica at room temperature (20 °C) is  $dn/dT = 1 \times 10^{-5} \text{ }^{\circ}\text{C}^{-1}$  thus  $\Delta T = (dn/dt)^{-1} \times \Delta n = 54 \text{ }^{\circ}\text{C}$ , which at room temperature requires 74 °C to give a 2π phase shift. To calculate the resistance  $R$  of each heater note the resistivity of Ta<sub>2</sub>N<sup>2</sup> is  $r = 400\mu\Omega \text{ cm}^{-1}$ , using  $R = (rL)/(WT)$  with a heater thickness of  $T \approx 1\mu\text{m}$  gives  $R \approx 100\Omega$ , matching values measured in the lab.

The fundamental principle governing thermo-optic phase shifts is the conversion of electrical energy into heat energy (see Section 3.4.3 for an atomic explanation). To estimate the switching time  $t$  for a 2π phase shift, we first calculate the energy required to raise the temperature from the mass of the heater ( $m = \rho LWT$ , where density  $\rho = 16 \text{ g mm}^{-3}$ ) the specific heat capacity of Ta<sub>2</sub>N ( $C = 0.14 \text{ J g}^{-1} \text{ }^{\circ}\text{C}^{-1}$ ) and the change in temperature  $\Delta T$  as  $E = m \times C \times \Delta T = 9 \text{ mJ}$ . Applying a power  $P \approx 0.8 \text{ W}$  (the observed power necessary for a 2π phase shift) for time  $t$  requires energy  $E = P \times t$  hence the switching time is  $t = 0.9 \times 10^{-3}/0.8 \approx 10\text{ms}$ .

This back of the envelope calculation serves as a heuristic for understanding the induced phase shift, but in reality the model is much more complicated than this; waveguide geometry considerations such as heat insulation grooves and cladding thickness also affect modulation speeds. Using NTT corporation in house simulation software, we estimate the time required for a 90% temperature change is 1.4ms. Whilst this is relatively slow by telecommunications standard (with typical switching times > GHz [152]) for our purpose clock speeds are limited by multi-photon source rates and millisecond switching suffices.

The silica-based waveguide device, multi-photon source, single photon counting and electrical control are fully interfaced to realise the *universal LPU*, as shown

---

<sup>2</sup>All Ta<sub>2</sub>N properties in the proceeding calculations are taken from Vishay Intertechnology Inc. [258].

in Figure 6.3. Further details of constituent components are given Chapter 3.

## 6.4 CHARACTERISATION

### 6.4.1 PHASE SHIFTER CALIBRATION

From above, the induced phase shift is approximately proportional to the temperature and hence applied power, so is quadratic in voltage. Therefore each thermo-optic phase shifter is described by a nonlinear phase-voltage relationship

$$\Phi(V) = \alpha + \beta V^2 + \gamma V^3, \quad (6.15)$$

where  $\Phi$  is the resulting phase shift due to an applied voltage  $V$  and  $\alpha, \beta$  and  $\gamma$  are real numbers to be determined (with  $\beta \gg \gamma$ ), which in general vary for each heater due to imperfections in the fabrication process. The internal phase with at zero voltage is given by  $\alpha$ , the ohmic response by  $\beta$ , and the non-ohmic response (due to a change in resistance at high temperature) by  $\gamma$ . To determine  $\Phi(V)$  we inject heralded single photons into the fundamental TM mode of an isolated MZI ( $\alpha_{i,j}$ ) or phase shifter ( $\phi_{i,j}$ ) then sweep the voltage  $1.8 \rightarrow 10V$  producing an interference fringe given by

$$C = A - B \cdot \cos \Phi(V), \quad (6.16)$$

where  $C$  is the count rate in the bar mode and  $A$  and  $B$ , along with  $\alpha, \beta$  and  $\gamma$  are free parameters to be determined via a least squares fitting procedure. See Figure 6.4 for typical interference fringes.

The arrangement of our device circuitry allows each phase shifter to be independently characterised. We first characterise the diagonal  $\alpha_{1,j}$  [Fig. 6.4(a)] by:

1. injecting single photons into mode 1
2. measure interference fringe on  $\alpha_{1,1}$
3. set  $\alpha_{1,1} = 2\pi$

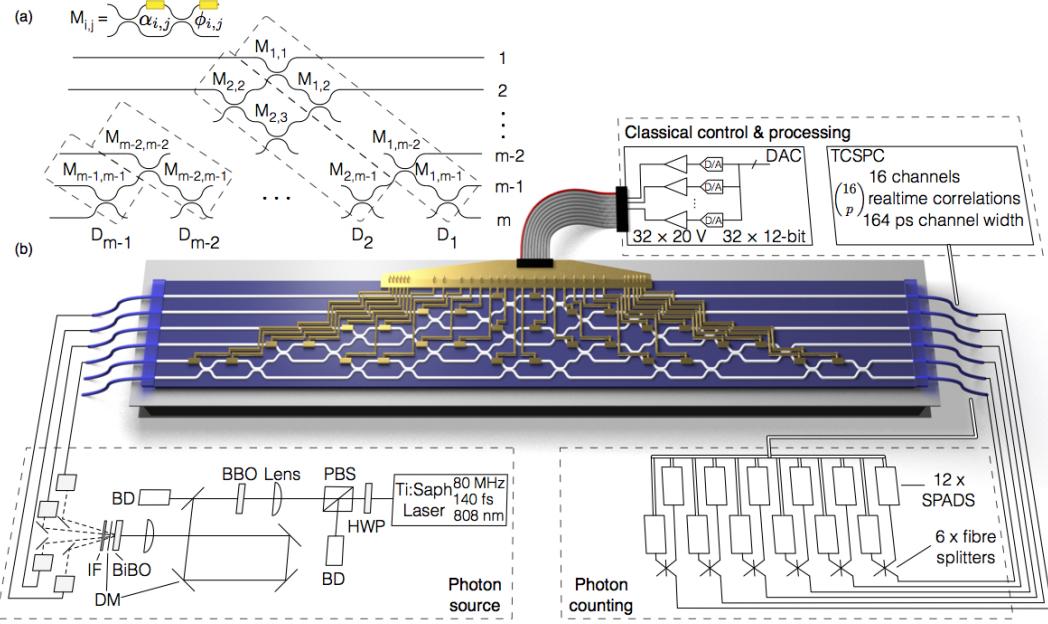


Figure 6.3: **Universal linear optical processor (LPU).** (a) Decomposition of a fully parametrised unitary for an  $m$ -mode circuit to realise any LO operation. Sub-unitaries  $D_i$  consist of Mach-Zehnder interferometers  $M_{i,j}$  (MZIs) built from phase shifters (yellow) and beam splitters, to control photon amplitudes ( $\alpha_{i,j}$ ) and phases ( $\phi_{i,j}$ ). (b) Multi-photon ensembles are generated via spontaneous parametric down-conversion (SPDC), comprising a BiBO crystal, dichroic mirrors (DM) and interference filter (IF); preceded by a pulsed Ti:sapphire laser and second harmonic generation from a BBO crystal. Photons are collected into polarisation maintaining fibres and delivered to the waveguide device via a packaged V-Groove fibre array (VGA). The processor is constructed over six modes as a cascade of 15 Mach-Zehnder interferometers, controlled by 30 thermo-optic phase shifters, set by a digital-to-analog converter (DAC) and actively cooled by a Peltier cooling unit. Photons are then out-coupled into a 2nd packaged VGA and sent to six (or 12 with fibre splitters for single-mode photon number resolving capability) single photon avalanche diodes (SPADs) and counted using a 12-channel time-correlated single-photon counting module (TCSPC).

## 6.4. CHARACTERISATION

---

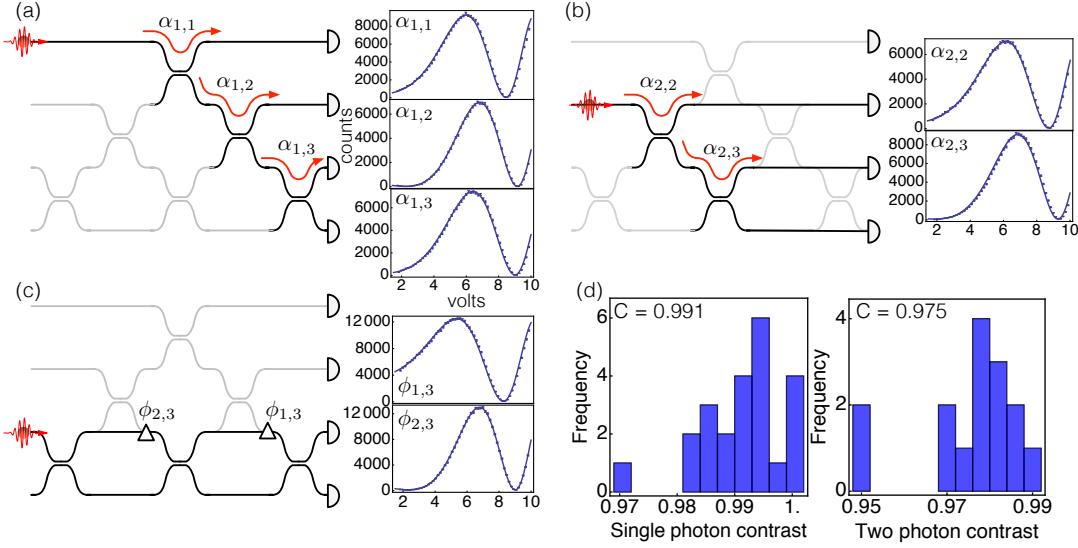


Figure 6.4: **Automated LPU characterisation.** (a) The diagonal  $\hat{D}_1$  is first characterised by sending single photons into mode 1 and measuring interference fringes on consecutive MZI's (represented as BS's) as shown adjacently. (b) All  $\alpha_{1,i} = \pi$  and the process is repeated for  $\hat{D}_2$ . (c) Phase shifters  $\phi_{i,j}$  are characterised by setting certain  $\alpha = \pi/2$  and measuring interference fringes on larger interferometers. (d) Histograms of single photon and two-photon interferometric extinction ratio's. We note that for a given input, this process is fully automated.

4. repeat for  $\alpha_{1,j}$  for  $j = [2, 5]$

completing the characterisation of  $\alpha_{1,j}$ . We repeat this procedure for  $\alpha_{i,j}$  with  $i = [2, 5]$  by injecting photons into mode  $i$  and setting all  $\alpha_{i-1,j} = \pi$  [Fig. 6.4(b)], thus completing the characterisation of all  $\alpha_{i,j}$ . We then characterise  $\phi_{i,5}$  by:

1. injecting single photons into mode 5
2. set  $\alpha_{i,5} = \pi$  for  $i = [3, 5]$
3. set  $\alpha_{i,4} = \pi$  for  $i = [1, 4]$
4. set  $\alpha_{2,5}, \alpha_{1,5} = \pi/2$
5. measure interference fringe on  $\phi_{1,5}$

6. repeat for  $\phi_{i,5}$ , with  $\alpha_{i,5}, \alpha_{i+1,5} = \pi/2$  and  $i = [2, 4]$

completing the characterisation of  $\phi_{i,5}$  [Fig. 6.4(c)]. Finally we repeat this procedure for  $\phi_{i,j}$  with  $j = [2, 4]$  by injecting photons into mode  $j$  and setting  $\alpha_{i,j+1}, \alpha_{i,j-1} = \pi$ , thus completing the characterisation of all  $\phi_{i,j}$  and therefore all phase shifters.

Once characterised, we tested the stability of the device by setting all heaters to some nontrivial phase, injected single photons and measured single photon output fluctuations; observing, over a period of 140 hours, an average power variation of  $< 0.1\%$ ,

#### 6.4.2 CROSSTALK

Crosstalk is an effect whereby the phase of one interferometer is a function of the phase in another. Many physical processes can give rise to crosstalk, for example nonlinear effects in silicon such as free-carrier and two-photon absorption [259], but in glass low nonlinearities make this effect negligible.

A more relevant source of crosstalk is *thermal coupling*. Here, the heating of a waveguide isn't well localised meaning nearest neighbour MZI's couple to one another. This can either be corrected after fabrication or mitigated during design. In the former you characterise all thermal crosstalk (in fact this can be generalised to all crosstalk) in a black box scenario and build a model which solves this many-body problem. The second approach, and the one which we opt for here, requires fabricating heat-insulating grooves between waveguides [Fig. 6.2(a)]. Not only does this mitigate thermal propagation it also significantly reduces power consumption (by up to 80% [166]).

*Electrical crosstalk* can occur due to coupling between channels in multichannel voltage supplies which can be caused by a variety of physical processes. In our case we observed electrical cross talk due certain heaters sharing a common ground. For small circuits each heater can have its own ground rail, but as circuits become

## 6.5. BENCHMARKING

---

more complex, common grounds are inevitable<sup>3</sup>. When a voltage is applied across a common ground with non-zero resistance, the ground voltage raises so that any heater attached to that ground must be supplied with a higher effective voltage to achieve the desired phase shift. If the ground has very small resistance this effect is negligible, but in our case we observed ground resistances of  $\mathcal{O}(10 \text{ m}\Omega)$  which given our heater resistances required correction.

To do this we characterised all shared resistances and built a model which calculated the set voltages  $\{V'_i\}$  which yields the actual voltages  $\{V_i\}$  required for a desired phase shift. Once corrected for no evidence of cross talk, thermal or otherwise, was observed.

A final correction is applied due to an observed reduction in quantum interference at certain points within the chip caused by polarisation rotation. We correct for this by inserting polarising beam splitters at the output of the chip filtering out undesired polarisation states.

## 6.5 BENCHMARKING

With the device fully characterised we perform benchmarking; implementing prototypical experiments with which we know (in an ideal case) the output, and where deviations from this output are a metric for the performance of the device.

### 6.5.1 CLASSICAL AND QUANTUM INTERFERENCE

The calibration procedure itself, Section 6.4.1, provides us with an important first benchmark. By assessing at the quality of single photon and pair photon interference fringes we can estimate how well the device supports classical and quantum interference.

Specifically, we calculate the mean single photon interferometric extinction ratio  $C = (N_{\max} - N_{\min})/(N_{\max} + N_{\min})$ , where  $N_{\max}$  and  $N_{\min}$  are the maximum

---

<sup>3</sup>See Allman et al. [260] for a solution to this problem in the context of large arrays of superconducting detectors.

and minimum count rates for a given interference given fringe, for all MZI's and find it to be 20.5 dB (99.1%). We then perform a similar experiment by injecting indistinguishable pairs of photons, finding the mean two photon extinction ratio to be 16dB (97.5%), indicating good single photon and two photon operation. A histogram of these results is displayed in Fig 6.4(d).

### 6.5.2 PHASE ACCURACY

To determine the typical accuracy in setting a phase we implement a randomized benchmarking inspired experiment by injecting heralded single photons into mode 1, then setting 100 different vectors  $\vec{\alpha}_{1,j} = (\alpha_{1,1}, \alpha_{1,2}, \alpha_{1,3}, \alpha_{1,4}, \alpha_{1,5})$ , chosen from the Haar measure, to give a mean fidelity  $\mathcal{F}^{\text{exp}}$  between our experimental and theoretical distributions. We then run a Montecarlo simulation of the experiment by applying Gaussian noise  $\delta_\phi$  to each phase shifter and fitting this fidelity  $\mathcal{F}^m$  as a function of this noise, giving  $\mathcal{F}^m(\delta_\phi)$ . We solve  $\mathcal{F}^m(\delta_\phi) = \mathcal{F}^{\text{exp}}$  finding  $\delta_\phi = 0.035$  rad. This value includes errors caused by the circuit, the control electronics and the calibration procedure, and therefore provides a useful estimate for our effective accuracy in setting a phase.

