UNIVERSITY OF CALGARY

Multi-Mode Multi-Photon Interferometry Applications for Quantum Information Processing

by

Abdullah Khalid

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN PHYSICS AND ASTRONOMY

CALGARY, ALBERTA
SEPTEMBER, 2018

Abstract

Quantum information holds enormous potential to achieve communication and computational tasks that are impossible using classical systems. Many quantum information processing tasks can be implemented by exploiting the passive interference of photons. In this thesis, we reports advances towards the analysis, simulation, characterization, and design of passive interferometry experiments for quantum information processing applications.

First, we develop a theory of passive optical interferometry experiments that relates coincidence rates at the output of an interferometer to the permutational symmetries of partially distinguishable photons. In our formalism, coincidence rates are elegantly expressed in terms of immanants, which are matrix functions that exhibit permutational symmetries, and the immanants appearing in our coincidence-rate expressions share permutational symmetries with the input state. Our formalism thus provides an intuitive qualitative understanding of how the permutational symmetries of distinguishable photons determine their interference. Our approach can be used to better understand the effect of partial distinguishability in modeling passive interferometry experiments aiming to perform quantum information tasks such as linear optical quantum computing and BosonSampling. By exploiting symmetries, we can also reduce some calculational tasks and provide additional insights into relations between the coincidence rates in various situations.

Second, we tackle the problem of characterizing passive interferometers, essential for modeling any passive interferometry experiment. We develop a characterization procedure that uses only one- and two-photon coincidence data, and makes a number of advancements over existing procedures. We estimate the errors in the characterization via bootstrapping, a statistical technique with the advantage of not assuming any particular error model on the experimental data. We also introduce a scattershot approach to reduce the experimental data collection time quadratically in the number of modes of the interferometer.

Third, we study a relativistic quantum information task called quantum summoning. We cast quantum summoning as an interactive protocol between a verifier and a possibly

dishonest prover. For the prover, we present a protocol and quantum codes to summon in any valid configuration of causal diamonds, and design the encoding and decoding circuits for our code. Our protocol decreases the space complexity for encoding by a factor of two compared to the previous best result and reduces the gate complexity from scaling as the cube to the square of the number of causal diamonds. Within our interactive protocol framework, we construct an operational definition of quantum summoning, and use this definition to present a verification test. We prove that our verification test is sound and complete, thereby showing that quantum summoning can be verified by a resource-limited verifier in an adversarial setting. Our protocol and verification procedures are amenable to implementation by passive interferometry, thereby extending the reach of passive interferometry in the field of relativistic quantum information processing.

Acknowledgments

I am eternally grateful to many people for the help and support they provided during the course of my PhD studies. I would like to thank my advisor Barry Sanders for his scientific guidance and generous support during the course of this degree. I would also like to thank my many collaborators during the course of this degree, especially Yadong Wu and Hubert de Guise. I am deeply grateful to Hubert for his incredible patience, insight and wisdom. I would like to thank my group mates for insightful discussions and words of encouragement, especially Jonny Johannes, Priyaa Varshinee Srinivasan, Pantita Palittapongarnpim, Ehsan Zahedinejad, Namrata Shukla and Archismita Dalal. I am thankful to Lucia Wang, Nancy Jing Lu, Tracy Korsgaard, and Gerri Evans for their administrative assistance throughout my degree.

I would also like to thank my family for their unwavering support in my pursuit of physics. I would like to thank Rabia Aslam Chaudary, Aleena Tasneem Khan, Ahmed Umer Ashraf and Taha Hasan for their friendship throughout my degree. Finally, I would like to thank Anna Ordog for her love and support, and without whose faith this thesis would have been impossible.

Table of Contents

List of Figures and Illustrations

List of Tables

List of Abbreviations and Nomenclature

Symbol or abbreviation	Definition
irrep	irreducible representation of a group
PDF	probability-density function
CSS code	Calderbank-Shor-Steane code
CNOT	quantum controlled-not gate

Thesis content previously published

The work presented in this thesis has been previously published in the following papers:

[1] Abdullah Khalid, Dylan Spivak, Barry C. Sanders, and Hubert de Guise. Permutational symmetries for coincidence rates in multimode multiphotonic interferometry. *Phys. Rev. A*, 97:063802, 2018.

[2] Ish Dhand, Abdullah Khalid, He Lu, and Barry C. Sanders. Accurate and precise characterization of linear optical interferometers. *Journal of Optics*, 18(3):035204, 2016.

[3] Ya-Dong Wu, Abdullah Khalid, and Barry C Sanders. Efficient code for relativistic quantum summoning. *New Journal of Physics*, 20(6):063052, 2018.

I have also presented this work as oral or poster presentations at conferences as:

- Yadong Wu, Abdullah Khalid, and Barry C. Sanders, Codes for Quantum Information Summoning (contributed, oral). Conference on Quantum Information and Quantum Control VII, The Fields Institute, University of Toronto, Toronto, Canada, 28 August - 1 September, 2017.

- Ish Dhand, Abdullah Khalid, He Lu, Hubert de Guise and Barry C. Sanders. Characterization and simulation of linear optics (contributed, poster). 19th Conference on Quantum Information Processing. Banff, Canada. 11-15 January 2016.

- Ish Dhand, Abdullah Khalid, He Lu and Barry C. Sanders. Accurate and precise characterization of linear optical interferometers (contributed, poster). Canadian Summer School on Quantum Information 2015. University of Toronto, Toronto, Canada. 10-14 August 2015.

I outline below which content in this thesis has been taken directly from these publications. All such copied text has been appropriately modified, reordered or at time rewritten to make it more suitable for inclusion in this thesis. Most of the material from Ref. [2] has been completely rewritten to make the formalism, notation and language consistent with that of my other work. The source of each chapter is outlined below.

- Sec. 1.2 is borrowed from the introduction of Ref. [1].
- Sec. 1.4 borrows some material from the introduction of Ref. [3].
- Chapter 2 consists of the background chapters from Ref. [1] and contains a rewrite of the background of Ref. [2]. However, figures and their captions are borrowed from Ref. [2].
- Chapter 3 is borrowed from the background of Ref. [3].
- Chapter 4 contains material from the main sections and appendices of Ref. [1]. Most of this material has been heavily reorganized.
- Chapter 5 is a complete rewrite of the main sections and appendices of Ref. [2]. However, figures and their captions are borrowed.
- Chapter 6 is mostly borrowed from Ref. [3], except for Sec. 6.3.3 which is completely new.
- Chapter 7 consists of material from Ref. [3] and new material.

Chapter 1

Introduction

1.1 Motivation and aims

Quantum information science investigates the computational, communication and cryptographic capabilities of quantum systems, especially how these powers differ from those of classical systems. The potential of quantum information processing has been demonstrated through several powerful theoretical results, among them faster-than-classical computation [4, 5, 6], stronger-than-classical correlations [7] and secure quantum key distribution [8]. To benefit from these theoretical results requires their implementation on physical media, first as experiment to verify and validate these results and later as commercial technology.

The past few decades have seen growing control over several different physical systems for the purpose of implementing various quantum information tasks [9, 10, 11, 12, 13, 14, 15]. One of the more accessible and useful of these testbeds is the optical bench, on which the interference of light can be used to process information. An optical interferometry setup consists of light sources, measurement devices, and devices that transform a set of input light beams into a set of output light beams. The transformation devices are classified as active or passive, where the former pump energy into the system and the latter conserve the total energy of the system [16].

There exists methods of exploiting active quantum optics to implement quantum information protocols [17, 18, 19]. However, such systems suffer from excessive noise, and natural Kerr nonlinearities are not strong enough [16] to justify using active optics for quantum information processing. On the other hand, passive quantum optical interferometry is technologically attractive for a number of reasons. It has been shown that passive interferometers, single-photon sources and photon-counting detectors can be employed to construct a universal quantum computer [20]. Moreover, photons suffer low degree of absorption and decoherence, and travel faster than any other physical instantiation, making optics the dominant way to transfer quantum information across long distances [21]. Consequently, passive interferometry, supplemented with devices such as optical quantum memories [22, 11], is universal for quantum information processing, i.e., can be used solely to implement any quantum computation or communication protocol - a feature not shared by any other implementation technique.

Furthermore, there exists a universal passive device, called a multi-mode passive interferometer, that can perform any and all possible passive transformations on a set of optical modes [23, 16, 24], allowing for a uniform approach towards experimental design of quantum information protocols. Recent advances in optical technology [25, 26, 27] include photonic circuits etched into silicon chips [28, 29, 30, 31, 32], as well as the development of reconfigurable passive optical interferometers [33, 34, 35, 36]. Other advances include construction of high fidelity single-photon sources [37, 38, 39, 40, 36], and high efficiency photon number-resolving detectors [41, 42, 43, 44, 45, 36]. These advances have engendered implementations of various quantum computation protocols such as BosonSampling, quantum gates, and state preparation [46, 47, 48, 49, 50, 51, 34, 36], and, quantum communication and cryptography protocols such as quantum teleportation [52], quantum repeaters [53], loop-hole free Bell inequality violation [10], and quantum key distribution [54, 36].

Despite this progress, there are various obstacles to exploiting passive optical interferometry for quantum information processing. Optical implementations of quantum information

tasks usually require indistinguishable single-photon sources [20, 6], but state-of-the-art experiments have distinguishable sources that sometimes emit multiple photons [46, 47, 48, 49, 50, 51, 34, 36]. Therefore, it is important to characterize the interference of partially distinguishable photons to understand the relevance of experimental implementations of quantum information tasks, while at the same time advancing the analysis and simulation of these implementations. Another requirement for using passive interferometry for quantum information processing is the ability to characterize the interferometer accurately and precisely. An accurate model of the interferometer, along with knowledge of the errors in the characterization is necessary to compare experimental outputs with the theoretical ideals demanded by the task at hand. It is also important to challenge the limits of passive interferometry technology by designing implementations of new quantum information tasks.

In order to alleviate these problems, this thesis reports advances towards the analysis, simulation, characterization, and design of procedures and experiments that exploit passive interferometry for quantum information processing. We develop a qualitative and quantitative theory to analyze the output probabilities, also known as coincidence rates, in multi-mode multi-photon passive interferometry experiments [1]. We exploit the representation theory of the symmetric group to reveal the symmetries of the coincidence rates. These symmetries are useful for describing the features of the coincidence rate landscape formed by varying the distinguishability of the input photons, as well as demonstrating that coincidence rate expressions are invariant or covariant under permutation of photons and modes. We develop a procedure to characterize a multi-mode interferometer using single- and two-photon coincidence rates [2]. The procedure includes an algorithm to estimate the random errors in the characterization, and a method to reduce experimental data collection time. We also cast quantum summoning, a relativistic quantum information task, into an interactive protocol, and develop codes to perform quantum summoning [3]. We present a summoning protocol for agents spread across spacetime, and encoding and decoding circuits for our codes that can be implemented optically. Finally, we present a verification procedure

for quantum summoning. In the next few sections, we introduce each of these three projects with more detail.

1.2 Permutational symmetries for coincidence rates

We develop a theory of passive optical interferometry experiments that relates coincidence rates to the permutational symmetries of partially distinguishable photons. The distinguishability of the photons plays a crucial role in determining their interference, first studied theoretically by Fearn and Loudon [55, 56] and experimentally by Hong, Ou and Mandel [57] for a system of two photons. A number of recent studies provide theories of distinguishable multi-photon passive interferometry experiments to elucidate qualitative features of optical systems [58, 59, 60, 51, 61]. One research direction has been to determine whether the interference of partially distinguishable photons yields a probability distribution that is close to the probability distribution pertinent to the BosonSampling problem [62, 63]. Others have investigated the bunching behavior of partially distinguishable bosons [60] and whether such behavior can be exploited to create hypothetical particles that possess arbitrary permutational symmetries [60]. It has been suggested that pairwise distinguishability may not be sufficient to characterize the interference of many photons [64]. Partial distinguishability can be controlled via degrees of freedom such as path, time-of-arrival at the interferometer or polarization, and control via polarization can be achieved by doubling the number of paths instead [65].

We build upon a recently proposed description of multi-photonic interferometry experiments, that relates the interference of photons to the symmetries of their state [66, 67, 51]. For instance, the Hong-Ou-Mandel effect occurs because two perfectly indistinguishable photons maximally interfere because their state is symmetric in the exchange of the photons, but two partially indistinguishable photons partially interfere because their state is a linear combination of the fully-symmetric and anti-symmetric basis states. The work we build

upon analyzes multi-photonic systems using the representation theory of the symmetric group, where previous authors limit themselves to systems with exactly one photon in each input and output mode. They show that by exploiting the permutational symmetries of multi-photon states the photonic Hilbert space decomposes into subspaces, where elements in each subspace possess known permutational symmetries [68]. Distinguishability of the input photons determines which subspaces their state lives in. For instance, if photons are fully indistinguishable, then, because they are bosons, their state is fully symmetric under any permutation of the photons. As their distinguishability increases, the multi-photon state extends into other subspaces.

Tillmann *et al.* [51] have advanced that the coincidence rate can be expressed in closed form in terms of immanants of the scattering matrix. Immanants are matrix functions constructed from the symmetric group; some of them, including the permanent, are known to be hard to compute [69, 70, 71]. Specifically, coincidence rates are sums of squared moduli of linear combinations of immanants where the coefficients in the sum are functions of the photonic distinguishability. We assume that photons are only distinguishable by their time-of-arrival at the interferometer.

Here we present major extensions to the results of Refs. [66, 67, 51]. We discuss arbitrary input and output configuration of partially distinguishable photons, i.e. possibly multiple photons in each input and output mode. We employ the term input configuration to refer to fixed number of photons in each input mode and the term output configuration to refer to a fixed number of counts at detectors located in each output mode. We use symmetry arguments to show that, if there are multiple photons in some input or output modes, then subspaces possessing certain symmetries do not appear in the Hilbert space decomposition.

One of the aforementioned works [51] provides a procedure to calculate coincidence rates for arbitrary total number of photons. Crucial to the procedure is the factorization of the coincidence rate into a matrix product [67, 51]. One of these matrices, called the rate matrix, features in other partial indistinguishability theories [62, 59, 60]. The elegant decomposition

of the rate into a matrix product provides insights into the symmetry of the coincidence rate because the symmetric group links partial distinguishability to representations, and allows for the expression of the rates in terms of immanants. Unfortunately, it is not shown that the Tillman *et al.* [51] procedure is correct and works in all cases.

In this thesis, we fill this gap and extend their results by providing procedures to understand coincidence rates at the output modes of a passive interferometer for any given input and output photon configuration, and proving that these procedures work. We show that for any input and output configuration, the coincidence rate can always be factored. Furthermore, we prove that the rate matrix carries a representation of the symmetric group, and hence can be block-diagonalized by standard methods [68], leading to the expression of the coincidence rates in terms of immanants.

We use symmetry arguments to show that if there are multiple photons in some input or output modes, then subspaces possessing certain symmetries do not appear in the Hilbert space decomposition. Hence, given knowledge of the distinguishability of the input photons, we are able to identify which immanants appear in the coincidence rate expression using physical arguments alone. Finally, we discuss how the problem of reducing the rate matrix to block diagonal form can be cast as an eigenvalue problem using class operators. This implies in particular that when some subspaces are known to be excluded by symmetry arguments, one can better focus the computational resources on the relevant subset of eigenvectors and related immanants.

We also show that, under a rearrangement of photons at the input of the interferometer, the coincidence rates at the output of the interferometer are covariant (but generally not invariant): the rates are expressed in terms of the same immanants but with different coefficients. We show these coefficients transform linearly under the rearrangement of the input photons. Therefore, once the rate for one input is known, the rates for any permuted input is easy to calculate. We also discuss the transformation of rates under permutation of modes.

Our formalism thus provides an intuitive qualitative understanding of how the permutational symmetries of distinguishable photons determine their interference. Our approach can be used to better understand the effect of partial distinguishability in modeling passive interferometry experiments aiming to perform quantum information tasks such as linear optical quantum computing [20] and BosonSampling [6, 46, 47, 48, 49, 50, 51, 34]. By exploiting symmetries, we can also reduce some calculational tasks and provide additional insights into relations between the coincidence rates in various situations.

1.3 Characterization of passive interferometers

The characterization of a passive interferometer is the task of estimating the unitary matrix encoding the transformation on the input states effected by the interferometer. This characterization task is essential for modeling any passive interferometry experiment, hence a number of procedures have been developed and used to characterize passive interferometers. Some of these have use classical light or coherent states [72, 73, 74, 75, 76, 77, 36], while others use photon sources [73, 48, 51, 78, 79]. One prominent and simple approach to classical light characterization is to use the transmitted intensities of a single beam of input light to estimate the amplitudes of the interferometer matrix, and use the interference of two beams of light (classical or coherent) with varying relative phase to estimate the phases of the interferometer matrix [74, 75, 77]. Different numerical techniques have been employed to improve the estimate of the phases and reduce the amount of data needed for this method. Another approach is the use the reconstruction method suitable for any quantum optical process, that uses optical homodyne tomography of coherent states with maximum-likelihood methods to estimate the interferometer matrix [72].

While the classical light approach is convenient due to reduced intricacy of experimental devices and faster data collection, it suffers from a number of problems. First, the interferometer transformation is usually dependent on the spatio-temporal and polarization modes

of the input light. Therefore, the classical light sources must be mode matched with the quantum sources used in the actual experiment. A photon source approach avoids this problem by using the same sources for both the characterization and the experiment. Second, state-of-the-art passive interferometry experiments are done with reconfigurable chipped interferometers, where the light sources and detectors are embedded on the same chip [34, 36]. On such interferometers, a photon source approach for characterization is appropriate.

One prominent and oft used photon based characterization procedure is by Laing and O'Brien[73]. It is convenient because it uses only single and two-photon coincidence data to characterize and data collection is efficient in the size of the interferometer. It is also not sensitive to losses at the input and output ports of the interferometer. However, it assumes large-number statistics on the detected photons and that photon sources are perfectly mode-matched. The first assumption implies that the procedure ignores the random errors in the experiment that result in an imprecise characterization. The second assumption means that the characterization is inaccurate if the sources are mode-mismatched as is the case in state-of-the-art passive interferometry implementations [46, 47, 48, 49, 50, 51, 34]. Variations of this procedure have been used in other experiments [48, 51, 78].

Here we present a procedure to characterize passive interferometers that also uses only single and two-photon coincidence data. This procedure improves upon the Laing-O'Brien procedure in a number of ways. We account for and correct systematic errors due to spatial and polarization mismatches by calibrating the sources, resulting in increased accuracy of the characterization. We increase accuracy and precision by fitting experimental coincidence data to curves simulated using measured spectra of the sources. Despite these improvements, because of random errors, the characterized matrix compatible with the experimental data is not unitary. Therefore, we use a maximum likelihood technique to find the nearest unitary matrix, as is required from the characterization procedure. To estimate the errors on the characterized interferometer parameters, we use bootstrapping, a statistical technique that does not assume any particular error model. In this way our estimates of the errors are

more accurate than those procedures assuming a shot noise error model [80, 32, 51]. Finally, we introduce a scattershot approach to data collection that improves experimental time quadratically over the previous approach [73]. In summary, we construct a characterization procedure for passive interferometers that is accurate and precise, reports the precision of the characterization and only depends on singe and two-photon coincidence data.

1.4 Summoning of quantum information

Quantum summoning is the task of encoding and transmitting quantum information to a configuration of spacetime causal diamonds such that the quantum information can be reconstructed in any one of these causal diamonds [81, 82, 83, 84]. Quantum summoning cannot be guaranteed to work for every configuration of causal diamonds because quantum information cannot be copied [85, 86, 87, 88] or transmitted superluminally [86]. Summoning is only possible for a configuration of causal diamonds if every pair of diamonds is causally related, where two diamonds are causally related if the earliest point of one can communicate with the latest point of the other [82]. Our aim is to construct efficient protocols for summoning quantum information in any configuration of N pairwise-related causal diamonds.

A variety of work has been done on summoning ever since Kent introduced this task and presented a no-summoning theorem [81]. Hayden and May [82] show that quantum summoning can be reduced to the primitives of quantum secret sharing [89, 90, 91] and teleportation [92, 93]. They exploited a codeword-stabilized quantum code [94] to design a summoning protocol that is efficient in the sense that the number of qubits Q used by the code is polynomial in N. Hayden et al. [83] proposed a continuous-variable version of summoning and an efficient protocol to perform this task, as well as showing that optical circuits can be used to realize summoning experimentally. In 2016, Adlam and Kent [84] proposed a summoning task with multiple summones and provided a protocol, which employs teleportation, to accomplish this task for the configuration being an ordered set of causal

diamonds.

Here, we formulate quantum summoning as an interactive protocol between a possibly dishonest prover and a verifier [95, 96, 97, 98]. Within this framework we define an operational definition of summoning, based on entanglement fidelity [99, 100], that allows the verifier to test if the prover can summon. We present a verification test and show that it is sound and complete.

For the prover, we develop a protocol to summon a qubit in any valid configuration of causal diamonds. Our protocol uses a Calderbank-Shor-Steane (CSS) code [101, 102], constructed from the relation between graphs and linear algebra [103, 104], to encode one logical qubit into $\mathcal{O}(N^2)$ physical qubits. Our code is a qubit version of the homological continuous-variable quantum error correcting code [83] and corrects erasure errors that occur in summoning.

We provide a procedure to construct the encoding and decoding circuits for our CSS code for arbitrary N. The number of qubits Q used by our protocol is reduced by a factor of two compared to the previous best, and the number of quantum gates G is reduced from $\mathcal{O}\left(N^3\right)$ to $\mathcal{O}\left(N^2\right)$ [82]. Our decoding procedure has gate complexity $\mathcal{O}(N)$. We discuss how to efficiently implement these circuits using passive interferometry. These results are significant in that we complete the quantum summoning protocol [81, 82, 83] by providing both encoding and decoding schemes, a method to optically implement these circuits, and analyze the quantum resources required to summon.

1.5 Overview of chapters

This section outlines the contents of the chapters to follow. The research presented in this thesis requires knowledge of quantum optics, group theory, and quantum error correction codes. Therefore, the next two chapters present the necessary background information needed to understand my work.

Chapter 2 provides the mathematical foundations of passive optical interferometry and group theory, required for understanding my advances towards the symmetries of coincidence rates and the characterization of interferometers. We describe multi-mode multi-photon states, the action of interferometers, photon counting detectors and coincidence rates for some simple cases. We also define actions of the symmetric group on photonic states and show that this results in a representation of the symmetric group.

In Chapter 3, we start with a description of the summoning task. Next we provide some mathematical tools underpinning quantum error correction that are needed to develop our summoning code. In the rest of the chapter we discuss an isomorphism between graphs and linear spaces, also required for our summoning code.

We introduce our result on the symmetries of coincidence rates in passive interferometry [1] in Chapter 4. I prove two key theorems that form the basis of a procedure to express any coincidence rate in terms of immanants. We illustrate our results with a fully worked out example of four photons in three modes. We conclude the chapter with two additional results about how the rate changes under a permutation of the photons or the input modes.

In Chapter 5, we present our procedure to characterize passive interferometers [2]. We explain what experimental data has to be collected for the characterization. We then explain the computational steps that lead to an estimate of the matrix representing the action of the interferometer. Finally, I explain the bootstrapping procedure required to estimate the random errors in the characterized matrix.

Chapter 6 presents our results on summoning. We formulate summoning as an interactive protocol. We present a quantum error correcting code that can be used to summon quantum information in any valid set of causal diamonds [3]. We rigorously prove that the code is a stabilizer code and provide encoding and decoding procedures between the logical space and code space. Finally, we provide a verification procedure for summoning.

Concluding remarks are given in Chapter 7. I suggest some possible extensions of the work presented in this thesis.

Chapter 2

Background on passive interferometry

In this section, we provide the necessary background on passive interferometry. In Sec. 2.1 we formally define our model of passive interferometry experiments. In Sec. 2.3 we define the action of the symmetric group on photonic states. We will use Fig. 2.1 to provide examples of our description of passive optical experiments.

2.1 Passive interferometry

We define multi-mode multi-photon states, the action of the interferometer and the behavior of photon-counting detectors. We will discover that any passive interferometry setup, such as the examples shown in Fig. 2.1, can be described using four pieces of information: the path of the photons (encoded in the strings $\boldsymbol{\eta}$ and $\boldsymbol{\upsilon}$), the temporal state of the photons (encoded in the string $\boldsymbol{\tau}$), the measurement result (encoded in the string $\boldsymbol{\mu}$) and the action of the interferometer (encoded in the matrix U). We describe and discuss each of these now.

2.1.1 Photonic states

Photonic states are defined using the monochromatic photonic creation and annihilation operators, $a_i(\omega_k), a_j^\dagger(\omega_l)$, for modes i, j and frequencies ω_k, ω_l, satisfying the canonical com-

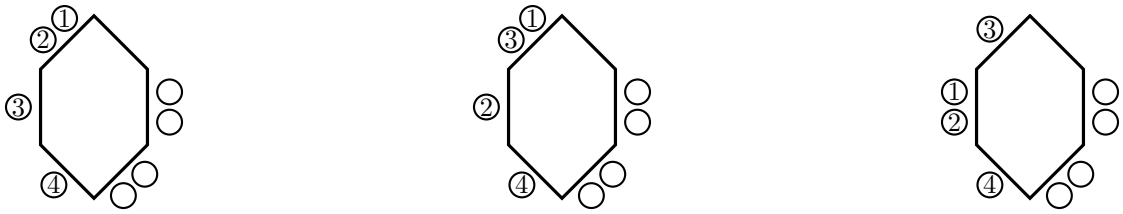


Figure 2.1: An interferometer (hexagon) with three inputs (left edges) and three outputs (right edges). The numbered and unnumbered circles represent photons at the input and output modes. The photons at the input are numbered as their distinguishability can be controlled but those at the output are unlabelled as the detectors only count the number of photons in each output mode. The input states in the three examples are (a) $|211;1123;\boldsymbol{\tau}\rangle$, (b) $|211;1213;\boldsymbol{\tau}\rangle$ and (c) $|121;2213;\boldsymbol{\tau}\rangle$.

mutation relations,

$$\Big[a_i(\omega_k), a_j^\dagger(\omega_l)\Big] = \delta_{ij}\delta(\omega_k - \omega_l). \tag{2.1}$$

Realistic photons are not monochromatic, but rather have a frequency spectrum captured by a complex-valued function $\phi(\omega)$. A single photon pulse in mode i has state

$$|1;i;\tau\rangle \coloneqq A_i^\dagger(\tau)|0\rangle \coloneqq \int \mathrm{d}\omega \phi(\omega)\mathrm{e}^{-\mathrm{i}\omega\tau}a_i^\dagger(\omega)|0\rangle, \tag{2.2}$$

where $A_i(\tau)$ is the creation operator of a photon pulse that arrives at the interferometer at time τ.

The state of n photons in m modes is specified using the mode-occupation string, the photon-occupation string and the distinguishability string. We label an input configuration by two strings. The first string $\boldsymbol{\eta}$, called the input *mode-occupation* string, records the number of photons in each input mode. The string $\boldsymbol{\eta}$ is of length m, and η_i is the number of photons in mode $i \in \{1,\ldots,m\}$ and $\sum \eta_i = n$. For the three examples in Fig. 2.1, $\boldsymbol{\eta}$ is 211, 211 and 121, respectively. If the photons are all indistinguishable this is all that is needed to describe the configuration of the photons.

If the photons are distinguishable, more information is needed. The string $\boldsymbol{\upsilon}$, called the *photon-occupation* string, stores in which mode each photon is placed. The string $\boldsymbol{\upsilon}$ is of

length n, and υ_i is the mode occupied by the i-th photon for $i \in \{1, \ldots, n\}$. For the first example in Fig. 2.1, $\boldsymbol{\upsilon}$ is 1123 because the first two photons are in the first mode while the third and fourth photons are in the second and third mode respectively. For the other two examples, $\boldsymbol{\upsilon}$ is 1213 and 2213 respectively. The string $\boldsymbol{\upsilon}$ contains all information needed to label the configuration of distinguishable photons. The string $\boldsymbol{\eta}$ can be found if $\boldsymbol{\upsilon}$ is known, but we specify both in order to simplify mathematical expressions that appear in this paper.

Photons have degrees of freedom besides path such as spectra, polarizations, times of arrival at the interferometer, etc. Therefore, to define a multi-mode multi-photon state we need to specify the labels of each of these degrees of freedom. We assume that the distinguishing degrees of freedom are under the experimentalist's control and the distinguishability of the photons with respect to each other can be controllably tuned. To keep the analysis simple we only model one such degree of freedom, the time-of-arrival of the photon at the interferometer. The time-of-arrival of the photons at the interferometer is stored in the length n string $\boldsymbol{\tau}$, where $\tau_i \in \mathbb{R}$ is the time-of-arrival of the i-th photon.

Using $\boldsymbol{\eta}$, $\boldsymbol{\upsilon}$ and $\boldsymbol{\tau}$ we can define the state of n photons in m modes as

$$|\boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle := \frac{1}{\sqrt{\mathcal{N}}} \prod_{i=1}^{n} A^{\dagger}_{\upsilon_i}(\tau_i)|0\rangle, \tag{2.3}$$

where $\frac{1}{\sqrt{\mathcal{N}}}$ is the normalization of this wavefunction that we evaluate in the proof of Proposition 1 in Sec. 4.2. The input states of the three examples shown in Fig. 2.1 are $|211; 1123; \boldsymbol{\tau}\rangle$, $|211; 1213; \boldsymbol{\tau}\rangle$ and $|121; 2213; \boldsymbol{\tau}\rangle$, respectively.

2.1.2 Interferometer

The next aspect of the passive interferometry experiment to be described is the interferometer. An optical interferometer is a device that allows for the interference of light in different modes. Loss and dephasing are two errors that exist in any realistic interferometer. In a simplified model of the interferometer [73], it is assumed that the light undergoes losses and

dephasing in the input modes, followed by a unitary transformation from the input modes to the output modes, and ending with further losses and dephasing in the output modes. A realistic interferometer transformation may depend on the frequency of the photons, on the time-of-arrival of the photons or other internal degrees of freedom of the photons. However, we assume that these variations are negligible. The factorization of the errors and the transformation effected by the interferometer allows for the use of finite sized matrices to represent the interferometer action.

For an m-mode interferometer, the $m \times m$ matrix U^{u} describes the unitary part of the overall transformation, while the $m \times m$ matrix U describes the transformation including the errors at the input and output modes. The interferometer transforms the input creation operators to output creation operators according to

$$a^{\dagger}_{i,\mathrm{in}}(\omega_j) = \sum_{k=1}^{m} U_{ik} a^{\dagger}_{k,\mathrm{out}}(\omega_j), \tag{2.4}$$

where, in U_{ik}, the first index i denotes the input mode and the second index k denotes the output mode. Elsewhere in this manuscript, for typographical reasons, we suppress the subscripts $_{\mathrm{in}}$ and $_{\mathrm{out}}$ on the creation and annihilation operators as the difference is clear from context. For a three-mode interferometer shown in Fig. 2.1, U is a 3×3 matrix that is identical for all three examples.