## 6.6 BOSON SAMPLING

Acting on three-photon ensembles  $|1_1, 1_2, 1_3\rangle$ , our device was programmed to implement 100 different boson sampling routines. Each circuit configuration was chosen randomly from the Haar measure, which was implemented via a direct parameterisation of phase shifters. This means the unitary doesn't have to be generated first to be compiled onto the circuit, rather on-chip phase settings  $(\alpha, \phi)$  can be directly set. In the same way selecting spherical polar coordinates uniformly from  $\theta \in [0, 2\pi]$ ,  $\phi \in [0, \pi]$  doesn't sample uniformly from the surface of a sphere, sampling phase shifter settings doesn't draw uniformly from the space of unitaries. As prescribed in Russell, Laing and O'Brien [261], we draw from the

## 6.7. VERIFYING BOSON SAMPLING

---

probability density functions (PDFs)

$$\mathcal{P}_\alpha = n \sin(\alpha/2) (\cos(\alpha/2))^{2n-1} \quad (6.17)$$

$$\mathcal{P}_\phi = 1/2\pi \quad (6.18)$$

where  $n$  is the row number, with the bottom row ( $\hat{M}_{i,5}$ ) defined as  $m = 1$  and so on, as displayed in Fig. 6.5(a).

For each implementation [Fig. 6.5(b)] five minutes worth of detection events were counted for each of the  $|d_3^6| = 20$  collision free ways in which three photons can exit the six output ports of the device. Figure 6.5(c) displays a histogram of fidelities with statistics based on calculations of matrix permanents, with a mean statistical fidelity  $\mathcal{F}_s = \sum_i \sqrt{p_i^{\text{exp}} p_i^{\text{th}}}$  between experimental  $p^{\text{exp}}$  and theoretical  $p^{\text{th}}$  distributions of  $\bar{\mathcal{F}}_s = 0.950 \pm 0.020$ <sup>§</sup>. These results demonstrate the performance of our LPU over many circuit configurations, randomly and unbiasedly chosen from the full space of all possible configurations. We also injected ensembles of one and two photon states  $|1_1\rangle$  and  $|1_1, 1_2\rangle$ , yielding statistical fidelities (between ideal and measured probability distributions) of  $0.999 \pm 0.001$  and  $0.990 \pm 0.007$  respectively.

For the three individual boson sampling experiments that produced the highest, lowest, and mode fidelity, we recalculated the statistical fidelities for the recovered transfer matrix  $M$  (see Chapter 4). This increased the mean statistical fidelity and reduced the range  $\mathcal{F}_s^{\text{max}} - \mathcal{F}_s^{\text{min}}$  from 0.102 to 0.036; implying dialling errors are non-uniform across the space of unitaries.

## 6.7 VERIFYING BOSON SAMPLING

The control our universal LPU affords means we can simultaneously realise boson sampling protocols and verification procedures on the same device. *The zero transmission law* (ZTL) [262] predicts that correlated photon detection for most of the

---

<sup>§</sup>Throughout this thesis two error analysis methods are used: those for individual fidelities  $\mathcal{F}$  calculated by propagating Poissonian count rate errors, and those for mean fidelities  $\bar{\mathcal{F}}$  calculated as  $1\sigma_{\mathcal{F}}$ . The bar symbol will be used to denote which method is used.

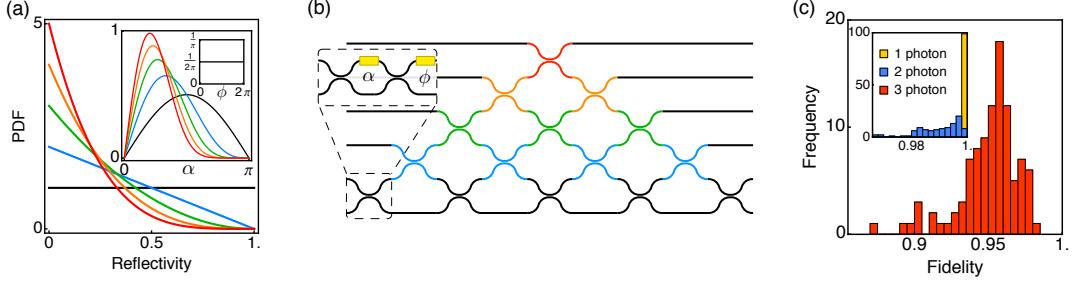


Figure 6.5: **Universal LPU boson sampling.** (a, b) A Haar random unitary can be directly implemented by choosing beamsplitter reflectivities (or equivalently MZI phases  $\alpha$  (inset 1)), and phase shifter values  $\phi$  (inset 2) from the probability density functions in (a). (c) A histogram of measured statistical fidelities for 100 three-photon boson sampling experiments, with one and two photon histograms inset.

exponentially growing number of configurations is strictly suppressed if the circuit is set to implement the Fourier transform (FT) on optical modes [Figs. 6.6(a,b)]. This is known because the structure of the FT allows these matrix permanents to be efficiently evaluated without explicit calculation. Because large scale many-photon quantum interference is at the core of the ZTL, it has been proposed as a certificate for the capability of a device to implement boson sampling [251].

The most general form of the ZTL applies to any periodic input state to the FT matrix [263]. For an  $p$ -photon  $n$ -periodic initial state

$$|\psi_{\text{in}}\rangle = |1, n+1, 2n+1, \dots, n(p-1)+1\rangle \quad (6.19)$$

input into the FT (written in the mode number basis where  $|i_j\rangle$  represents the  $j^{\text{th}}$  photon in the  $i^{\text{th}}$  mode), output states  $|s\rangle$  are suppressed when the sum of the mode assignment list (i.e. the list of positions of the photons in the output state) multiplied by  $n$  is not divisible by  $p$

$$\text{mod}\left(n \sum_j s_j, p\right) \neq 0 \implies \text{Prob}(|s\rangle) = 0. \quad (6.20)$$

For our implementation we input the three-photon periodic state  $|1_1, 3_2, 5_3\rangle$  into the FT, so states such as  $|1_1, 2_2, 4_3\rangle$  — where  $\sum_j s_j = 7$ , and  $\text{mod}(2 \times 7, 3) \neq$

## 6.7. VERIFYING BOSON SAMPLING

---

0 — are suppressed; whilst states such as  $|1_1, 2_2, 3_3\rangle$  — where  $\sum_j s_j = 6$ , and  $\text{mod}(2 \times 6, 3) = 0$  — are not suppressed. In the collision free subspace, 12 out of the total of 20 outputs are suppressed, and the experimental violation of the ZTL is calculated as  $\nu = N_s/N$ , the ratio of the number of predicted suppressed events  $N_s$  to the total number of events  $N$ .

The LPU was programmed to implement 16 examples of the  $F_6^{(2)}(\theta_1, \theta_2)$  two-parameter set of six dimensional matrices, including  $F_6$  (the six dimensional FT), which occurs at  $\theta_1, \theta_2 = \pi, 0$ . Using statistics from three-photon ensembles, the experimental violation of the ZTL was calculated; the results of which are plotted in Fig. 6.6(c) alongside the theoretical manifold. The experimental points follow the shape of the manifold with the minimal violation of the ZTL  $\nu_{\min} = 0.319 \pm 0.009$  occurring when  $F_6$  is implemented. The average ZTL violation of the nine points that are predicted to maximally violate is  $\bar{\nu}_{\max} = 0.638 \pm 0.029$ .

The deviation from  $\nu_{\min} = 0$  can be attributed to two effects: dialling error, and imperfect quantum interference. To quantify this we use known source dip visibilities to build a model of the experiment and calculate an expected violation in the absence of dialling errors, finding  $\nu_{\min}^{\text{exp}} = 0.149$ . We therefore attribute the deviation from this value as dialling errors.

### 6.7.1 SIX PHOTON VERIFICATION

An essential requirement of boson sampling is that of indistinguishability among photons. With the LPU set to implement  $F_6$ , the six-photon state  $|3_1, 3_2\rangle$  was injected and six-photon statistics were counted with an all-fibre beam-splitter between each output mode and two single photon avalanche diodes (SPADs) to give probabilistic number-resolved photon detection over a total of 12 SPADs. While the complexity of states that are not one-photon-per-mode is less understood, the input state used here allows us to implement a protocol designed to verify indistinguishability among many photons with only a small number of detection events.

Bayesian model comparison (see Section 5.5) was used to update, in realtime,

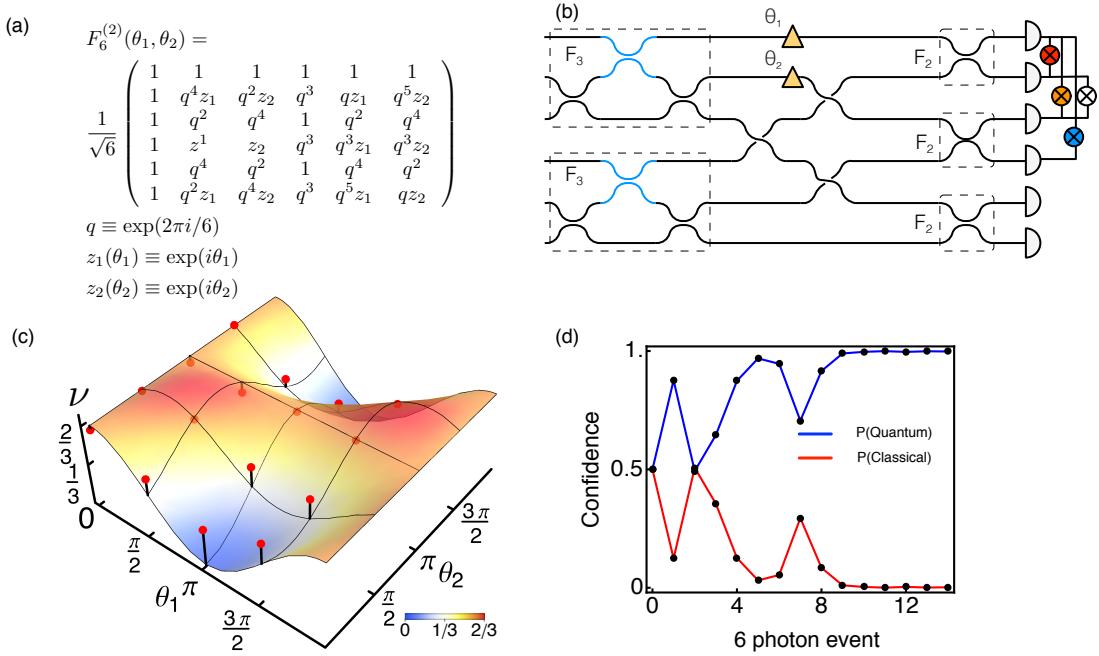


Figure 6.6: **Universal LPU verification.** (a) The  $F_6^{(2)}$  two parameter  $(\theta_1, \theta_2)$  family of 6-dimensional complex Hadamard matrices, and (b) A circuit customised to implement  $F_6^{(2)}$  with defining parameters  $\theta_1, \theta_2$  explicitly realised. Due to the particular decomposition of our LPU, compiling  $F_6^{(2)}$  requires unique phase shift values across the entire device for each implementation  $\theta_1, \theta_2 \in [0, 2\pi)$  (c) Three-photon violations ( $\nu$ ) of the zero transmission law from scanning over  $F_6^{(2)}(\theta_1, \theta_2)$ . Experimental points in red are plotted with the ideal theoretical manifold; black lines are to guide the eye. (d) Dynamic updating of the confidence that six-photon detection events are sampled from a distribution of indistinguishable (quantum, blue) or distinguishable (classical, red) photons.

## 6.8. COMPLEX HADAMARD MATRICES

---

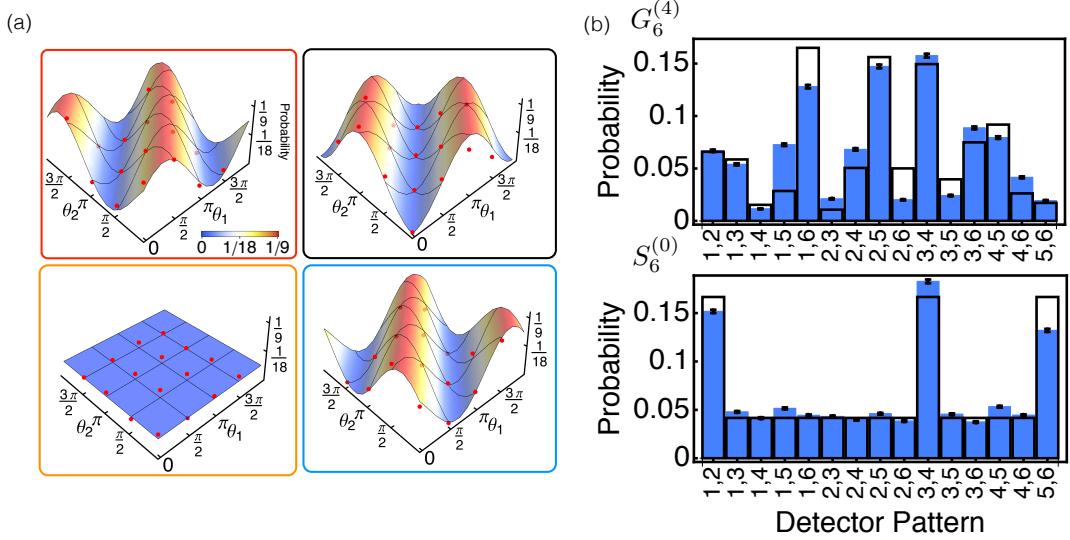


Figure 6.7: **Complex Hadamard matrices.** (a) Two photon correlation manifolds in  $F_6^{(2)}$  for the probability of a given detection event [as colour coded in Fig. 6.6(b)] with experimental points in red. (b) The measured probability for a given detection event when two photons are injected into an instance of  $G_6^{(4)}$  and  $S_6^{(0)}$ , with ideal theoretical black bars (error bars assume Poissonian counting statistics).

the confidence that events are sampled from a (pre-calculated) quantum probability distribution (arising from completely indistinguishable photons) or from a classical probability distribution (arising from completely distinguishable photons), shown in Fig. 6.6(d). After collecting 15 six-fold coincidence events over a period of two weeks, a confidence of  $p = 0.998$  is determined that these are drawn from a quantum (not classical) distribution.

## 6.8 COMPLEX HADAMARD MATRICES

The FT and  $F_6^{(2)}$  are examples in the more general class of complex Hadamard matrices (CHMs), which are related to mutually unbiased bases [264] and are of fundamental interest in quantum information theory [265]. CHMs are defined as  $N \times N$  unitary matrices with entries of squared absolute value equal to  $1/N$ . While this definition is straightforward, classification of these matrices is far from

trivial and is concerned with identifying CHMs that are inequivalent up to pre and post multiplication with permutation matrices and diagonal unitaries [266]. In the  $N = \{2, 3, 5\}$  case, all CHMs are equivalent to the respective FT matrix, while for  $N = 4$  there exists a one parameter equivalence class. Whilst a full classification of  $N = 6$  CHMs is unknown, it is currently conjectured that the set consists of an isolated matrix  $S_6^{(0)}$  which does not belong to any family [267], and a newly discovered four-parameter generic family  $G_6^{(4)}$  [268].

In LO experimental implementations, discrimination among CHMs can be accomplished via the observation of characteristic patterns of photonic quantum interference [269–272]. Up until now, these observations have been too experimentally challenging for the six-dimensional case. Here, correlation manifolds of two-photon detection events are reconstructed by scanning over the  $F_6^{(2)}$  matrices, displaying four (out of the 15 sets collected) in Fig. 6.7(a). A mean statistical fidelity of  $\bar{\mathcal{F}}_s = 0.979 \pm 0.007$  is found.

Finally, an instance of  $G_6^{(4)}$  (that is not contained in  $F_6^{(2)}$ ) and  $S_6^{(0)}$  is implemented, and predicted characteristic two-photon quantum interference patterns are observed [Fig. 6.7(b)], with respective statistical fidelities of  $\mathcal{F}_s = 0.986 \pm 0.001$  and  $\mathcal{F}_s = 0.998 \pm 0.001$ . The intractability of calculating the permanents of certain CHMs is an interesting research line, as is the possibility of searching for new CHMs using photonic statistics.

## 6.9 CONCLUDING REMARKS

We have demonstrated how a single universal LPU, equipped with modulation capabilities, can be rapidly programmed to implement a host of linear optical protocols; from simultaneous boson sampling and verification procedures, to implementing 100 Haar random unitaries with an average fidelity of  $0.999 \pm 0.001$ , to exploring newly discovered six-dimensional complex Hadamard operations.

The comparable three-photon boson sampling experiment with the passive

## **6.9. CONCLUDING REMARKS**

---

waveguide device described in Chapter 5, took five days. A single experiment here took five minutes demonstrating the orders of magnitude increase in complexity and control that low loss, high fidelity universal LPU's offer.

These results point the way to universal devices with the ability to arbitrarily “dial-up” operations replacing a multitude of existing and future prototype systems. In the following chapter we examine this claim in the context of quantum information processing.

## 6. UNIVERSAL LINEAR OPTICS

# 7

## Quantum Computation with Universal Linear Optics

### STATEMENT OF WORK

The work presented in this chapter was published in J. Carolan et al. *Science* **349**, 711 (2015) [255]. All data was taken by myself, C. Harrold and N. Matsuda. The LPU implementation of the KLM gate and BSG was proposed, developed and analysed by myself, C. Sparrow, and C. Harrold. The loop measurements were proposed by myself and J.C.F. Matthews, and developed by myself and C. Sparrow. Process tomography theory was provided by C. Sparrow, as was data analysis. The project was supervised by A. Laing.

## 7.1 INTRODUCTION

We have so far demonstrated the high fidelity operation of a universal linear optical processor. A key application of such a device is as a testbed to develop new protocols, and as a means of testing our known protocols in experimentally realistic scenarios. We therefore apply our universal LPU to a variety quantum information processing protocols. We implement heralded quantum logic gates at the heart of the circuit model of LO quantum computing and new heralded entangling gates that underpin the measurement-based model of LO quantum computing, both of which are the first of their kind in integrated photonics. We demonstrate arbitrary state preparation and measurement, which allows us to perform two qubit process tomography on a unheralded CNOT operation, achieving fidelities surpassing those previously reported. Finally, we use the hardware level characterisation methods previously presented, to verify these gates independent of error prone photon sources. These results demonstrate unprecedented control and performance of a universal quantum device.

## 7.2 UNIVERSAL GATE SET

### 7.2.1 UNIVERSAL CLASSICAL GATES

A key ingredient for the universality of classical computers is the existence of universal gate sets. A logic gate takes as input binary entries (bits) and conditional on this input, outputs a new set of bits. This mapping between inputs and outputs (represented by truth tables, for example Table. 7.1) completely defines the gate. A computer is said to be universal if it has access to a basic set of gates, a universal gate set, which can be combined together in such a way as to generate *any possible gate*. For a classical computer, a possible universal gate set is AND and NOT. To see how new gates can be created out of just these two, note we can construct

## 7.2. UNIVERSAL GATE SET

---

A	B	NOT B AND OR XOR		
0	0	1	0	0
0	1	0	0	1
1	0	-	0	1
1	1	-	1	0

Table 7.1: **Classical logic gates.** Single and two bit classical truth tables which take as input bit entries A,B and output a single bit.

OR, in the language of boolean logic<sup>1</sup>, via the equality  $X \vee Y = \neg(\neg X \wedge \neg Y)$ .

If this was all there was to computing it would all be rather boring. However, the beauty and interest in building computers is that certain gate sets are more *efficient* for certain tasks. To see this let us borrow an example from Feynman [48] and consider the English language. In English we've developed the word ‘car’ to refer to the four wheeled metal machine that takes us from A to B. But we could just as easily imagine a Amazonian tribe who have never come across such thing. If they wanted to describe a ‘car’ they may have to describe each of the individual components — the sounds, the textures, the colours — in their own language; which, whilst doing an equally good job, may well require more words and be less efficient.

### 7.2.2 UNIVERSAL QUANTUM GATES

In analogy to classical computing, the definition of BQP and hence the possibility of a universal quantum computer is predicted upon the existence of a universal *quantum* gate set [see Table 7.2]. Universal quantum gate sets have been studied extensively and various sets have been proven, including:

1. The complete set of single qubit gates  $[U(2)]$  plus CNOT [273],
2. CNOT, Hadamard and  $\pi/8$ -gate [274],

---

<sup>1</sup>Where  $\vee = \text{OR}$ ,  $\wedge = \text{AND}$ ,  $\neg = \text{NOT}$ .

A	B	$\hat{I}$	$\hat{X}$	$\hat{Y}$	$\hat{Z}$	CNOT	CPHASE
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ +\rangle$	$ +i\rangle$	$ 0\rangle$	$ 00\rangle$	$ 00\rangle$
$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$ -\rangle$	$ -i\rangle$	$- 1\rangle$	$ 01\rangle$	$ 01\rangle$
$ 1\rangle$	$ 0\rangle$	-	-	-	-	$ 11\rangle$	$ 10\rangle$
$ 1\rangle$	$ 1\rangle$	-	-	-	-	$ 10\rangle$	$- 11\rangle$

Table 7.2: **Quantum logic gates.** Single qubit gates take as input qubit B, and two qubit gates use A and B as control and target respectively.

3. Toffoli and Hadamard<sup>2</sup> [275].

Moreover, the Solovay-Kitaev theorem tells us any single qubit gate can always be efficiently decomposed into a sequence of gates from a finite universal gate set [276].

With this plethora of gate sets to choose from, one may be forgiven for thinking we can freely choose any single qubit and two qubit gates to build our quantum computer — but a word of warning! The beautiful Gottesman-Knill Theorem [277] tells us that a circuit consisting entirely of Hadamard and CNOT gates *can* be efficiently simulated on a classical computer. This means, that large scale entanglement alone isn't sufficient for classical intractability.

A final point should be made here that the existence of multiple universal gate sets isn't merely some mathematical nicety, but of practical interest as well. It means that if some physical system can intrinsically perform Toffoli and Hadamard, but not CNOT, it still has the potential for universality. As we will see much effort has been spent in showing that linear optics is capable of precisely this.

### 7.3 HERALDED QUANTUM LOGIC GATES

Manipulating single photonic qubits is relatively straight forward, relying entirely on wave interference effects — physics known since the early 19th century. But notice from the list in Section 7.2.2 that a universal gate set requires two-qubit,

---

<sup>2</sup>Or more generally, any basis changing single qubit real gate (which is *a lot* of gates).

### 7.3. HERALDED QUANTUM LOGIC GATES

---

*conditional* operations: “If A, do B”. It is precisely the properties which make photons exceptional single qubit systems (ease of manipulation, robustness to environmental noise), which makes these conditional operations so problematic. Not only do they not interact with their environment, *photons do not interact with one another*.

Up until 2001 it was widely believed that single photons and linear optical elements alone, were not sufficient for universal quantum computation. Remarkably this all changed when Knill, Laflamme and Milburn (KLM) proved<sup>3</sup> it was possible to induce the necessary nonlinearities for universal quantum computation via single photon measurement and active feedforward of classical information [10]. In their scheme they construct a photonic quantum logic gate which works non-deterministically, but unlike the gate presented in Section 2.6.7 the operation is *heralded*; meaning non-computational ancilla photons are used in addition to computational photons to signal successful operation of the gate.

A gate which works with probability  $p$ , doesn’t sound like much use for large scale computation. If  $n$  gates are required for a calculation, the probability it succeeds is  $p^n$ . However, by using the technique of gate teleportation [278], KLM showed it was possible to perform non-deterministic gates offline, then teleport the gate, when successful, onto the computational qubits — thus preserving computational photons. The subtlety with the scheme is that in linear optics the Bell measurements required for teleportation are probabilistic; so KLM’s real breakthrough was in constructing a near-deterministic teleportation scheme which uses  $n$  ancillary photons to boost the teleportation probability to  $n^2/(n + 1)^2$ . Using this technique they prove that scalable, universal linear optical quantum computer (LOQC) is possible.

---

<sup>3</sup>KLM actually set out to prove the very intuition that it was *not* possible to build a universal linear optical quantum computer, but as sometimes happens in science, a much more exciting and beautiful result was shown.

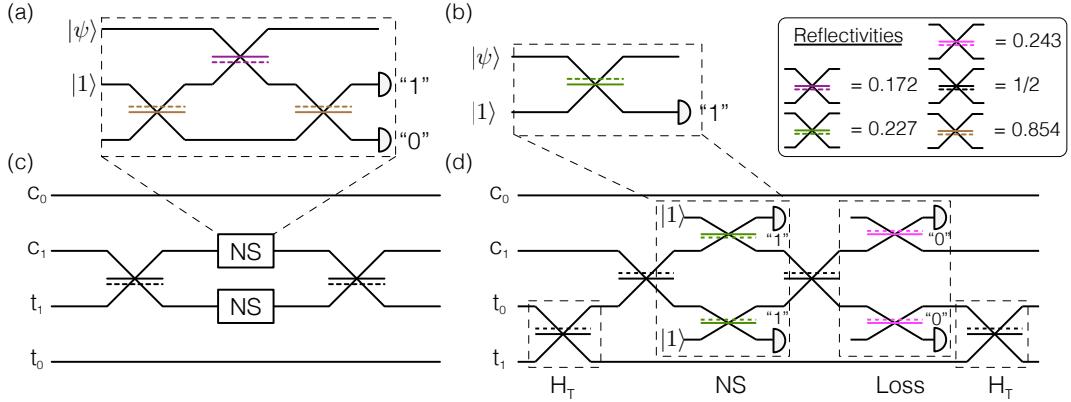


Figure 7.1: **Heralded linear optical gates.** (a) The original KLM NS gate takes as input an ancilla photon, and based on a single photon and vacuum detection heralds the NS operation. (b) The simplified Ralph et. al. biased NS gate, uses only a single ancilla mode. (c) A heralded CZ gate can be made out of two NS gates. (d) A heralded CNOT gate can be made from two NS gates, plus the respective balancing loss modes and Hadamard operations  $\hat{H}_T$  on the target. Reflectivities of beamsplitters are shown in inset, and phase shift is picked up off dashed side.

### 7.3.1 NONLINEAR SIGN SHIFT

A key component of their scheme is the nonlinear sign shift (NS) gate, which, in the Fock basis takes

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \xrightarrow{\text{NS}} \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle. \quad (7.1)$$

This cannot be achieved via linear optics alone. To see this, note the necessary creation operator transformation for a  $\pi$  shift on the  $|2\rangle$  term is  $\hat{a}^\dagger|0\rangle \rightarrow i\hat{a}^\dagger|0\rangle$  which transforms the entire state

$$\left(\alpha|\text{vac}\rangle + \beta\hat{a}^\dagger + \gamma\hat{a}^{\dagger 2}/\sqrt{2}\right)|0\rangle \rightarrow \left(\alpha|\text{vac}\rangle + i\beta\hat{a}^\dagger - \gamma\hat{a}^{\dagger 2}/\sqrt{2}\right)|0\rangle, \quad (7.2)$$

hence the  $|1\rangle$  term will always have an amplitude proportional to the square root of the  $|2\rangle$  term. However this operation *can* be achieved, probabilistically, due to quantum interference [92] with ancillary photons.

### 7.3. HERALDED QUANTUM LOGIC GATES

---

KLM demonstrate a NS gate across three modes as shown in Fig. 7.1(a). The gate takes as input the state  $|\psi_1, 1_2, 0_3\rangle$  (in the photon number bases) and conditional on detecting the ancillary state  $|1_2, 0_3\rangle$  successfully implements  $\text{NS}|\psi\rangle_1$  with  $p = 1/4$  (see Refs. [10, 279] for details of the calculation).

A simplification was made by Ralph et al. [279] who showed only a single beam splitter was necessary to realise a NS gate at the cost of a biased sign flip. To see this, consider a beam splitter with reflectivity  $\eta$  and input state  $|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1 + \gamma|2\rangle_1$ . If the ancillary state is  $|1\rangle_2$ , then detecting the state  $|1\rangle_2$  yields [Fig. 7.1(b)]

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \rightarrow \alpha\sqrt{\eta}|0\rangle + \beta(1 - 2\eta)|1\rangle - \gamma\sqrt{\eta}(2 - 3\eta)|2\rangle. \quad (7.3)$$

This operation is biased in the sense that not all terms scale equally, however this can be balanced by adding heralded loss on the input or output mode. To see this consider impinging the output state of (7.3) onto a beam splitter of reflectivity  $\eta'$ , and heralding on a vacuum detection. In this instance the state becomes  $\alpha\sqrt{\eta}|0\rangle + \beta\sqrt{\eta'}(1 - 2\eta)|1\rangle - \gamma\eta'\sqrt{\eta}(2 - 3\eta)|2\rangle$ , which has a balanced solution at  $\eta = (3 - \sqrt{2})/7 \approx 0.227$  and  $\eta' = 5 - 3\sqrt{2} \approx 0.757$ , at the cost of a slight reduction in success probability from  $p = 0.25 \rightarrow 0.23$ .

#### 7.3.2 HERALDED CNOT GATE

Given an NS gate it is straight forward to construct a heralded CZ gate by placing NS gates on each arm of a balanced MZI, as shown in Fig. 7.1(c). Clearly  $|0_C 0_T\rangle \rightarrow |0_C 0_T\rangle$  (where  $C$  and  $T$  subscripts denote the logical control and target qubits respectively), and — recall from Section 2.6.3 — when the MZI has zero internal phase (i.e. only contains a single photon) it realises the identity on modes  $\{|1_C\rangle, |0_T\rangle\}$ , thus  $|1_C 0_T\rangle \rightarrow |1_C 0_T\rangle$  and  $|0_C 1_T\rangle \rightarrow |0_C 1_T\rangle$ .

If however both photons are input in the state  $|1_C 1_T\rangle$  then they maximally interfere on the first beam splitter giving the HOM state  $|20\rangle - |02\rangle$  (in the photon number basis and ignoring normalisation), which triggers the NS gates and picks up an overall negative phase. The photons then re-interfere to produce the state

$-|1_C1_T\rangle$  with the desired sign shift. The gate requires two NS gates, thus the overall success probability is  $p = 1/16$

The CNOT can be constructed via a CZ gate with the addition of Hadamard operations before and after the target qubits. To see this note the unitary operators describing

$$\hat{U}_{\text{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}; \hat{U}_{\text{CZ}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (7.4)$$

hence

$$(\hat{I}_C \otimes \hat{H}_T) \hat{U}_{\text{CZ}} (\hat{I}_C \otimes \hat{H}_T) = \hat{U}_{\text{CNOT}}. \quad (7.5)$$

Thus by placing beamsplitters before and after the target qubits a CNOT can be realised, and it is this construction, shown in Fig. 7.1(d), we use as the basis for the LPU implementation of the heralded-CNOT gate.

### 7.3.3 LPU IMPLEMENTATION

We use our LPU to implement, to the best of our knowledge, the first integrated heralded-CNOT operation. For completeness the term ‘heralding’ refers to the addition of ancillary photons (in addition to photons onto which qubit information is encoded), which when measured in a particular pattern induce a nonlinearity on the photonic qubits. When the ancillary photons are measured in a configuration which is consistent with successful gate operation (such as one photon per ancillary mode), the entire multi-photon state is collapsed onto the computational subspace of the photonic qubits. If however such ancilla configuration is not measured, the multi-photon state collapses onto a non computational subspace of the photonic qubits (such as two photons in the control modes) and the state is discarded. Crucially, this heralding process does not destroy the photonic qubits which means they can be used as part of some trial-until-success based multiplexing scheme [134] for processing later in the computation.