The matrix U^{u} is constrained by

$$U^{\mathrm{u}} U^{\mathrm{u}\dagger} = U^{\mathrm{u}\dagger} U^{\mathrm{u}} = \mathbb{1}. \tag{2.5}$$

For instance, for the a two-mode interferometer, commonly called a beam splitter, we have

$$U = \mathrm{e}^{\mathrm{i}\theta_0} \begin{pmatrix} \mathrm{e}^{-\frac{1}{2}\mathrm{i}(\theta_1+\theta_3)} \cos\frac{\theta_2}{2} & -\mathrm{e}^{-\frac{1}{2}\mathrm{i}(\theta_1-\theta_3)} \sin\frac{\theta_2}{2} \\ \mathrm{e}^{\frac{1}{2}\mathrm{i}(\theta_1-\theta_3)} \sin\frac{\theta_2}{2} & \mathrm{e}^{\frac{1}{2}\mathrm{i}(\theta_1+\theta_3)} \cos\frac{\theta_2}{2} \end{pmatrix}. \tag{2.6}$$

The matrix U^{u} is not unique, if the input state is not entangled in photon-number and

only photon-counting measurements are performed on the output state as described above. Under this promise, phase shifts at the input or output of the interferometer will not change the measurement outcome probabilities. Therefore, for any given diagonal unitary matrices D_1 and D_2, that describe input and output phase shifts, $D_1 U^{\mathrm{u}} D_2$, is equivalent to U^{u}. In other words, we have an equivalence class of matrices to describe a given interferometer. We can now define for each equivalence class a representative element that will be useful for our work. We will assume that the representative element has its first row and column consist only of real numbers. Then the entry

$$U^{\mathrm{u}}_{ij} \coloneqq t_{ij} \mathrm{e}^{\mathrm{i}\theta_{ij}}, \quad t_{ij} \in [0,1], \theta_{ij} \in (-\pi, \pi], \theta_{i1} \coloneqq 0, \theta_{1j} \coloneqq 0 \; \forall i,j \in \{1,2,\ldots,m\}\,. \tag{2.7}$$

The signs of the arguments are defined as

$$\mathrm{sgn}\theta_{ij} \coloneqq \begin{cases} -1 & \text{if } \theta_{ij} < 0, \\ 0 & \text{if } \theta_{ij} = 0, \\ 1 & \text{if } \theta_{ij} > 0. \end{cases} \tag{2.8}$$

The restriction on the first row and column admits the following parameterization of U^{u},

$$U^{\mathrm{u}} \coloneqq B \times A \times G, \tag{2.9}$$

where

$$B = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & \sqrt{\beta_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \ldots & \sqrt{\beta_m} \end{pmatrix}, \tag{2.10}$$

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha_{22}\mathrm{e}^{\mathrm{i}\theta_{22}} & \dots & \alpha_{2m}\mathrm{e}^{\mathrm{i}\theta_{2m}} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{m2}\mathrm{e}^{\mathrm{i}\theta_{m2}} & \dots & \alpha_{mm}\mathrm{e}^{\mathrm{i}\theta_{mm}} \end{pmatrix}, \tag{2.11}$$

$$G = \begin{pmatrix} \sqrt{\gamma_1} & 0 & \dots & 0 \\ 0 & \sqrt{\gamma_2} & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & \sqrt{\gamma_m} \end{pmatrix}. \tag{2.12}$$

In this way, the parameters $\{\beta_i\}, \{\alpha_{ij}\}, \{\theta_{ij}\}$ and $\{\gamma_i\}$ specify the class representative unitary matrix U^{u} describing a given interferometer.

In order to account for the losses at the input and output modes of the interferometer, I introduce additional parameters. The loss of photons can be described by the probability of photon transmission, and the parameters ν_i and κ_j capture these probabilities for input mode i and output mode j, respectively. We ignore any dephasing at the input and output modes of the interferometer, as dephasing is modeled by phase shifts which do no affect photon-counting statistics.

In summary, the transformation effected by a unitary interferometer with losses at the input and outputs is given by a matrix U, which has elements

$$\begin{aligned} U_{ij} &= \sqrt{\kappa_i} U_{ij} \sqrt{\nu_j} \qquad (2.13) \\ &= \sqrt{\kappa_i}\sqrt{\beta_i}\alpha_{ij}\mathrm{e}^{\mathrm{i}\theta_{ij}}\sqrt{\gamma_j}\sqrt{\nu_j}, \quad \kappa_i, \beta_i, \alpha_{ij}, \gamma_j, \nu_j \in [0,1], \beta_1 \coloneqq 1, \\ &\qquad \theta_{ij} \in (-\pi, \pi], \theta_{i1} \coloneqq 0, \theta_{1j} \coloneqq 0 \ \forall i, j \in \{1, 2, \dots, m\}. \qquad (2.14) \end{aligned}$$

For the purpose of characterizing interferometers, we will require a notion of distance on

the space of general linear matrices. The Frobenius norm of a $m \times m$ matrix A is defined as

$$||A||_{\mathrm{F}} \coloneqq \sqrt{\sum_{i,j=1}^{m} |A_{ij}|^2}. \tag{2.15}$$

This can be used to define the Frobenius-norm distance between matrices U and V as

$$\mathrm{dist}(U,V) \coloneqq ||U-V||_{\mathrm{F}} = \sqrt{\sum_{i,j=1}^{m} |U_{ij}-V_{ij}|^2}. \tag{2.16}$$

This is a symmetric, positive-definite and subadditive distance function.

2.1.3 Measurement scheme

Finally, we outline the measurement scheme. We treat the detectors at the output of the interferometer as devices that count the total number of photons in a mode regardless of when they arrived at the detector. The lack of information about the paths of the photons through the interferometer generates the observed interference between the photon paths [56]. This is why, for instance, the photons at the outputs in Fig. 2.1 are not labelled.

Much like the input mode-occupation string, the number of photons detected in each output mode are collected in a output mode-occupation string $\boldsymbol{\mu}$, where μ_i is the number of photons detected in the ith output mode and $\sum_i \mu_i = n$. The measurement operator $M_{\boldsymbol{\mu}}$ is defined using the length n string

$$\boldsymbol{\xi} \coloneqq (\overbrace{1,\ldots,1}^{\mu_1 \text{ times}},\ldots,\overbrace{i,\ldots,i}^{\mu_i \text{ times}},\ldots,\overbrace{m,\ldots,m}^{\mu_m \text{ times}}).$$

Then the measurement operator

$$M_{\boldsymbol{\mu}} \coloneqq \frac{1}{\mu_1!,\cdots,\mu_n!} \int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n |\varphi(\omega_1)|^2 \cdots |\varphi(\omega_n)|^2 \\ a^\dagger_{\xi_1}(\omega_1)\cdots a^\dagger_{\xi_n}(\omega_n)|0\rangle\langle 0|a_{\xi_1}(\omega_1)\cdots a_{\xi_n}(\omega_n), \tag{2.17}$$

where the $\varphi(\omega_i)$ specifies the spectral range of the detectors. Usually, this spectral range is much broader than the spectral width of the photonic wavefunction [105, 47], and therefore everywhere we make the assumption that $\varphi(\omega_i)\phi(\omega_i) = \phi(\omega_i)$.

If the state $|\boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle$ is measured, the probability $\Pr(\boldsymbol{\mu}|\boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau})$ of outcome $\boldsymbol{\mu}$ is

$$\Pr(\boldsymbol{\mu}|\boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau}) = \langle \boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau}|M_{\boldsymbol{\mu}}|\boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle. \tag{2.18}$$

The coincidence rate is the probability of an outcome at the output of an interferometer. Given an m-mode n-photon state $|\boldsymbol{\eta}, \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle$ and an interferometer described by the matrix U, then for the output event $\boldsymbol{\mu}$, the coincidence rate is

$$C_{\boldsymbol{\upsilon},\boldsymbol{\xi}}(\boldsymbol{\tau}) \coloneqq \langle \boldsymbol{\eta}, \boldsymbol{\upsilon}; \boldsymbol{\tau}|U^\dagger M_{\boldsymbol{\mu}} U|\boldsymbol{\eta}, \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle. \tag{2.19}$$

This completes our mathematical description of passive optical interferometry.

2.2 Coincidence rates for one- and two-photon inputs

For some our analysis in later section, I will need the coincidence rate for one and two photons inputs. In this subsection, these rates are presented, using the results of the previous section.

The case for single-photon input is rather simple, as there is no interference. Moreover, the time of arrival of the photon does not matter. Assuming the photon starts in input mode i ($\boldsymbol{\upsilon} = i$), the probability of detecting in output mode j ($\boldsymbol{\xi} = j$) is just the modulus squared of the interferometer matrix entry,

$$C_{i,j} = |U_{ij}|^2 = \kappa_i \beta_i \alpha_{ij}^2 \gamma_j \nu_j, \tag{2.20}$$

where we drop the τ argument on the left hand side because it is not needed.

A more complicated case is when two photons, with controllable delay between their

arrival at the interferometer, are interferred. If the pair of photons start in input modes i and i' ($\boldsymbol{\upsilon} = ii'$), with times of arrival 0 and τ respectively, then the probability of detecting them in output modes j and j' ($\boldsymbol{\xi} = jj'$) is [106, 107]

$$\begin{aligned} C_{ii'jj'}(\tau) = \kappa_i\kappa_{i'}\beta_i\beta_{i'}\gamma_j\gamma_{j'}\nu_j\nu_{j'}[(\alpha_{ij}^2\alpha_{i'j'}^2 + \alpha_{ij'}^2\alpha_{i'j}^2)\int \mathrm{d}\omega_1\mathrm{d}\omega_2|\phi_1(\omega_1)\phi_2(\omega_2)|^2 \\ + 2\epsilon\alpha_{ij}\alpha_{i'j'}\alpha_{ij'}\alpha_{i'j}\int \mathrm{d}\omega_1\mathrm{d}\omega_2\phi_1(\omega_1)\phi_2(\omega_2)\phi_1(\omega_2)\phi_2(\omega_1) \\ \times \cos(\omega_2\tau - \omega_1\tau + \theta_{ij} - \theta_{ij'} - \theta_{i'j} + \theta_{i'j'})]. \end{aligned} \tag{2.21}$$

In this expression, I have relaxed the assumption made previously that the photons are only distinguishable by their time of arrival at the interferometer. First, I have introduced a labelling for the spectral functions signifying that this expression treats the two photons as distinguishable in their spectra. I have also introduced the additional parameter ϵ, called the mode-matching parameter, which is used to describe any additional distinguishability that the photons might have besides time of arrival or spectra [106]. The mode-matching parameter, $\epsilon = 1$ when the two photons are perfectly mode-matched and $\epsilon = 0$ when they are completely distinguishable from each other. The effect of the mode-mismatch parameter on the coincidence rate is illustrated in Fig. 2.2.

2.3 Permutation of photons and modes

In this subsection we employ the symmetric group to formally define the permutation of photons and modes. The symmetric group S_n is the group of all $n!$ permutations of n objects. The objects can be the n photons in the system, or the n possible modes of the system.

The state of n photons (2.3), described by the product of n bosonic creation operators, allows for the definition of the actions of the symmetric group S_n on photonic states. Given

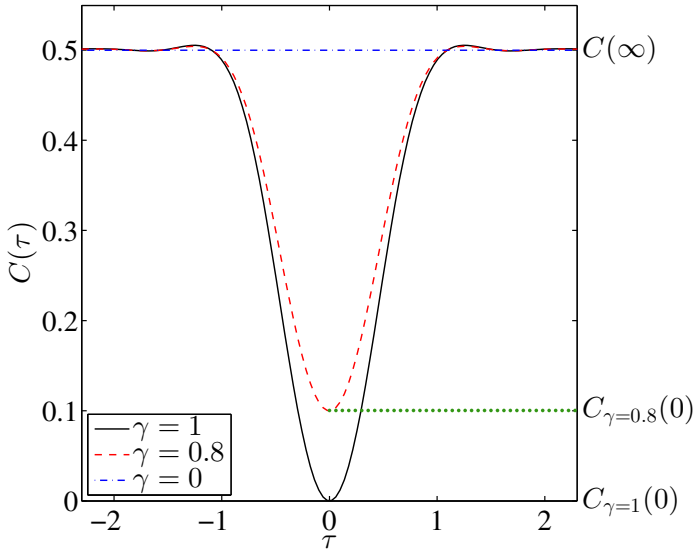


Figure 2.2: Plots of coincidence probability versus time delay for different values of γ for a lossless balanced beam splitter. The time delay τ is in units inverse special width of incoming photons.

an element $\sigma \in S_n$, the action P_σ on an n-photon state is defined as

$$\begin{aligned} P_\sigma|\boldsymbol{\eta};\boldsymbol{\upsilon};\boldsymbol{\tau}\rangle &\coloneqq \frac{1}{\sqrt{\mathcal{N}}}\prod_i A^\dagger_{\upsilon_{\sigma(i)}}(\tau_i)|0\rangle \\ &= |\boldsymbol{\eta};P_\sigma\boldsymbol{\upsilon};\boldsymbol{\tau}\rangle, \end{aligned} \tag{2.22}$$

where $P_\sigma\boldsymbol{\upsilon}$ is a reordering of the entries of $\boldsymbol{\upsilon}$. There are $N = n!/\prod_i \eta_i!$ distinct permutations of $\boldsymbol{\upsilon}$. We arbitrarily order and collect these N permutations in the set

$$\Upsilon = \left\{\bar{\boldsymbol{\upsilon}}^1,\ldots,\bar{\boldsymbol{\upsilon}}^N\right\}. \tag{2.23}$$

The elements of the symmetric group transform between the N states (2.23) with mode-occupation $\boldsymbol{\eta}$. The input shown in Fig. 2.1b is related to the canonical input (Fig. 2.1a) by a permutation of the photons. Specifically, the second and third photons have been swapped,

which is apparent by comparing $\boldsymbol{\upsilon} = 1123$ and $\boldsymbol{\upsilon}' = 1213$. Formally, we have the relationship

$$\begin{aligned} P_{(23)}|211;1123;\boldsymbol{\tau}\rangle &= |211;P_{(23)}1123;\boldsymbol{\tau}\rangle \\ &= |211;1213;\boldsymbol{\tau}\rangle, \end{aligned} \tag{2.24}$$

where $\sigma = (23) \in S_4$ because it is a system of four photons.

We also define Q, the action of the symmetric group on photonic states that permutes modes. To describe all mode permutations of m-mode states we require the symmetric group S_m. Given an element $\sigma \in S_m$,

$$\begin{aligned} Q_\sigma|\boldsymbol{\eta};\boldsymbol{\upsilon};\boldsymbol{\tau}\rangle &\coloneqq \frac{1}{\sqrt{\mathcal{N}}}\prod_i A^\dagger_{\sigma(\upsilon_i)}(\tau_i)|0\rangle \\ &= |Q_\sigma\boldsymbol{\eta};Q_\sigma\boldsymbol{\upsilon}\rangle, \end{aligned} \tag{2.25}$$

where $Q_\sigma\boldsymbol{\eta}$ reorders the entries of $\boldsymbol{\eta}$ and $Q_\sigma\boldsymbol{\upsilon}$ maps υ_i to $\sigma(\upsilon_i)$. The input shown in the third example Fig. 2.1c is related to the canonical input by a permutation of the input modes: the first and second modes have been swapped, which can be determined by comparing their photon-occupation strings. Formally, we also have the relationship

$$\begin{aligned} Q_{(12)}|211;1123;\boldsymbol{\tau}\rangle &= |Q_{(12)}211;Q_{(12)}1123;\boldsymbol{\tau}\rangle \\ &= |121;2213;\boldsymbol{\tau}\rangle, \end{aligned} \tag{2.26}$$

where $\sigma' = (12) \in S_3$ because the example in Fig. 2.1 is a system of three spatial modes.

Results from representation theory of the symmetric group will be required in Chapter 4. The action (2.22) naturally leads to an N-dimensional representation of S_n. For the

permutations $\sigma \in S_n$ its representation $\Gamma(\sigma)$ has entries

$$\Gamma_{ij}(\sigma) = \begin{cases} 1 & \text{if } P_\sigma \overline{\boldsymbol{v}}^i = \overline{\boldsymbol{v}}^j, \\ 0 & \text{otherwise.} \end{cases} \tag{2.27}$$

Any representation of the symmetric group can be decomposed into a sum of the irreducible representations (irreps) of the symmetric group. The irreps of S_n are in one to one correspondence with the conjugacy classes of S_n, where each conjugacy class can be labelled by a partition of n. Partitions can be graphically depicted by Young diagrams, so each irrep of the permutation group can be labelled by an n-box Young diagrams. A standard Young tableau is an n-box Young diagram filled with $\{1, \ldots, n\}$, such that numbers strictly increase across rows and columns. A semi-standard Young tableau is an n-box Young diagram filled by n, possibly repeating, positive integers such that the numbers strictly increase across columns and weakly across rows.

I will express coincidence rates in terms of immanants, which are matrix functions associated with the irreps of the symmetric group. The irrep labelled by Young diagram λ is associated with the immanant

$$\mathrm{imm}^\lambda T \coloneqq \sum_{\sigma \in S_n} \chi^\lambda(\sigma) \left(\prod_{i=1}^{n} T_{i\sigma(i)} \right), \tag{2.28}$$

where $\chi^\lambda(\sigma)$ is the character of the permutation σ in the irrep λ.

Chapter 3

Background on relativistic quantum summoning

In this chapter we provide the background required to develop our results on quantum summoning in Chapter 6. We explain the quantum information processing task of summoning and the conditions for the configurations to make summoning feasible [81, 82, 83]. Then we give the background knowledge on stabilizer quantum error correcting codes [108], especially CSS codes [101, 102]. We introduce the relation between graphs and binary vectors [103], which is useful for the construction of the CSS stabilizer code.

3.1 Summoning

Summoning is an information processing task involving two parties, Alice and Bob [81, 82, 83]. Bob's role is to provide the quantum information to Alice and to designate where the quantum information is to be summoned and Alice's role is to summon quantum information at the designated spacetime location. Associated to each request point y is a reveal point z_y that is in the causal future of y. The intersection of the future light cone of y with the past light cone of z_y is called a causal diamond, expressed as $\diamondsuit$. We label causal diamonds and show a label i in the diamond as $\langle i \rangle$. Besides the request and reveal points, Alice and Bob

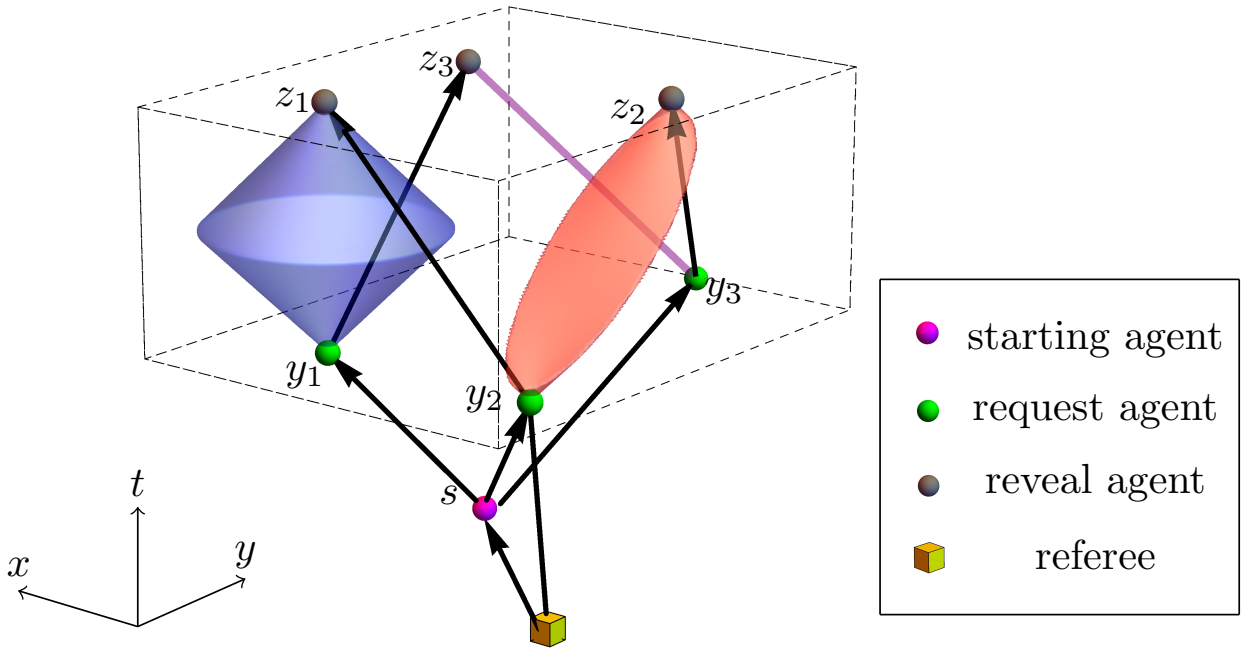


Figure 3.1: Three causal diamonds (red, blue and purple) in spacetime. A referee, a starting agent, three request agents and three reveal agents are arranged in spacetime. An arrow represents a quantum communication channel from one agent to another agent, and a line segment between two agents represents a classical channel from one to the other. The referee sends a quantum state $|\psi\rangle$ to the starting agent, and randomly chooses y_2 to send a classical request to A_{y_2}. The starting agent encodes $|\psi\rangle$ to three qutrits and distribute them to three request agents respectively. A_{y_2} sends her qutrit to A_{z_2}. Receiving no request, the request agents at y_1 and y_3 send their qutrits to A_{z_3} and A_{z_2} respectively. Hence, A_{z_2} receives two qutrits and decodes the state $|\psi\rangle$.

also agree upon a starting point s, where Bob provides the quantum information to Alice.

Alice and Bob can arrange their agents at various points in spacetime prior to the start of summoning [83]. Bob designates one agent to be the referee who sends quantum information to point s and classical information to all the request points. Alice designates one agent to be the starting agent S, who is situated at point s, and she delegates agents to each request and reveal point. We label the agent at point x by A_x. Figure 3.1 shows an example of Alice's and Bob's agents arranged in spacetime.

When summoning starts, the referee prepares a quantum state

$$|\psi\rangle \in \mathscr{H}, \tag{3.1}$$

where $\mathscr{H}$ is a finite d-dimensional Hilbert space [82], and transmits $|\psi\rangle$ to the starting agent. Alice and all her agents do not have any knowledge of $|\psi\rangle$. The referee randomly chooses one request point, say y, and sends the request only to A_y. Then Alice's task is to present the quantum state $|\psi\rangle$ at the corresponding reveal point z_y, by her agents' collaboration.

Given a set of causal diamonds $\left\{\diamondsuit_i\right\}_{i=1}^{N}$, summoning might be infeasible [81] due to the restrictions of both the no-cloning theorem [85, 86, 87, 88] and no superluminal communication [86]. Summoning is possible if and only if the following two conditions are satisfied [82].

C1 All reveal points are in the causal future of s.

C2 Each pair of causal diamonds is causally related, which means that there exists a point in one causal diamond that is causally related with at least one point in the other causal diamond.

We call a set of causal diamonds satisfying these two conditions a "valid configuration" for summoning. We represent a configuration of causal diamonds by a graph G as follows [82, 83]. We assign each causal diamond to a vertex and use the label of the causal diamond to label the vertex. If two causal diamonds are causally related, an edge e is inserted between the two corresponding vertices in G. A valid configuration of N causal diamonds is represented by an N-vertex complete graph denoted by K_N, for which each pair of vertices is connected by an edge [103].

In Fig. 3.1, we present an example of using quantum secret sharing [89, 90, 91] to summon quantum information [82]. After receiving a qubit $|\psi\rangle$, the starting agent encodes $|\psi\rangle$ into three qutrits [89] and distributes the three qutrits to the three request agents. If A_{y_i} ($i = 1, 2,$ or 3) receives the request, then the request agent sends her qutrit to the reveal point

$$z_i \coloneqq z_{y_i}. \tag{3.2}$$

Otherwise, she sends her qutrit to the reveal point $z_{(i-1) \bmod 3}$. In such a way, no matter which request agent receives the request, the associated reveal agent receives two qutrits to

retrieve the original qubit $|\psi\rangle$.

3.2 Stabilizer codes

In this subsection, we begin by introducing the Pauli group and the representation of Pauli operators using binary vectors. We explain the parameters characterizing a quantum error correcting code and the definition of erasure errors. Then we explain stabilizer codes [108], specially CSS codes [101, 102]. Finally, we show the encoding of a stabilizer code.

An n-qubit Pauli group [109] is

$$\mathcal{G}_n \coloneqq \pm\{I, X, Y, Z\}^{\otimes n}, \tag{3.3}$$

where

$$X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } Y \coloneqq ZX. \tag{3.4}$$

The Pauli group module sign is isomorphic to a cartesian product of binary vector spaces according to

$$\mathcal{I}_P : \mathcal{G}_n/\mathbb{Z}_2 \to \mathbb{Z}_2^n \times \mathbb{Z}_2^n : \bigotimes_{i=1}^{n} Z^{u_i} X^{v_i} \mapsto \begin{bmatrix} \boldsymbol{u} & \boldsymbol{v} \end{bmatrix}, \tag{3.5}$$

where

$$\boldsymbol{u} \coloneqq [u_1 \dots u_n], \ \boldsymbol{v} \coloneqq [v_1 \dots v_n]. \tag{3.6}$$

Two Pauli operators represented as binary vectors, $\begin{bmatrix} \boldsymbol{u} & \boldsymbol{v} \end{bmatrix}$ and $\begin{bmatrix} \boldsymbol{u}' & \boldsymbol{v}' \end{bmatrix}$, mutually commute if and only if [109]

$$\boldsymbol{u} \cdot \boldsymbol{v}' + \boldsymbol{v} \cdot \boldsymbol{u}' = 0, \tag{3.7}$$

where $\cdot$ is the indefinite inner product

$$\boldsymbol{u} \cdot \boldsymbol{v} \coloneqq \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_2. \tag{3.8}$$

Otherwise, these two Pauli operators anti-commute with each other.

In quantum error correcting codes, $[[n, k, d]]$ denotes a quantum code, where k qubits are encoded into n qubits, and d is the distance of the code [109]. Given a Pauli operator $P \in \mathcal{G}_n$, the weight of P is the number of nonidentity single-qubit Pauli operators, i.e., X, Y and Z in the tensor product P. The distance of a quantum error correcting code is the minimum weight of a Pauli operator P such that

$$\langle i|P|j\rangle \neq C(P)\delta_{ij}, \tag{3.9}$$

where $|i\rangle$ and $|j\rangle$ are basis elements of the code, $C(P)$ is a constant depending on P, and δ_{ij} is the Kronecker delta function. When transmitting a block of n qubits, if t qubits ($t < n$) are lost or never received, while the other $n - t$ qubits are undamaged, then the errors at these t qubits are called erasure errors [110].

A stabilizer code [108] is the simultaneous eigenspace of all the elements of an Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_n$ with eigenvalue one. A generator set of $\mathcal{S}$ is a set of independent elements in $\mathcal{S}$ such that every element of $\mathcal{S}$ can be expressed as a product of the elements in this generator set. An $[[n, k, d]]$ stabilizer code has $n - k$ independent stabilizer generators, each of which can be represented by a $2n$-dimensional binary vector. The $[[n, k, d]]$ stabilizer code is characterized by an $(n - k) \times 2n$ stabilizer generator matrix, where each row represents a stabilizer generator.

Now we introduce CSS codes, which are a type of stabilizer codes. A CSS code [101, 102] is specified by two classical linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$, where $\mathcal{C}_2$ is a subcode of $\mathcal{C}_1$, i.e.,

$$\mathcal{C}_2 \subseteq \mathcal{C}_1. \tag{3.10}$$

Each basis element of a CSS code corresponds to a coset [111] of $\mathcal{C}_2$ in $\mathcal{C}_1$, where the basis element is an equally weighted superposition of all the codewords in the coset. A CSS code is a stabilizer code whose stabilizer generators are either tensor products of X operators and

identities, or tensor products of Z operators and identities [108]. Hence, the CSS stabilizer code is characterized by an $(n-k) \times 2n$ stabilizer generator matrix

$$\begin{bmatrix} H_Z & \mathbf{0} \\ \mathbf{0} & H_X \end{bmatrix}, \tag{3.11}$$

where H_Z and H_X are two matrices, and the $\mathbf{0}$s are appropriately sized zero matrices.

Here we explain the encoding of a stabilizer code with stabilizer $\mathcal{S}$. The Pauli operators that preserve the stabilizer code space but act nontrivially on the encoded state are the logical Pauli operators on the encoded state [108]. The logical Pauli operators commute with all stabilizers in $\mathcal{S}$ but lie outside $\mathcal{S}$.

For an $[[n, 1, d]]$ stabilizer code with stabilizer $\mathcal{S}$, we denote $\bar{Z}$ and $\bar{X}$ as the logical Z and logical X operators on an n-qubit encoded state. Suppose

$$\bar{Z}|\psi_0\rangle = |\psi_0\rangle, \tag{3.12}$$

and

$$\{M_i\}_{i=1}^{n-1}$$

are $n-1$ independent stabilizer generators of $\mathcal{S}$. The encoded logical states are [108]

$$|0\rangle_L \coloneqq \prod_{i=1}^{n-1}(I + M_i)|\psi_0\rangle, \tag{3.13}$$

and

$$|1\rangle_L \coloneqq \bar{X}\prod_{i=1}^{n-1}(I + M_i)|\psi_0\rangle = \prod_{i=1}^{n-1}(I + M_i)\bar{X}|\psi_0\rangle. \tag{3.14}$$

Equations (3.13) and (3.14) indicate how to encode one qubit by a stabilizer code.

We have discussed quantum error correction, especially stabilizer codes in this subsection. Next we study the close relation between a graph and a binary vector, which provides a

powerful tool to construct our CSS stabilizer code.

3.3 Graphs and linear algebra

In this subsection, we begin by defining graphs and the binary linear space. After explaining these two concepts, we describe an isomorphism from sets of edges of an n-vertex graph to binary vectors with length $\binom{n}{2}$ [103]. Our approach is inspired by homology theory to construct quantum error correcting codes [83, 104]. Finally, we present the examples of triangle graphs and star graphs.

A graph [103]

$$G \coloneqq (V, E) \tag{3.15}$$

comprises a set of vertices V and a set of edges

$$E \subseteq V \times V. \tag{3.16}$$

One example of a graph is the n-vertex complete graph, K_n.

To explain the binary linear space, we introduce $GF(2)$, which is the smallest finite field containing two elements $\{0, 1\}$, together with addition and multiplication operations [112]. The linear space [111] over field $GF(2)$, denoted by $\mathbb{Z}_2^m$, is a set $\{0, 1\}^m$, together with vector addition,

$$+ : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m, \tag{3.17}$$

and scalar multiplication,[1]

$$\cdot : GF(2) \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m. \tag{3.18}$$

Next we explain the relation between an edge set E of a graph G and a binary vector with length $\binom{|V|}{2}$, where $|V|$ is the cardinality of V.

[1]Note we use $\cdot$ for the scalar multiplication only in Eq. (3.18) and Table 3.1. After this subsection, we use $\cdot$ only for the indefinite inner product.

Given $K_n = (V_K, E_K)$, the power set of E_K, which is the set of all the subsets of E_K, forms a binary linear space $\mathscr{E}$ [103]. The power set of E_K is denoted 2^{E_K}. For U, $U' \in 2^{E_K}$, the addition of U and U' amounts to the symmetric difference of U and U',

$$U + U' \coloneqq (U \cup U') \setminus (U \cap U') \,. \tag{3.19}$$

The empty set $\emptyset$ is the zero element and

$$\forall U \in 2^{E_K},\ -U \coloneqq U. \tag{3.20}$$

For $\langle i \rangle$ and $\langle j \rangle$, an edge e_{ij} is a unit vector in $\mathscr{E}$, and $e_{ji} = e_{ij}$ because we are dealing with undirected graphs. The set of edges

$$\{e_{ij}\}_{1 \le i < j \le n} \tag{3.21}$$

forms an orthonormal basis of $\mathscr{E}$. As $\binom{n}{2}$ edges exist in K_n,

$$\dim \mathscr{E} = \binom{n}{2}. \tag{3.22}$$

Now we show that $\mathscr{E}$ is isomorphic to $\mathbb{Z}_2^{\binom{n}{2}}$ [103]. Given any $U \in \mathscr{E}$, an isomorphism is

$$\mathcal{I}_G : \mathscr{E} \to \mathbb{Z}_2^{\binom{n}{2}} : U \mapsto \boldsymbol{u} = \left[u_1 \ \ldots \ u_{\binom{n}{2}} \right], \tag{3.23}$$

where

$$\{u_i\}_{i=1}^{\binom{n}{2}}$$

are the coefficients of U with respect to the basis in Eq. (3.21). The isomorphic mappings of the vector addition and the scalar multiplication are shown in Table 3.1.

Here we introduce two types of $\binom{n}{2}$-dimensional binary vectors and two linear subspaces

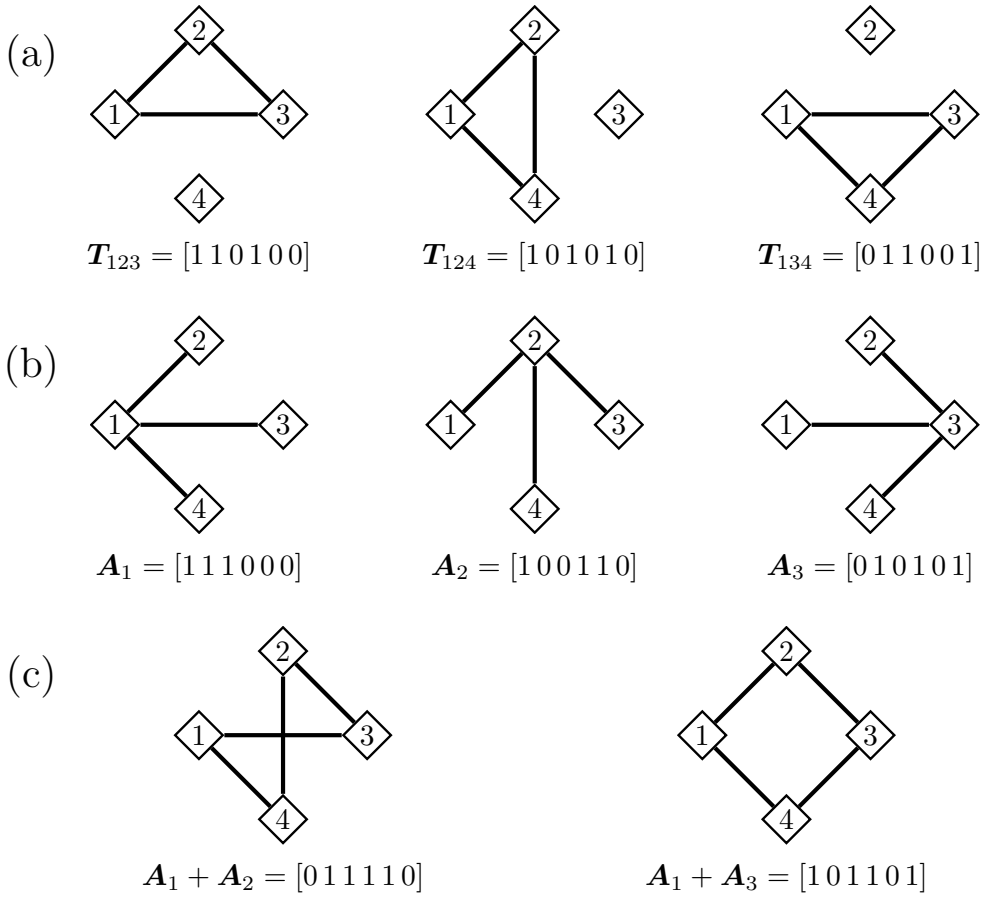


Figure 3.2: For $n = 4$, (a) the triangle graphs representing $\boldsymbol{T}_{1jk}$ $(2 \leq j < k \leq 4)$, (b) the star graphs representing $\boldsymbol{A}_l$ $(1 \leq l \leq 3)$ and (c) the graphs representing $\boldsymbol{A}_1 + \boldsymbol{A}_m$ $(2 \leq m \leq 3)$.

spanned by these two types of vectors as examples of the isomorphism (3.23). These examples are used later for the construction of the CSS stabilizer code. The two types of vectors in $\mathbb{Z}_2^{\binom{n}{2}}$ are

$$\boldsymbol{T}_{ijk} \coloneqq \boldsymbol{e}_{ij} + \boldsymbol{e}_{jk} + \boldsymbol{e}_{ki},\ \boldsymbol{A}_j \coloneqq \sum_{1\leq l\leq n,\, l\neq j} \boldsymbol{e}_{lj}, \tag{3.24}$$

where $\boldsymbol{e}_{ij}$ is the unit vector $\mathcal{I}_G(e_{ij})$. From the isomorphism (3.23), these two types of vectors can be represented by two different types of graphs. $\boldsymbol{T}_{ijk}$ is represented by a triangle graph connecting vertices

$$\left\{ \langle i \rangle, \langle j \rangle, \langle k \rangle \right\}, \tag{3.25}$$

and $\boldsymbol{A}_j$ is represented by a star graph with vertex $\langle j \rangle$ connected to every other vertex.

We construct the linear space,

$$\mathcal{C}_1 \coloneqq \mathrm{span}\left\{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_{n-1}\right\}, \tag{3.26}$$

spanned by $n-1$ linearly independent $\{\boldsymbol{A}_j\}$, and the orthogonal linear space,

$$\mathcal{C}_1^{\perp} \coloneqq \mathrm{span}\left\{\boldsymbol{T}_{123}, \boldsymbol{T}_{124}, \ldots, \boldsymbol{T}_{12n}, \boldsymbol{T}_{134}, \ldots, \boldsymbol{T}_{1\,n-1\,n}\right\}, \tag{3.27}$$

spanned by $\binom{n-1}{2}$ linearly independent $\{\boldsymbol{T}_{ijk}\}$. The elements in $\mathcal{C}_1^{\perp}$ are represented by Eulerian cycles (graph cycles that use each edge exactly once) [103]. Meanwhile, $\mathcal{C}_1$ comprises

	$\mathscr{E}$	$\mathbb{Z}_2^{\binom{n}{2}}$
$+$	$(U \cup U') \setminus (U \cap U')$	$\boldsymbol{u} + \boldsymbol{u}'$
$\cdot$	$0U = \emptyset$, $1U = U$	$0\boldsymbol{u} = \boldsymbol{0}$, $1\boldsymbol{u} = \boldsymbol{u}$

Table 3.1: The mapping of the vector addition and the scalar multiplication on $\mathscr{E}$ to those operations on $\mathbb{Z}_2^{\binom{n}{2}}$

vectors orthogonal to all vectors in $\mathcal{C}_1^{\perp}$ [103], i.e.,

$$\mathcal{C}_1 = \left(\mathcal{C}_1^{\perp}\right)^{\perp}. \tag{3.28}$$

We introduce an $(n-2)$-dimensional linear subspace of $\mathcal{C}_1$

$$\mathcal{C}_2 \coloneqq \operatorname{span}\left\{\boldsymbol{A}_1 + \boldsymbol{A}_2, \boldsymbol{A}_1 + \boldsymbol{A}_3 \ldots, \boldsymbol{A}_1 + \boldsymbol{A}_{n-1}\right\} \subset \mathcal{C}_1. \tag{3.29}$$

Figure 3.2(a), (b) and (c) depict the graphs representing bases of linear spaces $\mathcal{C}_1^{\perp}$, $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively for $n = 4$.

This subsection has shown that the power set of the edge set of an n-vertex complete graph forms a binary linear space, isomorphic to $\mathbb{Z}_2^{\binom{n}{2}}$. Hence, we have constructed a graph representation of any $\binom{n}{2}$-binary vector. The examples given in this subsection are useful for constructing our CSS code for summoning.

Chapter 4

Permutational symmetries for coincidence rates in multi-mode multi-photonic interferometry

4.1 Introduction

In this chapter we present our results on the analysis and simulation of passive interferometry experiments. Our aim is to show that the interference of partially distinguishable photons can be explained by the permutational symmetries of the input photons. Interference of photons is studied via their coincidence rates, i.e., the probability of observing different output events. Interference or the coincidence rates are a function of distinguishability of the input photons [57, 67]. Here, we show that for any multi-mode multi-photon input state, the coincidence rate can be expressed in terms of immanants. Immanants are functions with definite symmetries and we show that only those immanants appear in the coincidence rate expression that share symmetries with the input state. In this way, we are able to connect the symmetries of the input photons with their interference.

This chapter is laid out as follows. Section 4.2 presents and proves a theorem that states

that for any input state and detection, the coincidence rate can be factorized as a product of matrices. This is important because it paves the way for the application of the (matrix) representation theory of the symmetric group to analyze coincidence rates. Section 4.3 shows that the photonic Hilbert space can be decomposed into a set of subspaces with definite symmetries. Using this decomposition, we prove a theorem stating that the coincidence rate matrix product carries a representation of the symmetric group. This result is exploited to reduce the coincidence rate into a sum of the irreducible representations (irreps) of the symmetric group. Finally, we use the fact that immanants span these symmetric subspaces and irreps to express the rate in terms of immanants.

Following these two technical results, we show the power of our decomposition by analyzing an example in Sec. 4.4. We work out the details of this example exhaustively to show the coincidence rate for one particular output event. The section concludes with an analysis of this rate, showing how it can be used to unearth multiple regimes of distinguishability with qualitatively different interference behavior. We conclude this chapter with two short sections, 4.5 and 4.6, detailing two additional minor results.

4.2 Coincidence rates for arbitrary inputs

In this section, we present our first technical result, suggested in Refs. [67, 51]. In this way of calculating the coincidence rate, it is expressed as

$$C(\boldsymbol{\tau}) = \boldsymbol{u}^\dagger R(\boldsymbol{\tau}) \boldsymbol{u}, \tag{4.1}$$

where $\boldsymbol{u}$ is a vector, called the *interferometer* vector, which depends only on the properties of the interferometer, whereas the *rate* matrix R captures the effects of the time-of-arrival of the photons on the coincidence rate. Our work generalizes the terminology and formalism of previous work which was restricted to one photon in each input and output mode [67, 51], to systems with arbitrary number of photons in each input and output mode. This is the

content of the following theorem.

Theorem 1. *Given an m-mode n-photon state $|\boldsymbol{\eta}, \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle$, an interferometer described by the matrix U, and the output event $\boldsymbol{\mu}$, the coincidence rate* (2.19) *is*

$$C_{\boldsymbol{\upsilon},\boldsymbol{\xi}}(\boldsymbol{\tau}) = \boldsymbol{u}^\dagger R(\boldsymbol{\tau})\boldsymbol{u}. \tag{4.2}$$

Proof. The action of the interferometer (2.4) on the state (2.3) results in the state

$$U|\boldsymbol{\eta}; \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle = \sum_{\boldsymbol{\upsilon'}\in\{1,\ldots,m\}^n} \prod_{k=1}^{n} U_{\upsilon_k \upsilon'_k} |\boldsymbol{\eta}'; \boldsymbol{\upsilon}'; \boldsymbol{\tau}\rangle, \tag{4.3}$$

the superposition of all possible states with n photons. Here we have suppressed the normalization factor from Eq. (2.3) but calculate it shortly. In the sum above, the only states $|\boldsymbol{\eta}'; \boldsymbol{\upsilon}'; \boldsymbol{\tau}\rangle$ that have a non-zero contribution to the expectation value

$$\langle \boldsymbol{\eta}, \boldsymbol{\upsilon}; \boldsymbol{\tau}| U^\dagger M_{\boldsymbol{\mu}} U |\boldsymbol{\eta}, \boldsymbol{\upsilon}; \boldsymbol{\tau}\rangle \tag{4.4}$$

are those for which $\boldsymbol{\eta}' = \boldsymbol{\mu}$. The states for which this condition is true are collected in basis

$$B = \left\{ |\boldsymbol{\mu}; P_\sigma \boldsymbol{\xi}; \boldsymbol{\tau}\rangle : \sigma \in S_n \right\}. \tag{4.5}$$

This basis set has $N = n!/\prod_{i=1}^{m} \mu_i!$ elements, labelled by the N permutations

$$\Upsilon = \left\{ \bar{\boldsymbol{\xi}}^1, \ldots, \bar{\boldsymbol{\xi}}^N \right\} \tag{4.6}$$

of $\boldsymbol{\xi}$. Therefore, the coincidence rate

$$C(\boldsymbol{\tau}) = \sum_{i,j=1}^{N} \prod_{k=1}^{n} U^*_{\upsilon_k \bar{\xi}^i_k} \langle \boldsymbol{\mu}; \bar{\boldsymbol{\xi}}^{\boldsymbol{i}}; \boldsymbol{\tau}| M_{\boldsymbol{\mu}} \prod_{k'=1}^{n} U_{\upsilon_{k'} \bar{\xi}^j_{k'}} |\boldsymbol{\mu}; \bar{\boldsymbol{\xi}}^{\boldsymbol{j}}; \boldsymbol{\tau}\rangle. \tag{4.7}$$

Such a sum of products can equivalently be written as the matrix product $C(\boldsymbol{\tau}) = \boldsymbol{u}^\dagger R(\boldsymbol{\tau})\boldsymbol{u}$,

where the entries of $\boldsymbol{u}$ are

$$u_k \coloneqq \prod_{i=1}^{n} U_{v_i \bar{\xi}_i^k}, \tag{4.8}$$

and

$$R_{ij}(\boldsymbol{\tau}) = \langle \boldsymbol{\mu}; \bar{\boldsymbol{\xi}}^{\boldsymbol{i}}; \boldsymbol{\tau} | M_{\boldsymbol{\mu}} | \boldsymbol{\mu}; \bar{\boldsymbol{\xi}}^{\boldsymbol{j}}; \boldsymbol{\tau} \rangle. \tag{4.9}$$

Employing definition (2.17) of $M_{\boldsymbol{\mu}}$ and definition (2.3) of photonic states,

$$R_{ij}(\boldsymbol{\tau}) = \int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n r_i r_j^{\dagger}, \tag{4.10}$$

where

$$r_k = \langle 0 | \prod_{i=1}^{n} A_{\bar{\xi}_i^k}(\tau_i) \prod_{j=1}^{n} a_{\xi_j}^{\dagger}(\omega_j) | 0 \rangle. \tag{4.11}$$

The elements of $\boldsymbol{r}$ can be simplified as follows. First note that by using the definition of the creation operators (2.2) an integral over the frequencies is obtained. This integral can be calculated by defining for element r_k the set

$$C_k \coloneqq \left\{ \sigma \in S_n : P_\sigma \bar{\boldsymbol{\xi}}^k = \boldsymbol{\xi} \right\}. \tag{4.12}$$

Assuming $\boldsymbol{\xi}^1 \coloneqq \boldsymbol{\xi}$, the set C_1 stabilizes $\boldsymbol{\xi}$ and is therefore a subgroup of S_n. The sets $\{C_k\}$ are the right cosets of S_n with respect to C_1. Then by using the commutation relations (2.1) the integral over the frequencies reduces to the sum

$$r_k = \sum_{\sigma \in C_k} \phi(\omega_1) \cdots \phi(\omega_n) \mathrm{e}^{\mathrm{i}\omega_1 \tau_{\sigma(1)}} \cdots \mathrm{e}^{\mathrm{i}\omega_n \tau_{\sigma(n)}}. \tag{4.13}$$

Using this, the entries of the rate matrix turn into

$$\begin{aligned} R_{ij}(\boldsymbol{\tau}) = \frac{1}{\mathcal{N}} \frac{1}{\mu_1!, \cdots, \mu_n!} \int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n |\phi(\omega_1)|^2 \cdots |\phi(\omega_n)|^2 \\ \times \left(\sum_{\sigma' \in C_i} \mathrm{e}^{\mathrm{i}\omega_1 \tau_{\sigma'(1)}} \cdots \mathrm{e}^{\mathrm{i}\omega_n \tau_{\sigma'(n)}} \right) \left(\sum_{\tilde{\sigma} \in C_j} \mathrm{e}^{-\mathrm{i}\omega_1 \tau_{\tilde{\sigma}(1)}} \cdots \mathrm{e}^{-\mathrm{i}\omega_n \tau_{\tilde{\sigma}(n)}} \right), \end{aligned} \tag{4.14}$$

where we have reintroduced the normalization factors from Eq. (2.3) and Eq. (2.17). The normalization factor $\mathcal{N}$ is

$$\mathcal{N} = |\langle \boldsymbol{\eta}, \boldsymbol{\upsilon}, \boldsymbol{\tau} | \boldsymbol{\eta}, \boldsymbol{\upsilon}, \boldsymbol{\tau} \rangle|^2 = \left| \langle 0 | \prod_{i=1}^{n} A_{\upsilon_i}(\tau_i) \prod_{j=1}^{n} A^\dagger_{\upsilon_j}(\tau_j) | 0 \rangle \right|^2 . \tag{4.15}$$

This expression is similar to Eq. (4.11) and can be simplified in the same way. Let C' be subset of elements of S_n that stabilize $\boldsymbol{\upsilon}$. Then,

$$\mathcal{N} = \left| \int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n |\phi(\omega_1)|^2 \cdots |\phi(\omega_n)|^2 \mathrm{e}^{\mathrm{i}\omega_1 \tau_1} \cdots \mathrm{e}^{\mathrm{i}\omega_n \tau_n} \sum_{\sigma \in C'} \left[\mathrm{e}^{-\mathrm{i}\omega_1 \tau_{\sigma(1)}} \cdots \mathrm{e}^{-\mathrm{i}\omega_n \tau_{\sigma(n)}} \right] \right|^2 . \tag{4.16}$$

Hence, the coincidence rate (4.2) can be calculated from Eqs. (4.8) and (4.14). □

Theorem 1 provides convenient expressions to calculate the coincidence rate. The entries of the interferometer vector can be calculated using Eq. (4.8), the entries of rate matrix can be calculated using Eq. (4.14), and the total coincidence rate can then be calculated using Eq. (4.2). The rate matrix and interferometer matrix are of size N (see Eq. (4.5)). The expressions in Proposition 1 are amenable to execution by computer code. MATHEMATICA® code for these expressions, which was also used to do all calculations in this work, can be found on GitHub [113].

The factorization of the rate into a matrix product follows from the linearity of the interferometer's action (2.4) on photonic states. The dependence of the entries of the rate matrix on permutations arises due to swapping present in the commutation relations (2.1). The specific form of the wavefunction that we have assumed in Eq. (2.3) is not important, as the same factorization of the rate happens for photons distinguished by (one or more) other non-path degrees of freedom.

Expressing the rate in the form (4.1) is attractive for a number of reasons. First, this form separates the effects on the rate of the interferometer and the time-of-arrival of the photons. The interferometer vector $\boldsymbol{u}$ depends only on the entries of the interferometer

matrix U but not on the time-of-arrival of the photons. In the basis B (4.5), the entries of the interferometer vector are the amplitudes of the transitions from the input state $|\boldsymbol{\eta};\boldsymbol{\upsilon};\boldsymbol{\tau}\rangle$ to the states B associated with the output event $\boldsymbol{\mu}$.

The rate matrix R, a square Hermitian matrix, depends on the time-of-arrival of the photons, which determines their distinguishability. The entry R_{ij} of the rate matrix is determined by how distinguishable are the ith and jth transitions whose amplitudes are recorded in the interferometer vector. The rate matrix does not depend in any way on the input configuration of the photons. For a fixed output event such as $\boldsymbol{\mu}$, the rate matrix is the same irrespective of the input. For instance, for all inputs shown in Fig. 2.1, and for any other input of four photons which are not related by permutations to them (say $|400;1111;\boldsymbol{\tau}\rangle$), the rate matrix is the same. The effect of the input configuration on the rate expression is only felt through the interferometer vector.

4.3 Coincidence rates in terms of immanants

In this section, we show that the coincidence rates can be expressed in terms of immanants and provide a procedure to do so. First, we show, using results from the representation theory of the symmetric group [68], that the photonic Hilbert space decomposes into permutationally symmetric subspaces. Next, we show that the rate matrix carries a representation of the symmetric group. This representation can be reduced using the the same basis that decomposes the photonic Hilbert space. In this basis, the entries of the rotated interferometer vector can be transformed into sums of immanants. Thus, the coincidence rate can be expressed in terms of immanants.

The Hilbert space H of photon mode-occupations of n photons in m modes is m^n-dimensional. The Hilbert space H is composed of orthogonal subspaces, where each subspace

$H^{\boldsymbol{\mu}}$ corresponds to a distinct mode occupation $\boldsymbol{\mu}$, i.e.

$$H = \bigoplus_{\substack{\mu_i \in \{0,\ldots,n\}, \\ \sum_i \mu_i = n}} H^{\boldsymbol{\mu}}. \tag{4.17}$$

These orthogonal subspaces can be further decomposed into permutationally symmetric subspaces. The space $H^{\boldsymbol{\mu}}$ is naturally spanned by the N-dimensional basis (4.5). This basis defines the reducible representation Γ (2.27) of S_n. Using standard representation theory methods, Γ can be decomposed into a direct sum of irreps of S_n [68] as

$$\Gamma = \bigoplus_{\lambda \vdash n} p^\lambda \lambda, \tag{4.18}$$

where the sum is over all partitions of n and p^λ is the multiplicity of the irrep λ. Young tableaux, obtained by filling Young diagrams with positive integers, provide information about the size and multiplicity of the blocks that occur in this block-diagonalization. The dimension d of irrep λ is the number of standard Young tableaux of λ. The multiplicity p^λ is the number of semi-standard Young tableaux formed using Young diagram λ and the string $\boldsymbol{\xi}$. This information about the decomposition of Γ is useful for determining the size and number of blocks in the decomposition of the rate matrix (4.21) explained below.

The action of the permutation group commutes with the action of the unitary group on photonic states [114, 115, 116], i.e.

$$[U, P_\sigma] = 0, \qquad \sigma \in S_n. \tag{4.19}$$

Consequently, the space $H^{\boldsymbol{\mu}}$ block-diagonalizes as

$$H^{\boldsymbol{\mu}} = \bigoplus_{\lambda \vdash n} p^\lambda H^\lambda, \tag{4.20}$$

where the sum is over all partitions of n, and p^λ is the multiplicity of the the subspace H^λ,

which is determined as above. Both Γ and $H^{\boldsymbol{\mu}}$ can be block-diagonalized in the same basis that we call V. This basis can be obtained using a variety of methods, one of which is provided in chapter 4 of Ref. [68]. An example application of this method is presented in the next section and an implementation can be found in our reference code [113].

Now that we know how to decompose Γ and the photonic Hilbert space $H^{\boldsymbol{\mu}}$, we turn to the task of expressing the rate in terms of the immanants. To do this, we show that the rate matrix carries a representation Γ. This means, that the rate matrix can be expressed as a linear combination of the representations of all σ in S_n. The following theorem formalizes this notion.

Theorem 2. *The rate matrix carries the representation* (2.27)*; i.e. the rate matrix may be expressed as*

$$R(\boldsymbol{\tau}) = \sum_{\sigma \in S_n} \Delta_\sigma(\boldsymbol{\tau}) \Gamma(\sigma). \tag{4.21}$$

Proof. First note that Eqs. (4.21) and (2.27) imply that

$$R_{ij}(\boldsymbol{\tau}) = \sum_{\sigma \in S_n} \begin{cases} \Delta_\sigma(\boldsymbol{\tau}) & \text{if } P_\sigma \bar{\boldsymbol{\xi}}^i = \bar{\boldsymbol{\xi}}^j \\ 0 & \text{otherwise} \end{cases}. \tag{4.22}$$

We show that Eq. (4.14) is equivalent to this expression. The double sum in Eq. (4.14) has entries

$$\begin{aligned} &\int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n |\phi(\omega_1)|^2 \cdots |\phi(\omega_n)|^2 \\ &\qquad \times \mathrm{e}^{\mathrm{i}\omega_1(\tau_{\sigma'(1)} - \tau_{\tilde{\sigma}(1)})} \cdots \mathrm{e}^{\mathrm{i}\omega_n(\tau_{\sigma'(n)} - \tau_{\tilde{\sigma}(n)})} \qquad (4.23) \\ = &\int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n |\phi(\omega_1)|^2 \cdots |\phi(\omega_n)|^2 \\ &\qquad \times \mathrm{e}^{\mathrm{i}\omega_1(\tau_{\tilde{\sigma}^{-1}\sigma'(1)} - \tau_1)} \cdots \mathrm{e}^{\mathrm{i}\omega_n(\tau_{\tilde{\sigma}^{-1}\sigma'(n)} - \tau_n)}, \qquad (4.24) \end{aligned}$$

where the equality is obtained by a suitable relabelling of the $\{\omega_i\}$. Note that from the

definitions of $\sigma' \in C_i$ and $\tilde{\sigma} \in C_j$ it follows that $(P_{\tilde{\sigma}})^{-1} P_{\sigma'} \bar{\boldsymbol{\xi}}^i = \bar{\boldsymbol{\xi}}^j$. Hence, if we set $\sigma = \tilde{\sigma}^{-1}\sigma'$ in Eq. (4.24) then Eq. (4.22) is satisfied. Explicitly, by comparing Eq. (4.14) and Eq. (4.22), it is clear that

$$\Delta_{\tilde{\sigma}^{-1}\sigma'}(\boldsymbol{\tau}) = \int \mathrm{d}\omega_1 \cdots \mathrm{d}\omega_n |\phi(\omega_1)|^2 \cdots |\phi(\omega_n)|^2 \times \left(\mathrm{e}^{\mathrm{i}\omega_1 \tau_{\sigma'(1)}} \cdots \mathrm{e}^{\mathrm{i}\omega_n \tau_{\sigma'(n)}}\right) \left(\mathrm{e}^{-\mathrm{i}\omega_1 \tau_{\tilde{\sigma}(1)}} \cdots \mathrm{e}^{-\mathrm{i}\omega_n \tau_{\tilde{\sigma}(n)}}\right). \tag{4.25}$$

□

The expression of the rate matrix in the form (4.21) implies that the basis V that reduces Γ also block-diagonalizes the rate matrix. Then, the coincidence rate (4.1) is calculated by employing the formula

$$C(\boldsymbol{\tau}) = (V\boldsymbol{u})^\dagger \left[V R(\boldsymbol{\tau}) V^\dagger\right] (V\boldsymbol{u}). \tag{4.26}$$

In this expression, both the rotated rate matrix and interferometer vector are block-diagonal, where each block is associated with an irrep of S_n and is of the same size as the dimension of the irrep.

The entries of the rotated interferometer vector $V\boldsymbol{u}$ can be expressed as as sums of immanants. The immanants in question are those of the scattering matrix T, which is a four-dimensional matrix formed by taking the $\boldsymbol{\upsilon}$ rows (input) and $\boldsymbol{\xi}$ columns (output) of the interferometer matrix U. It has entries

$$T_{ij} \coloneqq U_{\upsilon_i, \xi_j}. \tag{4.27}$$

We define T_σ as the matrix T with its rows permuted by $\sigma \in S_n$ (note $T = T_{\mathrm{e}}$).

The immanants of type λ are vectors in the subspace H^λ as they are related to the same irreps of S_n. In particular, the subspace H^λ is spanned by up to d distinct immanants of λ type, which will happen if there is no multiplicity of photons in the input or output modes. If there are multiple photons in any of the input or output modes, then the number of distinct

immanants are reduced, because the number of distinct states that can be obtained by permuting the photons is reduced. The rule for determining the actual number of immanants of certain type λ is rather simple. Count the number of semi-standard Young tableaux of λ, once using input photon-occupation string $\boldsymbol{\upsilon}$ and once using the output photon-occupation string $\boldsymbol{\mu}$: the minimum of these two counts is the number of distinct immanants of the type λ. Let this set of distinct immanants be I^λ

The block of $V\boldsymbol{u}$ labelled by γ can be linearly transformed to express it in terms of the immanants I^λ. Explicitly, suppose the element $(V\boldsymbol{u})_i$ is associated with the irrep λ. Then, the element $(V\boldsymbol{u})_i$ is a vector in the space H^λ, and can be expressed in terms of the elements of the set I^λ. In this way, $V\boldsymbol{u}$ and the coincidence rate (4.26) can be expressed in terms of immanants.

The decomposition of the rate as a matrix product (4.26) provides computational shortcuts for calculating coincidence rates for repeated simulations of experiments in two cases. If the interferometer parameters are fixed but the photon delays vary across simulations, then the immanants do not change and have to be computed only once whereas the coefficients do change between computational runs. On the other hand, if the photon delays are fixed but the interferometer parameters vary across simulations, then only the immanants have to be computed anew in each computational run.

This section and previous section have provided our technical results on the decomposition of the coincidence rate. However, in order to follow through the calculation for a particular system requires usage of other standard tools. Therefore, in the next section, we calculate the coincidence rate in full detail for one particular example.

4.4 Example of four photons in three modes

In this section we analyze the example presented in Fig. 2.1a, consisting of four photons in three modes. We calculate explicit expressions for the interferometer vector and the rate

matrix. We use class operator methods to find the basis V in which the rate matrix is block-diagonal and the entries of the interferometer matrix are the immanants of the scattering matrix.

The experimental setup in Fig. 2.1a is described by $\boldsymbol{\eta} = 211$, $\boldsymbol{\upsilon} = 1123$, and $\boldsymbol{\mu} = 022$. The temporal state of the photons is encoded by $\boldsymbol{\tau}$ and the interferometer matrix is U. We can use the results of Theorems 1 and 2 to calculate the coincidence rate. However, before doing so we will employ Eq. (2.19) to give the reader some intuition. The input state,

$$|211;1123\rangle = A_1^\dagger(\tau_1)A_1^\dagger(\tau_2)A_2^\dagger(\tau_3)A_3^\dagger(\tau_4)|0\rangle, \tag{4.28}$$

transforms under the action of the interferometer to

$$\begin{aligned} U|211;1123\rangle = &\Big(U_{11}A_1^\dagger(\tau_1) + U_{12}A_2^\dagger(\tau_1) + U_{13}A_3^\dagger(\tau_1)\Big) \\ &\times \Big(U_{11}A_1^\dagger(\tau_2) + U_{12}A_2^\dagger(\tau_2) + U_{13}A_3^\dagger(\tau_2)\Big) \\ &\times \Big(U_{21}A_1^\dagger(\tau_3) + U_{22}A_2^\dagger(\tau_3) + U_{23}A_3^\dagger(\tau_3)\Big) \\ &\times \Big(U_{31}A_1^\dagger(\tau_4) + U_{32}A_2^\dagger(\tau_4) + U_{33}A_3^\dagger(\tau_4)\Big)|0\rangle, \end{aligned} \tag{4.29}$$

where we have ignored the normalization factor in these expressions for simplicity. We are interested in the output event $\boldsymbol{\mu} = 022$. Of the 81 terms in the expansion of (4.29), only six correspond to two photons in each of the second and third modes, coinciding with the six permutations of $\boldsymbol{\xi} = 2233$. Only these six terms give a non-zero contribution to the rate (2.19),

$$C(\boldsymbol{\tau}) = \langle 221;1123|U^\dagger M_{022}U|221;1123\rangle. \tag{4.30}$$

The amplitude of these six terms is $w^\dagger|0\rangle\boldsymbol{u}$, where the interferometer vector

$$\boldsymbol{u} = \begin{pmatrix} U_{12}U_{12}U_{23}U_{33} \\ U_{12}U_{13}U_{22}U_{33} \\ U_{12}U_{13}U_{23}U_{32} \\ U_{13}U_{12}U_{22}U_{33} \\ U_{13}U_{12}U_{23}U_{32} \\ U_{13}U_{13}U_{22}U_{32} \end{pmatrix}, \tag{4.31}$$

and vector

$$\boldsymbol{w} = \begin{pmatrix} A_2(\tau_1)A_2(\tau_2)A_3(\tau_3)A_3(\tau_4) \\ A_2(\tau_1)A_3(\tau_2)A_2(\tau_3)A_3(\tau_4) \\ A_2(\tau_1)A_3(\tau_2)A_3(\tau_3)A_2(\tau_4) \\ A_3(\tau_1)A_2(\tau_2)A_2(\tau_3)A_3(\tau_4) \\ A_3(\tau_1)A_2(\tau_2)A_3(\tau_3)A_2(\tau_4) \\ A_3(\tau_1)A_3(\tau_2)A_2(\tau_3)A_2(\tau_4) \end{pmatrix}. \tag{4.32}$$

Employing the measurement operator M_{022} for detecting two photons in each mode the rate (2.19) is

$$C(\boldsymbol{\tau}) = \boldsymbol{u}^\dagger\langle 0|\boldsymbol{w}M_{022}\boldsymbol{w}^\dagger|0\rangle\boldsymbol{u}. \tag{4.33}$$

In this expression, the 6×6 matrix

$$R(\boldsymbol{\tau}) \coloneqq \langle 0|\boldsymbol{w}M_{022}\boldsymbol{w}^\dagger|0\rangle \tag{4.34}$$

is the rate matrix. This expression is equivalent to the intermediate expression (4.10) of the rate matrix in Theorem 1. The rate matrix can be calculated from this expression using tedious calculations. We use the simplified expression (4.14) to calculate the rate matrix.