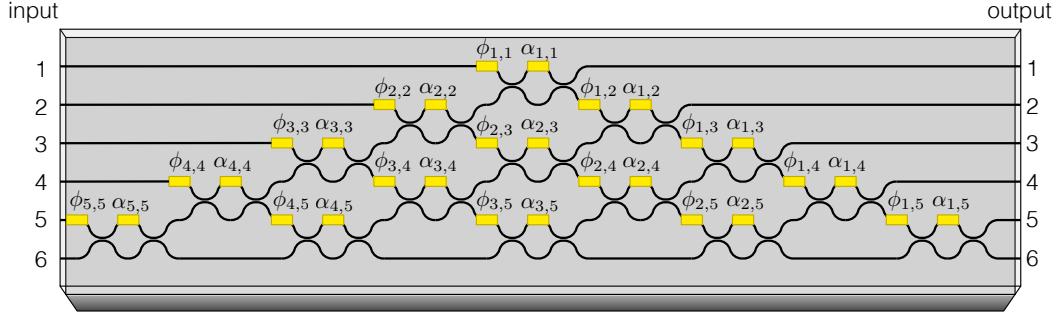


Figure 7.2: **Universal LPU labelling.** Labelling convention for LPU including variable beamsplitters ( $\alpha_{i,j}$ ) and phase shifts ( $\phi_{i,j}$ ) shown in yellow.

The Ralph et al. heralded-CNOT (experimentally realised in bulk optics [142]) works with four photons over eight photonic modes: four computational modes, two ancillary modes, and two balancing modes as shown in Fig. 7.1(d). We adapt this scheme for use with the six-mode LPU by employing an auxiliary coupling waveguide as the control-zero, and implementing the eighth lossy balancing mode in post-processing as an equivalent reduction in detection efficiency on the control-one mode, see Fig. 7.3(b).

Control and target qubits  $c_{0,1}$  and  $t_{0,1}$  are implemented via the modes  $\{0, 2, 3, 4\}$  respectively, and heralding modes via  $\{1, 5\}$ . Crucially the photons  $\{N, S, E, W\}$  must be input into modes  $\{H, H, C, T\}$  where  $\{N, S\}$  and  $\{E, W\}$  represent pairs of photons from the same creation events. This means that the four photon term  $|\psi_4\rangle \approx |1111\rangle + |2200\rangle + |0022\rangle$  does not give rise to events in the computational subspace, in the ideal case, and can therefore be removed in postselection.

The unitary operation describing the heralded-CNOT  $\hat{U}_{\text{HCNOT}}$  can be determined entirely from the beamsplitter construction  $\hat{U}_{\text{BS}}$  described in Fig. 7.1(d),

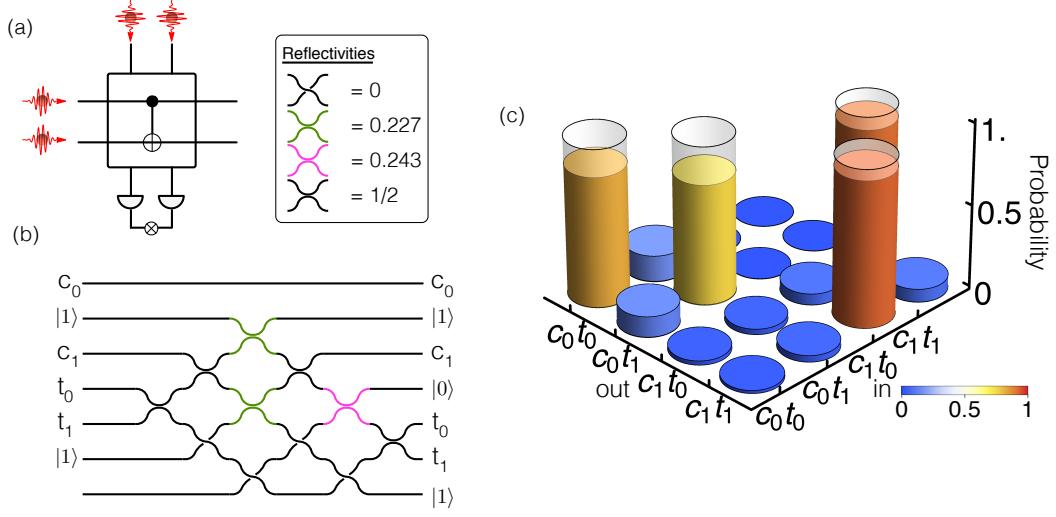


Figure 7.3: **LPU heralded-CNOT.** (a) The heralded-CNOT gate is successfully implemented on the two photonic qubits, upon detection of the two ancilla photons. (b) The linear optical protocol realising the heralded CNOT operation on the control  $c_{0,1}$  and target  $t_{0,1}$  qubits, with herald states  $|1\rangle$ . (c) Experimental data showing the computational truth table, with the ideal theoretical truth table overlaid. Data is corrected for measured detector efficiencies.

hence

$$\hat{U}_{\text{HCNOT}} = \begin{pmatrix} 0.476 & -0.622 & -0.440 & 0.440 & 0 & 0 \\ -0.622 & -0.476 & 0 & 0 & 0.622 & 0 \\ -0.383 & 0 & 0.293 & 0.707 & -0.383 & -0.348 \\ 0.383 & 0 & 0.707 & 0.293 & 0.383 & 0.348 \\ 0 & 0.622 & -0.440 & 0.440 & 0.476 & 0 \\ 0.306 & 0 & 0.166 & -0.166 & 0.306 & -0.870 \end{pmatrix}.$$

However, directly compiling this to on-chip phases for LPU implementation is less straightforward due to  $\hat{U}_{\text{DC}} \neq \hat{U}_{\text{BS}}$ . To do so we use the (constructive) circuit finding algorithm described in Section 6.2 to determine the on-chip phases  $R_{\text{HCNOT}}$  necessary to realise  $\hat{U}_{\text{HCNOT}}$ , finding

$$R_{\text{HCNOT}} = \begin{pmatrix} (0.000, 0.992) & (4.712, 1.571) & (4.544, 4.957) & (5.375, 1.792) & (3.816, 0.000) \\ & (0.000, 1.571) & (1.571, 0.992) & (2.188, 0.000) & (4.712, 0.000) \\ & & (0.000, 1.571) & (5.498, 0.000) & (1.571, 2.226) \\ & & & (0.000, 3.142) & (3.142, 0.000) \\ & & & & (0.000, 0.000) \end{pmatrix}$$

where  $R_{ij} = (\phi_{ij}, \alpha_{ij})$  as labelled in Fig. 7.2. The resulting circuit is displayed in Fig. 7.3(c), where the green splitters represent the NS gates and the pink splitter the balancing loss mode [cf. Fig. 7.1(d)].

### 7.3.4 RESULTS

Via four separate measurements, each taking 5 hours and collecting  $\sim 120$  four-fold coincidences, we measured the logical truth table for this operation in the computational basis. The measured truth table for mapping between computational basis states is given in Table 7.3, and displayed in Fig. 7.3(c). We found the mean statistical fidelity  $\mathcal{F}_s = \sum_i \sqrt{p_i^{\text{exp}} \cdot p_i^{\text{th}}}$  [43] between experimental  $p^{\text{exp}}$  and theoretical  $p^{\text{th}}$  probability distributions, when averaged over all computational inputs, to be  $0.930 \pm 0.003$ . From Table. 7.3 we see that input states with  $c_1$  have higher fidelity, this can be understood by noting that given this input state a photon can never end up in  $c_0$ , thus reducing the number of failure modes and raising fidelity.

We attribute the primary cause of deviations from unit fidelity as imperfections in the photon source, such as reduced quantum interference between different pair creation events [146], and higher-order terms in the spontaneous parametric down-conversion process — see Section 3.2.3 for a detailed discussion.

## 7.4 HERALDED ENTANGLED STATES

### 7.4.1 MEASUREMENT BASED QUANTUM COMPUTATION

Whilst KLM proves the ‘in principle’ possibility of an all linear optical quantum computer (LOQC), its interest now is mainly pedagogic. First, for a scheme to be

Input	Output			
	$c_0, t_0$	$c_0, t_1$	$c_1, t_0$	$c_1, t_1$
$c_0, t_0$	0.837 (1)	0.131 (0)	0.019 (0)	0.013 (0)
$c_0, t_1$	0.166 (0)	0.779 (1)	0.025 (0)	0.030 (0)
$c_1, t_0$	0 (0)	0.001 (0)	0.069 (0)	0.931 (1)
$c_1, t_1$	0 (0)	0 (0)	0.919 (1)	0.081 (0)

Table 7.3: **Heralded CNOT results.** Measured logical truth table in the computational basis for the heralded CNOT, along with theoretical probabilities in brackets. Experimental data is corrected for measured detector efficiencies.

scalable in the presence of loss, photons must pass through a logarithmic number of optical elements (as opposed to the linear number in KLM). Second, due to the requirement of teleportation to boost non-deterministic gates, the resources required for full KLM quantum computation are wholly impractical. New computation models have therefore been developed to deal with both these challenges.

It was shown by Raussendorf and Briegel [280] that by making only single qubit measurements on a particular class of highly entangled ‘resource’ state, universal quantum computation is possible. In this model of measurement-based quantum computing (MBQC), single qubit measurements serve to encode, process and readout information [281]; which due to the simplicity of these operations in a photonic setting, suggests it may be well suited for LOQC. Nielsen was the first to confirm this intuition and showed that by directly applying the principles of KLM to a MBQC (namely non-deterministic gates and teleportation) one can achieve an order of magnitude reduction in resources [282]. Shortly after Browne and Rudolph [283] made a significant break through and proposed a scheme that removes the need for teleportation and drastically reducing overheads by several orders of magnitude. Moreover, their scheme significantly simplified experiments by relying on quantum interference as opposed to classical interference; requiring stability on the order of the coherence length of the photons  $10^{-3}$  m as opposed to their wavelength  $10^{-6}$  m.

## 7.4. HERALDED ENTANGLED STATES

---

Their scheme uses small entangled resource states, and probabilistically fuses them together to create a larger cluster state. The probabilistic nature of this operation can be overcome either via redundantly encoding multiple connections [284], or using techniques such as percolation to create a logical qubit out of many physical photons [285]. Error and loss thresholds for these schemes have also been studied [178].

Regardless of the particular architecture, it is likely that any MB-LOQC will require entangled states to be generated from single photons. A scheme for this was first presented and demonstrated by Zhang et al. [286] which takes four photons as input (over eight modes) and with probability  $p = 1/4$  generates a maximally entangled Bell state<sup>4</sup>. In the following we programme the LPU to realise a new, more compact four-photon Bell state generator over six spatial modes, along with tomographic capabilities to witness entanglement.

### 7.4.2 BELL STATE GENERATOR

Our Bell state generator (BSG) is shown in Fig. 7.4(a,b) and accepts four photons into the modes  $\{1, 3, 4, 5\}$  of our LPU. Detection in ancilla modes  $\{3, 4\}$  occurs with probability  $p = 2/27$  and heralds the Bell state  $|\Phi^+\rangle = (|1_1 0_2 1_5 0_6\rangle + |0_1 1_2 0_5 1_6\rangle)/\sqrt{2}$  over the remaining modes with unit probability in the ideal case. To see how the circuit operates consider injecting the four photon state  $\hat{a}_1^\dagger \hat{a}_3^\dagger \hat{a}_4^\dagger \hat{a}_5^\dagger$ . After the first set of 50/50 beamsplitters we have

$$\frac{1}{4} (\hat{a}_1^\dagger + \hat{a}_2^\dagger) (\hat{a}_3^\dagger + \hat{a}_4^\dagger) (\hat{a}_3^\dagger - \hat{a}_4^\dagger) (\hat{a}_5^\dagger + \hat{a}_6^\dagger), \quad (7.6)$$

which after the second set of  $\eta = 1/3$  splitters transforms to

$$-\frac{1}{216} (3\sqrt{2}\hat{a}_1^\dagger + \sqrt{6}\hat{a}_2^\dagger + 2i\sqrt{3}\hat{a}_3^\dagger) (\sqrt{2}\hat{a}_2^\dagger - i\hat{a}_3^\dagger - \hat{a}_4^\dagger - \sqrt{2}\hat{a}_5^\dagger) \\ (\sqrt{2}\hat{a}_2^\dagger - i\hat{a}_3^\dagger + \hat{a}_4^\dagger + \sqrt{2}\hat{a}_5^\dagger) (-2\sqrt{3}\hat{a}_4^\dagger + \sqrt{6}\hat{a}_5^\dagger - 3\sqrt{2}\hat{a}_6^\dagger). \quad (7.7)$$

---

<sup>4</sup>Zhang et al. [286] quote  $p = 3/16$ , but this probability can be boosted to  $p = 1/4$  with additional circuitry [287].

We then impinge modes 3 and 4 on a final 50/50 splitter to give

$$\begin{aligned}
 & -\frac{1}{216} \left( 3\sqrt{2}\hat{a}_1^\dagger + \sqrt{6} \left( \hat{a}_2^\dagger + i(\hat{a}_3^\dagger + \hat{a}_4^\dagger) \right) \right) \\
 & \left( (i-1)\hat{a}_2^\dagger + \hat{a}_3^\dagger + i\hat{a}_4^\dagger + (1-i)\hat{a}_5^\dagger \right) \left( (1+i)\hat{a}_2^\dagger + \hat{a}_3^\dagger - i\hat{a}_4^\dagger + (1+i)\hat{a}_5^\dagger \right) \\
 & \quad \left( \sqrt{6}\hat{a}_3^\dagger - \sqrt{6}\hat{a}_4^\dagger - \sqrt{6}\hat{a}_5^\dagger + 3\sqrt{2}\hat{a}_6^\dagger \right) \quad (7.8)
 \end{aligned}$$

which, by multiplying through and heralding on terms  $\hat{a}_3^\dagger \hat{a}_4^\dagger$  gives

$$\frac{\hat{a}_1^\dagger \hat{a}_5^\dagger}{3\sqrt{3}} + \frac{\hat{a}_2^\dagger \hat{a}_6^\dagger}{3\sqrt{3}} |0\rangle = \frac{\sqrt{2}}{3\sqrt{3}} \left( \frac{|1_1 1_5\rangle + |1_2 1_6\rangle}{\sqrt{2}} \right) \quad (7.9)$$

or in the computational basis as labelled in Fig. 7.4,  $|\Phi^+\rangle = (|0_a 0_b\rangle + |1_a 1_b\rangle)/\sqrt{2}$  with probability  $p = 2/27$ .