First we note that the string $\boldsymbol{\xi} = 2233$ has permutations

$$\Upsilon = \{2233, 2323, 2332, 3223, 3232, 3322\}\,. \tag{4.35}$$

Using this, we can find the cosets of $\boldsymbol{\xi} = 2233$. The string $\boldsymbol{\xi} = 2233$ is stabilized by the S_4 subgroup $C_1 = \{\mathrm{e}, (12), (34), (12, 34)\}$: for instance $P_{12,34}2233 = 2233$. This subgroup has right cosets

$$\begin{aligned}
C_1 &= \{\mathrm{e}, (12), (34), (12, 34)\},\\
C_2 &= \{(23), (132), (234), (1342)\},\\
C_3 &= \{(24), (142), (243), (1432)\},\\
C_4 &= \{(13), (123), (134), (1234)\},\\
C_5 &= \{(14), (124), (143), (1243)\},\\
C_6 &= \{(1324), (1423), (13, 24), (14, 23)\}.
\end{aligned} \tag{4.36}$$

By definition (4.12), the elements of coset C_k maps $\bar{\boldsymbol{\xi}}^k$ to $\boldsymbol{\xi} = \bar{\boldsymbol{\xi}}^1$: for instance $(23) \in C_2$ acts as $P_{23}2323 = 2233$.

To calculate an explicit expression for the rate matrix we assume that all photons have an identical Gaussian spectrum,

$$\phi_i(\omega) = \frac{1}{(\pi\sigma^2)^{1/4}} \exp\left(-\frac{(\omega - \omega_0)^2}{2\sigma^2}\right) \quad \forall i \in \{1, \ldots, n\}\,. \tag{4.37}$$

For modeling a real experiment, the rates can be calculated using experimentally measured spectra of the input photons. Using this Gaussian spectrum and employing the expression (4.14) we find that the rate matrix is

$$R(\boldsymbol{\tau}) = \begin{pmatrix} \tilde{R}_1 & \tilde{R}_2 & \tilde{R}_3 \end{pmatrix}, \tag{4.38}$$

where

$$\tilde{R}_1 = \begin{pmatrix} \Delta_{\mathrm{e}} + \Delta_{(12)} + \Delta_{(12,34)} + \Delta_{(34)} & \Delta_{(132)} + \Delta_{(1342)} + \Delta_{(23)} + \Delta_{(234)} \\ \Delta_{(123)} + \Delta_{(1243)} + \Delta_{(23)} + \Delta_{(243)} & \Delta_{\mathrm{e}} + \Delta_{(13)} + \Delta_{(13,24)} + \Delta_{(24)} \\ \Delta_{(1234)} + \Delta_{(124)} + \Delta_{(234)} + \Delta_{(24)} & \Delta_{(1324)} + \Delta_{(134)} + \Delta_{(243)} + \Delta_{(34)} \\ \Delta_{(13)} + \Delta_{(132)} + \Delta_{(143)} + \Delta_{(1432)} & \Delta_{(12)} + \Delta_{(123)} + \Delta_{(142)} + \Delta_{(1423)} \\ \Delta_{(134)} + \Delta_{(1342)} + \Delta_{(14)} + \Delta_{(142)} & \Delta_{(12,34)} + \Delta_{(1234)} + \Delta_{(14,23)} + \Delta_{(1432)} \\ \Delta_{(13,24)} + \Delta_{(1324)} + \Delta_{(14,23)} + \Delta_{(1423)} & \Delta_{(124)} + \Delta_{(1243)} + \Delta_{(14)} + \Delta_{(143)} \end{pmatrix}, \tag{4.39}$$

$$\tilde{R}_2 = \begin{pmatrix} \Delta_{(142)} + \Delta_{(1432)} + \Delta_{(24)} + \Delta_{(243)} & \Delta_{(123)} + \Delta_{(1234)} + \Delta_{(13)} + \Delta_{(134)} \\ \Delta_{(1423)} + \Delta_{(143)} + \Delta_{(234)} + \Delta_{(34)} & \Delta_{(12)} + \Delta_{(124)} + \Delta_{(132)} + \Delta_{(1324)} \\ \Delta_{\mathrm{e}} + \Delta_{(14)} + \Delta_{(14,23)} + \Delta_{(23)} & \Delta_{(12,34)} + \Delta_{(1243)} + \Delta_{(13,24)} + \Delta_{(1342)} \\ \Delta_{(12,34)} + \Delta_{(1243)} + \Delta_{(13,24)} + \Delta_{(1342)} & \Delta_{\mathrm{e}} + \Delta_{(14)} + \Delta_{(14,23)} + \Delta_{(23)} \\ \Delta_{(12)} + \Delta_{(124)} + \Delta_{(132)} + \Delta_{(1324)} & \Delta_{(1423)} + \Delta_{(143)} + \Delta_{(234)} + \Delta_{(34)} \\ \Delta_{(123)} + \Delta_{(1234)} + \Delta_{(13)} + \Delta_{(134)} & \Delta_{(142)} + \Delta_{(1432)} + \Delta_{(24)} + \Delta_{(243)} \end{pmatrix}, \tag{4.40}$$

$$\tilde{R}_3 = \begin{pmatrix} \Delta_{(124)} + \Delta_{(1243)} + \Delta_{(14)} + \Delta_{(143)} & \Delta_{(13,24)} + \Delta_{(1324)} + \Delta_{(14,23)} + \Delta_{(1423)} \\ \Delta_{(12,34)} + \Delta_{(1234)} + \Delta_{(14,23)} + \Delta_{(1432)} & \Delta_{(134)} + \Delta_{(1342)} + \Delta_{(14)} + \Delta_{(142)} \\ \Delta_{(12)} + \Delta_{(123)} + \Delta_{(142)} + \Delta_{(1423)} & \Delta_{(13)} + \Delta_{(132)} + \Delta_{(143)} + \Delta_{(1432)} \\ \Delta_{(1324)} + \Delta_{(134)} + \Delta_{(243)} + \Delta_{(34)} & \Delta_{(1234)} + \Delta_{(124)} + \Delta_{(234)} + \Delta_{(24)} \\ \Delta_{\mathrm{e}} + \Delta_{(13)} + \Delta_{(13,24)} + \Delta_{(24)} & \Delta_{(123)} + \Delta_{(1243)} + \Delta_{(23)} + \Delta_{(243)} \\ \Delta_{(132)} + \Delta_{(1342)} + \Delta_{(23)} + \Delta_{(234)} & \Delta_{\mathrm{e}} + \Delta_{(12)} + \Delta_{(12,34)} + \Delta_{(34)} \end{pmatrix}, \tag{4.41}$$

and

$$\Delta_{\mathrm{e}} = 1, \qquad \Delta_{(12)} = \mathrm{e}^{-\sigma^2(\tau_1-\tau_2)^2},$$

$$\Delta_{(13)} = e^{-\sigma^2(\tau_1-\tau_3)^2}, \qquad \Delta_{(14)} = e^{-\sigma^2(\tau_1-\tau_4)^2},$$

$$
\begin{aligned}
\Delta_{(23)} &= \mathrm{e}^{-\sigma^2(\tau_2-\tau_3)^2}, & \Delta_{(24)} &= \mathrm{e}^{-\sigma^2(\tau_2-\tau_4)^2},\\
\Delta_{(34)} &= \mathrm{e}^{-\sigma^2(\tau_3-\tau_4)^2}, & \Delta_{(123)} &= \mathrm{e}^{-\sigma^2\left(\tau_1^2+\tau_2^2+\tau_3^2-\tau_1\tau_2-\tau_1\tau_3-\tau_2\tau_3\right)},\\
\Delta_{(124)} &= \mathrm{e}^{-\sigma^2\left(\tau_1^2+\tau_2^2+\tau_4^2-\tau_1\tau_2-\tau_1\tau_4-\tau_2\tau_4\right)}, & \Delta_{(132)} &= \Delta_{123}\\
\Delta_{(134)} &= \mathrm{e}^{-\sigma^2\left(\tau_1^2+\tau_3^2+\tau_4^2-\tau_1\tau_3-\tau_1\tau_4-\tau_3\tau_4\right)}, & \Delta_{(142)} &= \Delta_{124}\\
\Delta_{(143)} &= \Delta_{134} & \Delta_{(234)} &= \mathrm{e}^{-\sigma^2\left(\tau_2^2+\tau_3^2+\tau_4^2-\tau_2\tau_3-\tau_2\tau_4-\tau_3\tau_4\right)},\\
\Delta_{(243)} &= \Delta_{234} & \Delta_{(1234)} &= \mathrm{e}^{-\sigma^2\left(\tau_1^2+\tau_2^2+\tau_3^2+\tau_4^2-\tau_1\tau_2-\tau_1\tau_4-\tau_2\tau_3-\tau_3\tau_4\right)},\\
\Delta_{(1243)} &= \mathrm{e}^{-\sigma^2\left(\tau_1^2+\tau_2^2+\tau_3^2+\tau_4^2-\tau_1\tau_2-\tau_1\tau_3-\tau_2\tau_4-\tau_3\tau_4\right)}, & \Delta_{(1324)} &= \mathrm{e}^{-\sigma^2\left(\tau_1^2+\tau_2^2+\tau_3^2+\tau_4^2-\tau_1\tau_3-\tau_1\tau_4-\tau_2\tau_3-\tau_2\tau_4\right)},\\
\Delta_{(1342)} &= \Delta_{1243}, & \Delta_{(1423)} &= \Delta_{1324},\\
\Delta_{(1432)} &= \Delta_{1234}, & \Delta_{(12,34)} &= \mathrm{e}^{-\sigma^2\left[(\tau_1-\tau_2)^2+(\tau_3-\tau_4)^2\right]},\\
\Delta_{(13,24)} &= \mathrm{e}^{-\sigma^2\left[(\tau_1-\tau_3)^2+(\tau_2-\tau_4)^2\right]}, & \Delta_{(14,23)} &= \mathrm{e}^{-\sigma^2\left[(\tau_1-\tau_4)^2+(\tau_2-\tau_3)^2\right]}.
\end{aligned}
\tag{4.42}
$$

This compact form of the rate matrix in terms of Δ_σ (4.25) is provided because we also want to verify that the rate matrix carries the representation (2.27).

We take a short detour to construct this representation. Note that the Hilbert space H of photon mode-occupations of four photons in three modes is 3^4-dimensional. The Hilbert space H is composed of orthogonal subspaces , where each subspace $H^{\boldsymbol{\mu}}$ corresponds to a distinct mode occupation $\boldsymbol{\mu}$, i.e.

$$
H = \bigoplus_{\substack{\mu_i\in\{0,\ldots,4\},\\ \sum_i \mu_i = 4}} H^{\boldsymbol{\mu}}. \tag{4.43}
$$

One of these subspaces is H^{022}, which corresponds to the output event of Fig. 2.1. These orthogonal subspaces can be further decomposed into permutationally symmetric subspaces. As the procedure is the same for all of them, we only discuss the decomposition of H^{022}.

The H^{022} subspace is $4!/(0!2!2!) = 6$ dimensional. A natural basis (4.5) for this subspace is spanned by the six distinct vectors obtained by applying the permutation operator P_σ to $|022;2233\rangle$ for $\sigma \in S_4$. Using Eqs. (4.35) and (4.5) we find that the representation Γ has

basis

$$B = \{|022;2233;\boldsymbol{\tau}\rangle, |022;2323;\boldsymbol{\tau}\rangle, |022;2332;\boldsymbol{\tau}\rangle,$$
$$|022;3223;\boldsymbol{\tau}\rangle, |022;3232;\boldsymbol{\tau}\rangle, |022;3322;\boldsymbol{\tau}\rangle\}\,. \tag{4.44}$$

The action P_σ of S_4 on this basis defines a six-dimensional reducible representation Γ of S_4 (2.27). In simple terms, given any element $\sigma \in S_4$, $\Gamma(\sigma)$ is the 6×6 permutation matrix that exchanges the elements of B according to how P_σ acts on B.

In this basis, using Eq. (2.27), the representation of the elements of S_4 are

$$\Gamma_{\mathrm{e}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \Gamma_{(12)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\Gamma_{(13)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(14)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(23)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \Gamma_{(24)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(34)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \Gamma_{(123)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(124)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(132)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\Gamma_{(134)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(142)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(143)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(234)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\Gamma_{(243)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(1234)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(1243)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(1324)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(1342)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \Gamma_{(1423)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\Gamma_{(1432)} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(12,34)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\Gamma_{(13,24)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \Gamma_{(14,23)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4.45}$$

Using these representations it is easy to verify via inspection that Eq. (4.21) is true, which means the rate matrix does carry the representation Γ of S_4. Therefore, in order to block-diagonalize the rate matrix we have to reduce Γ to the irreps of S_4.

The irreps of S_4 are labelled by the Young diagrams  , ,  , and (the diagram corresponds to the partition $3 + 1$ etc.). The Young diagram corresponding to each irrep indicates the symmetries of the irrep, where the irrep is symmetric across each row and anti-symmetric across each column. The rule for determining which irreps do occur is to count the number of semi-standard Young tableau for each irrep using the string $\boldsymbol{\xi} = 2233$. For each of the first three Young diagrams there is only one possible semi-standard Young tableau. These are

$$\begin{array}{|c|c|c|c|}\hline 2&2&3&3\\\hline\end{array}, \qquad \begin{array}{|c|c|c|}\hline 2&2&3\\\hline 3\\\cline{1-1}\end{array}, \qquad \begin{array}{|c|c|}\hline 2&2\\\hline 3&3\\\hline\end{array}. \tag{4.46}$$

For the last two Young diagrams, and there is no possible way to construct a valid semi-standard Young tableau. Physically, this is because the output event $\boldsymbol{\mu} = 022$, requires symmetry in the placement of third and fourth photon since they are in the same mode, but

 and  are anti-symmetric in the third and fourth boxes. Therefore, the corresponding irreps do not occur in the decomposition. Γ decomposes as

$$\Gamma = \square\square\square\square \oplus \begin{array}{|c|c|c|}\hline & & \\ \hline \\ \cline{1-1}\end{array} \oplus \begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}. \tag{4.47}$$

This can also be verified using orthogonality of characters [68]. This decomposition is also identical to the decomposition of the tensor product $(2,0,0) \otimes (2,0,0)$ of su(4) irrep; the irrep $(2,0,0)$ is appropriate to describe the possible states of two indistinguishable photons, as required by our detection scheme where output photons in a given output mode are indistinguishable [68]. The Young tableau manipulations of Eq.((4.46)) are simply an application of the well-known Littlewood-Richardson rule for decomposing tensor products of su(n) irreps. The dimension of each irrep λ is the number of standard Young tableaux that can be constructed from the Young diagram λ. For the irreps that occur in (4.47) the standard Young tableaux are

$$\begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 \\ \cline{1-1}\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 \\ \cline{1-1}\end{array}, \quad \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 \\ \cline{1-1}\end{array}, \quad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline\end{array}, \quad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 4 \\ \hline\end{array}. \tag{4.48}$$

Based on these constructions we can infer that the irrep $\square\square\square\square$ is one dimensional, the irrep $\begin{array}{|c|c|c|}\hline & & \\ \hline \\ \cline{1-1}\end{array}$ is three dimensional and the irrep $\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}$ is two dimensional. The sum of these dimensions is six, the same as the size of the rate matrix and the dimension of Γ.

We now find the basis which reduces Γ to block-diagonal form. We use the method of class-operators. The basis vectors for a irrep are the linear combinations of the eigenvectors of the complete set of commuting operators (CSCO). A CSCO of symmetric group S_n is formed from the set $\left\{D_k^{(2)}\right\}_{k=2}^{n}$ of two-cycle class operators [68],

$$D_k^{(2)} = \sum_{\sigma^{(2)} \in S_k} \sigma^{(2)}, \tag{4.49}$$

of the canonical subgroup chain $S_n \supset S_{n-1} \cdots \supset S_2$. Using the representations of the two

cycles we can construct the two-cycle class operators,

$$D_2(2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$D_3(2) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$D_4(2) = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 & 0 & 1 \\ 1 & 1 & 2 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}. \tag{4.50}$$

Next, the eigenbasis V that simultaneously diagonalizes the operators $\left\{D_k^{(2)}\right\}_{k=2}^{n}$ is found. The eigenbasis can be found using numerical simultaneous diagonalization algorithms [117]. However, for small n, a simpler procedure is as follows. The two-cycle class operators have eigenvalues

$$\kappa_\lambda^{(2)} = \frac{n}{2} + \frac{1}{2}\sum_{\ell=1}^{m} \lambda_\ell(\lambda_\ell - 2\ell), \tag{4.51}$$

where each eigenvalue is labelled by a Young diagram λ and λ_ℓ is the number of boxes on

the ℓ-th row of the Young diagram λ. The chains for S_4 are

$$\begin{array}{ccccc}
\ydiagram{4} & \to & \ydiagram{3} & \to & \ydiagram{2}, \\
(6) & & (3) & & (1) \\
\ydiagram{3,1} & \to & \ydiagram{3} & \to & \ydiagram{2}, \\
(2) & & (3) & & (1) \\
\ydiagram{3,1} & \to & \ydiagram{2,1} & \to & \ydiagram{2}, \\
(2) & & (0) & & (1) \\
\ydiagram{3,1} & \to & \ydiagram{2,1} & \to & \ydiagram{1,1}, \\
(2) & & (0) & & (-1) \\
\ydiagram{2,2} & \to & \ydiagram{2,1} & \to & \ydiagram{2}, \\
(0) & & (0) & & (1) \\
\ydiagram{2,2} & \to & \ydiagram{2,1} & \to & \ydiagram{1,1}, \\
(0) & & (0) & & (-1)
\end{array} \tag{4.52}$$

where the eigenvalue associated with each Young diagram via Eq. (4.51) is given below it. Each of the chains of Young diagrams is associated with one simultaneous eigenvector of $\left\{D_k^{(2)}\right\}_{k=2}^{n}$. For instance, the first eigenvector has eigenvalue 6 for $D_4^{(2)}$, eigenvalue 3 for $D_3^{(2)}$ and eigenvalue 1 for $D_2^{(2)}$.

A simple way of finding the eigenbasis is to use the operator

$$D^{(2)} = \sum_{k=2}^{4} \alpha_i D_k^{(2)}, \tag{4.53}$$

where the constants α_i are chosen so that $D^{(2)}$ has no repeated eigenvalues. For $n \leq 6$ the

choice of $\alpha_i = i + 7$ works. With this choice

$$D^{(2)} = \begin{pmatrix} 41 & 21 & 11 & 21 & 11 & 0 \\ 21 & 32 & 11 & 30 & 0 & 11 \\ 11 & 11 & 32 & 0 & 30 & 21 \\ 21 & 30 & 0 & 32 & 11 & 11 \\ 11 & 0 & 30 & 11 & 32 & 21 \\ 0 & 11 & 21 & 11 & 21 & 41 \end{pmatrix}. \tag{4.54}$$

The eigenbasis of $D^{(2)}$ is

$$V = \begin{pmatrix} \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ 0 & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{\sqrt{3}} & \frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} \\ 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}, \tag{4.55}$$

where the vectors (rows) have been ordered to match the ordering of the irreps in (4.47). In this basis the rate matrix $VR(\boldsymbol{\tau})V^{\mathrm{T}}$ is block-diagonal.

Irrep λ/Character	χ^λ (□□□□)	χ^λ (□□□)	χ^λ (□□)	χ^λ (□□ / □)	χ^λ (□ / □ / □)
□□□□	1	1	1	1	1
□□□ / □	−1	0	−1	1	3
□□ / □□	0	−1	2	0	2

Table 4.1: Characters for three irreps of S_4. Each row provides the characters of one irrep, where each column entry is the character of one class of S_4.

We now analyze the effects of the basis change V on the interferometer matrix $\boldsymbol{u}$. Using Eqs. (4.31) and (4.55), we find

$$V\boldsymbol{u} = \frac{1}{\sqrt{6}} \begin{pmatrix} U_{23}U_{33}U_{12}^2 + 2U_{13}U_{23}U_{32}U_{12} + 2U_{13}U_{22}U_{33}U_{12} + U_{13}^2U_{22}U_{32} \\ 0 \\ -\sqrt{2}U_{23}U_{33}U_{12}^2 - \sqrt{2}U_{13}U_{23}U_{32}U_{12} + \sqrt{2}U_{13}U_{22}U_{33}U_{12} + \sqrt{2}U_{13}^2U_{22}U_{32} \\ -U_{23}U_{33}U_{12}^2 + 2U_{13}U_{23}U_{32}U_{12} - 2U_{13}U_{22}U_{33}U_{12} + U_{13}^2U_{22}U_{32} \\ 0 \\ \sqrt{2}U_{23}U_{33}U_{12}^2 - \sqrt{2}U_{13}U_{23}U_{32}U_{12} - \sqrt{2}U_{13}U_{22}U_{33}U_{12} + \sqrt{2}U_{13}^2U_{22}U_{32} \end{pmatrix}. \tag{4.56}$$

The entries of $V\boldsymbol{u}$ can be expressed as immanants. Immanants are defined using the characters of the symmetric group. For S_4 the relevant characters are provided in Table 4.1.

The immanants are functions of the scattering matrix T or the matrix found by permuting the rows of T. Using the definition of the scattering matrix (4.27), where $\boldsymbol{\upsilon} = 1123$ and $\boldsymbol{\xi} = 2233$, the matrix

$$T = \begin{pmatrix} U_{12} & U_{12} & U_{13} & U_{13} \\ U_{12} & U_{12} & U_{13} & U_{13} \\ U_{22} & U_{22} & U_{23} & U_{23} \\ U_{32} & U_{32} & U_{33} & U_{33} \end{pmatrix}. \tag{4.57}$$

Using Eq. (2.28) and Table 4.1, we find that this matrix has associated immanants

$$\operatorname{imm}^{\square\square\square\square} T = 4U_{23}U_{33}U_{12}^2 + 8U_{13}U_{23}U_{32}U_{12} + 8U_{13}U_{22}U_{33}U_{12} + 4U_{13}^2U_{22}U_{32}, \tag{4.58}$$

$$\operatorname{imm}^{\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} T = 4U_{12}^2U_{23}U_{33} - 4U_{13}^2U_{22}U_{32}, \tag{4.59}$$

$$\operatorname{imm}^{\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}} T_{(13)} = 4U_{12}U_{13}U_{22}U_{33} - 4U_{12}U_{13}U_{23}U_{32}, \tag{4.60}$$

$$\operatorname{imm}^{\begin{smallmatrix}\square\square\\\square\square\end{smallmatrix}} T = 4U_{23}U_{33}U_{12}^2 - 4U_{13}U_{23}U_{32}U_{12} - 4U_{13}U_{22}U_{33}U_{12} + 4U_{13}^2U_{22}U_{32}, \tag{4.61}$$

where we remind the reader that $T_{(13)}$ is the matrix T with its first and third rows permuted. This is the complete set of distinct immanants of types $\square\square\square\square$, $\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}$ and $\begin{smallmatrix}\square\square\\\square\square\end{smallmatrix}$ that can be formed

from T_σ for all $\sigma \in S_4$. The set of immanants

$$\left\{\text{imm}^{\lambda} T_\sigma : \sigma \in S_4\right\}, \tag{4.62}$$

has fewer distinct elements than $|S_4| = 24$ because the immanants for two different σ may be be equal (up to a constant), i.e. its possible that

$$\text{imm}^{\lambda} T_\sigma \propto \text{imm}^{\lambda} T_{\sigma'}. \tag{4.63}$$

For instance, the permanent $\text{imm}^{\ydiagram{4}} T$ is fully symmetric under any permutation of the rows of T, i.e. for all $\sigma \in S_4$, we find that $\text{imm}^{\ydiagram{4}} T_\sigma = \text{imm}^{\ydiagram{4}} T$. On the other hand, for half the $\sigma \in S_4$, $\text{imm}^{\ydiagram{3,1}} T_\sigma$ is proportional to $\text{imm}^{\ydiagram{3,1}} T$, and for the other half $\text{imm}^{\ydiagram{3,1}} T_\sigma$ is proportional to $\text{imm}^{\ydiagram{3,1}} T_{(13)}$. Finally, due to the multiplicity of photons in input and output modes (repetition of the rows and columns of T), for all $\sigma \in S_4$, we find that $\text{imm}^{\ydiagram{2,2}} T_\sigma$ is proportional to $\text{imm}^{\ydiagram{2,2}} T$.

To transform the entries of $V\boldsymbol{u}$ into immanants, we require the help of Eq. (4.48) which specifies the sizes of each block of the rotated interferometer vector $V\boldsymbol{u}$. We note that the first block associated with irrep $\ydiagram{4}$ is of size 1. The first entry in Eq. (4.56), must then be the permanent $\text{imm}^{\ydiagram{4}} T$ of the scattering matrix up to a constant. We can verify this is so. The next block, associated with irrep $\ydiagram{3,1}$ is three-dimensional. We should able to express the second to fifth entries of Eq. (4.56) in terms of the two immanants $\text{imm}^{\ydiagram{3,1}} T$ and $\text{imm}^{\ydiagram{3,1}} T_{13}$. The simple rotation,

$$\frac{1}{4\sqrt{6}} \begin{pmatrix} 0 & 0 \\ -\sqrt{2} & \sqrt{2} \\ -1 & -2 \end{pmatrix} \begin{pmatrix} \text{imm}^{\ydiagram{3,1}} T \\ \text{imm}^{\ydiagram{3,1}} T_{13} \end{pmatrix}, \tag{4.64}$$

is indeed equal to the second to fifth entries of Eq. (4.56). The same procedure can be followed for the final two-dimensional block associated with the irrep $\ydiagram{2,2}$. Hence, in the basis

V the entries of the interferometer vector,

$$V\boldsymbol{u} = \frac{1}{4\sqrt{6}} \begin{pmatrix} \mathrm{imm}^{\square\square\square\square}T \\ 0 \\ -\sqrt{2}\mathrm{imm}^{\square\square\square}T + \sqrt{2}\mathrm{imm}^{\square\square\square}T_{(13)} \\ -\mathrm{imm}^{\square\square\square}T - 2\mathrm{imm}^{\square\square\square}T_{(13)} \\ 0 \\ \sqrt{2}\mathrm{imm}^{\square\square}T \end{pmatrix}, \tag{4.65}$$

are transformed to immanants.

Finally, using the rate expression (4.26), we find that

$$\begin{aligned} C(\boldsymbol{\tau}) = \frac{1}{96}&(\Delta_{\mathrm{e}} + \Delta_{(12)} + \Delta_{(123)} + \Delta_{(12,34)} + \Delta_{(1234)} + \Delta_{(124)} \\ &+ \Delta_{(1243)} + \Delta_{(13)} + \Delta_{(132)} + \Delta_{(13,24)} + \Delta_{(1324)} + \Delta_{(134)} \\ &+ \Delta_{(1342)} + \Delta_{(14)} + \Delta_{(142)} + \Delta_{(14,23)} + \Delta_{(1423)} + \Delta_{(143)} \\ &+ \Delta_{(1432)} + \Delta_{(23)} + \Delta_{(234)} + \Delta_{(24)} + \Delta_{(243)} + \Delta_{(34)})|\mathrm{imm}^{\square\square\square\square}T|^2 \\ &+ \frac{1}{32}(\Delta_{\mathrm{e}} + \Delta_{(12)} + \Delta_{(12,34)} - \Delta_{(13,24)} - \Delta_{(1324)} - \Delta_{(14,23)} \\ &- \Delta_{(1423)} + \Delta_{(34)})|\mathrm{imm}^{\square\square\square}T|^2 \\ &+ \frac{1}{96}(2\Delta_{\mathrm{e}} + 2\Delta_{(12)} + \Delta_{(123)} - 2\Delta_{(12,34)} - \Delta_{(1234)} + \Delta_{(124)} \\ &- \Delta_{(1243)} + \Delta_{(13)} + \Delta_{(132)} - \Delta_{(134)} - \Delta_{(1342)} + \Delta_{(14)} \\ &+ \Delta_{(142)} - \Delta_{(143)} - \Delta_{(1432)} + \Delta_{(23)} - \Delta_{(234)} + \Delta_{(24)} \\ &- \Delta_{(243)} - 2\Delta_{(34)})|\mathrm{imm}^{\square\square\square}T_{(13)}|^2 \\ &+ \frac{1}{96}(\Delta_{(123)} - \Delta_{(1234)} - \Delta_{(124)} + \Delta_{(1243)} + \Delta_{(13)} + \Delta_{(132)} \\ &- \Delta_{(134)} - \Delta_{(1342)} - \Delta_{(14)} - \Delta_{(142)} + \Delta_{(143)} + \Delta_{(1432)} \\ &+ \Delta_{(23)} - \Delta_{(234)} - \Delta_{(24)} + \Delta_{(243)})(\mathrm{imm}^{\square\square\square}T)(\mathrm{imm}^{\square\square\square}T_{(13)})^* \\ &+ \frac{1}{96}(\Delta_{(123)} + \Delta_{(1234)} - \Delta_{(124)} - \Delta_{(1243)} + \Delta_{(13)} + \Delta_{(132)} \end{aligned}$$

$$
\begin{aligned}
&+\Delta_{(134)}+\Delta_{(1342)}-\Delta_{(14)}-\Delta_{(142)}-\Delta_{(143)}-\Delta_{(1432)}\\
&+\Delta_{(23)}+\Delta_{(234)}-\Delta_{(24)}-\Delta_{(243)})(\mathrm{imm}^{\ydiagram{3,1}}T_{(13)})(\mathrm{imm}^{\ydiagram{3,1}}T)^*\\
&+\frac{1}{96}(2\Delta_{\mathrm{e}}+2\Delta_{(12)}-\Delta_{(123)}+2\Delta_{(12,34)}-\Delta_{(1234)}-\Delta_{(124)}\\
&-\Delta_{(1243)}-\Delta_{(13)}-\Delta_{(132)}+2\Delta_{(13,24)}+2\Delta_{(1324)}-\Delta_{(134)}\\
&-\Delta_{(1342)}-\Delta_{(14)}-\Delta_{(142)}+2\Delta_{(14,23)}+2\Delta_{(1423)}-\Delta_{(143)}\\
&-\Delta_{(1432)}-\Delta_{(23)}-\Delta_{(234)}-\Delta_{(24)}-\Delta_{(243)}+2\Delta_{(34)})|\mathrm{imm}^{\ydiagram{2,2}}T|^2. \qquad (4.66)
\end{aligned}
$$

For further analysis, we can re-express this rate in simplified form by introducing coefficients $\alpha^{\lambda}_{\sigma,\sigma'}(\boldsymbol{\tau})$, to obtain

$$
\begin{aligned}
C(\boldsymbol{\tau}) = {}& \alpha^{\ydiagram{4,1}}_{\mathrm{e,e}}(\boldsymbol{\tau})\,|\mathrm{imm}^{\ydiagram{4,1}}T|^2+\alpha^{\ydiagram{3,1,1}}_{\mathrm{e,e}}(\boldsymbol{\tau})\left|\mathrm{imm}^{\ydiagram{3,1}}T\right|^2+\alpha^{\ydiagram{3,1,1}}_{(13),(13)}(\boldsymbol{\tau})\left|\mathrm{imm}^{\ydiagram{3,1}}T_{(13)}\right|^2\\
&+\left[\alpha^{\ydiagram{3,1,1}}_{\mathrm{e},(13)}(\boldsymbol{\tau})\left(\mathrm{imm}^{\ydiagram{3,1}}T\right)^{\dagger}\mathrm{imm}^{\ydiagram{3,1}}T_{(13)}+\mathrm{cc}\right]+\alpha^{\ydiagram{2,2}}_{\mathrm{e,e}}(\boldsymbol{\tau})\left|\mathrm{imm}^{\ydiagram{2,2}}T_{(22)}\right|^2. \qquad (4.67)
\end{aligned}
$$

The coefficients $\alpha^{\lambda}_{\sigma,\sigma'}(\boldsymbol{\tau})$ in (4.67) have well defined behavior for different regimes of the distinguishability of the photons. We treat these cases one by one. If the photons are all indistinguishable i.e. $\forall i,j\ \tau_i=\tau_j$ then the coefficients take values such that the rate reduces to

$$
C(\boldsymbol{\tau}) = |\mathrm{imm}^{\ydiagram{4,1}}T|^2\,. \qquad (4.68)
$$

The rate depends only on the permanent of the scattering matrix because permuting indistinguishable photons cannot change the rate, and the permanent is the only immanant that does not change under any permutation of its rows.

If three photons are indistinguishable but the fourth is distinguishable from the three, then the rate depends on not only the permanent but also on the $\ydiagram{3,1}$ type immanants. In this regime, the $\alpha^{\ydiagram{2,2}}_{\mathrm{e,e}}(\boldsymbol{\tau})$ in (4.67) vanishes. The next case is when the photons are divided into two pairs such that the two photons in each pair are indistinguishable with respect to each other, but the two pairs are mutually distinguishable. In this case all immanants appear

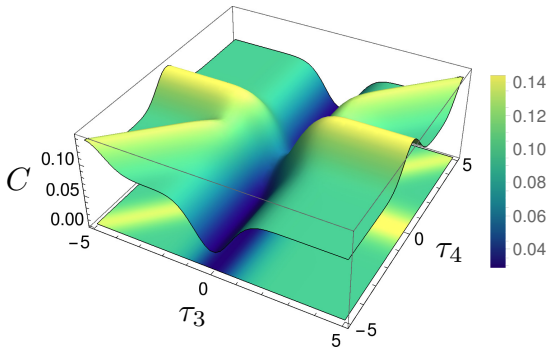


Figure 4.1: The coincidence rate $C(\tau)$ for input state $|211;1123;(0,0,\tau_3,\tau_4)\rangle$ and output $\boldsymbol{\mu} = 022$. The matrix chosen for this plot is provided in Eq. (4.69). The rate is shown both as a three-dimensional plot as well as a contour plot at the base of the figure.

in the rate and the rate has its most general form of Eq. (4.67).

It is possible to make the photons even more distinguishable. A pair of photons can be mutually indistinguishable, but the pair is distinguishable with the third photon which is further distinguishable with respect to the fourth photon. An example coincidence landscape associated with this last scenario is plotted in Fig. 4.1, using the interferometer matrix

$$U = \begin{pmatrix} 0.232231 + 0.437219\mathrm{i} & -0.271046 + 0.371938\mathrm{i} & 0.168757 + 0.717374\mathrm{i} \\ -0.430781 + 0.406851\mathrm{i} & -0.447972 - 0.0160114\mathrm{i} & 0.539331 - 0.396341\mathrm{i} \\ -0.170262 - 0.612224\mathrm{i} & -0.476765 + 0.599963\mathrm{i} & -0.0840731 - 0.043172\mathrm{i} \end{pmatrix}. \tag{4.69}$$

The point at the center of the landscape $\tau_3 = \tau_4 = 0$ only depends on the permanent. To calculate the coincidence rate along the line $\tau_3 = 0$, the line $\tau_4 = 0$ or the line $\tau_3 = \tau_4$ requires the additional computation of $\square\!\square$-type immanants. Any other point on the landscape requires computing all immanants appearing in Eq. (4.67), as in this case none of the coefficients are zero.

The final scenario is one where all four photons are distinguishable with respect to each other. Calculating the coincidence rate at a general point in this case requires the entirety of Eq. (4.67).

We have calculated the coincidence rate for the input state $|211;1123;\boldsymbol{\tau}\rangle$ and output event $\boldsymbol{\mu} = 022$ in terms of the three immanants of the scattering matrix. Using this coincidence expression we have shown that, for this input and output pair three regimes of distinguishability of the photons exist.

4.5 Rate transformation under permutation of photons

Now we turn to the problem of analyzing how the rate for a fixed output event changes under the permutation of the photons at the input. Fig. 2.1b shows an example where the photons at the interferometer input have been permuted with respect to the photons shown in Fig. 2.1a. The second and third photons have been swapped so the second photon is now in the second input and the third photon is in the first input. This input state is represented by $|211;1213\rangle$.

As discussed above, the action P_σ for $\sigma \in S_4$ captures permutations of the photons at the input of the interferometer. Though S_4 has 24 elements there are only twelve distinct ways of placing four photons in the input modes with mode occupations $\boldsymbol{\eta} = 211$. This is due to the multiplicity of photons in the first input mode. The coincidence rates for any of these 12 distinct permutations have the same form as (4.67), except the coefficients $\alpha^{\lambda}_{\sigma,\sigma'}$ are different in each case. We now describe how coefficients for one input permutation are related to the coefficients for some other input permutation.

Under the action P_σ, the vector $\boldsymbol{u}$ transforms to $\Gamma(\sigma)\boldsymbol{u}$, while the rate matrix remains unaffected as it does not depend on the input configuration. Some straightforward matrix algebra results in the rate $C_\sigma(\boldsymbol{\tau})$ for the permuted input in the form

$$C_\sigma(\boldsymbol{\tau}) = (V\boldsymbol{u})^\dagger \left[V\Gamma(\sigma)^\dagger R(\boldsymbol{\tau})\Gamma(\sigma)V^\dagger\right](V\boldsymbol{u}). \tag{4.70}$$

The interferometer vector is unmodified for any σ but the rate matrix is rotated by $V\Gamma(\sigma)^\dagger$. The expression (4.67) remains covariant. For any permutation of the input photons the rate

expression is obtained by mixing the coefficients $\alpha^{\lambda}_{\sigma,\sigma'}$ linearly into each other. Note that Eq. (4.70) is a completely general result.

4.6 Rate transformation under permutation of modes

The rate also remains covariant under a permutation of the modes. The example shown in Fig. 2.1c has its input modes permuted with respect to the input modes of the example in Fig. 2.1a. In total, there are three possible ways of permuting the modes, explicitly specified by the input mode-occupation strings 211, 121 and 112. The action Q_σ transforms between these various possible inputs.

The rate for each of these inputs has the form of (4.67) except for each input the scattering matrix T is different. The matrix T is a matrix formed by choosing the appropriate rows and columns of the interferometer matrix U. Therefore, it is straightforward to calculate the rate for any permutation of the modes once the form (4.67) is known. This result has a straightforward generalization for different input states.

4.7 Discussion

We have developed a theory of passive optical interferometry that relates the coincidence rates at the output of an interferometer with the permutational symmetries of the input photons. The permutational symmetry of the input photons can be controlled by varying their distinguishability, which in our case is done by tuning the time-of-arrival of the photons at the interferometer. Our results are obtained by exploiting the representation theory of the symmetric group.

The coincidence rates at the output of the interferometer are expressed in terms of the immanants of the scattering matrix, where the relative weights of the immanants depends on the distinguishability of the input photons. If any exchange symmetries of the input photons are forbidden because of the multiplicity of photons in input modes then immanants

with those exchange symmetries do not appear in the coincidence rate expressions. For inputs related by a permutation their rates are correspondingly related by a simple linear transformation.

Chapter 5

Characterization of passive interferometers

5.1 Introduction

In this chapter we present our procedure to characterize passive interferometers. Our goal is to construct a procedure that outputs a unitary matrix that best estimates the coincidence rate for any multi-mode multi-photon input state and any photon-counting output event. We also want to estimate the random errors on the characterized matrix.

This chapter is laid out as follows. In Sec. 5.2 we provide a bird's-eye view of the characterization procedure. Sec. 5.3 details the experimental data needed for the computations in the following sections. In Sec. 5.4, we describe how to use the collected data to estimate the amplitudes of the interferometer matrix. The arguments of the interferometer matrix are inferred by curve-fitting two-photon coincidence data to the expected rate as discussed in Sec. 5.5. The inferred matrix is then shifted to the nearest unitary matrix by using a maximum-likelihood technique provided in Sec. 5.6. In Sec. 5.7 we discuss how to estimate the errors in the characterization using a bootstrapping procedure. Sec. 5.8 outlines a way of parallelizing the data collection to speed it up. We conclude the chapter in Sec. 5.9.

5.2 Overview of the characterization procedure

In this subsection, we give a short overview of the characterization procedure that we explain in the next few subsections. The goal of the characterization procedure is to estimate a representative matrix, that can be used to predict any coincidence rate $C_{\boldsymbol{v},\boldsymbol{\xi}}(\boldsymbol{\tau})$ (2.19) for the interferometer.

As explained in Sec. 2.1, in our model, the interferometer matrix is parameterized by the sets of variables $\{\alpha_{ij}\}, \{\beta_i\}, \{\gamma_j\}, \{\theta_{ij}\}$. Our model also includes losses, parameterized by the sets $\{\kappa_i\}, \{\nu_j\}$. As we show below, using only photon inputs and photon counting at the outputs, only the parameters $\{\alpha_{ij}\}$ and $\{\theta_{ij}\}$ can be directly estimated. The output probabilities consist of the products of the interferometer parameters $\{\gamma_j\}, \{\theta_{ij}\}$ and the losses $\{\kappa_i\}, \{\nu_j\}$, so $\{\gamma_j\}, \{\theta_{ij}\}$ cannot be directly inferred without knowledge of the losses, which are generally unknown and can change between experiments.

Therefore, our procedure is as follows. We use the experimental data to estimate $\{\alpha_{ij}\}$ and $\{\theta_{ij}\}$. Then we choose the values of $\{\gamma_j\}, \{\theta_{ij}\}$ such that the interferometer matrix is unitary. Throughout this procedure, we assume that $\{\alpha_{ij}\}$ and $\{\theta_{ij}\}$ are random variables that are amenable to random errors from under-sampling and experimental imperfections. Therefore, we also discuss below how to calculate as well as minimize random errors in the estimation of these variables. In the following, we distinguish between the real value of the parameter with its estimate from experimental data. For the parameter $\bullet$, we represent its estimate by $\tilde{\bullet}$.

Finally, a reference code for our characterization procedure is available [118].

5.3 Experimental procedure and data collection

In this subsection, we outline the experimental procedure to be followed and the data that has to be collected and inputed into the characterization procedure outlined in the next few sections. Before doing so, we note that the accuracy and precision of the characterization

procedure will depend on the number of data points collected for each of the data sets. Therefore, to improve the effectiveness of the characterization, the experimentalist must collect as much data as possible, and at least must collect enough data such that the mean and standard deviation of the relevant distributions converge [119]. The procedure in the next few subsections include those that estimate the precision in the amplitude and arguments of the interferometer. These estimated errors may be used by an experimentalist to infer an empirical relationship between the amount of data collected and the precision of the characterization with their setup.

Now, we discuss the data to be collected. There are four set of sets of data to be collected, which are

1. single-photon detection counts from the interferometer,
2. the spectral function of the input photons,
3. singe-photon detection counts from a beam splitter
4. two-photon coincidence counts from a beam splitter, and
5. two-photon coincidence counts from the interferometer.

We discuss the procedure to collect each of these data sets now.

Single-photon detection counts from the interferometer are used to estimate the amplitudes $\{\alpha_{ij}\}$. Single-photons are created in input mode i and the number of photons detected in each output port j are recorded. This is repeated $B \in \mathbb{Z}^+$ times for each input mode where N_{b_i} single-photons are created in input mode i on iteration for $b_i \in \{1, \ldots, B\}$. This yields the set of numbers

$$\left\{N_{ijb_i} \in \mathbb{Z}^+, \quad i, j \in \{1, \ldots, m\}, b_i \in \{1, \ldots, B\}\right\}, \tag{5.1}$$

where N_{ijb_i} is the number of photons detected in output mode j on the b_i iteration, when

photons where created in input mode i. Note that knowledge of N_{b_i} is not required for our characterization procedure.

The other three data sets are used to estimate the arguments $\{\theta_{ij}\}$. The spectral functions of the photons are used to curve-fit the experimental two-photon coincidence counts to the theoretical curve. The spectral function are measured for a discrete set of frequencies $\Omega = \{\omega_1, \ldots, \omega_k\}$. The larger the range of frequencies for which the spectrum is measured and smaller the step size for the frequencies, the better the curve fitting will be, and consequently better the characterization of interferometer matrix.

Single-photon detection counts from the beam splitter are used to estimate the reflectivity of the beam splitter. Single photons are created in input mode 2 of the beam splitter and the number of photons detected in output mode 2 are recorded.

Two-photon coincidence counts on a beam splitter with known reflectivity is used to estimate the mode-matching parameter. Single-photons are created in each of the two input modes of the beam splitter, with a controllable delay between each pair, and the number of coincidence counts are recorded in the two output modes. In this way, for discrete set of delays, $T = \{\tau_1, \ldots, \tau_l\}$, coincidence counts $C^{\text{cal}}_{12,12}(\tau)$ are obtained, appropriately collected in the set

$$\left\{C^{\text{cal}}_{12,12}(\tau) : \tau \in T = \{\tau_1, \ldots, \tau_l\}\right\}. \tag{5.2}$$

Finally, two-photon coincidence data from the interferometer is used to estimate the arguments $\{\theta_{ij} \in (-\pi, \pi]\}$. Different subsets of two-photon coincidence data are used to estimate the absolute value and signs of the arguments. For the absolute values $\{|\theta_{ij}|\}$, single-photons are created in input modes 1 and $i \in \{2, \ldots, m\}$ and coincidence measurement are made for output modes 1 and $j \in \{2, \ldots, m\}$. The choice of the labelling of the input and output ports is arbitrary. This procedure results in $(m-1)^2$ discrete coincidence curves

$$\left\{C^{\text{exp}}_{1i,1j}(\tau) : \tau \in T = \{\tau_1, \ldots, \tau_l\}, \forall i, j \in \{2, \ldots, m\}\right\}. \tag{5.3}$$

The signs of the arguments are estimated using $(m-1)^2$ coincidence curves, described as follows.

- To estimate $\mathrm{sgn}\theta_{22}$, reuse the measurement of $C^{\mathrm{exp}}_{12,12}(\tau)$, which is part of data set (5.3).
- For the signs of the remaining arguments in the second row, $\{\mathrm{sng}\theta_{2j} : j \in \{3,\ldots,m\}\}$, record

$$\left\{C^{\mathrm{exp}}_{21,j2}(\tau) : j \in \{3,\ldots,m\}\right\}. \tag{5.4}$$

- For the signs of the remaining arguments in the second column, $\{\mathrm{sng}\theta_{i2} : i \in \{3,\ldots,m\}\}$, record

$$\left\{C^{\mathrm{exp}}_{i2,21}(\tau) : i \in \{3,\ldots,m\}\right\}. \tag{5.5}$$

- For the signs of the remaining arguments,

$$\{\mathrm{sng}\theta_{ij} : (i,j) \in \{3,\ldots,m\} \times \{3,\ldots,m\}\}, \tag{5.6}$$

  record

$$\left\{C^{\mathrm{exp}}_{i2,j2}(\tau) : (i,j) \in \{3,\ldots,m\} \times \{3,\ldots,m\}\right\}. \tag{5.7}$$

The algorithms to estimate the signs of arguments can suffer from numerical instabilities for certain values of the arguments. In this case, more data is required as described in Subsec. 5.5.5.

5.4 Single-photon transmission counts to estimate the amplitudes

In this subsection, we provide the procedure to estimate the amplitudes $\{\alpha_{ij}\}$. We have available the data of the single photon transmission counts, the theoretical expression for which is provided by Eq. (2.20). Suppose that in the the b_ith iteration, N_{b_i} photons are

created in input mode i, and N_{ijb_i} of them are detected in output mode j. Then the frequencies yields an estimate of the single photon transmission probabilities according to

$$\tilde{C}_{ij} = \text{mean}\left\{\frac{N_{ijb_i}}{N_{b_i}} : b_i \in \{1,\ldots,B\}\right\}. \tag{5.8}$$

Using Eq. (2.20), the following fraction simplifies as

$$\frac{C_{11}C_{ij}}{C_{i1}C_{1j}} = \frac{\kappa_1\beta_1\alpha_{11}^2\gamma_1\nu_1}{\kappa_i\beta_i\alpha_{i1}^2\gamma_1\nu_1}\frac{\kappa_i\beta_i\alpha_{ij}^2\gamma_j\nu_j}{\kappa_1\beta_1\alpha_{1j}^2\gamma_j\nu_j} = \frac{\alpha_{11}^2\alpha_{ij}^2}{\alpha_{i1}^2\alpha_{1j}^2}. \tag{5.9}$$

Now, according to our parametrization (2.12), $\alpha_{11} = \alpha_{i1} = \alpha_{1j} = 1$, hence,

$$\alpha_{ij} = \sqrt{\frac{C_{11}C_{ij}}{C_{i1}C_{1j}}}. \tag{5.10}$$

Therefore, an estimate of the amplitude α_{ij} is found by combing Eqs. (5.8) and (5.10), yielding

$$\tilde{\alpha}_{ij} = \text{mean}\left\{\sqrt{\frac{N_{11b_1}N_{ijb_i}}{N_{i1b_i}N_{1jb_1}}} : b_1, b_j \in \{1,\ldots,B\}\right\}. \tag{5.11}$$

Using this same data, an estimate of the standard deviation, also called the error bars, is found as

$$\tilde{\alpha}_{ij} = \text{std. dev.}\left\{\sqrt{\frac{N_{11b_1}N_{ijb_i}}{N_{i1b_i}N_{1jb_1}}} : b_1, b_j \in \{1,\ldots,B\}\right\}. \tag{5.12}$$

Note that these expressions for the estimate of α_{ij} and its error are independent of the number of photons created in the input modes, $\{N_{b_i}\}$. This means that the this method of estimating the amplitudes is resistant to fluctuations in the strength of the light source and the coupling efficiencies. The only requirement we place on $\{N_{b_i}\}$ and B is that they be large enough that any random errors due to experimental imperfections are minimized.

5.5 Two-photon interference curves to estimate the arguments

In this section, we describe our procedure to estimate the arguments of the representative matrix. This section is broken into several subsections. A required curve-fitting process is discussed in Subsec. 5.5.1. We avoid inaccuracies in the curve-fitting by estimating the spatial and polarization mismatch between the photon sources, a topic outlined in Subsec. 5.5.2. Subsecs. 5.5.3 and 5.5.4 discuss how to estimate respectively the absolute value and signs of the arguments of the interferometer matrix by curve-fitting the experimental data. Subsec. 5.5.5 discusses a method to avoid instabilities in the estimation of the signs of the arguments.

5.5.1 Curve-fitting procedure

Our characterization procedures requires a curve-fitting algorithm to determine the values of the mode-matching parameter ϵ and the arguments $\{\theta_{ij}\}$, where the curve-fitting algorithm determines the best-fit between the experimental and expected coincidence data. In this section, we describe the inputs and outputs of the curve-fitting algorithm, as well as present heuristics to calculate initial guesses of the fitted parameters.

The inputs to the curve-fitting algorithm are

- the experimental coincidence curve $\{(\tau, C^{\exp}(\tau)) : \tau \in T\}$,
- an objective function, which characterizes the error between the expected and experimental counts,
- the values of the known parameters,
- an initial guess for the unknown parameter.

A weighted least-squares curve-fitting procedure is appropriate for fitting coincidence data. The objective function for such a procedure is [120]

$$\sum_{\tau \in T} w(\tau) |C^{\text{exp}}(\tau) - C'(\tau)|^2, \tag{5.13}$$

where $C(\tau)$ is the expected coincidence rate explained below, and $w(\tau)$ is the weight function. We assume the probability-density functions (PDFs) of the residues are proportional to $\sqrt{C^{\text{exp}}}$ and assign the weights

$$w(\tau) = \begin{cases} 1/C^{\text{exp}}(\tau) & \text{if } C^{\text{exp}}(\tau) \neq 0, \\ 1 & \text{if } C^{\text{exp}}(\tau) = 0. \end{cases} \tag{5.14}$$

In case the PDFs of the residuals for different values of τ are not known, standard methods for non-parametric estimation of residual distribution can be employed to estimate the PDFs [121, 122].

Now, we turn to the problem of calculating the expected coincidence rate. There are three types of parameters that appear in Eq. (2.21): the amplitudes $\{\alpha_{ij}\}$, the angles $\{\theta_{ij}\}$, and the mode-matching parameter ϵ, where only the last two are estimated using curve-fitting. In any given call to the curve-fitting procedure, one of these parameters will be known while the other will be unknown. We will refer to this unknown parameter as the shape parameter as it determines the shape of the coincidence curve as illustrated in Fig. 2.2 for the mode-matching parameter and Fig. 5.1 for the arguments.

Two are other parameters are needed to fit the experimental data. First, the point of zero time-delay between the two photons is not exactly identifiable in the experimental data, making it necessary to introduce an abscissa shift parameter. Second, as the total number of photon pairs successfully created during the experiment (after losses) are not known exactly, the vertical scaling of the coincidence curve is not known. In Eq. (2.21), the overall multiplicative factor is this unknown vertical scaling that we call the ordinate

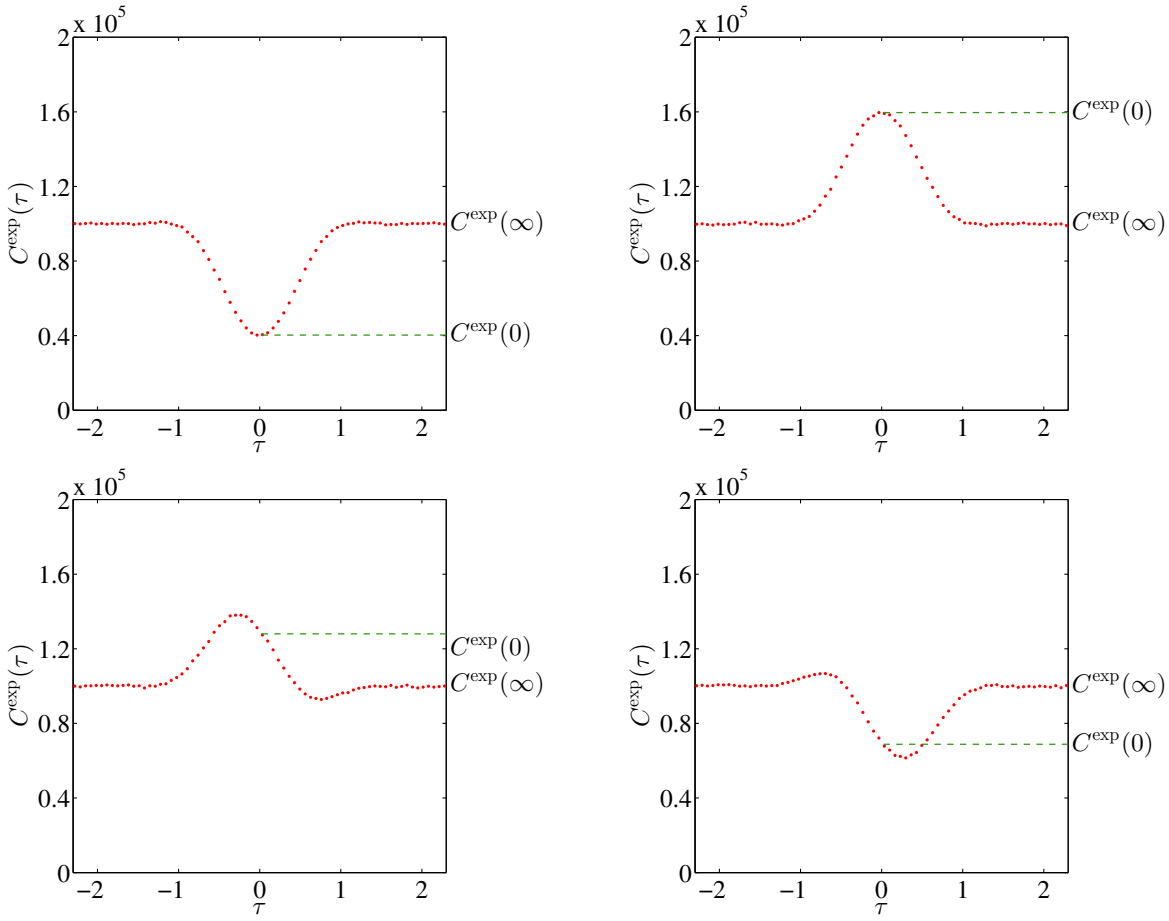


Figure 5.1: Simulated coincidence counts for output ports i, i' and input ports j, j' of interferometer with $\alpha_{ii} = \alpha_{i'j'} = \sqrt{3}/4$ and $\alpha_{ii'} = \alpha_{ij'} = 1/4$ and for different values of $\beta_{ii'jj'}$. The value of $\beta_{ii'jj'}$ in each respective figure is (a) π, (b) 0, (c) $\pi/3$ and (d) $2\pi/3$. The coincidence counts corresponding to $\tau = 0$ and $\tau \to \infty$ are marked on each plot by $C^{\text{exp}}(0)$ and $C^{\text{exp}}(\infty)$ respectively.

scaling parameter. The curve-fitting algorithm will return the best-fit values of the shape parameter, the abscissa shift, and the ordinate scaling.

We now discuss heuristics to make initial guesses of the abscissa shift and the ordinate scaling. Good guesses are required as the curve-fitting procedure optimizes the fitness function (5.13) over the domain of the fitting parameter values and the optimization is sensitive to the initial values of the parameters. The ordinate scaling guess is found using an estimate

of the coincidence rate at large time delay,

$$C^{\exp}(\infty) \coloneqq \frac{C^{\exp}(\tau_1) + C^{\exp}(\tau_l)}{2}. \tag{5.15}$$

Then a guess for the ordinate scaling is the ratio

$$\frac{C^{\exp}(\infty)}{C_{ii'jj'}(\infty)}, \tag{5.16}$$

where

$$C_{ii'jj'}(\infty) = \tilde{\alpha}_{ij}^2 \tilde{\alpha}_{i'j'}^2 + \tilde{\alpha}_{i'j}^2 \tilde{\alpha}_{ij'}^2, \tag{5.17}$$

from Eq. (2.21). A reasonable guess for the abscissa shift is the global minimum or the maximum of the experimental coincidence curve, where we can differentiate between rightside and upside curves (see Fig. 5.1) by choosing whichever of the minima or maxima is further from $C^{\exp}(\infty)$. Let this estimate be called $C^{\exp}(0)$.

The initial guesses for the shape parameters will be discussed at the appropriate points in the next few sections. We will require the experimental estimate of the visibility,

$$V^{\exp} = \left| \frac{C^{\exp}(\infty) - C^{\exp}(0)}{C^{\exp}(\infty)} \right|, \tag{5.18}$$

of the coincidence curve to make these guesses. The expected value of the visibility according to Eq. (2.21) is

$$V = \frac{2\epsilon \alpha_{ij}\alpha_{i'j'}\alpha_{ij'}\alpha_{i'j}}{(\alpha_{ij}^2\alpha_{i'j'}^2 + \alpha_{ij'}^2\alpha_{i'j}^2)} \cos(\theta_{ij} - \theta_{ij'} - \theta_{i'j} + \theta_{i'j'}). \tag{5.19}$$

5.5.2 Calibration to estimate mode-matching parameter

In this subsection, we discuss the procedure to calibrate the light sources for imperfect mode-matching. The mode-matching parameter ϵ is found using one- and two-photon coincidence data from an arbitrary beam splitter. First, a representative matrix for the beam splitter (a

two-mode interferometer) is found. Next, two-photon coincidence data is fit to the theoretical curve to estimate a value of ϵ.

The beam splitter matrix U_{BS} in the parametrization introduced in Eq. (2.12) is

$$U_{BS} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\beta_2} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & \alpha_{22}\mathrm{e}^{\mathrm{i}\theta_{22}} \end{pmatrix} \begin{pmatrix} \sqrt{\gamma_1} & 0 \\ 0 & \sqrt{\gamma_2} \end{pmatrix}. \tag{5.20}$$

The value of α_{22} can be found using the procedure provided in the last section. The argument $\theta_{22} \coloneqq \pi$ for a unitary beam splitter [107].

Now, the value of ϵ can be found by fitting the two-photon coincidence data to Eq. (2.21). In this equation, ignoring the ordinate scaling, and after plugging in the values of the various amplitudes, we are left with the equation

$$\begin{aligned} C_{12,12}(\tau) \propto (\tilde{\alpha}_{22}^2 + 1) \int \mathrm{d}\omega_1 \mathrm{d}\omega_2 |\phi_1(\omega_1)\phi_2(\omega_2)|^2 \\ - 2\epsilon\tilde{\alpha}_{22} \int \mathrm{d}\omega_1 \mathrm{d}\omega_2 \phi_1(\omega_1)\phi_2(\omega_2)\phi_1(\omega_2)\phi_2(\omega_1) \cos(\omega_2\tau - \omega_1\tau). \end{aligned} \tag{5.21}$$

The values of α_{22} and the spectral functions are already known, so the coincidence data (5.2), can be used to estimate the best-fit value of the remaining variable ϵ in this equation via curve-fitting. An initial guess for ϵ is found using the visibility (5.19),

$$\frac{\tilde{\alpha}_{22}^2 + 1}{2\tilde{\alpha}_{22}} V^{\mathrm{exp}}. \tag{5.22}$$

The estimated mode-matching parameter $\tilde{\epsilon}$ is used in the next section to further estimate the values of $\{\theta_{ij}\}$.

5.5.3 Estimation of the absolute value of the arguments

In this subsection, we describe the procedure to estimate the absolute value of the arguments $\{\theta_{ij}\}$ of the representative matrix U^{u}. This will be done using two-photon coincidence

data (5.3) from $(m-1)^2$ choices of the input and output ports.