This circuit is described by the unitary matrix:

$$\hat{U}_{\text{BSG}} = \begin{pmatrix} 0.707 & 0.707 & 0 & 0 & 0 & 0 \\ 0.408 & -0.408 & -0.577 & 0.577 & 0 & 0 \\ 0.408 & -0.408 & 0.289 + 0.289i & -0.289 + 0.289i & -0.408i & -0.408i \\ 0.408 & -0.408 & 0.289 - 0.289i & -0.289 - 0.289i & 0.408i & 0.408i \\ 0 & 0 & 0.333 - 0.471i & 0.333 - 0.471i & 0.236 - 0.333i & 0.236 - 0.333i \\ 0 & 0 & 0 & 0 & 0.707 & 0.707 \end{pmatrix}$$

which corresponds to an on-chip phase configuration of

$$R_{\text{BSG}} = \begin{pmatrix} (0.000, 1.571) & (0.000, 1.231) & (0.000, 1.571) & (0.000, 3.141) & (0.000, 3.142) \\ & (0.000, 3.142) & (0.000, 1.571) & (1.571, 1.231) & (0.000, 3.142) \\ & & (0.000, 3.142) & (0.000, 3.142) & (0.000, 1.571) \\ & & & (0.000, 3.142) & (0.000, 3.142) \\ & & & & (0.000, 3.142) \end{pmatrix}.$$

#### 7.4.3 EXPERIMENT

For Bell states, measurements in similar bases should be correlated while measurements in different bases should be uncorrelated. To confirm the successful generation of a Bell state we make both types of measurements and use the subsequent results to witness entanglement

## 7.4. HERALDED ENTANGLED STATES

---

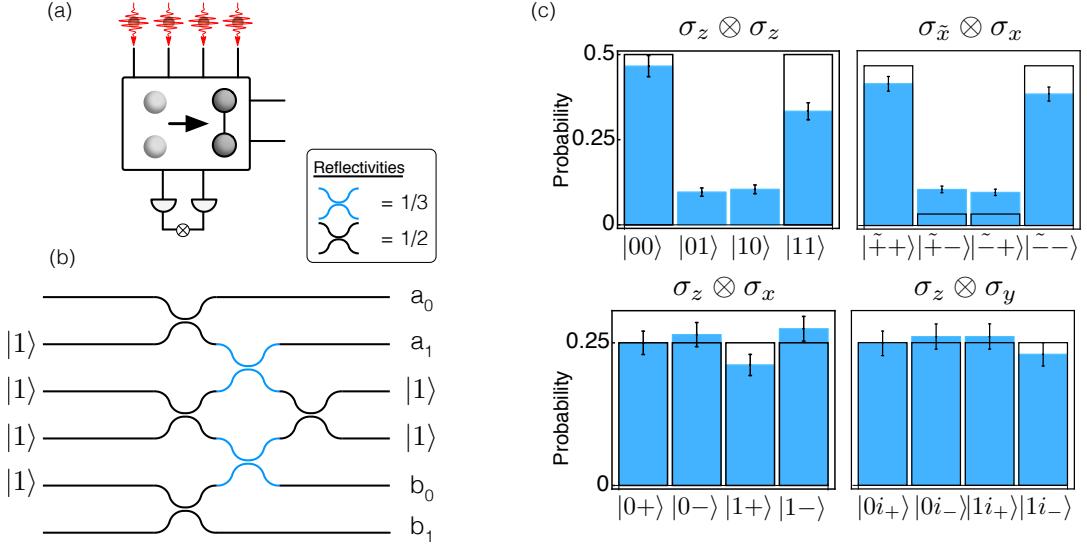


Figure 7.4: **LPU heralded Bell state generator.** (a) The heralded Bell state generator receives four photons and emits two of them in a maximally entangled state upon detection of the remaining two. (b) Our linear optical protocol emits a Bell state on modes  $\{a, b\}$  with input and heralding modes labelled by  $|1\rangle$ . The closed interferometer has  $\pi/2$  phase (not shown) and in the beamsplitter construction phase shifts result from the underside of each splitter. (c) Experimental data measuring Bell state correlations in a given basis (blue), with ideal theoretical values overlaid; error bars assume Poissonian counting statistics.

We inject the photons  $\{N, S, E, W\}$  into modes  $\{1, 3, 4, 5\}$  of our LPU. In this configuration the four-photon state arising from two independent SPDC events does not give rise to events in the computational subspace. After implementing the BSG, measurements on both qubits in the computational basis  $\sigma_z \otimes \sigma_z$  are straightforward [Fig. 7.5(a)] and arbitrary single qubit measurements on the  $b_{0,1}$  modes  $\sigma_z \otimes \sigma_{\hat{n}}$  are possible with the unused MZI  $\hat{M}_{1,5}$  [Fig. 7.5(b)].

To obtain statistics for the  $\sigma_x$  measurement on qubit 1, we create a fibre looped Sagnac interferometer between the output of modes  $a_0$  and  $a_1$  [shown in Fig. 7.5(c)] injecting the photon back through the chip with a stable phase. Due to the configuration of the circuit, the photon sees a 1/3 reflectivity MZI between modes 2

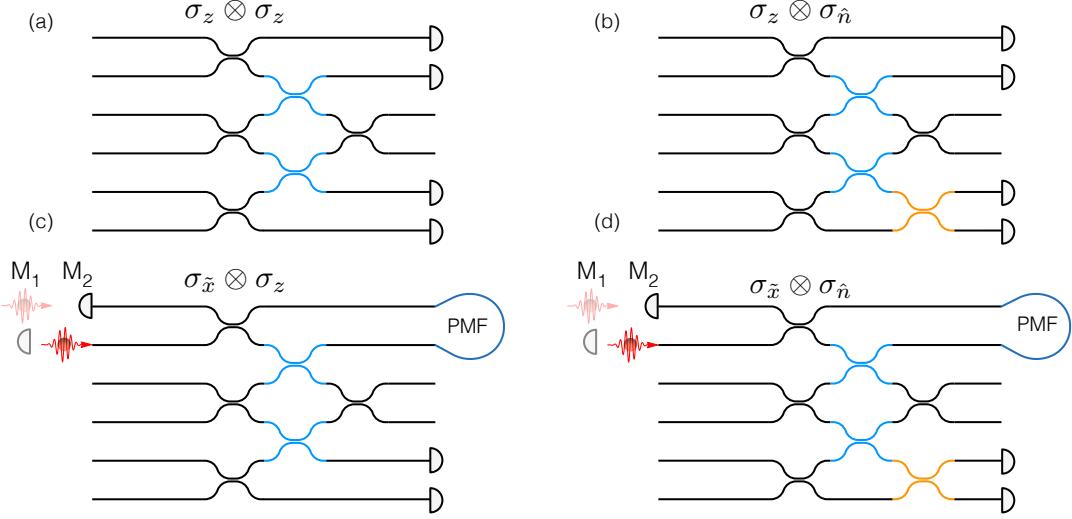


Figure 7.5: **Heralded Bell state generator measurements.** (a) Measurements in the computational basis are taken directly from detectors. (b) Arbitrary single qubit measurements on modes  $b_{0,1}$  can be made with a unused MZI (orange). (c) Non-computational measurements on modes  $a_{0,1}$  are made via a fibre looped Sagnac interferometer (PMF), injecting the qubit back through the LPU to implement a POVM on modes 1 and 2, which is reconstructed via two separate measurements  $M_1, M_2$ . (d) Both techniques can be combined to implement an entanglement witness.

and 3, before a 1/2 reflectivity MZI between modes 1 and 2. This circuit therefore implements a single qubit positive-operator valued measure (POVM) with three elements,  $\{E_+, E_-, E_1\}$  where

$$\begin{aligned} E_+ &= \frac{1}{6} |1\rangle\langle 1| + \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2\sqrt{3}} (|1\rangle\langle 0| + |0\rangle\langle 1|) \\ E_- &= \frac{1}{6} |1\rangle\langle 1| + \frac{1}{2} |0\rangle\langle 0| - \frac{1}{2\sqrt{3}} (|1\rangle\langle 0| + |0\rangle\langle 1|) \\ E_1 &= \frac{2}{3} |1\rangle\langle 1| \end{aligned}$$

corresponding to detection in modes  $\{1, 2, 3\}$  respectively. Since we cannot detect in mode 3 (this is one of the inputs), we postselect on events where the photon is detected in modes 1 and 2, which should occur with probabilities given by

## 7.4. HERALDED ENTANGLED STATES

---

Basis	Output			
	$a_0, b_0$	$a_0, b_1$	$a_1, b_0$	$a_1, b_1$
$\sigma_z \otimes \sigma_z$	0.466 (0.5)	0.096 (0)	0.104 (0)	0.334 (0.5)
$\sigma_{\tilde{x}} \otimes \sigma_x$	0.414 (0.467)	0.105 (0.033)	0.097 (0.033)	0.384 (0.467)
$\sigma_z \otimes \sigma_x$	0.250 (0.25)	0.264 (0.25)	0.211 (0.25)	0.275 (0.25)
$\sigma_z \otimes \sigma_y$	0.249 (0.25)	0.261 (0.25)	0.261 (0.25)	0.230 (0.25)

Table 7.4: **Heralded Bell state generator results.** Experimentally measured probabilities for the heralded Bell state to be found in a given basis, along with the theoretical probabilities in brackets (see Fig. 7.4(b) for output labelling). Experimental data is corrected for measured detector efficiencies.

$$\begin{aligned} p_+ &= \frac{\text{Tr}(E_+\rho)}{\text{Tr}(E_+\rho) + \text{Tr}(E_-\rho)} \\ p_- &= \frac{\text{Tr}(E_-\rho)}{\text{Tr}(E_+\rho) + \text{Tr}(E_-\rho)} \end{aligned}$$

which leads to an expectation value

$$p_+ - p_- = \langle \sigma_{\tilde{x}} \rangle = \frac{\frac{1}{\sqrt{3}} \langle \sigma_x \rangle}{\frac{1}{3} \text{Tr}(\rho |1\rangle\langle 1|) + \text{Tr}(\rho |0\rangle\langle 0|)}$$

such that, with knowledge of the data from the  $\sigma_z$  measurement, we are able to calculate the expectation of  $\sigma_x$ .

Since the experiment would require both input and detection in mode 1, we implement it in two stages, first inputting in mode 1 and detecting four-fold coincidences in modes  $\{2, 3, 4, 5\}$  and  $\{2, 3, 4, 6\}$  [ $M_1$  in Fig. 7.5(c,d)], then inputting in mode 2 and detecting four-fold coincidences in modes  $\{1, 3, 4, 5\}$  and  $\{1, 3, 4, 6\}$  [ $M_2$  in Fig. 7.5(c,d)]. Note that by inputting in mode 2, the state would pick up a relative  $\pi$  phase shift so this is offset by setting  $\phi_{35} = 3\pi/2$ . The two data sets are then normalised with respect to each other by the ratio of total counts in each experiment.

#### 7.4.4 RESULTS

Measurements with the Sagnac interferometer are taken for  $\sim 60$  hours, whilst measurements without are taken  $\sim 16$  hours, collecting in total  $\sim 200$  four-folds for each experiment. The experimentally determined probabilities to find the Bell state in a given basis are displayed in Figure 7.4(c) and Table 7.4.

We found the statistical fidelity for the common basis measurements  $\sigma_z \otimes \sigma_z$  and  $\sigma_{\tilde{x}} \otimes \sigma_x$  to be  $\mathcal{F}_s = 0.891 \pm 0.015$  and  $0.979 \pm 0.003$  respectively, and the uncommon bases  $\sigma_z \otimes \sigma_x$  and  $\sigma_z \otimes \sigma_y$  to be  $0.999 \pm 0.002$  and  $1.000 \pm 0.002$ . These measurements were used to verify the entanglement of our state by calculating  $E = 1/2(\langle \sigma_x \otimes \sigma_x \rangle + \langle \sigma_z \otimes \sigma_z \rangle)$ , finding a value of  $E = 0.673 \pm 0.031$  where  $E > 1/2$  witnesses entanglement [288]

## 7.5 QUANTUM PROCESS TOMOGRAPHY

Whilst the measurements above give partial information about the process — such as the map between logical basis states or a bound on entanglement — capturing complete information requires full process tomography; which due to the versatility of our LPU, we are able to perform for the unheralded CNOT gate presented in Section 2.6.7. With no ancillas, this unscalable gate requires two photons which are consumed as part of its operation [shown in Fig. 7.6(a)]. Several examples of photonic chips specifically fabricated to implement such two-qubit gates have been reported [14, 155, 289]. To compare the performance of our universal processor against devices fabricated for a specific task, we implemented a two-photon unheralded CNOT gate [96, 97, 118] [shown in Fig. 7.6(b)] with single qubit preparation and measurement capabilities and performed full quantum process tomography [181].

Two-qubit states were prepared and measured in the form  $|\psi_n\rangle \otimes |\psi_m\rangle$  and  $|\psi_n\rangle \langle \psi_n| \otimes |\psi_m\rangle \langle \psi_m|$  respectively, where  $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ . An estimate of the Choi-Jamiolkowski state  $\rho_{\mathcal{E}}^{est}$  corresponding to the process was

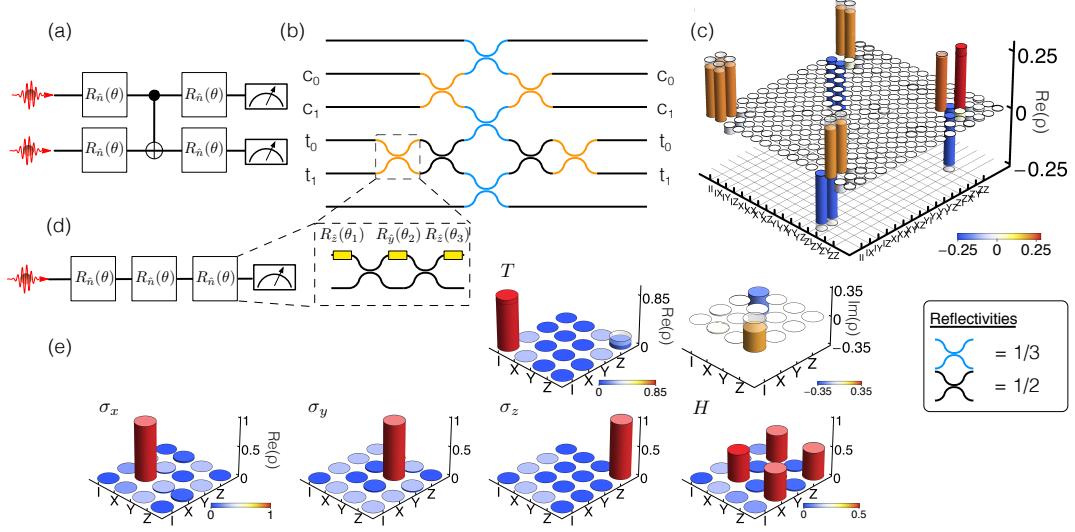


Figure 7.6: **Quantum process tomography.** (a) Quantum process tomography of an unheralded two-qubit CNOT gate can be performed with the addition of arbitrary single qubit preparation and measurement operations. (b) The linear optical circuit realising the un-heralded CNOT gate, with MZIs (inset, orange) allowing single qubit operations. (c) Experimentally determined process matrix with ideal theoretical values overlaid. (d) An arbitrary single qubit rotation  $R_{\hat{n}}(\theta)$  about some vector  $(\hat{n})$  on the Bloch sphere can be realised with an MZI and additional phase shifters. Three consecutive MZIs allows us to perform full process tomography on any single qubit operation. (e) Experimental data showing the measured process matrices for the three Pauli operations, the Hadamard gate ( $\hat{H}$ ), and the  $\pi/8$  phase gate ( $\hat{T}$ ). Experimental data is corrected for measured detector efficiencies.

found using maximum-likelihood estimation (MLE) by minimisation of an approximation to the negative loglikelihood function:

$$\rho_{\mathcal{E}^{est}} = \underset{\rho_{\mathcal{E}}}{\operatorname{argmin}} \left\{ \sum_{i,j} \frac{N_{ij}(p_{ij} - d \operatorname{Tr}[\rho_{\mathcal{E}} E_{ij}])^2}{p_{ij}(1-p_{ij})} \right\} \quad (7.10)$$

$$(7.11)$$

where  $p_{ij} = n_{ij}/N_{ij}$  are the experimental frequencies and  $E_{ij} = (\rho_i)^T \otimes \Pi_j$ ,  $i$  labelling the preparation and  $j$  the measurement effect. To avoid problems associated with zero probabilities in MLE we use hedged MLE [290], where the

experimental probabilities are adjusted to

$$p_{ij} = \frac{n_{ij} + \beta}{N_{ij} + K\beta} \quad (7.12)$$

where  $K$  is the number of outcomes in the measurement of  $p_{ij}$  and  $\beta = 0.1$  is the hedging parameter. The minimisation is performed by phrasing it as a Semidefinite Program (SDP) and solved using the CSDP solver [291].

The average gate fidelity  $\mathcal{F}_g$  defined as  $\int d\psi \langle \psi | U^\dagger \mathcal{E}(|\psi\rangle\langle\psi|) U | \psi \rangle$  was calculated from the process fidelity via the relation  $\mathcal{F}_g = (d\mathcal{F}_p + 1)/(d + 1)$  and errors were calculated by a bootstrapping method, where the raw experimental counts were resampled 100 times with Poissonian noise and the statistics of the resulting distributions analysed. The process matrix  $\text{Re}(\rho_{\mathcal{E}^{\text{est}}})$  is shown in Fig. 7.6(c); the process fidelity was found to be  $\mathcal{F}_p = 0.909 \pm 0.001$ , and the average gate fidelity  $\mathcal{F}_g = 0.927 \pm 0.001$ , greater than those previously reported [14, 155, 185].

From Section 7.2, combined with two-qubit operations, a small set of single qubit gates [Fig. 7.6(d)], including the Hadamard ( $\hat{H}$ ) and  $\pi/8$  ( $\hat{T}$ ) gates are sufficient to realise a universal gate set for quantum computing. We implemented and performed full quantum process tomography for these two gates and for the three Pauli gates [Fig. 7.6(e)], finding an average process fidelity of  $\mathcal{F}_p = 0.992 \pm 0.008$ .

## 7.6 VERIFYING GATE OPERATION

From an experimental perspective the requirement of heralding adds a significant layer of complexity. As we have seen in Section 3.3, two photon states are produced with speed and with high fidelity, but four photon states are produced at a much lower rate and with lower indistinguishability. Therefore robust and accurate characterisation techniques are necessary to assess the gate fidelity before embarking on long data runs.

To measure the performance of our device directly, independent of multi-photon source errors, we adapt previous super-stable tomography techniques [187] to re-

## 7.7. CONCLUDING REMARKS

---

cover the raw transfer matrix  $\hat{M}$  describing the interferometer. Methods presented in Chapter 4 reconstruct a unitary matrix, hence assume the device is lossless; a highly unphysical assumption! In reality there are propagation losses, losses per optical component, non-uniform facet loss, moreover these losses can be path dependent meaning they don't simply factor out. To that end we reconstructed the transfer matrix  $\hat{M}$  for three of our quantum logic gates, making no assumption about the unitarity of the device.

We first tested the stability of our device by setting the circuit to implement the Fourier Transform, injecting single photons into modes 1 and 2, and monitoring single photon output fluctuations. Over a period of 140 hours we observed an average power variation of  $< 0.1\%$ , implying the device is well described by a single transfer matrix, particularly on the timescale of a typical single experiment, which is several orders of magnitude shorter.

As in Chapter 4, the transfer matrix  $\hat{M}$  was recovered using measurements of single photon ensembles to determine the absolute value of matrix entries, and two-photon ensembles to determine phases [187]. However, the entire matrix is normalised by a *single* scalar quantity (rather than each column) given by the sum of counts in the largest column. Unitarity of the transfer matrix is not assumed in its reconstruction: orthogonality between matrix columns is not enforced; columns are not individually normalised.

As before, the circuit fidelity between  $\hat{M}$  and the intended unitary  $\hat{U}$  is defined as  $\mathcal{F}_c = \text{Tr}(|U^\dagger \cdot M|^2)/6$ . For the Bell state generator, the heralded- and unheralded CNOT respectively we found  $\mathcal{F}_c = 0.943 \pm 0.004, 0.941 \pm 0.018$  and  $0.939 \pm 0.040$ .

## 7.7 CONCLUDING REMARKS

We have applied our universal LPU to a variety of quantum information processing protocols: from new entanglement generation schemes, to the first integrated implementation of scalable quantum logic gates — our LPU switches between these

---

## 7. QUANTUM COMPUTATION WITH UNIVERSAL LINEAR OPTICS

and any other protocol in seconds. The breadth of tasks we implement highlights a key functionality of universal quantum devices: namely, to serve as a testbed for developing and discovering new quantum protocols. It is in this context — rather than as a component in a universal LOQC — we expect it to find application; replacing a multitude of existing and future prototype systems.

Combining LPUs with existing higher-efficiency sources and detectors will expand their capabilities, and the development of LPUs with high-speed modulation [160] will enable the dynamically adaptive circuitry necessary for LO quantum computing. Integration of these components [20, 292] with larger low-loss circuits [293] will open up new avenues of research and application.

# 8

## Discussion

### 8.1 KEY RESULTS

Over the course of this thesis and my PhD in Bristol, I have demonstrated how the generation, manipulation and detection of single photon states can be bought together in a single machine — a linear optical processor — capable of performing a multitude of quantum information processing tasks. Here, I summarise the key results:

#### **1. Efficient hardware level characterisation techniques.**

Building on a previous proposal, we implemented a series of device level characterisation techniques, and proposed practical extensions, making the protocol both more robust and more accurate. We fully characterised a nine mode waveguide device (which to our knowledge is the largest interferometer

characterised with these techniques) and observed time evolution in a 21 mode quantum walk — results of which would have been unobtainable via traditional tomographic techniques.

**2. Verification of boson sampling against tractable distributions.**

Using a linear optical processor based on passive waveguide technology, we implemented two key protocols for the verification of a formally unverifiable algorithm. First, we implemented a protocol which rules out the sampling of bosons from a trivial distribution; second, we proposed and implemented an experimentally motivated protocol, relying on bosonic bunching, which rules out sampling from a distribution of distinguishable particles.

**3. Verification via predictable quantum correlations.**

We proposed a new approach to verification whereby a circuit configuration is set which engenders large-scale, ordered, photonic quantum interference; yet produces an efficiently predictable probability distribution. Confirmation of this predictable structure is then used as evidence for correct operation when the device is set to an unverifiable mode of operation. We used this technique, and the phenomena of bosonic clouding, to verify quantum interference of up to five photons in 21 modes — a Hilbert space of  $> 50,000$  dimensions.

**4. A universal linear optical processor.**

We presented the first fully reconfigurable universal linear optical processor. Whilst it has been known for 30 years that such a device was possible it was only until now that the necessary technology existed for the high fidelity fabrication and operation of many reconfigurable waveguide elements. Our six-mode universal system consists of a cascade of 15 Mach-Zehnder interferometers with 30 thermo-optic phase shifters. Alongside this device we present methods for characterisation, calibration and benchmarking.

**5. Verification with universal linear optics.** We programmed the universal linear optical processor to implement 100 boson sampling protocols, and si-

## 8.2. OUTLOOK

---

multaneously realise newly proposed verification procedures (based upon our previous results). We implemented 100 single photon Haar random unitaries with average fidelity  $0.999 \pm 0.001$ , and explore newly discovered complex Hadamard matrices. Finally, we verified that six photon events are drawn from a quantum distribution with confidence  $p = 0.998$ .

6. **Quantum information processing with universal linear optics.** We programmed the universal linear optical processor to implement (to the best of our knowledge) the first integrated heralded CNOT gate; reproducing the computational basis truth table. We implemented the first on-chip heralded entanglement generation scheme and performed a series of measurements to witness entanglement. We performed full quantum process tomography of a unheralded-CNOT, and achieved fidelities surpassing those previously reported in linear optical quantum computing.

## 8.2 OUTLOOK

The general approach of Chapters 4 and 5 is to leverage the experimentalists information about a system to significantly reduce the size of a characterisation or verification problem. In the context of characterisation, for any quantum technology to have a hope of scaling efficient hardware characterisation techniques are essential. This information can be used for *in situ* error correction, shaping future device designs, and informing platform specific error correction codes [177, 178]. Whilst hardware level analysis has been provided for platforms such as superconducting qubits [76], it is lacking from linear optics, and until this analysis is provided there will always be a question mark over scalability. The iterative SST protocol will likely find application in the rapid characterisation of many devices from large fabrication runs where time is a constraint. Similar large scale fabrication runs of integrated photon sources [20] and detectors [294] are on the horizon, and we expect similar rapid device level characterisation techniques to emerge (see for example Jizan et al. [193]).

The first machines to solve problems intractable to classical computers, are likely to tackle bespoke problems suited to their own particular physical capabilities. Boson sampling is one example of this in the context of photonics, but other analogue quantum simulators exist, for example: large scale quantum annealing machines [252, 253], ion traps with hundreds of spins [254] and ultra-cold quantum gasses [295]. Our results demonstrate both the enormity of the task of verification as systems scale up in size, and the efficacy of utilising physical knowledge about a system. We therefore expect machine level approaches to verification to find application for systems which exhibit their own physical properties (for example anti-bunching in a fermionic gas [250]).

In Chapters 6 and 7 we present a universal linear optical processor. The immediate resource savings such a universal system offers is significant. Experiments that previously took months or years to build and collect data, now take milliseconds to build and hours to collect data. Compare for example the months taken for the first bulk KLM-CNOT gate, to the hours it took for our implementation. The capabilities of linear optical processors will be expanded further with high-speed modulation [160], integrated sources [20] and detectors [21] and larger low-loss circuitry [293, 296].

The breadth of tasks we implement, and the speed with which we do so, highlights a key functionality of universal quantum devices: namely, to serve as a testbed for developing new quantum protocols. It is this functionality, rather than as a component in a universal linear optical quantum computer, where we expect it to find application; replacing a multitude of existing and future prototype systems. In particular, this author predicts universal linear optical processors will find application in exploring pre-universal models of quantum computation which make use of the nature of photons themselves. Recent work has provided tantalising evidence for this in the context of quantum chemistry [297], and further application may be found in more nascent fields such as quantum machine learning [64–66]. It is this authors opinion that pre-universal models of quantum computation are the next frontier for quantum photonic science, and his hope that some of the results presented in this thesis may contribute towards that journey.

## Bibliography

- [1] D. Hanneke, S. Fogwell, and G. Gabrielse, Phys. Rev. Lett. **100**, 120801 (2008).
- [2] R. Pohl, A. Antognini, F. Nez, F. D. Amaro, F. Biraben, J. M. R. Cardoso, D. S. Covita, A. Dax, S. Dhawan, L. M. P. Fernandes, A. Giesen, T. Graf, T. W. Hänsch, P. Indelicato, L. Julien, C.-Y. Kao, P. Knowles, E.-O. Le Bigot, Y.-W. Liu, J. A. M. Lopes, L. Ludhova, C. M. B. Monteiro, F. Mulhauser, T. Nebel, P. Rabinowitz, J. M. F. dos Santos, L. A. Schaller, K. Schuhmann, C. Schwob, D. Taqqu, J. F. C. A. Veloso, and F. Kottmann, Nature **466**, 213 (2010).
- [3] T. S. Kuhn, *The Structure of Scientific Revolutions*, 50th Anniversary Edition (University of Chicago Press, 2012).
- [4] A. Einstein, Annalen der Physik **322**, 132 (1905).
- [5] J. S. Bell, Physics **1**, 195 (1964).
- [6] S. J. Freedman and J. Clauser, Phys. Rev. Lett. **28**, 938 (1972).
- [7] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
- [8] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).
- [9] J. L. O'Brien, Science **318**, 1567 (2007).

---

## BIBLIOGRAPHY

- [10] E. Knill, R. Laflamme, and G. Milburn, *Nature* **409**, 46 (2001).
- [11] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, *Science* **320**, 646 (2008).
- [12] J. L. O'Brien, A. Furusawa, and J. Vučković, *Nat. Photon.* **3**, 687 (2009).
- [13] G. D. Marshall, A. Politi, J. C. F. Matthews, P. Dekker, M. Ams, M. J. Withford, and J. L. O'Brien, *Opt. Exp.* **17**, 12546 (2009).
- [14] A. Crespi, R. Ramponi, R. Osellame, L. Sansoni, I. Bongioanni, F. Sciarrino, G. Vallone, and P. Mataloni, *Nat. Comms.* **2**, 566 (2011).
- [15] J. C. F. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien, *Nat. Photon.* **3**, 346 (2009).
- [16] B. J. Smith, D. Kundys, N. Thomas-Peter, P. G. R. Smith, and I. A. Walmsley, *Opt. Exp.* **17**, 13516 (2009).
- [17] A. Laing, A. Peruzzo, A. Politi, M. R. Verde, M. Hadler, T. C. Ralph, M. G. Thompson, and J. L. O'Brien, *App. Phys. Lett.* **97**, 211109 (2010).
- [18] A. Peruzzo, M. Lobino, J. Matthews, N. Matsuda, A. Politi, K. Poulios, X.-Q. Zhou, Y. Lahini, N. Ismail, K. Worhoff, Y. Bromberg, Y. Silberberg, M. G. Thompson, and J. L. O'Brien, *Science* **329**, 1500 (2010).
- [19] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, and R. Osellame, *Phys. Rev. Lett.* **108**, 010502 (2012).
- [20] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G. Thompson, *Nat. Photon.* **8**, 104 (2014).
- [21] W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, and H. X. Tang, *Nat. Comms.* **3**, 1325 (2012).

## BIBLIOGRAPHY

---

- [22] S. Aaronson and A. Arkhipov, in *Proceedings of the 43rd annual ACM symposium on Theory of computing* (ACM, 2011) pp. 333–342.
- [23] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, *Science* **339**, 798 (2013).
- [24] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, *Science* **339**, 794 (2013).
- [25] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, *Nat. Photon.* **7**, 540 (2013).
- [26] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, *Nat. Photon.* **7**, 545 (2013).
- [27] M. Reck, A. Zeilinger, H. J. Bernstein, and H. Bertani, *Phys. Rev. Lett.* **73**, 58 (1994).
- [28] R. Feynman, R. Leighton, and M. Sands, (1963).
- [29] C. Jönsson, *Z. Physik* **161**, 454 (1961).
- [30] A. Zeilinger, R. Gähler, C. G. Shull, W. Treimer, and W. Mampe, *Rev. Mod. Phys.* **60**, 1067 (1988).
- [31] D. W. Keith, M. L. Schattenburg, H. I. Smith, and D. E. Pritchard, *Phys. Rev. Lett.* **61**, 1580 (1988).
- [32] O. Carnal and J. Mlynek, *Phys. Rev. Lett.* **66**, 2689 (1991).
- [33] W. Schöllkopf and J. P. Toennies, *Science* **266**, 1345 (1994).
- [34] M. Arndt, O. Nairz, J. Vos-Andreae, and C. Keller, *Nature* **401**, 680 (1999).

---

## BIBLIOGRAPHY

- [35] B. S. Zhao, G. Meijer, and W. Schöllkopf, Science **331**, 892 (2011).
- [36] T. Juffmann, A. Milic, M. Müllneritsch, P. Asenbaum, A. Tsukernik, J. Tüxen, M. Mayor, O. Cheshnovsky, and M. Arndt, Nature Nanotechnology **7**, 297 (2012).
- [37] J. Preskill, *Quantum Computation Lecture Notes* (2012) pp. 1–40.
- [38] R. Landauer, Physics Letters A **217**, 188 (1996).
- [39] I. L. Markov, Nature **512**, 147 (2014).
- [40] R. Landauer, IBM Journal of Research and Development **5**, 183 (1961).
- [41] C. H. Bennett and R. Landauer, Scientific American (1985).
- [42] J. Lee, Y. Ahn, Y. Park, M. Kim, D. Lee, K. Lee, C. Cho, T. Chung, and K. Kim, in *VLSIT-03* (Japan Soc. Applied Phys, 2003) pp. 57–58.
- [43] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
- [44] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [45] N. Brunner, D. Cavalcanti, S. Pironio, and V. Scarani, Rev. Mod. Phys. **86**, 419 (2014).
- [46] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
- [47] A. M. Turing, Proc. London Math. Soc. **s2-42**, 230 (1936).
- [48] R. P. Feynman, *Feynman Lectures On Computation*, edited by A. Hey and R. W. Allen (Westview Press, 1996).
- [49] S. Arora and B. Barak, *Computational Complexity*, A Modern Approach (Cambridge University Press, 2009).