The procedure to estimate the absolute values of the arguments is as follows. The data (5.3) is two-photon coincidence data using input ports 1 and i and output ports 1 and j for $i, j \in \{2, \ldots, m\}$. Using Eq. (2.21), and again ignoring ordinate scaling, we have the proportionality

$$C_{1i,1j}(\tau) \propto (\tilde{\alpha}_{ij}^2 + 1) \int \mathrm{d}\omega_1 \mathrm{d}\omega_2 |\phi_1(\omega_1)\phi_2(\omega_2)|^2 + 2\epsilon\tilde{\alpha}_{ij} \int \mathrm{d}\omega_1 \mathrm{d}\omega_2 \phi_1(\omega_1)\phi_2(\omega_2)\phi_1(\omega_2)\phi_2(\omega_1) \cos(\omega_2\tau - \omega_1\tau + \theta_{ij}). \tag{5.23}$$

In this equation, the only unknown is θ_{ij} as we already have the estimates for the other variables, $\tilde{\phi}_1(\omega), \tilde{\phi}_i(\omega), \tilde{\alpha}_{ij}, \tilde{\epsilon}$. This equation is generally not invariant under the transformation $\theta_{ij} \to -\theta_{ij}$. However, if the two spectral functions are identical or close to identical, as is likely for sources used in a lab, then Eq. (5.23) is indeed invariant. Therefore, under this assumption of near identicalness of the spectral function, a curve-fitting routine is used to estimate the absolute value $|\tilde{\theta_{ij}} \in [0, \pi]$, that best fits the data (5.3). This means that if the curve-fitting routine returns a negative sign for the fitted argument, this sign is discarded.

The initial guess for θ_{ij} is estimated using the visibility (5.19) as

$$\cos^{-1}\left(\frac{(\tilde{\alpha}_{ij}^2 + 1)}{2\tilde{\epsilon}\tilde{\alpha}_{ij}} V^{\exp}\right). \tag{5.24}$$

5.5.4 Estimation of the signs of the arguments

Now, we turn to the more involved task of estimating the signs of the arguments $\{\mathrm{sgn}\theta_{ij}\}$. This will be an iterative procedure requiring at least $(m-1)^2$ coincidence measurements. First, recall that in our parametrization, all phases are determined with respect to those of the first input and output ports, which are assumed to be phase free. This means that the arguments in the first row and column of U^{u} are without a sign. Therefore, we need to establish the sign of another argument, relative to which other signs can be determined.

Arbitrarily, we choose to first determine $\mathrm{sgn}\theta_{22}$. This sign can be determined from the shape of the coincidence curve $C_{12,12}(\tau)$, which only depends on θ_{22} as $\theta_{11} = \theta_{12} = \theta_{21} = 0$. However, this will work only if the spectral functions are not identical or near identical. If they are, then the shape of the coincidence curve $C_{12,12}(\tau)$ is invariant under the transformation $\theta_{22} \to -\theta_{22}$. In the case of near identical spectral function we can arbitrarily choose

$$\mathrm{sgn}\theta_{22} \coloneqq 1. \tag{5.25}$$

The other signs can be determined with respect to $\mathrm{sgn}\theta_{22}$ in the following way. we define the following three variables,

$$\Theta_{ii'jj'} \coloneqq |\theta_{i'j'} - \theta_{ij'} - \theta_{i'j} + \theta_{ij}| \in [0, \pi], \tag{5.26}$$

$$\Theta^{\pm}_{ii'jj'} \coloneqq |\theta_{i'j'} - \theta_{ij'} - \theta_{i'j} \pm |\theta_{ij}|| \in [0, \pi], \tag{5.27}$$

which respect the identity

$$\mathrm{sgn}\theta_{ij} = \mathrm{sgn}(|\Theta_{ii'jj'} - \Theta^{-}_{ii'jj'}| - |\Theta_{ii'jj'} - \Theta^{+}_{ii'jj'}|). \tag{5.28}$$

If the value of the $\Theta_{ii'jj'}, \theta_{i'j'}, \theta_{ij'}, \theta_{i'j}$ and $|\theta_{ij}|$ are known, then this identity can be used to find the sign of θ_{ij}. If θ_{ij} is positive, then $\Theta_{ii'jj'} = \Theta^{+}_{ii'jj'}$, and Eq. (5.28) returns a positive sign. Otherwise, $\Theta_{ii'jj'} = \Theta^{-}_{ii'jj'}$, and Eq. (5.28) returns a negative sign. Algorithmically, Eq. (5.28) can be implemented by determining if $\Theta_{ii'jj'}$ is closer to $\Theta^{+}_{ii'jj'}$ or $\Theta^{-}_{ii'jj'}$ and returning the corresponding angle.

Therefore, the strategy is to pick values of i', j' such that $\theta_{i'j'}, \theta_{ij'}, \theta_{i'j}$ are already known and $\Theta_{ii'jj'}$ is determined via experimental data. If a two-photon coincidence experiment is done with input modes i and i' and output modes j and j', then the expected coincidence

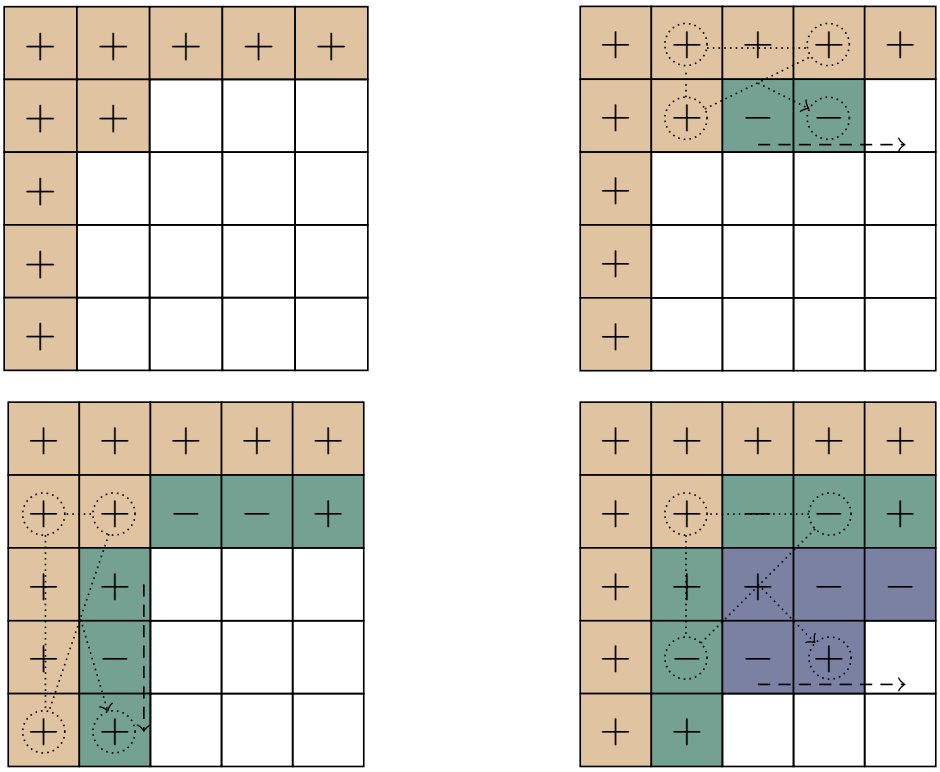


Figure 5.2: A depiction of the sign estimation procedure. (a) The first row and first column arguments $\{\theta_{i1}\}, \{\theta_{1j}\}$ are zero, so their signs are arbitrarily set as positive. θ_{22} is set as positive according to (5.25). (b) The sign of each second row argument θ_{i2} is set using the known values $|\theta_{22}|, |\theta_{i2}|$ and coincidence measurement for input ports $1, 2$ and output ports $2, i$. (c) The sign of each second column argument θ_{2j} is set using the known values $|\theta_{22}|, |\theta_{2j}|$ and coincidence measurement for input ports $2, j$ and output ports $1, 2$. (d) The signs of each remaining argument θ_{ij} is set using the known values $|\theta_{22}|, |\theta_{i2}|, |\theta_{2j}|$ and coincidence measurement for input ports $2, j$ and output ports $2, i$.

probability is

$$\begin{aligned} C_{ii'jj'}(\tau) \propto (\alpha_{ij}^2 \tilde{\alpha}_{i'j'}^2 + \tilde{\alpha}_{ij'}^2 \tilde{\alpha}_{i'j}^2) \int \mathrm{d}\omega_1 \mathrm{d}\omega_2 |\phi_1(\omega_1)\phi_2(\omega_2)|^2 \\ + 2\tilde{\epsilon}\tilde{\alpha}_{ij}\tilde{\alpha}_{i'j'}\tilde{\alpha}_{ij'}\tilde{\alpha}_{i'j} \int \mathrm{d}\omega_1 \mathrm{d}\omega_2 \phi_1(\omega_1)\phi_2(\omega_2)\phi_1(\omega_2)\phi_2(\omega_1) \\ \times \cos(\omega_2\tau - \omega_1\tau + \Theta_{ii'jj'}). \end{aligned} \tag{5.29}$$

from which $\Theta_{ii'jj'}$ can be estimated by curve-fitting.

One suitable sequence of determination of the signs, illustrated in Fig. 5.2 is follows.

- Use the first row of U^{u} as reference to determine the signs of the second row, i.e. set $i' = 1, j' = 2$ to determine $\mathrm{sgn}\theta_{2j}$ for $j \in \{3, \ldots, m\}$.

- Use the first column of U^{u} as reference to determine the signs of the second column, i.e. set $i' = 2, j' = 1$ to determine $\mathrm{sgn}\theta_{i2}$ for $i \in \{3, \ldots, m\}$.

- Use the second row and second column of U^{u} as reference to determine the signs of the remaining arguments, i.e. set $i' = 2, j' = 2$ to determine $\mathrm{sgn}\theta_{ij}$ for $(i, j) \in \{3, \ldots, m\} \times \{3, \ldots, m\}$.

The initial guess for $\Theta_{ii'jj'}$ is estimated using the visibility (5.19) as

$$\cos^{-1}\left(\frac{(\alpha_{ij}^2\alpha_{i'j'}^2 + \alpha_{ij'}^2\alpha_{i'j}^2)}{2\epsilon\alpha_{ij}\alpha_{i'j'}\alpha_{ij'}\alpha_{i'j}}V^{\mathrm{exp}}\right). \tag{5.30}$$

5.5.5 Removal of instabilities in characterization procedure

For certain interferometer matrices U^{u}, our characterization procedure can infer incorrect signs due to small errors in the two-photon coincidence data. Here we present a method of identifying when it is possible to make such an error and a strategy to circumvent this instability.

Recall that $\mathrm{sgn}\theta_{ij}$ is estimated using the values of $\Theta_{ii'jj'}, \theta_{i'j'}, \theta_{ij'}, \theta_{i'j}$ and $|\theta_{ij}|$. These variables are all determined experimentally and the estimated values may suffer from random or systematic errors. If the value of $\theta_{i'j'} - \theta_{ij'} - \theta_{i'j}$ is close to 0 or π, then Eqs. (5.26) and (5.27), and identity (5.28) are no longer reliable for determining the sign of θ_{ij}. This is because $\Theta_{ii'jj'}$ becomes very close to both $\Theta^{+}_{ii'jj'}$ and $\Theta^{-}_{ii'jj'}$ and the errors might be larger than both these differences. In this case, the sign returned by Eq. (5.28) is suspect. In other words, to identify a potential instability, $\theta_{i'j'} - \theta_{ij'} - \theta_{i'j}$ is calculated and it is determined if its distance from 0 or π is smaller than the error in the estimated angles.

If a instability in identified, the following modification of the procedure presented previously can be used to mitigate it. First, consider the potential for the instability in the

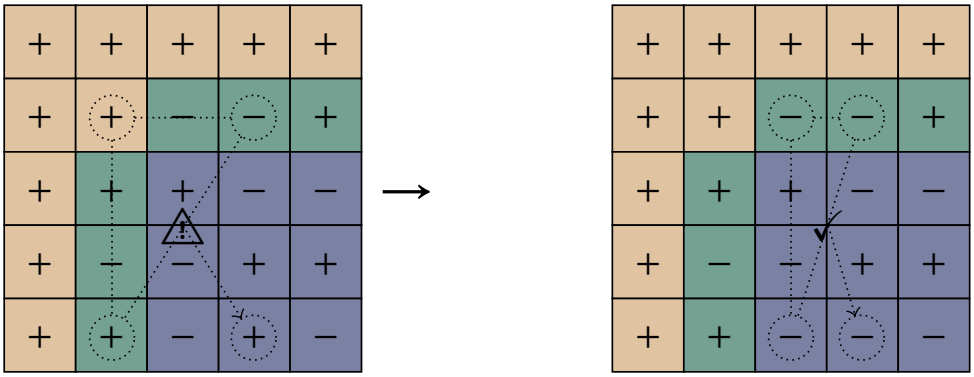


Figure 5.3: An illustration of the instability in the θ_{ij} characterization procedure for an interferometer with $m = 5$ modes. (a) If the value of $|\theta_{22} - \theta_{52} - \theta_{24}|$ is close to 0 or π, then small error in $C^{\text{exp}}_{2524}(\tau)$ can lead to an error in the estimation of $\text{sgn}(\theta_{54})$. (b) The instability in the θ_{54} can be removed by collecting two-photon coincidence data for input ports $2, 5$ and output ports $3, 4$ and using the values of $\theta_{23}, \theta_{53}, \theta_{24}$ instead of $\theta_{22}, \theta_{52}, \theta_{24}$ values.

second row and column. As these angles are determined with reference to only θ_{22} (the other reference angles in the first row and column being 0), we only need to ensure that θ_{22} is not close to 0 or π. If it is, then a simple solution is to relabel the input and output ports such that the new θ_{22} is not close to 0 or π. Ideally, this relabelling should be done before any of the data is collected for the estimating the signs. However, for reconfigurable interferometers whose parameters are controlled using thermocouples [34, 36], the targeted value of every parameter is known and the initial labelling can be chosen so that θ_{22} is far from 0 or π.

Next, consider any potential instability in the signs of the remaining arguments, estimated with reference to the second row and column. The sign $\text{sgn}\theta_{ij}$ is determined with reference to the arguments in the second row and column. If a potential instability is detected, a solution is to choose a different reference set of arguments from which to determine this sign. An example of this is presented in Fig. 5.3.

5.6 Maximum-likelihood estimation for finding unitary matrix

At this point, the matrix A from (2.12) has been estimated. The experimentally determined $\tilde{A}$ is different from the actual A because of systematic and random errors in the experimental procedure. we now present a procedure to estimate the matrices B and G by employing $\tilde{A}$.

The representative matrix U^{u} is unitary, so

$$U^{\mathrm{u}}U^{\mathrm{u}\dagger} = \mathbb{1}. \tag{5.31}$$

Substituting $U^{\mathrm{u}} = BAG$ from Eq. (2.12), we obtain

$$BAGG^*A^\dagger B^* = \mathbb{1} \tag{5.32}$$

$$\implies AGG^*A^\dagger = B^{-1}B^{*-1}. \tag{5.33}$$

We will only require the first column on both sides. On the left hand side, recall that G is diagonal and the first column entries of A are all 1, so the ith entry of the first column on the left hand side is

$$\sum_k A_{ik}G_{kk}^2, \tag{5.34}$$

which is just the matrix product

$$A\begin{pmatrix}\gamma_1\\ \gamma_2\\ \vdots\\ \gamma_m\end{pmatrix}. \tag{5.35}$$

On the right hand side, B is also diagonal, so the first column is just

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.36}$$

Putting this all together, we have the linear system,

$$A \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.37}$$

Following a similar methodology with

$$U^{\mathrm{u}\dagger} U^{\mathrm{u}} = \mathbb{1}, \tag{5.38}$$

We obtain the linear system

$$A \begin{pmatrix} 1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix} = \frac{1}{\gamma_1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.39}$$

Equations (5.37) and (5.39) are linear systems that can be solved for $\{\gamma_i\}$ and $\{\beta_i\}$, respectively, using standard methods [123]. This yields estimates $\tilde{B}$ and $\tilde{G}$. An estimate of the representative matrix can be calculated using

$$\tilde{U}^{\mathrm{u}} = \tilde{B}\tilde{A}\tilde{G}. \tag{5.40}$$

As the estimates $\tilde{B}, \tilde{A}$ and $\tilde{G}$ are marred by experimental errors in the determination of A, so is the estimate $\tilde{U}^{\mathrm{u}}$. This means that $\tilde{U}^{\mathrm{u}}$ is in general not equal to U^{u}, not unitary, and can be considered a random matrix drawn from the set of general linear matrices.

We now present a maximum-likelihood estimation method to calculate a unitary matrix that best fits the collected data. We assume that the error on $\tilde{U}^{\mathrm{u}}$ is a Gaussian random matrix, i.e., every entry $\tilde{U}^{\mathrm{u}}_{ij}$ is a complex independent and identically distributed Gaussian random variable centered at the true value U_{ij}. Then the unitary matrix closest to $\tilde{U}^{\mathrm{u}}$ with respect to the Frobenius-norm distance (2.16) is the best fit to the data, and is found using [124, 125],

$$\tilde{W} = \left(\tilde{U}^{\mathrm{u}}\tilde{U}^{\mathrm{u}\dagger}\right)^{-\frac{1}{2}}\tilde{U}^{\mathrm{u}}. \tag{5.41}$$

Thus, $\tilde{W}$ is the best estimate for the representative unitary matrix of the interferometer.

5.7 Bootstrapping to estimate errors

In this section, we present a procedure to estimate the error bars on the matrix entries $\left\{\tilde{W}_{ij}\right\}$ of the characterized representative matrix. The entries $\left\{\tilde{W}_{ij}\right\}$ are random variables because of random errors in the experiment. Estimating the errors accurately is important for using characterized interferometers for quantum computation and communication applications.

Current procedures calculate error bars under the assumption that the only error in the experiment is Poissonian shot noise [33, 25]. However, errors found this way are not accurate as there are other sources of errors in experiment, some of which are not understood. We employ a technique known as bootstrapping to estimate the error bars [126, 127, 128, 129, 130]. Bootstrapping does not require any assumptions on the type of errors present in the experiment, as it samples the errors from the measured data itself and uses them to estimate the error bars. In this way, bootstrapping yields more accurate estimates of the errors on the entries $\left\{\tilde{W}_{ij}\right\}$.

We now outline the bootstrapping procedure. The characterization of the interferometer

is repeated N_B times with simulated data. In the bth iteration, data is simulated as described below and the matrix $\tilde{W}^b$ is estimated as described in the last few sections. At the end of the N_B repetition, the set

$$\left\{\tilde{W}^b : b \in \{1, \ldots, N_B\}\right\} \tag{5.42}$$

is collected. From this set, the standard deviation (the error bars) of each of the entries in $\left\{\tilde{W}_{ij}\right\}$ can be determined. If N_B is large enough, the estimated standard deviation will converge to the true standard deviation of the entries [131, 132].

The procedure to simulate the one- and two-photon data for each iteration is as follows. Recall that for each pair of input and output modes, i and j, data (5.1),

$$\{N_{ijb_i} : b_i \in \{1, \ldots, B\}\}, \tag{5.43}$$

was collected. From this set, N_B samples are drawn with replacement to create the dataset for the bth bootstrapping iteration. Resampling two-photon coincidence data is more involved. Suppose that for experimental data $C^{\text{exp}}_{ii'jj'}(\tau)$ the curve fitting procedure yields the fitted curve $\tilde{C}_{ii'jj'}(\tau)$. Then the residuals from the fitting are

$$\left\{C^{\text{exp}}_{ii'jj'}(\tau) - \tilde{C}_{ii'jj'}(\tau) : \tau \in T\right\}. \tag{5.44}$$

We assume that the pdf of the residuals at different values of τ are functionally identical, but have width proportional to $\sqrt{\tilde{C}(\tau)}$. The residuals in the above set are first normalized using the assumed widths of the distributions. Next, $|T|$ entries are sampled with replacement from the set of normalized residuals. These are 'unnormalized' by multiplying with $\sqrt{\tilde{C}(\tau)}$, and then added onto $\tilde{C}_{ii'jj'}(\tau)$ for $\tau \in T$. This yields a new coincidence data that can act as the two-photon data for the bth iteration of the bootstrapping procedure.

This completes the characterization of the representative matrix of the interferometer and the errors on its entries.

5.8 Scattershot data collection

In this section, we present a scattershot-based data collection approach to reduce the experimental time [133, 134]. This approach reduces the data collection time from $\mathcal{O}(m^4)$ to $\mathcal{O}(m^2)$ with constant error in the entries of the interferometer matrix.

The obvious approach towards data collection involves successive coupling and decoupling of light sources from the input modes for each one- and two-photon measurement. Our procedure requires $\mathcal{O}(m^2)$ single-photon counting measurements and $\mathcal{O}(m^2)$ coincidence-counting measurements for an m-mode interferometer. However, the data to be collected for each measurement must increase as the size of the interferometer increases in order to keep the random errors constant. This is because as m increases, the amplitudes decrease as $\mathcal{O}(1/\sqrt{m})$ because of the unitarity of the interferometer matrix. This in turn causes the one- and two-photon transmission probabilities (Eqs. (2.20) and (2.21)) to drop as $1/m$ and $1/m^2$ respectively. Therefore, in order to offset this drop in the transmission probabilities the number of incident photons have be increased correspondingly by $\mathcal{O}(m)$ and $\mathcal{O}(m^2)$. Therefore, an overall $\mathcal{O}(m^4)$ scaling of the experimental time is required in the straightforward approach.

Now, we discuss a method to simultaneously collect data for different measurements which yields an improvement in the scaling of the experimental time. The scattershot method requires m heralded non-deterministic single-photon sources, each coupled to a different input mode. Detectors are present in each of the output modes. All sources and detectors are turned on simultaneously and controllable delays are introduced in first just the first input mode and next just in the second input mode. As the sources are non-deterministic and heralded, each source will only sometimes produce a photon (with some probability p), but whenever any does it is known due to the heralding detection. If only one source fires, then the count from that instance is included in the single-photon data (5.1). If the first source and any of the other source produce photons, a photon is detected in the first output mode, and a delay is in the first input mode, then that count is added to two-photon

data (5.3) used for estimating the absolute value of the arguments. Similarly, when the delay is added to the second input port, other appropriate combinations of two photons being produced and detected can be added to the datasets (5.4), (5.5), and (5.7), used for estimating the signs of the arguments.

The experimental time required for the straightforward approach outlined above is $\mathcal{O}(m^4)$. For the scattershot approach, $(m-1)^2$ different sets of two-photon data are collected simultaneously rather than sequentially. Therefore, the time required to collect the experimental data drops to $\mathcal{O}(m^2)$.

Now we discuss some potential problems with the scattershot approach. We assume that coupling losses are small and the probability p of photon emission is small enough that multi-photon events from the same source are not a concern. These assumptions are expected to be true for on-chip implementations of passive interferometers with integrated sources and detectors. Another complication that arises from using the scattershot approach is that each source has its own spectrum. Our equations fully account for the spectra of the sources and only requires that each source be characterized. Finally, the scattershot approach requires m sources and detectors each rather than two each. However, for reasons for ease of use, current implementations of on-chip passive interferometers already use separate sources and detectors for each mode.

5.9 Discussion

In summary, we have presented an accurate and precise procedure for characterizing a passive interferometer using only one and two-photon coincidence data. Our procedure is accurate in its estimation of the amplitudes because it uses the averaged value of the ratio of single-photon detections over many runs rather than the ratio of averaged values [73], minimizing the effects of the fluctuations in the number of the input photons. It is accurate in its estimation of the arguments because it corrects for spatio-temporal mode-mismatch between

the photon sources by calibrating this mismatch, and accounts for the spectrum of the input photons in the curve-fitting procedure. It is difficult to estimate the mode-matching in waveguide-based interferometers, therefore, this step might only be useful for free space implementations.

The procedure is precise because curve-fitting using measured spectra reduces the role of random errors in the characterization. Our procedure also reports the precision of the characterization using bootstrapping statistics. Bootstrapping computes accurate error bars for an unknown error model, and hence more useful than Monte Carlo based methods. The bootstrapping technique is suitable for applications in other quantum information tasks where random errors need to be estimated. Finally, the data collection for our procedure can occur in parallel, improving the experimental time quadratically in the size of the interferometer [73].

A number of other characterization procedures have been proposed since the publication of our work [2]. Poot et al. [76] characterize their wave-guide based interferometer using classical light, using transmitted intensities to infer the amplitudes and two-beam interference fringes to infer the arguments. They also provide a procedure to estimate the losses in their interferometer, which may complement our characterization procedure. Jacob et al. [77] are concerned with the problem that procedures [73, 74, 2] assume that the input and outputs of the interferometer are phase-free. They introduce an auxiliary mode and determine all interferometer phases, including the input and output mode phases, with respect to its phase. Our procedure may also be suitably modified to determine the arguments in a similar way. Tillmann et al. [78] determine all arguments and phases of the interferometer simultaneously, using a global optimization algorithm which constraints the interferometer matrix to be unitary. The data used for their procedure is identical to other procedures [73, 74] and they also suggest using one of these procedures to infer the initial values of the interferometer matrix entries. A novel characterization technique is one based on directly estimating the response of each thermo-optical phase-shifter inside the interferometer [36].

Chapter 6

Quantum summoning as an interactive protocol

6.1 Introduction

In this chapter, we formulate summoning as an interactive protocol between two parties, namely a prover and a verifier. The prover claims that she can summon quantum information in an agreed upon set of causal diamonds. The goal of the verifier is to test this claim.

In Sec. 6.2, we discuss the interactive protocol formalism for summoning. In Sec. 6.3, we present a qubit CSS code that can be used to summon quantum information in any valid configuration of causal diamonds. To show how this code can be used in practice, we also present a protocol, a variant of one previously presented [83], for the prover and her agents to follow. We specify the conditional logic that each agent has to follows in order to fulfill any summoning request. Finally, we also present encoding and decoding circuits for our code, and discuss how to implement them optically. In Sec. 6.4, we present a procedure the verifier can use to test the prover.

6.2 Summoning as an interactive protocol

An interactive protocol is a formal specification of a task in a way that allows for operational verification that the task has been performed [95, 96, 97, 98]. The verifier sends messages to the prover and the prover answers with his own messages. Based on the answers, the verifier decides if the prover is able to perform the task or not.

In the case of summoning, the verifier sends specifically prepared quantum states to the prover and requests these states at randomly chosen causal diamonds. The verifier performs measurements on the returned states to decide if the prover does have the claimed summoning ability. For this test, the verifier assumes the prover is all-powerful and can do anything allowed by the laws of physics. On the other hand, the verifier is technologically limited. The verifier's strategy must be such that he certifies with high probability any prover who does summon but denies with high probability any prover who fails to summon or uses dishonest means during the test.

We specify the requirements of a summoning task, and the powers of and the information available to the prover and verifier in Sec. 6.2.1. We discuss the limitations on what the prover and verifier can do in Sec. 6.2.2. We discuss soundness and completeness, the two central requirements of the verifier's strategy that ensure that the verifier successfully attains his goal in Sec. 6.2.3.

6.2.1 Operational summoning

An operational definition of summoning is key to its formulation as an interactive protocol. This definition contains the ingredients for the verifier to decide what states to send to the prover and what measurements to perform. In the following, first we describe how to specify a summoning task, and then provide our chosen definition of successful summoning.

A summoning task is specified by two pieces of information, mutually agreed upon by the prover and the verifier. First, they decide on a set of spacetime causal diamonds $\left\{\diamondsuit_k\right\}$

across which the quantum information is to be summoned, as well as the starting point s, in the past of all reveal points. Second, they mutually agree on an ensemble of states $\{p_i, |\psi_i\rangle\}$, deemed the quantum information that has to be summoned. Specifically, the prover claims that if the verifier provides her at point s any state $|\psi_i\rangle$ with probability p_i, she is able to summon it across the agreed upon set of causal diamonds.

Once a summoning task has been specified, we must decide what criteria must be fulfilled for the verifier to certify that the prover has summoned. We define that quantum information is successfully summoned subject to the following two desiderata. First, the quantum information must be undisturbed; i.e., if the prover is provided with the mixed state

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{6.1}$$

she returns this same state. Second, if the state provided to the prover is part of some larger entangled state, the summoning process must preserve this entanglement. The reason for the second condition is to ensure that summoning is non-trivial task for the prover even when the set $\{|\psi_i\rangle\}$ is orthogonal. In this case, the prover can simply measure-and-prepare the state sent to her, and broadcast copies to every causal diamond [135, 136, 137, 138, 139], a possibility we want to avoid.

The desiderata specified above can be tested by estimating the entanglement fidelity [99, 100],

$$F_{\mathrm{e}}(\rho, \mathcal{E}) \coloneqq \langle\psi| \left[(\mathcal{E} \otimes \mathcal{I})(|\psi\rangle\langle\psi|)\right] |\psi\rangle, \tag{6.2}$$

where $|\psi\rangle$ is any purification of ρ and $\mathcal{E}$ is a quantum channel [140] that captures the dynamics of the prover. Ideally, if the prover follows the protocol provided in Sec. 6.3 perfectly, the entanglement fidelity of their returned state will be maximum.

Non-ideally, the prover might have some errors in their encoding circuits or their transmission channels. To account for such errors, we define that quantum information $\{p_i, |\psi_i\rangle\}$

has been summoned across a set of diamonds $\left\{\diamond_k\right\}$ if and only if

$$\min_{\left\{\diamond_k\right\}} F_{\mathrm{e}}(\rho, \mathcal{E}_k) \geq t, \tag{6.3}$$

where $\mathcal{E}_k$ is the quantum channel from s to reveal point k, the minimum is taken over all causal diamonds, and $0 < t < 1$ is a threshold which allows for errors in the summoning process. In condition (6.3) we minimize over all diamonds rather than take the mean (or some other average value) over all diamonds. This is because the prover must be able to summon in every diamond to be able to pass the test.

Entanglement fidelity requires many measurements to estimate and it must be estimated for every causal diamond. Therefore, we assume that the verifier and prover communicate for many rounds before the verifier is able to make a decision. As the verifier is resource-limited a valid interactive protocol must terminate in expected number of rounds that is polynomial in the number of diamonds. In Sec. 6.4 we use this operational definition to propose a multi-round strategy to verify summoning.

6.2.2 Resources available to the verifier and the prover

The verifier and the prover have different limitations on their resources [140]. The resources can be classified as the size of their quantum and classical circuits, the capacity of their quantum and classical transmission channels, random number generation capabilities, and the number of agents they may deploy at different spacetime points. The resources are counted as a function of the number of diamonds, which define the size of an instance of the summoning task.

In an interactive protocol, the verifier is usually assumed to be technologically limited. We assume that the verifier's resources are a polynomial function of the number of diamonds. With bounded circuits, the verifier may only create states and do measurements up to some error. The verifier's computation are restricted to efficient classical computation. We assume

that he has access to random number generators that may be used to make random choices such as deciding which diamond to send a request to.

We make the restrictive assumption that the verifier knows nothing about resources of the prover, therefore he assumes the prover can perform any operations allowed by the laws of physics. He assumes the prover's circuits are error-free and their size intractable. He also assumes the prover is aware of the capabilities of the verifier and in fact is aware of the details of verification procedure that she will be subjected to. However, if the verifier tosses coins during the procedure, the prover may know the probability distribution of these coins but she does not have access to results of the tosses during the running of the verification procedure. The prover does not have access to the laboratory of the verifier and is unable to tamper with the communications between the agents of the verifier's party. In Sec. 6.3 we show that an honest prover has no need for such powers as summoning can be accomplished efficiently. Nevertheless, the verifier's strategy must be cognizant of any deceptive trickery by a cheating prover.

The two parties, the prover and the verifier have access to their own trusted agents that they can place at various points in spacetime prior to the start of the interactive protocol. These agents, already introduced in Sec. 3.1 and shown in Fig. 3.1, are able to execute quantum or classical instructions. They inherit the limitations, or lack thereof, of the verifier and prover stated above.

We name two of the verifier's agents, the dealer and the referee. The dealer prepares and sends states to the prover, while the referee measures the returned state and subsequently decides if the prover has summoned. These two agents are allowed to securely communicate with each other both quantumly and classically. This communication is important as the dealers needs to inform the referee what state was sent to the prover and which diamond the request was sent to.

6.2.3 Soundness and completeness

The limitations on the verifier's abilities along with the inherent uncertainity of measurements of quantum systems means that a prover incapable of summoning may be able to make the verifier believe that she has summoned when she has not. Therefore, the verifier must design a strategy such that he is able to certify a prover with summoning powers while rejecting one who fails to summon. These two opposing conditions are usually known as the soundness and completeness of an interactive protocol [95, 96, 97, 98].

A verifier's strategy is complete if a prover who does summon is able to convince the verifier of this fact except with some small probability. In the language of probability theory this condition is

$$\Pr(\text{verifier accepts} \mid \text{prover summons}) > 1 - \delta, \tag{6.4}$$

where $0 \leq \delta \leq 1$ allows the verifier to sometimes make the mistake of not certifying capable provers. A complete strategy is one which usually does not make Type I errors (false positives).

A verifier's strategy is sound if a cheating prover is unable to deceive the verifier except with some small probability. The soundness condition is expressed as

$$\Pr(\text{verifier rejects} \mid \text{prover does not summons}) > 1 - \delta, \tag{6.5}$$

where again δ means the verifier sometimes endorses incapable or cheating provers. A sound strategy is one which usually does not make Type II errors (false negatives).

A valid interactive protocol is one in which the verifier does not usually make an error in deciding if the prover has summoned. In Sec. 6.4 we will turn Eqs. (6.4) and (6.5) to concrete mathematical statements using the details of verifier's strategy. This will allow us to prove that our proposed verifier's strategy is indeed sound and complete. In the next section we discuss a strategy for the prover.

6.3 Efficient code for relativistic quantum summoning

In this section, we present our procedure for the prover to follow in order to summon quantum information efficiently. This section is laid out as follows. In Sec. 6.3.1, we present our summoning protocol. The protocol fully exploits the causal structure of the causal diamonds, transferring qubits from any causal diamond that did not receive a request to other diamonds that might have received it. Some information does not reach the causal diamond that receives the request due to limitations imposed by causality, and in the language of coding theory these qubits are considered to have undergone erasure errors. In this way of presentation, we naturally discover the erasure errors that occur for a request at each diamond. Therefore, we are able to discover the set of possible errors that the code must correct. Sec. 6.3.2 presents a code that does correct such errors. We formally define this code, and rigorously prove that this code corrects the erasure errors that occur during summoning. Sec. 6.3.3 shows how to implement this code by constructing the encoding and decoding circuits. It also discusses how to realize these circuits using passive interferometry. We conclude the chapter with a short discussion in Sec. 6.5.

6.3.1 Protocol

Here we propose a protocol to summon a logical qubit,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{6.6}$$

in any valid configuration of causal diamonds. We will specify the number of shares that the qubit is encoded in, the distribution of these shares in spacetime, and finally the recollection of some of these shares at the appropriate reveal point in order to satisfy the summoning request.

The protocol is slightly different if the total number of diamonds is even or odd, because our CSS code can only be used for summoning if the total number of diamonds is even.

Therefore, if given an odd set of diamonds, our protocol introduces a fictitious diamond to make the total number of diamonds even. To simplify our discussion of the protocol below, we introduce the variable $\tilde{N} \in 2\mathbb{Z}$, such that

$$\tilde{N} := \begin{cases} N & \text{if } N \in 2\mathbb{Z} \\ N+1 & \text{if } N \in 2\mathbb{Z}+1 \end{cases} \tag{6.7}$$

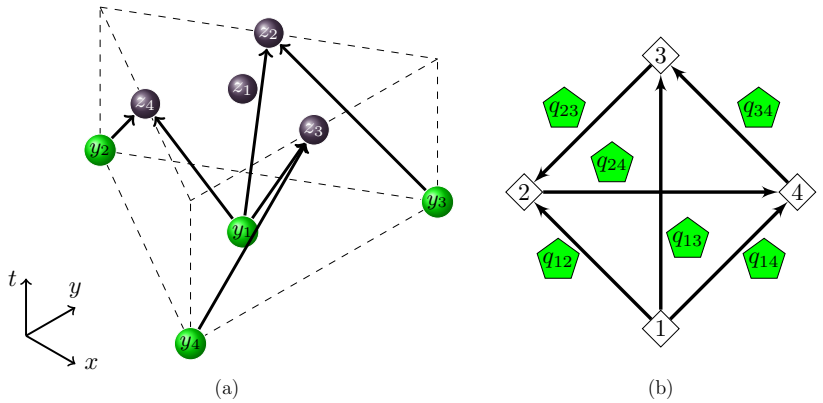
This variable is used to define the total number of encoded qubits used by the protocol. We use the graph, previously introduced to describe the causal relations between a set of causal diamonds, and assign one share to each edge of the graph $K_{\tilde{N}}$, i.e. for every edge e_{ij} in $K_{\tilde{N}}$, we introduce the encoded qubit q_{ij}. As it is a complete graph, $|\psi\rangle$ gets encoded into

$$Q = \binom{\tilde{N}}{2} \tag{6.8}$$

shares.

S distributes the encoded qubits using the edge relations in $K_{\tilde{N}}$, i.e. using the fact that e_{ij} is defined such that the causal diamond $\langle i \rangle$ is in the past of the causal diamond $\langle j \rangle$. For both even and odd cases, S sends q_{ij} to A_{y_i} for $i, j \in [\tilde{N}]$. Note that this means that a request agent may receive multiple encoded qubits. This distribution means that for every pair of diamonds, the encoded qubit is present in the earlier diamond. If the summoning request is received at the earlier diamond, the encoded qubit is already there. Otherwise, it is not needed in the earlier diamond and can be sent to the later diamond. Formally, if A_{y_i} receives a request, she sends q_{ij} to A_{z_i}. Otherwise, she sends the encoded qubit to A_{z_j}. Fig. 6.1, shows the initial distribution of shares for an example of four diamonds.

In the total number of diamonds are odd, then there are some additional qubits associated with fictitious diamond. Assuming this fictitious diamond is the future of all other diamonds, there are N qubits labelled as q_{iN+1} for $i \in [N]$. As the fictitious diamond will never receive a request, S can send q_{iN+1} to A_{z_i} for $i \in [N]$.



(a) (b)

Agent	Assigned qubits
A_{y_1}	q_{12}, q_{13}, q_{14}
A_{y_2}	q_{24}
A_{y_3}	q_{23}
A_{y_4}	q_{34}

(c)

Figure 6.1: (a) A configuration of four causal diamonds in $2+1$ dimensions. Three request points (y_2, y_3, y_4) are placed at the base vertices of a equilateral triangular prism and a fourth (y_4) is placed at the centroid of base vertices. The reveal points are placed at the midpoints of the top vertices (z_1, z_2, z_3) and the centroid of the top vertices. The volume of the diamond is not shown for visual clarity. The black arrows represent causal connections between points. (b) A complete graph representing the causal connections between the diamonds depicted in (a). For the CSS code the qubit q_{ij} is assigned to edge e_{ij}. (c) A table showing which requests agents is each physical qubit sent to.

If all agents follow the logic described above and $\langle r \rangle$ receives the summoning request, then A_{z_r} collects $\tilde{N}-1$ encoded qubits, described by the set

$$\left\{ q_{rk} : k \in [\tilde{N}] \backslash \{r\} \right\}. \tag{6.9}$$

We will prove in the next section how such a subset of encoded qubits can be used to decode $|\psi\rangle$.

6.3.2 Quantum error correction code

In this section, I present the CSS code that can be used in conjunction with the protocol presented in the previous section to summon a qubit. In order to formally define our code, I present the following theorem.

Theorem 3. *The stabilizer code, specified by a*

$$\left[\binom{\tilde{N}}{2}-1\right]\times 2\binom{\tilde{N}}{2}$$

stabilizer generator matrix

$$H_{\tilde{N}}=\left[\begin{array}{c|c} \boldsymbol{T}_{123} & \mathbf{0} \\ \boldsymbol{T}_{124} & \mathbf{0} \\ \vdots & \vdots \\ \boldsymbol{T}_{12\tilde{N}} & \mathbf{0} \\ \boldsymbol{T}_{134} & \mathbf{0} \\ \vdots & \vdots \\ \boldsymbol{T}_{1\,\tilde{N}-1\,\tilde{N}} & \mathbf{0} \\ \hline \mathbf{0} & \boldsymbol{A}_1+\boldsymbol{A}_2 \\ \mathbf{0} & \boldsymbol{A}_1+\boldsymbol{A}_3 \\ \vdots & \vdots \\ \mathbf{0} & \boldsymbol{A}_1+\boldsymbol{A}_{\tilde{N}-1} \end{array}\right], \tag{6.10}$$

where $\mathbf{0}$ *is an* $\binom{\tilde{N}}{2}$*-dimensional zero vector, is a*

$$\left[\left[\binom{\tilde{N}}{2},1,\frac{\tilde{N}}{2}\right]\right],\quad \tilde{N}=2\left\lceil\frac{N}{2}\right\rceil\in 2\mathbb{Z}, \tag{6.11}$$

CSS code, which can correct erasure errors at qubits q_{ij} *for* $i,j\in\{[N]\setminus\{r\}\}$ *for any* $r\in\left[\tilde{N}\right]$.

We will prove this theorem by breaking it down into three lemmas presented below. The first lemma proves that the code indeed encodes a single logical qubit into $\binom{\tilde{N}}{2}$ encoded qubits. The second lemma proves that the logical qubit can be decoded from some given $\tilde{N}-1$ sized subsets of the encoded qubits. Finally, even though we do not need to know it for summoning, for completeness we prove the distance of the code is indeed $\tilde{N}/2$.

The first lemma and its proof are presented now.

Lemma 4. *$H_{\tilde{N}}$ (6.10) is the stabilizer generator matrix of a CSS code that encodes one qubit into $\binom{\tilde{N}}{2}$ qubits.*

Proof. From Eqs. (3.26) and (3.27),

$$\boldsymbol{T}_{1jk} \cdot (\boldsymbol{A}_1 + \boldsymbol{A}_l) = 0, \quad \forall j,k,l : 2 \leq j < k \leq \tilde{N}, 2 \leq l \leq \tilde{N} - 1. \tag{6.12}$$

Using Eq. (3.7), we know that all the stabilizer generators in $H_{\tilde{N}}$ (6.10) commute with each other, thereby generating an Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_{\binom{\tilde{N}}{2}}$. There are $\binom{\tilde{N}}{2} - 1$ independent stabilizer generators, so this stabilizer code encodes one qubit into $\binom{\tilde{N}}{2}$ qubits. The first $\binom{\tilde{N}-1}{2}$ stabilizer generators contain only Z operators and identities and the other $\tilde{N} - 2$ stabilizer generators contain only X operators and identities. Thus, the stabilizer code is a CSS code.

In $H_{\tilde{N}}$, the vectors representing the Z-type stabilizers and the X-type stabilizers span $\mathcal{C}_1^{\perp}$ (3.27) and $\mathcal{C}_2$ (3.29) for $n = \tilde{N}$ respectively. Thus, the CSS code in Theorem 3 is specified by the linear codes $\mathcal{C}_1$ (3.26) and $\mathcal{C}_2$ (3.29) for $n = \tilde{N}$. □

Now we show that by assigning each of the $\binom{\tilde{N}}{2}$ physical qubits to an edge in $K_{\tilde{N}}$, this CSS code can correct the erasure errors at those qubits, which are not connected to vertex $\diamondsuit\!\!\!\!\!\!\diamondsuit r$, for any $r \in \left[\tilde{N}\right]$. Hence, by following the protocol of quantum summoning in Sec. 6.3.1, no matter which A_{y_r} receives the request, the associated reveal agent A_{z_r} can decode the original state $|\psi\rangle$ from her $\tilde{N} - 1$ qubits in Eq. (6.9).

Lemma 5. *For any $r \in \left[\tilde{N}\right]$, the CSS code in Theorem 3 can correct erasure errors at qubits q_{ij} for $i,j \in \left\{\left[\tilde{N}\right] \setminus \{r\}\right\}$.*

The proof of this lemma is a modified version of that for the continuous-variable code [83] with the infinite-dimensional field $\mathbb{R}$ replaced by the finite-dimensional field $\mathbb{Z}_2$. One side effect of this modification is that $\tilde{N}$ has to be even. Lemma 5 is no longer true if $\tilde{N}$ is

odd. To see this, we consider an example of a three-qubit code with stabilizer generators $\{ZZZ, IXX\}$. If $r = 3$, this code should correct any Pauli error at q_{12}. This is obviously false, because the Pauli error at q_{12}, ZII, commutes with both stabilizer generators but does not lie in the stabilizer group.

Proof. Denote $\mathcal{E}_r$ as the set of Pauli operators at qubits q_{ij} for $i, j \in \left[\tilde{N}\right] \setminus \{r\}$. For any Pauli operator $P \in \mathcal{E}_r$, its vector representation (3.5) is denoted

$$P = \begin{bmatrix} \boldsymbol{P}_Z & \boldsymbol{P}_X \end{bmatrix}. \tag{6.13}$$

As P acts nontrivially only at qubits q_{ij} for $i, j \in \left[\tilde{N}\right] \setminus \{r\}$,

$$\forall k \in \left[\tilde{N}\right] \setminus \{r\},\ \boldsymbol{P}_Z \cdot \boldsymbol{e}_{rk} = \boldsymbol{P}_X \cdot \boldsymbol{e}_{rk} = 0. \tag{6.14}$$

To show that the stabilizer code in Theorem 3 can correct any error in $\mathcal{E}_r$ for every r, it is sufficient to prove that [108]

$$\forall\, P \in \mathcal{E}_r,\ P \in C(\mathcal{S}) \Rightarrow P \in \mathcal{S}, \tag{6.15}$$

where $\mathcal{S}$ is the stabilizer group generated by the stabilizer generators in $H_{\tilde{N}}$ (6.10) and $C(\mathcal{S})$ is the centralizer of $\mathcal{S}$ in $\mathcal{G}_{\binom{\tilde{N}}{2}}$, i.e. the group of the Pauli operators commuting with all the elements of $\mathcal{S}$. Using Eq. (3.7), we know that $P \in C(\mathcal{S})$ if and only if

$$\forall\, \boldsymbol{v} \in \mathcal{C}_1^{\perp},\ \boldsymbol{P}_X \cdot \boldsymbol{v} = 0, \tag{6.16}$$

and

$$\forall\, \boldsymbol{u} \in \mathcal{C}_2,\ \boldsymbol{P}_Z \cdot \boldsymbol{u} = 0. \tag{6.17}$$

From $\boldsymbol{T}_{rij} \in \mathcal{C}_1^{\perp}$ and Eq. (6.16),

$$\boldsymbol{P}_X \cdot \boldsymbol{T}_{rij} = 0. \tag{6.18}$$

It implies that

$$\boldsymbol{P}_X \cdot (\boldsymbol{e}_{ri} + \boldsymbol{e}_{rj} + \boldsymbol{e}_{ij}) = 0. \tag{6.19}$$

Using Eq. (6.14), we know that

$$\boldsymbol{P}_X \cdot \boldsymbol{e}_{ij} = 0. \tag{6.20}$$

Equation (6.20), together with Eq. (6.14), implies that $\boldsymbol{P}_X = \boldsymbol{0}$.

Next we prove that Eq. (6.17) implies that $\boldsymbol{P}_Z \in \mathcal{C}_1^{\perp}$. Suppose

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_1 = 1. \tag{6.21}$$

Then Eq. (6.17) implies that for $2 \leq l \leq \tilde{N} - 1$,

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_l = 1. \tag{6.22}$$

As $\tilde{N}$ is even,

$$\sum_{m=1}^{\tilde{N}-1} \boldsymbol{P}_Z \cdot \boldsymbol{A}_m = 1. \tag{6.23}$$

As

$$\sum_{m=1}^{\tilde{N}} \boldsymbol{P}_Z \cdot \boldsymbol{A}_m = \boldsymbol{P}_Z \cdot \sum_{m=1}^{\tilde{N}} \boldsymbol{A}_m = 0, \tag{6.24}$$

we have

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_{\tilde{N}} = 1. \tag{6.25}$$

Hence,

$$\forall\, k \in \left[\tilde{N}\right],\ \boldsymbol{P}_Z \cdot \boldsymbol{A}_k = 1. \tag{6.26}$$

Equation (6.26) contradicts Eq. (6.14) because Eq. (6.14) implies that

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_r = 0. \tag{6.27}$$

Thus, (6.21) is false and

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_1 = 0. \tag{6.28}$$

Then Eq. (6.17) indicates that for $2 \leq l \leq \tilde{N} - 1$,

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_l = 0. \tag{6.29}$$

Hence

$$\sum_{m=1}^{\tilde{N}-1} \boldsymbol{P}_Z \cdot \boldsymbol{A}_m = 0. \tag{6.30}$$

From Eq. (6.24), we know that

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_{\tilde{N}} = 0. \tag{6.31}$$

Thus,

$$\forall\, k \in \left[\tilde{N}\right],\ \boldsymbol{P}_Z \cdot \boldsymbol{A}_k = 0, \tag{6.32}$$

which indicates that $\boldsymbol{P}_Z \in \mathcal{C}_1^{\perp}$. Since $\boldsymbol{P}_X = \boldsymbol{0}$, we know that P is a Z-type stabilizer in $\mathcal{S}$. □

Now we find the distance of the CSS code, which is an important parameter characterizing the capability of the code to detect and correct errors.

Lemma 6. *The distance of the CSS code in Theorem 3 is* $\tilde{N}/2$.

Lemma 6 implies that the CSS code can correct any $\left(\tilde{N}/2 - 1\right)$-qubit erasure errors. Although the distance of this CSS code scales as $O\left(\tilde{N}\right)$, Lemma 5 implies that the CSS code can correct particular erasure errors at $O\left(\tilde{N}^2\right)$ qubits.

Proof. The distance (3.9) of the stabilizer code in Theorem 3 equals to the minimum weight of the Pauli operators in $C(\mathcal{S}) \setminus \mathcal{S}$ [108]. To prove the minimum weight of the Pauli operators

in $C(\mathcal{S}) \setminus \mathcal{S}$ is $\tilde{N}/2$, we first show that there exists a Pauli operator

$$P \coloneqq \bigotimes_{i=1}^{\tilde{N}/2} Z_{q_{2i-1,\,2i}} \tag{6.33}$$

with weight $\tilde{N}/2$ such that $P \in C(\mathcal{S}) \setminus \mathcal{S}$. Then we show that no Pauli operator with weight less than $\tilde{N}/2$ lies in $C(\mathcal{S}) \setminus \mathcal{S}$.

From Eq (6.33), we know that

$$\boldsymbol{P}_Z = \sum_{i=1}^{\tilde{N}/2} \boldsymbol{e}_{2i-1,\,2i},\ \boldsymbol{P}_X = \boldsymbol{0}. \tag{6.34}$$

From Eq. (6.34), we find that

$$\forall\, l \in \left[\tilde{N}\right],\ \boldsymbol{P}_Z \cdot \boldsymbol{A}_l = 1. \tag{6.35}$$

Hence,

$$\forall\, \boldsymbol{v} \in \mathcal{C}_2,\ \boldsymbol{P}_Z \cdot \boldsymbol{v} = 0. \tag{6.36}$$

From the fact that $\boldsymbol{P}_X = \boldsymbol{0}$, we know that P (6.33) commutes with all the stabilizers in $\mathcal{S}$, i.e., $P \in C(\mathcal{S})$. As $\boldsymbol{P}_Z$ cannot be represented by an Euclidean cycle,

$$\boldsymbol{P}_Z \notin \mathcal{C}_1^{\perp}. \tag{6.37}$$

Thus, $E \notin \mathcal{S}$, and hence

$$P \in C(\mathcal{S}) \setminus \mathcal{S}. \tag{6.38}$$

For any Pauli operator P' with weight less than $\tilde{N}/2$, there exists an $r \in \left[\tilde{N}\right]$ such that

$$\forall k \in \left[\tilde{N}\right] \setminus \{r\},\ \boldsymbol{P}'_Z \cdot \boldsymbol{e}_{rk} = \boldsymbol{P}'_X \cdot \boldsymbol{e}_{rk} = 0. \tag{6.39}$$

From the proof of Lemma 5, we know that

$$P' \in C(\mathcal{S}) \Rightarrow P' \in \mathcal{S}. \tag{6.40}$$

It implies that

$$P' \notin C(\mathcal{S}) \setminus \mathcal{S}. \tag{6.41}$$

Thus, no Pauli operator with weight less than $\tilde{N}/2$ lies in $C(\mathcal{S}) \setminus \mathcal{S}$. □

This subsection has specified the CSS code (6.11) by its stabilizer generator matrix (6.10). We have shown the erasure errors that the CSS code, can correct and the distance of the CSS code. In next subsection, we explain how to encode and decode this CSS code.

6.3.3 Encoding and decoding

In last subsection, we have shown that the encoding of our CSS code employs $O(N^2)$ qubits while the decoding uses only $O(N)$ qubits. In this subsection, we present systematic methods to construct encoding and decoding circuits for our CSS code. The encoding method used here follows the standard method of encoding stabilizer codes [110], discussed in Sec. 3.2. Our decoding method differs from the stabilizer code decoding method because it only corrects erasure errors, which occur in summoning. We also calculate the gate complexity of both the encoding and the decoding circuits. It is shown that G in the encoding is $O(N^2)$ and G in the decoding is $O(N)$.

Encoding

To build the encoding circuit of this CSS code, we introduce logical operations on the encoded state. By using the vector representation (3.5), the logical operations are defined as

$$\bar{X} \coloneqq \begin{bmatrix} \mathbf{0} & \boldsymbol{A}_1 \end{bmatrix} \tag{6.42}$$

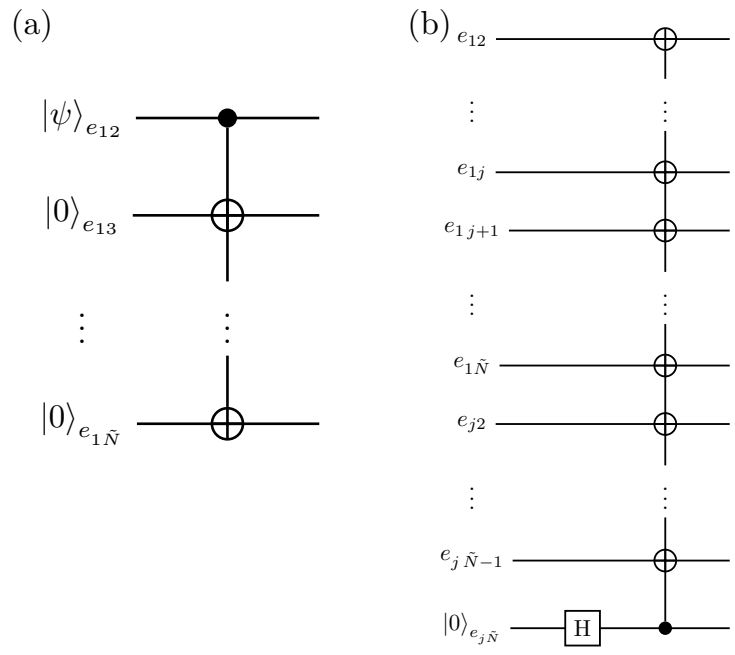


Figure 6.2: (a) Multiple CNOT gates with $|\psi\rangle_{e_{12}}$ as the control qubit and $\{|0\rangle_{e_{1i}}\}_{i=2}^{\tilde{N}}$ as the target qubits; (b) A Hadamard gate is applied at $|0\rangle_{e_{j\tilde{N}}}$ followed by multiple CNOT gates with $|0\rangle_{e_{j\tilde{N}}}$ as the control qubit and the qubits assigned to $\{e_{1l}\}_{l=[\tilde{N}],l\neq j} \cup \{e_{jk}\}_{k=2}^{\tilde{N}-1}$ as target qubits.

and

$$\bar{Z} \coloneqq \begin{bmatrix} \boldsymbol{A}_1 & \mathbf{0} \end{bmatrix}. \tag{6.43}$$

From $\boldsymbol{A}_1 \cdot \boldsymbol{A}_1 = 1$ and Eq. (3.7), $\bar{X}$ and $\bar{Z}$ anti-commute with each other.

We choose

$$|\psi_0\rangle = |\mathbf{0}\rangle \coloneqq |0\rangle^{\binom{\tilde{N}}{2}}, \tag{6.44}$$

which is an eigenstate of $\bar{Z}$ with eigenvalue one. To encode $|\psi\rangle$ (6.6), using Eqs. (3.13) and (3.14), and the fact that Z-type stabilizers act trivially on $|\psi_0\rangle$, we obtain the encoded state

$$\alpha|0\rangle_L + \beta|1\rangle_L = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \prod_{j=2}^{\tilde{N}-1} \left(I + \bigotimes_{i=1}^{\binom{\tilde{N}}{2}} X^{(\boldsymbol{A}_1+\boldsymbol{A}_j)_i} \right) \left(\alpha|\mathbf{0}\rangle + \beta|\boldsymbol{A}_1\rangle\right), \tag{6.45}$$

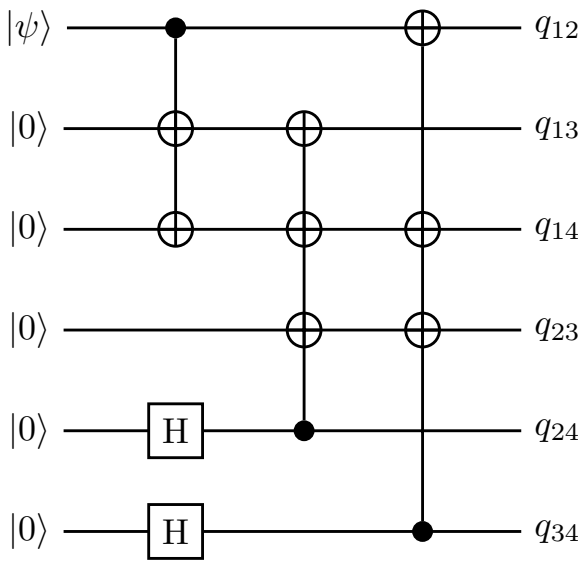


Figure 6.3: The encoding circuit of the CSS code comprising Hadamard gates and CNOT gates when $\tilde{N} = 4$. The inputs of this circuit are $|\psi\rangle \otimes |00000\rangle$ and the outputs of this circuit are the qubits assigned to each edge of the complete graph K_4 shown in Fig. 6.1(b).

where

$$|\boldsymbol{A}_1\rangle = \prod_{i=1}^{\binom{\tilde{N}}{2}} X^{(\boldsymbol{A}_1)_i} |\boldsymbol{0}\rangle, \tag{6.46}$$

and $(\boldsymbol{A}_1 + \boldsymbol{A}_j)_i$ and $(\boldsymbol{A}_1)_i$ are the i-th entries of vectors $\boldsymbol{A}_1 + \boldsymbol{A}_j$ and $\boldsymbol{A}_1$ respectively.

S applies CNOT gates as in Fig. 6.2(a) to the product state

$$|\psi\rangle \otimes |0\rangle^{\binom{\tilde{N}}{2}-1}, \tag{6.47}$$

to obtain

$$\alpha|\boldsymbol{0}\rangle + \beta|\boldsymbol{A}_1\rangle. \tag{6.48}$$

Then S implements each operation

$$I + \bigotimes_{i=1}^{m} X^{(\boldsymbol{A}_1 + \boldsymbol{A}_j)_i}, \tag{6.49}$$

where $1 \leq j \leq \tilde{N}-2$, by using CNOT gates and a Hadamard gate as in Fig. 6.2(b). Finally, S

obtains the encoded state (6.45). Figure 6.3 presents an example of the encoding circuit for $\tilde{N} = 4$.

The number of CNOT gates in Fig. 6.2(a) is $O(N)$. In Fig. 6.2(b), the number of CNOT gates is $O(N)$ and the number of Hadamard gate is one. As the circuit in Fig. 6.2(a) is only applied once and the circuit in Fig. 6.2(b) must be applied $O(N)$ times. The encoding of the CSS code consumes $O\left(N^2\right)$ CNOT gates and $O(N)$ Hadamard gates. Hence, for the encoding of the CSS code, $G \in O\left(N^2\right)$.

Decoding

In this subsection, I explain the decoding scheme. First, I give an overview of the scheme, following by a more detailed analysis. Suppose the request is sent to y_r. Reveal agent A_{z_r} cannot decode by measuring the syndromes as she has only $\tilde{N} - 1$ qubits. The encoded state (6.45) is an equally weighted superposition of the codewords given in Eqs. (6.51) and (6.52). After tracing out the lost qubits, the reduced state ρ_r (6.62) becomes a mixture of the codewords. To decode the original state $|\psi\rangle$ from the $\tilde{N}-1$ qubits with reduced density matrix ρ_r, reveal agent A_{z_r} measures the set of mutually commutative Hermitian operators

$$\left\{ Z_{q_{rk}} Z_{q_{r\,k+1}}; k \in \left[\tilde{N} - 1\right] \backslash \{r\} \right\}, \tag{6.50}$$

where $Z_{q_{rk}}$ represents the Z operator on the qubit q_{rk}. After applying the projective measurements, the reduced state is projected onto one codeword, becoming a pure state.

According to the measurement outcomes, by applying $\tilde{N} - 2$ CNOT gates with one control qubit and distinct target qubits, A_{z_r} obtains the original state $|\psi\rangle$ at the control qubit. Fig. 6.4 presents an example of the decoding circuit when the request is received at $\langle 4 \rangle$. In decoding, $G \in O(N)$ and the number of single-qubit measurements is also $O(N)$.