## BIBLIOGRAPHY

---

- [50] S. Aaronson, *Quantum Computing Since Democritus* (Cambridge University Press, Cambridge, 2013).
- [51] D. Deutsch, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **400**, 97 (1985).
- [52] A. Church, Am. J. Math. **58**, 345 (1936).
- [53] D. Deutsch and R. Jozsa, Proceedings: Mathematical and Physical Sciences **439**, 553 (1992).
- [54] E. Bernstein and U. Vazirani, in *STOC '93: Proceedings of the twenty-fifth annual ACM symposium on Theory of computing* ( ACM Request Permissions, New York, New York, USA, 1993) pp. 11–20.
- [55] D. R. Simon, in *SFCS-94* (IEEE Comput. Soc. Press, 1994) pp. 116–123.
- [56] M. S. Tame, B. A. Bell, C. Di Franco, W. J. Wadsworth, and J. G. Rarity, Phys. Rev. Lett. **113**, 200501 (2014).
- [57] L. M. Adleman, J. DeMarrais, and M.-D. A. Huang, SIAM J. Comput. **26**, 1524 (1997).
- [58] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (Society for Industrial and Applied Mathematics, 1994) pp. 124–134.
- [59] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21** (1978).
- [60] A. K. Lenstra and H. W. J. Lenstra (Springer-Verlag Berlin Heidelberg, 1993) p. 131.
- [61] A. Y. Kitaev, (1995), arXiv:quant-ph/9511026v1 .
- [62] L. K. Grover, in *STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing* ( ACM Request Permissions, 1998).

---

## BIBLIOGRAPHY

- [63] S. Lloyd, Science **273**, 1073 (1996).
- [64] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009).
- [65] S. Lloyd, M. Mohseni, and P. Rebentrost, (2013), arXiv:quant-ph/1307.0411v2 .
- [66] S. Aaronson, Nat. Phys. **11**, 291 (2015).
- [67] D. P. DiVincenzo, Fortschr. Phys. **48**, 771 (2000).
- [68] D. Gottesman, (2009), arXiv:quant-ph/0904.2557v1 .
- [69] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
- [70] P. Jurcevic, B. P. Lanyon, P. Hauke, C. Hempel, P. Zoller, R. Blatt, and C. F. Roos, Nature **511**, 202 (2014).
- [71] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas, Phys. Rev. Lett. **113**, 220501 (2014).
- [72] C. Monroe and J. Kim, Science **339**, 1164 (2013).
- [73] J. Clarke and F. K. Wilhelm, Nature **453**, 1031 (2008).
- [74] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O’Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, Nature **508**, 500 (2014).
- [75] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Phys. Rev. A **86**, 032324 (2012).
- [76] J. M. Martinis and A. Megrant, (2014), arXiv:quant-ph/1410.5793v1 .
- [77] I. Bloch, Nature **453**, 1016 (2008).

## BIBLIOGRAPHY

---

- [78] L. Vandersypen and I. L. Chuang, Rev. Mod. Phys. **76**, 1037 (2004).
- [79] S. C. Benjamin, B. W. Lovett, and J. M. Smith, Laser & Photon. Rev. **3**, 556 (2009).
- [80] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature **390**, 575 (1997).
- [81] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
- [82] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
- [83] M. Born and E. Wolf, *Principles of Optics, seventh expanded edition* (Cambridge, 1999).
- [84] N. K. Langford, *Encoding, Manipulating and Measuring Quantum Information in Optics*, Ph.D. thesis, University of Queensland (2007).
- [85] C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, 2005).
- [86] S. Scheel, (2004), arxiv:quant-ph/0406127v1 .
- [87] K. P. Zetie, S. F. Adams, and R. M. Tocknell, Phys. Educ. **35**, 46 (2000).
- [88] T. Tilma and E. C. G. Sudarshan, J. Phys. A: Math. Gen. **35**, 10467 (2002).
- [89] D. E. Chang, V. Vuletić, and M. D. Lukin, Nat. Photon. **8**, 685 (2014).
- [90] N. Matsuda, R. Shimizu, Y. Mitsumori, H. Kosaka, and K. Edamatsu, Nat. Photon. **3**, 95 (2009).
- [91] J. Shapiro and M. Razavi, New J. Phys. **9**, 16 (2007).
- [92] C. Hong, Z. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).

---

## BIBLIOGRAPHY

- [93] S. Popescu, Phys. Rev. Lett. **99**, 250501 (2007).
- [94] M. Tillmann, S.-H. Tan, S. E. Stoeckl, B. C. Sanders, H. de Guise, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, (2014), arXiv:quant-ph/1403.3433v3 .
- [95] M. C. Tichy, Phys. Rev. A **91**, 022316 (2015).
- [96] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, Phys. Rev. A **65**, 062324 (2002).
- [97] H. Hofmann and S. Takeuchi, Phys. Rev. A **66**, 024308 (2002).
- [98] A. H. Compton, Phys. Rev. **21**, 483 (1923).
- [99] W. Denk and K. Svoboda, Neuron **18**, 351 (1997).
- [100] <http://www.idquantique.com/quantum-safe-crypto/> ().
- [101] <http://www.magiqtech.com/Products.html> ().
- [102] <http://www.idquantique.com/photon-counting/id350-photon-pair-source/> ().
- [103] B. Lounis and M. Orrit, Rep. Prog. Phys. **68**, 1129 (2005).
- [104] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Rev Sci Instrum **82**, 071101 (2011).
- [105] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002).
- [106] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, Science **303**, 1992 (2004).
- [107] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, Nature **431**, 1075 (2004).

## BIBLIOGRAPHY

---

- [108] S. C. Kitson, P. Jonsson, J. G. Rarity, and P. R. Tapster, Phys. Rev. A **58**, 620 (1998).
- [109] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999).
- [110] P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoğlu, Science **290**, 2282 (2000).
- [111] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
- [112] D. C. Burnham and D. L. Weinberg, Phys. Rev. Lett. **25**, 84 (1970).
- [113] J. G. Rarity and P. R. Tapster, JOSA B **6**, 1221 (1989).
- [114] J. G. Rarity, P. R. Tapster, E. Jakeman, T. Larchuk, R. Campos, M. Teich, and B. Saleh, Phys. Rev. Lett. **65**, 1348 (1990).
- [115] Z. Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988).
- [116] Y. H. Shih and C. O. Alley, Phys. Rev. Lett. **61**, 2921 (1988).
- [117] J. G. Rarity and P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990).
- [118] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature **426**, 264 (2003).
- [119] E. Martín López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, Nat. Photon. **6**, 1 (2012).
- [120] B. P. Lanyon, J. D. Whitfield, G. G. Gillett, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik, and A. G. White, Nat. Chem. **2**, 1 (2010).
- [121] M. D'Angelo, M. V. Chekhova, and Y. Shih, Phys. Rev. Lett. **87**, 013602 (2001).

---

## BIBLIOGRAPHY

- [122] P. Walther, J. W. Pan, M. Aspelmeyer, R. Ursin, S. Gasparoni, and A. Zeilinger, *Nature* **429**, 158 (2004).
- [123] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg, *Nature* **429**, 161 (2004).
- [124] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, *Phys. Rev. Lett.* **75**, 4337 (1995).
- [125] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, *Phys. Rev. Lett.* **76**, 4656 (1996).
- [126] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **84**, 4729 (2000).
- [127] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, *Phys. Rev. Lett.* **84**, 4733 (2000).
- [128] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.* **84**, 4737 (2000).
- [129] Y.-F. Huang, B.-H. Liu, L. Peng, Y.-H. Li, L. Li, C.-F. Li, and G.-C. Guo, *Nat. Comms.* **2** (2011).
- [130] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, *Nat. Photon.* **6**, 225 (2012).
- [131] J. B. Spring, P. S. Salter, B. J. Metcalf, P. C. Humphreys, M. Moore, N. Thomas-Peter, M. Barbieri, X.-M. Jin, N. K. Langford, W. S. Kolthammer, M. J. Booth, and I. A. Walmsley, *Opt. Exp.* **21**, 13522 (2013).
- [132] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin, *Electronics Letters* **37**, 26 (2001).

## BIBLIOGRAPHY

---

- [133] J. Chen, A. J. Pearlman, A. Ling, J. Fan, and A. Migdall, Opt. Exp. **17**, 6727 (2009).
- [134] A. L. Migdall, D. Branning, and S. Castelletto, Phys. Rev. A **66**, 053805 (2002).
- [135] X.-s. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, Phys. Rev. A **83**, 043814 (2011).
- [136] M. J. Collins, C. Xiong, I. H. Rey, T. D. Vo, J. He, S. Shahnia, C. Reardon, T. F. Krauss, M. J. Steel, A. S. Clark, and B. J. Eggleton, Nat. Comms. **4**, 1 (2013).
- [137] T. Meany, L. A. Ngah, M. J. Collins, A. S. Clark, R. J. Williams, B. J. Eggleton, M. J. Steel, M. J. Withford, O. Alibart, and S. Tanzilli, Laser & Photonics Reviews **8**, L42 (2014).
- [138] G. J. Mendoza, R. Santagati, J. Munns, E. Hemsley, M. Piekarek, E. Martín López, G. D. Marshall, D. Bonneau, M. G. Thompson, and J. L. O'Brien, (2015), arXiv:quant-ph/1503.01215v1 .
- [139] V. G. Dmitriev, G. G. Gurzadyan, and D. N. Nikogosyan, *Handbook of Non-linear Optical Crystals*, Springer Series in Optical Sciences, Vol. 64 (Springer, Berlin, Heidelberg, 2013).
- [140] M. Ghotbi and M. Ebrahim-Zadeh, Opt. Lett., OL **30**, 3395 (2005).
- [141] Z.-Y. J. Ou, *Multi-Photon Quantum Interference* (Springer Science & Business Media, Boston, MA, 2007).
- [142] R. Okamoto, J. L. O'Brien, H. F. Hofmann, and S. Takeuchi, Proc. Natl. Acad. Sci. U.S.A **108**, 10067 (2011).
- [143] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Science **325**, 1221 (2009).

---

## BIBLIOGRAPHY

- [144] X.-Q. Zhou, T. C. Ralph, P. Kalasuwan, M. Zhang, A. Peruzzo, B. P. Lanyon, and J. L. O'Brien, Nat. Comms. **2**, 413 (2011).
- [145] A. Rossi, G. Vallone, A. Chiuri, F. De Martini, and P. Mataloni, Phys. Rev. Lett. **102**, 153902 (2009).
- [146] M. Tanida, R. Okamoto, and S. Takeuchi, Opt. Exp. **20**, 15275 (2012).
- [147] M. Ghotbi, M. Ebrahim-Zadeh, A. Majchrowski, E. Michalski, and I. V. Kityk, Opt. Lett., OL **29**, 2530 (2004).
- [148] J. Fulconis, O. Alibart, W. J. Wadsworth, and J. G. Rarity, New J. Phys. **9**, 276 (2007).
- [149] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature **434**, 169 (2005).
- [150] D. A. B. Miller, Proceedings of the IEEE **97**, 1166 (2009).
- [151] G. Lifante, *Integrated Photonics, Fundamentals* (John Wiley & Sons, 2003).
- [152] G. T. Reed, G. Mashanovich, F. Y. Gardes, and D. J. Thomson, Nat. Photon. **4**, 518 (2010).
- [153] J. Leuthold, C. Koos, and W. Freude, Nat. Photon. **4**, 535 (2010).
- [154] Y.-C. Chang and L. A. Coldren, *Optimization of VCSEL structure for high-speed operation* (IEEE, 2008).
- [155] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. F. Matthews, M. G. Thompson, and J. L. O'Brien, Nat. Photon. **6**, 45 (2011).
- [156] A. Peruzzo, J. McClean, P. Shadbolt, and M. H. Yung, Nat. Comms. **5**, 4213 (2014).
- [157] J. C. F. Matthews, A. Politi, D. Bonneau, and J. L. O'Brien, Phys. Rev. Lett. **107**, 163602 (2011).

## BIBLIOGRAPHY

---

- [158] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett., OL **29**, 2797 (2004).
- [159] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, Phys. Rev. Lett. **112**, 130501 (2014).
- [160] D. J. Thomson, F. Y. Gardes, J.-M. Fedeli, S. Zlatanovic, Y. Hu, B. P. P. Kuo, E. Myslivets, N. Alic, S. Radic, G. Z. Mashanovich, and G. T. Reed, IEEE Photon. Technol. Lett. **24**, 234 (2012).
- [161] R. P. Bell, Trans. Faraday Soc. **38**, 422 (1942).
- [162] J. Komma, C. Schwarz, G. Hofmann, D. Heinert, and R. Nawrodt, Appl. Phys. Lett. **101**, 041905 (2012).
- [163] N. Matsuda, P. Karkus, H. Nishi, T. Tsuchizawa, W. J. Munro, H. Takesue, and K. Yamada, Opt. Exp. **22**, 22831 (2014).
- [164] F. P. Payne and J. P. R. Lacey, Optical and Quantum Electronics **26**, 977 (1994).
- [165] <http://www.ozoptics.com/ALLNEWPDF/DTS0079.pdf> () .
- [166] M. Abe, Journal of the Ceramic Society of Japan **116**, 1063 (2008).
- [167] M. Kohtoku, T. Kominato, Y. Nasu, and T. Shibata, *New waveguide fabrication techniques for nextgeneration plcs* (NTT Technical Review, 2005).
- [168] T. Kominato, Y. Hida, M. Itoh, H. Takashashi, S. Sohma, and T. Kitoh, in *Proceedings of ECOC* (2004).
- [169] K. Wörhoff, C. G. H. Roeloffzen, R. M. de Ridder, A. Driessens, and P. V. Lambeck, Lightwave Technology, Journal of **25**, 1276 (2007).
- [170] K. Wörhoff, E. Klein, G. Hussein, and A. Driessens, *Silicon oxynitride based photonics*, Vol. 3 (IEEE, 2008).

---

## BIBLIOGRAPHY

- [171] J. C. F. Matthews, K. Poulios, J. D. A. Meinecke, A. Politi, A. Peruzzo, N. Ismail, K. Wörhoff, M. G. Thompson, and J. L. O'Brien, *Sci. Rep.* **3** (2013).
- [172] J. D. A. Meinecke, K. Poulios, A. Politi, J. C. F. Matthews, A. Peruzzo, N. Ismail, K. Wörhoff, J. L. O'Brien, and M. G. Thompson, *Phys. Rev. A* **88**, 012308 (2012).
- [173] J. F. Bauters, M. J. R. Heck, D. John, D. Dai, M.-C. Tien, J. S. Barton, A. Leinse, R. G. Heideman, D. J. Blumenthal, and J. E. Bowers, *Opt. Exp.* **19**, 3163 (2011).
- [174] S. Weiss, *Science* **283**, 1676 (1999).
- [175] N. S. Nightingale, *Exp. Astron.* **1**, 407 (1991).
- [176] A. McCarthy, N. J. Krichel, N. R. Gemmell, X. Ren, M. G. Tanner, S. N. Dorenbos, V. Zwiller, R. H. Hadfield, and G. S. Buller, *Opt. Exp.* **21**, 8904 (2013).
- [177] M. Varnava, D. E. Browne, and T. Rudolph, *Phys. Rev. Lett.* **97**, 120501 (2006).
- [178] S. D. Barrett and T. M. Stace, *Phys. Rev. Lett.* **105**, 200502 (2010).
- [179] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, *Nat. Photon.* **7**, 210 (2013).
- [180] P. J. Shadbolt, *Complexity and Control in Quantum Photonics*, Ph.D. thesis, University of Bristol (2014).
- [181] I. L. Chuang and M. A. Nielsen, *J. Mod. Opt.* **44**, 2455 (1997).
- [182] M. Riebe, K. Kim, P. Schindler, T. Monz, P. O. Schmidt, T. K. Körber, W. Hänsel, H. Häffner, C. F. Roos, and R. Blatt, *Phys. Rev. Lett.* **97**, 220407 (2006).

## BIBLIOGRAPHY

---

- [183] R. C. Bialczak, M. Ansmann, M. Hofheinz, E. Lucero, M. Neeley, A. D. O’Connell, D. Sank, H. Wang, J. Wenner, M. Steffen, A. N. Cleland, and J. M. Martinis, *Nat. Phys.* **6**, 409 (2010).
- [184] G. D. Fuchs, A. L. Falk, V. V. Dobrovitski, and D. D. Awschalom, *Phys. Rev. Lett.* **108**, 157602 (2012).
- [185] J. L. O’Brien, G. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, *Phys. Rev. Lett.* **93**, 080502 (2004).
- [186] S. Rahimi-Keshari, M. A. Broome, R. Fickler, A. Fedrizzi, T. C. Ralph, and A. G. White, *Opt. Exp.* **21**, 13450 (2013).
- [187] A. Laing and J. L. O’Brien, (2012), arXiv:quant-ph/1208.2868v1 .
- [188] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro, *Phys. Rev. A* **66**, 012303 (2002).
- [189] R. Sinkhorn, *The Annals of Mathematical Statistics* **35**, 876 (1964).
- [190] R. Sinkhorn and P. Knopp, *Pacific Journal of Mathematics* **21**, 343 (1967).
- [191] R. H. Brown and R. Q. Twiss, *Nature* (1956).
- [192] Y. Bromberg, Y. Lahini, R. Morandotti, and Y. Silberberg, *Phys. Rev. Lett.* **102**, 253904 (2009).
- [193] I. Jizan, L. G. Helt, C. Xiong, M. J. Collins, D.-Y. Choi, C. J. Chae, M. Liscidini, M. J. Steel, B. J. Eggleton, and A. S. Clark, *Sci. Rep.* , 1 (2015).
- [194] J. Carolan, J. D. A. Meinecke, P. J. Shadbolt, N. J. Russell, N. Ismail, K. Wörhoff, T. Rudolph, M. G. Thompson, J. L. O’Brien, J. C. F. Matthews, and A. Laing, *Nat. Photon.* **8**, 621 (2014).
- [195] N. Spagnolo, C. Vitelli, L. Sansoni, E. Maiorino, P. Mataloni, F. Sciarrino, D. J. Brod, E. F. Galvao, A. Crespi, R. Ramponi, and R. Osellame, *Phys. Rev. Lett.* **111**, 130503 (2013).

---

## BIBLIOGRAPHY

- [196] J. Preskill, (2012), arXiv:quant-ph/1203.5813v3 .
- [197] J. Simon, W. S. Bakr, R. Ma, M. E. Tai, P. M. Preiss, and M. Greiner, Nature **472**, 307 (2011).
- [198] M. H. Freedman, M. Larsen, and Z. Wang, Commun. Math. Phys. **227**, 605 (2002).
- [199] D. Aharonov, V. Jones, and Z. Landau, Algorithmica **55**, 395 (2008).
- [200] T. Kleinjung, K. Aoki, J. Franke, and A. K. Lenstra, in *Advances in Cryptology-CRYPTO 2010* (Springer, 2010) pp. 333–350.
- [201] C. Pomerance, Notice of the AMS **43**, 1473 (1996).
- [202] R. D. V. Meter, III, *Architecture of a Quantum Multicomputer Optimized for Shor’s Factoring Algorithm*, Ph.D. thesis, Keio University (2006).
- [203] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A **54**, 1034 (1996).
- [204] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **106**, 130506 (2011).
- [205] <http://techreport.com/news/27557/intel-broadwell-u-arrives-aboard-15w-28w-mobile-processors> ().
- [206] A. L. Cauchy, Journal de l’École Polytechnique **10**, 91 (1815).
- [207] T. Muir, in *Proceedings of the Royal Society of Edinburgh* (1882) pp. 409–418.
- [208] L. G. Valiant, Theor. Comput. Sci. **8**, 189 (1979).
- [209] S. Toda, SIAM J. Comput. **20**, 865 (1991).
- [210] J. E. Hopcroft and R. M. Karp, SIAM J. Comput. **2**, 225 (1973).

## BIBLIOGRAPHY

---

- [211] H. J. Ryser, Combinatorial Mathematics, *The Carus Mathematical Monographs #14*, (The Mathematical Association of America, 1963).
- [212] M. Jerrum, A. Sinclair, and E. Vigoda, Journal of the ACM (JACM) **51**, 671 (2004).
- [213] L. Gurvits, Mathematical Foundations of Computer Science 2005, Proceedings **3618**, 447 (2005).
- [214] E. R. Caianiello, Nuovo Cim **10**, 1634 (1953).
- [215] M. J. Bremner, A. Montanaro, and D. J. Shepherd, (2015), arXiv:quant-ph/1504.07999v1 .
- [216] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Phys. Rev. Lett. **113**, 100502 (2014).
- [217] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi, R. Ramponi, R. Osel-lame, and F. Sciarrino, Sci. Adv. **1**, e1400255 (2015).
- [218] K. R. Motes, A. Gilchrist, J. P. Dowling, and P. P. Rohde, Phys. Rev. Lett. **113**, 120501 (2014).
- [219] M. Pant and D. Englund, (2015), arXiv:quant-ph/1505.03103 .
- [220] H.-K. Lau and D. F. V. James, Phys. Rev. A **85**, 062329 (2012).
- [221] C. Shen, Z. Zhang, and L. M. Duan, Phys. Rev. Lett. **112**, 050504 (2014).
- [222] P. P. Rohde and T. C. Ralph, Phys. Rev. A **85**, 022332 (2012).
- [223] A. Leverrier and R. García-Patrón, Quant. Inf. Comp. **15**, 489 (2013).
- [224] S. Aaronson and A. Arkhipov, Quant. Inf. Comp. **14**, 1383 (2014).
- [225] C. Gogolin, M. Kliesch, L. Aolita, and J. Eisert, (2013), arXiv:quant-ph/1306.3995v2 .

---

## BIBLIOGRAPHY

- [226] A. Arkhipov and G. Kuperberg, Geom. Topol. Monogr. **18**, 1 (2011).
- [227] E. Fama, Financial Analysts Journal **21**, 55 (1965).
- [228] R. Motwani and P. Raghavan, *Randomized Algorithms* (Chapman & Hall, 1995).
- [229] E. Farhi and S. Gutmann, Phys. Rev. A **58** (1998).
- [230] A. Childs, R. Cleve, E. Deotto, and E. Farhi, Proceedings of STOC'2003 (2003).
- [231] A. Ambainis, SIAM J. Comput. **37**, 210 (2007).
- [232] A. Childs, Phys. Rev. Lett. **102** (2009).
- [233] G. S. Engel, T. R. Calhoun, E. L. Read, T.-K. Ahn, T. Mančal, Y.-C. Cheng, R. E. Blankenship, and G. R. Fleming, Nature **446**, 782 (2007).
- [234] M. Mohseni, P. Rebentrost, S. Lloyd, and A. Aspuru-Guzik, J Chem Phys **129**, (2008).
- [235] H. Schmitz, R. Matjeschk, C. Schneider, J. Glueckert, M. Enderlein, T. Huber, and T. Schaetz, Phys. Rev. Lett. **103**, 090504 (2009).
- [236] Zähringer, F, Kirchmair, G, Gerritsma, R, Solano, E, Blatt, R, and Roos, C F, Phys. Rev. Lett. **104**, 100503 (2010).
- [237] M. Karski, L. Förster, J.-M. Choi, A. Steffen, W. Alt, D. Meschede, and A. Widera, Science **325**, 174 (2009).
- [238] C. A. Ryan, M. Laforest, J. C. Boileau, and R. Laflamme, Phys. Rev. A **72**, 062317 (2005).
- [239] A. Ü. C. Hardal, P. Xue, Y. Shikano, Ö. E. Müstecaplıoğlu, and B. C. Sanders, Phys. Rev. A **88**, 022303 (2013).
- [240] J. Ghosh, Phys. Rev. A **89**, 022309 (2014).

## BIBLIOGRAPHY

---

- [241] B. Do, M. Stohler, S. Balasubramanian, D. Elliott, C. Eash, E. Fischbach, M. Fischbach, A. Mills, and B. Zwickl, JOSA B **22**, 499 (2005).
- [242] M. A. Broome, A. Fedrizzi, B. P. Lanyon, I. Kassal, A. Aspuru-Guzik, and A. G. White, Phys. Rev. Lett. **104**, 153602 (2010).
- [243] A. Schreiber, K. N. Cassemiro, V. Potoček, A. Gábris, P. J. Mosley, E. Andersson, I. Jex, and C. Silberhorn, Phys. Rev. Lett. **104**, 050502 (2010).
- [244] A. Schreiber, A. Gábris, P. P. Rohde, K. Laiho, M. Štefaňák, V. Potoček, C. Hamilton, I. Jex, and C. Silberhorn, Science **336**, 55 (2012).
- [245] H. Perets, Y. Lahini, F. Pozzi, M. Sorel, R. Morandotti, and Y. Silberberg, Phys. Rev. Lett. **100**, 170506 (2008).
- [246] R. P. Feynman, Int.J.Theor.Phys. **21**, 467 (1982).
- [247] P. Knight and E. Roldan, (2003).
- [248] K. Poulios, R. Keil, D. Fry, J. D. A. Meinecke, J. C. F. Matthews, A. Politi, M. Lobino, M. Gräfe, M. Heinrich, S. Nolte, A. Szameit, and J. L. O'Brien, Phys. Rev. Lett. **112**, 143604 (2014).
- [249] A. Crespi, R. Osellame, R. Ramponi, V. Giovannetti, R. Fazio, L. Sansoni, F. De Nicola, F. Sciarrino, and P. Mataloni, Nat. Photon. **7**, 322 (2013).
- [250] T. Rom, T. Best, D. van Oosten, U. Schneider, S. Fölling, B. Paredes, and I. Bloch, Nature **444**, 733 (2006).
- [251] M. C. Tichy, K. Mayer, A. Buchleitner, and K. Mølmer, Phys. Rev. Lett. **113**, 020502 (2014).
- [252] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, E. M. Chapple, C. Endres, J. P. Hilton, K. Karimi, E. Ladizinsky, N. Ladizinsky, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, C. J. S. Truncik, S. Uchaikin, J. Wang, B. Wilson, and G. Rose, Nature **473**, 194 (2011).

---

## BIBLIOGRAPHY

- [253] T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar, and M. Troyer, *Science* **345**, 420 (2014).
- [254] J. W. Britton, B. C. Sawyer, A. C. Keith, C. C. J. Wang, J. K. Freericks, H. Uys, M. J. Biercuk, and J. J. Bollinger, *Nature* **484**, 489 (2012).
- [255] J. Carolan, C. Harrold, C. Sparrow, E. Martín López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, *Science* **349**, 711 (2015).
- [256] A. Himeno, K. Kato, and T. Miya, *IEEE J. Sel. Top. Quantum Electron.* **4**, 913 (1998).
- [257] H. Takahashi, *Opt. Exp.* **19**, B173 (2011).
- [258] <http://www.vishay.com/docs/53044/epicappn.pdf> () .
- [259] Y. Okawachi, O. Kuzucu, M. A. Foster, R. Salem, A. C. Turner-Foster, A. Biberman, N. Ophir, K. Bergman, M. Lipson, and A. L. Gaeta, *IEEE Photon. Technol. Lett.* **24**, 185 (2012).
- [260] M. S. Allman, V. B. Verma, M. Stevens, T. Gerrits, R. D. Horansky, A. E. Lita, F. Marsili, A. Beyer, M. D. Shaw, D. Kumor, R. Mirin, and S. W. Nam, *App. Phys. Lett.* **106**, 192601 (2015).
- [261] N. J. Russell, J. L. O'Brien, and A. Laing, (2015), arXiv:quant-ph/1506.06220 .
- [262] M. C. Tichy, M. Tiersch, F. de Melo, F. Mintert, and A. Buchleitner, *Phys. Rev. Lett.* **104**, 220405 (2010).
- [263] M. C. Tichy, *Entanglement and interference of identical particles*, Ph.D. thesis, Universitat Freiburg (2011).

## BIBLIOGRAPHY

---

- [264] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski, *J. Math. Phys.* **48**, 052106 (2007).
- [265] R. F. Werner, *J. Phys. A: Math. Gen.* **34**, 7081 (2001).
- [266] W. Tadej and K. Życzkowski, *Open Syst. Inf. Dyn.* **13**, 133 (2006).
- [267] T. Tao, *Math Res. Lett.* **11**, 251 (2004).
- [268] F. Szollosi, *J. London Math. Soc.* **85**, 616 (2012).
- [269] K. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Zukowski, *Appl. Phys. B* **60**, S111 (2004).
- [270] A. Peruzzo, A. Laing, A. Politi, T. Rudolph, and J. L. O’Brien, *Nat. Comms.* **2**, 224 (2011).
- [271] A. Laing, T. Lawson, E. Martín López, and J. L. O’Brien, *Phys. Rev. Lett.* **108**, 260505 (2012).
- [272] N. Spagnolo, C. Vitelli, L. Aparo, P. Mataloni, F. Sciarrino, A. Crespi, R. Ramponi, and R. Osellame, *Nat. Comms.* **4** (2013).
- [273] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Phys. Rev. A* **52**, 3457 (1995).
- [274] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, *Information Processing Letters* **75**, 101 (2000).
- [275] Y. Shi, *Quant. Inf. Comp.* **3**, 84 (2003).
- [276] C. M. Dawson and M. A. Nielsen, *Quant. Inf. Comp.* **6**, 81 (2006).
- [277] D. Gottesman, (1998), quant-ph/9807006v1 .
- [278] D. Gottesman and I. L. Chuang, *Nature* **402**, 390 (1999).
- [279] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, *Phys. Rev. A* **65**, 012314 (2001).

---

## BIBLIOGRAPHY

- [280] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
- [281] R. Raussendorf, D. Browne, and H. Briegel, **68** (2003).
- [282] M. A. Nielsen, (2004), arxiv:quant-ph/0405134v2 .
- [283] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
- [284] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).
- [285] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, Phys. Rev. Lett. **115**, 020502 (2015).
- [286] Q. Zhang, X. H. Bao, C. Y. Lu, X. Q. Zhou, T. Yang, and T. Rudolph, Phys. Rev. A (2008).
- [287] J. Joo, P. L. Knight, J. L. O'Brien, and T. Rudolph, Phys. Rev. A **76**, 052326 (2007).
- [288] H. Wunderlich and M. B. Plenio, J. Mod. Opt. **56**, 2100 (2009).
- [289] H. W. Li, J. Wabnig, D. Bitauld, P. Shadbolt, A. Politi, A. Laing, J. L. O'Brien, and A. O. Niskanen, New J. Phys. **15**, 063017 (2013).
- [290] R. Blume-Kohout, Phys. Rev. Lett. **105**, 200504 (2010).
- [291] B. Borchers, Optim. Method. Softw. **11**, 613 (1999).
- [292] J. P. Sprengers, A. Gaggero, D. Sahin, S. Jahanmirinejad, G. Frucci, F. Mattioli, R. Leoni, J. Beetz, M. Lermer, M. Kamp, S. Höfling, R. Sanjines, and A. Fiore, Appl. Phys. Lett. **99**, 181110 (2011).
- [293] S. Sohma, T. Watanabe, N. Ooba, M. Itoh, T. Shibata, and H. Takahashi, in *Optical Communications, 2006. ECOC 2006. European Conference on* (IEEE, 2006) pp. 1–2.

## BIBLIOGRAPHY

---

- [294] F. Najafi, J. Mower, N. C. Harris, F. Bellei, A. Dane, C. Lee, X. Hu, P. Kharel, F. Marsili, S. Assefa, K. K. Berggren, and D. Englund, Nat. Comms. **6**, 1 (2014).
- [295] I. Bloch, J. Dalibard, and S. Nascimbène, Nat. Phys. **8**, 267 (2012).
- [296] N. C. Harris, G. R. Steinbrecher, J. Mower, Y. Lahini, M. Prabhu, T. Baehr-Jones, M. Hochberg, S. Lloyd, and D. Englund, (2015), arXiv:quant-ph/1507.03406v2 .
- [297] J. Huh, G. G. Guerreschi, B. Peropadre, J. R. McClean, and A. Aspuru-Guzik, Nat. Photon. **9**, 615 (2015).