I will now calculate the reduced density matrix ρ_r and show the state after the measure-

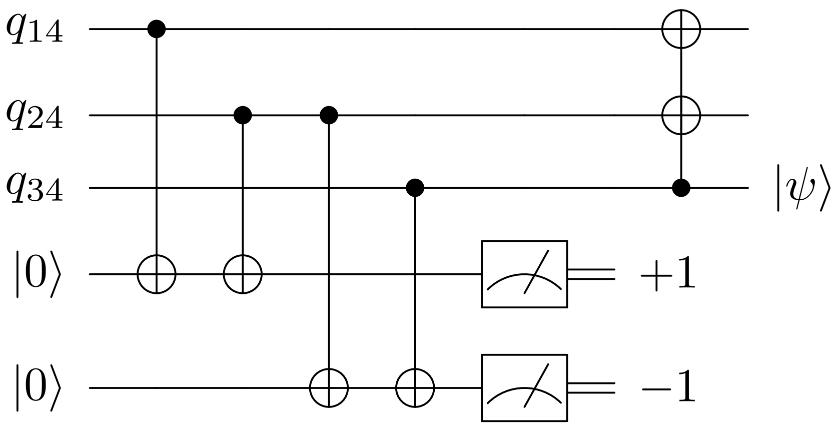


Figure 6.4: One example of the decoding circuit comprising CNOT gates and measurements of Z operators for $\tilde{N} = 4$. The inputs of the circuit are three physical qubits q_{14}, q_{24} and q_{34} and two ancillary qubits $|00\rangle$. The measurement outcomes on the two ancillary qubits are $+1$ and -1, based on which two CNOT gates are applied with the third qubit as the control qubit and the first two qubits as the target qubits. The third output qubit is the original qubit $|\psi\rangle$.

ments of the operators in Eq. (6.50). From Eqs. (3.13) and (3.14),

$$|0\rangle_L = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{x}\rangle, \tag{6.51}$$

$$|1\rangle_L = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{A}_1 + \boldsymbol{x}\rangle, \tag{6.52}$$

form a basis of the CSS code in Theorem 3. Hence, the density matrix of the $\binom{\tilde{N}}{2}$ physical qubits encoding $|\psi\rangle$ (6.6) is

$$\begin{aligned} \rho = & \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} \left(\alpha|\boldsymbol{x}\rangle + \beta|\boldsymbol{A}_1 + \boldsymbol{x}\rangle\right) \\ & \times \sum_{\boldsymbol{y} \in \mathcal{C}_2} \left(\alpha^*\langle\boldsymbol{y}| + \beta^*\langle\boldsymbol{A}_1 + \boldsymbol{y}||\right). \end{aligned} \tag{6.53}$$

To express the reduced density matrix, we give the following notations. The subset of edges connected to $\diamond r$ in $K_{\tilde{N}}$ is denoted by E_r and the complement of E_r in E, i.e. the subset of edges not connected to $\diamond r$, is denoted by E_r^c. In the same way as 2^{E_K} forms a

linear space

$$\mathscr{E} \cong \mathbb{Z}_2^{\binom{\tilde{N}}{2}},$$

the power set 2^{E_r} forms a linear subspace

$$\mathscr{E}_r \cong \mathbb{Z}_2^{\tilde{N}-1} \tag{6.54}$$

and the power set $2^{E_r^c}$ forms the orthogonal complement of $\mathscr{E}_r$ in $\mathscr{E}$, denoted by

$$\mathscr{E}_r^\perp \cong \mathbb{Z}_2^{\binom{\tilde{N}-1}{2}}. \tag{6.55}$$

For a vector $\boldsymbol{v} \in \mathscr{E}$, we use $\boldsymbol{v}_r$ to denote the projection of $\boldsymbol{v}$ onto $\mathscr{E}_r$, and $\boldsymbol{v}_r^\perp$ to denote the projection of $\boldsymbol{v}$ onto $\mathscr{E}_r^\perp$.

Now we calculate the reduced density matrix ρ_r of the $\tilde{N}-1$ qubits $\left\{q_{rk}; k \in \left[\tilde{N}\right] \setminus \{r\}\right\}$. As

$$\forall r \in \left[\tilde{N}\right],\ \sum_{\boldsymbol{x}\in\mathcal{C}_2} |\boldsymbol{A}_r + \boldsymbol{x}\rangle = \sum_{\boldsymbol{x}\in\mathcal{C}_2} |\boldsymbol{A}_1 + \boldsymbol{x}\rangle, \tag{6.56}$$

we have

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \operatorname{tr}_{E_r^c}\left[\sum_{\boldsymbol{x}\in\mathcal{C}_2}\left(\alpha|\boldsymbol{x}\rangle + \beta|\boldsymbol{A}_r + \boldsymbol{x}\rangle\right)\sum_{\boldsymbol{y}\in\mathcal{C}_2}\left(\alpha^*\langle\boldsymbol{y}| + \beta^*\langle\boldsymbol{A}_r + \boldsymbol{y}|\right)\right], \tag{6.57}$$

where $\operatorname{tr}_{E_r^c}$ denotes the partial trace over the qubits $\left\{q_{ij};\ i,j \in \left[\tilde{N}\right] \setminus \{r\}\right\}$. From the definition of partial trace [140],

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{v}\in\mathscr{E}_r^\perp} \left\langle \boldsymbol{v} \middle| \sum_{\boldsymbol{x}\in\mathcal{C}_2}\left(\alpha|\boldsymbol{x}\rangle + \beta|\boldsymbol{A}_r + \boldsymbol{x}\rangle\right)\sum_{\boldsymbol{y}\in\mathcal{C}_2}\left(\alpha^*\langle\boldsymbol{y}| + \beta^*\langle\boldsymbol{A}_r + \boldsymbol{y}|\right) \middle| \boldsymbol{v} \right\rangle. \tag{6.58}$$

For each $\boldsymbol{v} \in \mathscr{E}_r^\perp$, there is at most one $\boldsymbol{x} \in \mathcal{C}_2$ such that

$$\boldsymbol{x}_r^\perp = \boldsymbol{v}. \tag{6.59}$$

Hence, we get

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} \left\langle \boldsymbol{x}_r^{\perp} \right| \left(\alpha|\boldsymbol{x}\rangle + \beta|\boldsymbol{A}_r + \boldsymbol{x}\rangle\right) \left(\alpha^*\langle\boldsymbol{x}| + \beta^*\langle\boldsymbol{A}_r + \boldsymbol{x}|\right) \left|\boldsymbol{x}_r^{\perp}\right\rangle . \tag{6.60}$$

As

$$\langle \boldsymbol{x}_r^{\perp}|\boldsymbol{x}\rangle = |\boldsymbol{x}_r\rangle \text{ and } \langle \boldsymbol{x}_r^{\perp}|\boldsymbol{A}_r + \boldsymbol{x}\rangle = |\mathbf{1} + \boldsymbol{x}_r\rangle, \tag{6.61}$$

where $\mathbf{1}$ is an $(\tilde{N}-1)$-dimensional vector with all the entries equal to 1,

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} \left(\alpha|\boldsymbol{x}_r\rangle + \beta|\mathbf{1} + \boldsymbol{x}_r\rangle\right) \left(\alpha^*\langle\boldsymbol{x}_r| + \beta^*\langle\mathbf{1} + \boldsymbol{x}_r|\right) . \tag{6.62}$$

Consider the set of mutually commutative Hermitian operators in (6.50)

$$\left\{ Z_{q_{rk}} Z_{q_{r\,k+1}}; k \in \left[\tilde{N}-1\right] \backslash \{r\} \right\}.$$

$\forall \boldsymbol{x} \in \mathcal{C}_2$, $|\boldsymbol{x}_r\rangle$ and $|\mathbf{1} + \boldsymbol{x}_r\rangle$ are the eigenstates of each Hermitian operator in (6.50) with same eigenvalue, so any linear combination

$$\alpha|\boldsymbol{x}_r\rangle + \beta|\mathbf{1} + \boldsymbol{x}_r\rangle$$

is a common eigenstate of the Hermitian operators (6.50), with the eigenvalues forming a vector consisting of ± 1. For

$$\forall \boldsymbol{x}, \boldsymbol{z} \in \mathcal{C}_2 \text{ and } \boldsymbol{x} \neq \boldsymbol{z}, \tag{6.63}$$

the two eigenstates

$$\alpha|\boldsymbol{x}_r\rangle + \beta|\mathbf{1} + \boldsymbol{x}_r\rangle \tag{6.64}$$

and

$$\alpha|\boldsymbol{z}_r\rangle + \beta|\mathbf{1} + \boldsymbol{z}_r\rangle \tag{6.65}$$

have different eigenvalue vectors. This is because if (6.64) and (6.65) have the same eigen-

values, then either $\boldsymbol{x}_r = \boldsymbol{z}_r$ or $\boldsymbol{x}_r = \boldsymbol{z}_r + \mathbf{1}$, both of which contradict condition (6.63). Thus, ρ_r in Eq. (6.62) is an equally weighted mixture of the common eigenstates of the Hermitian operators (6.50) with different eigenvalue vectors.

After the projective measurements on all the Hermitian operators (6.50), the reduced state is projected onto

$$\alpha|\boldsymbol{y}_r\rangle + \beta|\mathbf{1} + \boldsymbol{y}_r\rangle, \tag{6.66}$$

where $\boldsymbol{y} \in \mathcal{C}_2$ and $\boldsymbol{y}_r$ is the projection of $\boldsymbol{y}$ onto $\mathscr{E}_r$. The corresponding measurement outcomes are $\left\{(-1)^{\boldsymbol{y}_r^{(i)}+\boldsymbol{y}_r^{(i+1)}}; i \in \left[\tilde{N}-2\right]\right\}$, where $\boldsymbol{y}_r^{(i)}$ is the i-th component in $\boldsymbol{y}_r$. (6.66) is the state after the measurements of the Hermitian operators in (6.50).

Optical Implementation

In this section, I discuss the optical implementation of the encoding and decoding circuits presented in the previous section. In the last section, we showed that the encoding and decoding circuits consist of CNOT gates, Hadamard gates and measurements in the Z basis. All these operations can be achieved using passive interferometry [20, 141, 142, 143] and have been demonstrated in large-scale integrated photonic circuits [34, 36].

Qubits are created by a superposition of a single-photon in one of two spatial modes. The presence of the photon in the first mode is considered a $|0\rangle$ and in the second mode as $|1\rangle$. This is commonly known as a dual-rail photonic qubit. Arbitrary single qubit operations can be performed on such a qubit using a beam splitter (2.6), with appropriate choice of the angles [20]. Measurements in any given basis may also be achieved by single-qubit gates [140].

A CNOT gate is more complicated as it cannot be implemented in a deterministic manner using passive interferometry. One method is to exploit the linear optical quantum computing formalism [20]. The controlled-sign gate presented by these authors can be transformed into a CNOT gate by appropriate single-qubit gate operations. The basic controlled-sign gate only succeeds with probability 1/16 but this can be efficiently amplified to arbitrarily high probability by using the teleportation trick. Another method is to combine the 1/9

probability non-deterministic CNOT gate [142, 143] with the 4/27 probability quantum non-demolition measurement setup [141] to create a heralded non-deterministic CNOT gate. The combined gate succeeds with probability 16/6561. This probability of success can be boosted by the teleportation trick [20].

In this way, the gates and measurements in the encoding and decoding circuits can be implemented efficiently with passive interferometry.

6.4 Sound and complete verification

In this section we propose a procedure a verifier can adopt to assess the claims of the prover. We show that our proposed procedure is sound and complete, as is required for a valid interactive protocol.

We propose a strategy based on the estimation of the entanglement fidelity which forms our definition of summoning (6.3). We provide a description of state preparation by the dealer and measurement by the referee that allows the verifier to estimate the entanglement fidelity for a single causal diamond. By repeating this process many times for each diamond, the verifier infers the minimum entanglement fidelity over all diamonds to some precision. Based on the threshold (6.3), the verifier decides if the prover can summon $\{p_i, |\psi_i\rangle\}$ in the causal diamonds $\{\langle k \rangle\}$.

The verifier can estimate the entanglement fidelity for diamond $\langle k \rangle$ in the following way. The dealer prepares the bipartite state $|\Psi\rangle^{PR}$ which is any purification of ρ. The system P is provided to the prover while the system R is provided to the referee. If the dealer sends the request to diamonds $\langle k \rangle$ then the state received by the referee is

$$(\mathcal{E}_k^P \otimes \mathcal{I}^R)(|\Psi\rangle^{PR}\langle\Psi|). \tag{6.67}$$

The referee makes a projective measurement on

$$\mathcal{P} = |\Psi\rangle^{PR}\langle\Psi|. \tag{6.68}$$

This measurement succeeds with probability

$$\mathrm{Tr}\left[(\mathcal{E}_k^P \otimes \mathcal{I}^R)(|\Psi\rangle^{PR}\langle\Psi|)|\Psi\rangle^{PR}\langle\Psi|\right] = F_{\mathrm{e}}\left(\rho, \mathcal{E}_k\right), \tag{6.69}$$

which is precisely the entanglement fidelity of the state returned at diamond $\langle k \rangle$.

The verifier uses the observed frequency of successful measurements to decide if the prover has summoned. Let n_k be the number of times a request is sent to diamond $\langle k \rangle$. Let m_k be the number of times the referee successfully projects on $\mathcal{P}$ for diamond $\langle k \rangle$. Then for diamond $\langle k \rangle$ the referee uses the decision function

$$D_t(m_k, n_k) = \begin{cases} \text{accept} & \text{if } m_k \geq n_k t \\ \\ \text{reject} & \text{if } m_k < n_k t \end{cases}. \tag{6.70}$$

We now want to prove that this decision function is sound and complete. In order to do so, we first convert (6.4)-(6.5) to mathematical statements. Then Theorem 7 stated below asserts the soundness and completeness of our proposed verification strategy.

Let the true value of $F_{\mathrm{e}}\left(\rho, \mathcal{E}_k\right) = f_k$. Successful summoning at diamond $\langle k \rangle$ is equivalent to $f_k > t$ and its failure equivalent to $f_k < t$. Each round of summoning, concluding with the projection on $\mathcal{P}$, results in the referee obtaining one bit of information about f_k. The referee's task is to estimate whether f_k is above or below the threshold t based on a sequence of n_k bits. In this picture, (6.4)-(6.5) can be stated as

$$\Pr(m \geq n_k t | f_k > t) > 1 - \delta \tag{6.71}$$

$$\Pr(m < n_k t | f_k < t) > 1 - \delta \tag{6.72}$$

We now want to prove that if the verifier and prover perform enough rounds of summoning these conditions hold. Stated formally this is equivalent to the following theorem.

Theorem 7. *For every* $0 < \delta < 1$ *there exists a* n_{0k} *such that for every* $n_k > n_{0k}$ *conditions* (6.71) *and* (6.72) *hold.*

Proof. The n_k bits obtained by the referee by projection on $\mathcal{P}$ can be treated as being drawn from a Binomial distribution with probability of success f_k. Conditions (6.71)-(6.72) claim bounds on the tails of this distribution and therefore can be proved using the Chernoff bound [144]. One form of the Chernoff bound asserts that for any $\zeta > 0$,

$$\Pr(m < (1-\zeta)n_k f_k) < \frac{\mathrm{e}^{-\zeta n_k f_k}}{(1-\zeta)^{(1-\zeta)n_k f_k}}.$$

Using this for n_k rounds, the completeness condition (6.71) simplifies as

$$\begin{aligned}\Pr(m \geq n_k t | f_k > t) &= 1 - \Pr(m < n_k t | f_k > t) \\ &< 1 - \frac{\mathrm{e}^{-(f_k - t)n_k}}{(t/f_k)^{n_k t}},\end{aligned}$$

where we have chosen $\zeta = (f_k - t)/f_k > 0$ because $f_k > t$. Comparing with inequality (6.71) we conclude that

$$n_k = \frac{\ln(1/\delta)}{f_k - t + t\ln(t/f_k)}. \tag{6.73}$$

Another form of the Chernoff bound states that for any $\zeta > 0$

$$\Pr(m \geq (1+\zeta)n_k f_k) < \frac{\mathrm{e}^{\zeta n_k f_k}}{(1+\zeta)^{(1+\zeta)n_k f_k}}.$$

This results in the soundness condition (6.72) simplifying to

$$\begin{aligned}\Pr(m < n_k t | f_k < t) &= 1 - \Pr(m \geq n_k t | f_k < t) \\ &< 1 - \frac{\mathrm{e}^{(t - f_k)n_k}}{(t/f_k)^{nt}},\end{aligned}$$

where we have chosen $\zeta = (t - f_k)/f_k > 0$ because $f_k < t$. Comparing this inequality with (6.72) we find

$$n_k = \frac{\ln(1/\delta)}{f_k - t + t\ln(t/f_k)}. \tag{6.74}$$

As Eqs. (6.73) and (6.74) are equivalent, we can conclude that

$$n_{0k} = \frac{\ln(1/\delta_c)}{f_k - t + t\ln(t/f_k)}. \tag{6.75}$$

□

Eq. 6.75 provides the number of rounds for one causal diamond after which the verifier is able to decide if the entanglement fidelity is above the threshold for that diamond. This must be repeated for all N diamonds. As requests must be sent uniformly randomly to each diamond it will take on average $\mathcal{O}\left(\sum_{k=1}^{N} n_{0k}\right)$ rounds for the verifier to be able to decide with high confidence if the prover exceeds the summoning threshold for every diamond.

In the discussion above we have assumed the verifier creates pure states and performs error free measurements which is contrary to the limitations placed on the verifier in Sec. 6.2. The dealer may only be able create mixtures of $|\Psi\rangle$ and $|\Psi^{\perp}\rangle$ and may only be able to project on a mixture of $\mathcal{P}$ and $\mathcal{P}^{\perp}$. We now argue that these limitations don't change the above arguments in any substantial way.

As quantum mechanics is linear we can assume that the dealer does indeed prepare the pure state $|\Psi\rangle$ and any limitations of the verifier's circuits appear in an imprecise measurement by the referee. Suppose the referee projects onto the operator $(1-\epsilon)\mathcal{P} + \epsilon P^{\perp}$ where $0 \leq \epsilon \leq 1$. The verifier can estimate the value of ϵ by characterizing his circuits separately from the prover. The dealer can prepare $|\Psi\rangle$ and the referee can make a measurement. If done many times an unbiased estimate of the ϵ may be found. If the referee modifies m_k to m_k/ϵ he will obtain an unbiased estimate of number of successful projection he would have received if the verifier's circuits were error free.

We have proposed a verifier's strategy and proved that this strategy is indeed sound and

complete. Therefore, a valid interactive protocol can be formulated for summoning using our proposed strategy.

6.5 Discussion

We have formulated quantum summoning as an interactive protocol in order to study if its possible to verify when some given quantum information has been summoned. We define quantum summoning in terms of the entanglement fidelity of the prover's process. We operationalize this definition into a procedure that the verifier can follow to test the prover's summoning ability. We show that this procedure, and consequently the summoning interactive protocol, is sound and complete.

We have also presented a protocol to summon quantum information efficiently in any valid configuration of causal diamonds. Central to our protocol is a CSS code that encodes one logical qubit into $O(N^2)$ physical qubits, where each physical qubit is assigned to an edge of a complete graph whose vertices correspond to causal diamonds. This code is a qubit version of the homological continuous-variable quantum error correcting code [83]. The CSS code is designed using the fact that the power set of edges of a complete graph can be cast as a vector space. The stabilizer generators of the CSS code correspond to triangle graphs and sums of star graphs.

The properties of these graphs are used to show that the logical qubit can be decoded from the subset of physical qubits that are assigned to edges adjacent to any vertex. In order to employ this code for summoning, the physical qubits are sent to the request points in such a way that the past of every reveal point contains enough physical qubits to decode the original qubit. Our protocol design, similar to one used previously [83], ensures that whenever a request agent receives the request the associated reveal agent receives all physical qubits required to decode the original qubit.

We also present procedures to design the encoding and decoding circuits for the CSS code.

Our protocol is less resource-intensive than the protocol based on the codeword-stabilized code [82] which uses circuits that are $O(N^2)$ wide and $O(N^3)$ deep [3]. The circuits for the CSS code have width that is also $O(N^2)$ but half that of the codeword-stabilized code and require only $O(N^2)$ gates.

Chapter 7

Conclusion and outlook

This thesis set out to advance the field of passive interferometry for quantum information processing applications. Before, evaluating our progress, I present a summary of our work and my contributions to it.

7.1 Summary of achievements and my contributions

7.1.1 Permutational symmetries for coincidence rates in multi-mode multi-photonic interferometry

We constructed a theory of multi-mode multi-photon passive interferometry to analyze the interference of distinguishable photons [1]. For any given non-entangled input photonic state we show that the coincidence rates at the output of a passive interferometers can be expressed in terms of immanants, which are functions with known symmetries. We show that it is possible to infer which immanants appear in the output rate from the symmetries of the input state. The symmetries of the input state are determined by the multiplicity of photons in the input modes and by the distinguishability of the input photons. We also show that coincidence rate expressions are covariant under a permutation of the input photons and modes. Our formalism provides a convenient way to simulate passive interferometry

experiments with distinguishable photons.

My contribution to Ref. [1] are as follows. I took the unproved proposition that the coincidence rate can be expressed as a matrix product for the case of one photon in each input and output mode [67, 51], generalized it to the case of arbitrary number of photons in each input and output mode, as expressed in Theorem 1. I fully contributed the proof of this theorem. I also took the unproven assumption of past work [67, 51] that the rate matrix carries a representation of the symmetric group, cast it as Theorem 2 and proved it. In order to do the calculations for examples such as those presented in Secs. 4.4, 4.5 and 4.6, I developed and used the MATHEMATICA® code [113]. My collaborators Hubert de Guise and Dylan Spivak provided the method to decompose the photonic Hilbert space and the representation of symmetric group using Young diagrams.

7.1.2 Characterization of passive interferometers

We develop a procedure to estimate the unitary matrix that determines the action of a passive interferometer on input states [2]. This procedure only takes in single and two-photon coincidence rates from the interferometer and outputs an accurate and precise estimate of the interferometer matrix. Our procedure is accurate and precise because it accounts for the distinguishability of the input photons in its calculations. We use the statistical technique known as bootstrapping to estimate the errors on the parameters of the interferometer matrix. Bootstrapping is an attractive technique because it outputs reliable error bars while remaining agnostic to type of random errors in the experiment. We also show that data required for our procedure can be collected in parallel, yielding a quadratic improvement in data collection time as the size of the interferometer increases.

My contributions to this project are related to the estimation of the arguments of the interferometer matrix. This includes developing some of the curve-fitting process, especially the guesses for each of the unknown parameters, while the objective function was designed by my collaborator Ish Dhand. I developed the expressions required to estimate the mode-

matching parameter. I studied the shape of the coincidence rate curve for the identical and non-identical spectral functions, which plays a significant role in the procedure to estimate the arguments of the interferometer matrix. Moreover, I identified the condition under which it is likely for an instability to occur in the estimation of the sign of an argument, and then along with my collaborater Ish Dhand worked on our procedure to avoid the instability. Finally, I developed a majority of the reference code for our characterization procedure [118].

7.1.3 Quantum summoning as an interactive protocol

We cast quantum summoning as an interactive protocol to assess if its possible to verify if a possibly dishonest prover can summon, and to develop a procedure that an honest prover can follow to summon quantum information. We develop a code to summon quantum information in any valid configuration of causal diamonds. Our code is a qubit CSS code that encodes one logical qubit into a quadratic number of encoded qubits where the problem size is defined to be the number of causal diamonds. We prove that our code corrects the erasure errors that occur in summoning due to restrictions of causality and present a protocol that uses the code to summon quantum information. We also use standard techniques to develop encoding and decoding circuits for our code. These circuits only use CNOT and Hadamard gates and therefore are suitable for implementation by passive interferometry. We also develop a verification procedure based on entanglement fidelity and prove that this procedure is sound and complete, and hence our interactive protocol is valid.

My contributions to this project include the formulation of summoning as an interactive protocol, as well as developing the operational definition of summoning in terms of entanglement fidelity. I also developed the verifier's procedure, including the proof that our procedure is sound and complete. I also contribute the discussion on how to realize our encoding and decoding circuits using passive interferometry.

7.2 Outlook

This thesis advances the analysis, simulation, characterization, and design of multi-mode multi-photon passive interferometry for quantum information processing. Our project on the symmetries of coincidence rates advance the qualitative and quantitative analysis and simulation of the interference of distinguishable photons. Our results demonstrate another area of physics which can be explained and analyzed using the symmetries of the system. Symmetry in the initial conditions of an experiment can be exploited to qualitatively predict the results. In the case of passive interferometric systems, the symmetry or lack thereof, occurs due to the partial distinguishability of the photons. The symmetries present in the input state are reflected in the coincidence rate because of the linear action of interferometer. The covariance of rates under a permutation of photons or modes at the input of the interferometer also highlight the role of symmetries in passive interferometry.

Our results are relevant for understanding the relevance of experimental implementations of BosonSampling to the computational speedup quantum systems can provide over classical systems [6]. The BosonSampling is classically hard because sampling from a distribution of permanants is computationally hard. On the other hand, when all photons are perfectly distinguishable, the coincidence rates are described by classical expressions and therefore easy to simulate. Our results show that the coincidence rates in modern photonic experiments are linear combination of immanants squared, and the computational complexity of sampling from such a distribution is still an open problem. Therefore, it is not clear which parts of the coincidence landscape are computationally easy to sample from and which parts are hard to sample from.

This thesis also presents two different verification procedures, the characterization of interferometers and the verification of summoning. The characterization of interferometers is important for verifying that passive interferometry experiments are performing to specification. Our main advancement for characterization interferometer is the use of superior modeling of the experimental setup to improve the accuracy and precision of the estimated

interferometer matrix. Our bootstrapping procedure to estimate errors without a definite error model is also a valuable advancement that can be used in other areas of passive interferometry or quantum information processing. Our verification procedure for summoning borrows the concept and techniques of the verification of classical computational problems in an adversarial setting and adapts them to the verification of quantum information processing tasks, a topic that has seen recent interest [97, 98]. Our work is a prerequisite to establishing quantum summoning as a quantum cryptographic primitive.

Our protocol and code for quantum summoning advance the design of passive interferometry for quantum information processing. Summoning can be used for secure transmission of quantum information on global quantum networks [21], and our optically implementable and efficient encoding and decoding circuits may be used for such a task. The impossibility of summoning in causally disconnected causal diamonds arises from the dual restrictions of quantum no-cloning and no-superluminal transmission. Our protocol and code may also be used to simultaneously test these two principles in a single optical experiment.

7.3 Future work

The results presented in this thesis can inspire further progress in exploiting passive interferometry for quantum information processing. We outline some of these possibilities now.

Our work on the symmetries of coincidence rates is limited to non-entangled state. Others have used similar techniques to analyze the interferometry of entangled states with restricted set of symmetries [145]. These results may be extended to arbitrary entangled states. Another aspects of our work that warrants further investigation are the coefficients of the immanants in the coincidence rate expressions. We have already shown that the elements of the rate matrix are constructed from cosets of natural photonic basis, but their structure in the symmetrized basis is not fully understood. Finally, the BosonSampling problem can be generalized to sampling from the coincidence rates of distinguishable photons.

Our characterization procedure separately estimates all $2m^2$ variables (m^2 amplitudes and m^2 arguments) specifying the interferometer matrix. However, modern implementations of interferometers [34, 36] use only m^2 total number of components to realize an arbitrary m-mode interferometer [23]. Therefore, a characterization procedure that exploits this decomposition, to either use lesser experimental data or improves accuracy and precision will be useful.

Our protocol for summoning is designed to work for any valid configuration of causal diamonds, where the underlying CSS code depends only on the number of causal diamonds. It is likely that codes can be designed that reduce resource usage by exploiting the structure of causal connections between the causal diamonds, examples being when a single causal curve connects multiple causal diamonds [83] or when the graph representing causal connections is acyclic [84].

While any given configuration of causal diamonds may be realized in man-made quantum networks, a useful avenue of research would be to classify the configurations that can occur naturally in flat or curved spacetimes. Our codes as well as other codes for quantum summoning assume that entangled states may be tranferred without decoherence in spacetime. Quantum summoning in curved spacetime or Rindler coordinates might require the usage of codes that protect against decoherence caused due to gravity or acceleration [146, 147, 148].

The work presented in this thesis is suitable for experimental implementation. The expression of coincidence rates has already experimental confirmation for systems of three photons [51], but experiments with large number of photons and multiple photons in some modes will provide a stronger certification of our results. The experimental verification of the characterization procedure is also attractive. In particular, the difference in accuracy and precision with classical light based procedures would be useful. Finally, an experimental implementation of our summoning protocol will simultaneously test the no-cloning theorem and no-faster-than-light information transfer restriction. Recent advances in the passive interferometry, such as the development of large-scale reconfigurable interferometers with

embedded light sources [34, 35, 36], put these experiments within reach.

Bibliography

[1] A. Khalid, D. Spivak, B. C. Sanders, and H. de Guise. Permutational symmetries for coincidence rates in multimode multiphotonic interferometry. *Phys. Rev. A*, 97:063802, 2018.

[2] I. Dhand, A. Khalid, H. Lu, and B. C. Sanders. Accurate and precise characterization of linear optical interferometers. *Journal of Optics*, 18(3):035204, 2016.

[3] Y.-D. Wu, A. Khalid, and B. C. Sanders. Efficient code for relativistic quantum summoning. *New Journal of Physics*, 20(6):063052, 2018.

[4] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124, 1994.

[5] A. W. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.*, 103:150502, 2009.

[6] S. Aaronson and A. Arkhipov. The Computational Complexity of Linear Optics. *Theory Comput.*, 9(4):143, 2013.

[7] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.

[8] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, Part 1:7, 2014.

[9] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien. Quantum computers. *Nature*, 464(7285):45, 2010.

[10] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, 2015.

[11] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682, 2015.

[12] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan. Experimental ten-photon entanglement. *arXiv:1605.08547*, 2016.

[13] M. H. Devoret and R. J. Schoelkopf. Superconducting Circuits for Quantum Information: An Outlook. *Science*, 339:1169, 2013.

[14] C. Monroe and J. Kim. Scaling the Ion Trap Quantum Processor. *Science*, 339:1164, 2013.

[15] T. Rudolph. Why i am optimistic about the silicon-photonic route to quantum computing. *APL Photonics*, 2(3):030901, 2017.

[16] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79:135, 2007.

[17] I. L. Chuang and Y. Yamamoto. Simple quantum computer. *Phys. Rev. A*, 52:3489, 1995.

[18] J. Clausen, L. Knöll, and D.-G. Welsch. Quantum state conversion by cross-kerr interaction. *Journal of Optics B: Quantum and Semiclassical Optics*, 4(2):155, 2002.

[19] J. C. Howell and J. A. Yeazell. Quantum computation through entangling single photons in multipath interferometers. *Phys. Rev. Lett.*, 85:198, 2000.

[20] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46, 2001.

[21] C. Simon. Towards a global quantum network. *Nature Photonics*, 11(11):678, 2017.

[22] S. Ritter, C. Nölleke, C. Hahn, A. Reiserer, A. Neuzner, M. Uphoff, M. Mücke, E. Figueroa, J. Bochmann, and G. Rempe. An elementary quantum network of single atoms in optical cavities. *Nature*, 484:195, 2012.

[23] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58, 1994.

[24] H. de Guise, O. Di Matteo, and L. L. Sánchez-Soto. Simple factorization of unitary transformations. *Phys. Rev. A*, 97:022328, 2018.

[25] N. C. Harris, D. Bunandar, M. Pant, G. R. Steinbrecher, J. Mower, M. Prabhu, T. Baehr-Jones, M. Hochberg, and D. Englund. Large-scale quantum photonic circuits in silicon. *Nanophotonics*, 5(3):456, 2016.

[26] J. W. Silverstone, D. Bonneau, J. L. O'Brien, and M. G. Thompson. Silicon quantum photonics. *IEEE Journal of Selected Topics in Quantum Electronics*, 22(6):390, 2016.

[27] S.-H. Tan and P. P. Rohde. The resurgence of the linear optics quantum interferometer — recent advances & applications. *ArXiv e-prints*, 2018.

[28] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien. Silica-on-silicon waveguide quantum circuits. *Science*, 320(5876):646, 2008.

[29] J. C. F. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien. Manipulation of multiphoton entanglement in waveguide quantum circuits. *Nature Photonics*, 3:346, 2009.

[30] A. Crespi, R. Ramponi, R. Osellame, L. Sansoni, I. Bongioanni, F. Sciarrino, G. Vallone, and P. Mataloni. Integrated photonic quantum gates for polarization qubits. *Nature Communications*, 2:566, 2011.

[31] 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. Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit. *Nature Photonics*, 6:45, 2011.

[32] B. J. Metcalf, N. Thomas-Peter, J. B. Spring, D. Kundys, M. A. Broome, P. C. Humphreys, X.-M. Jin, M. Barbieri, W. Steven Kolthammer, J. C. Gates, B. J. Smith, N. K. Langford, P. G. R. Smith, and I. A. Walmsley. Multiphoton quantum interference in a multiport integrated photonic device. *Nature Communications*, 4:1356, 2013.

[33] J. Mower, N. C. Harris, G. R. Steinbrecher, Y. Lahini, and D. Englund. High-fidelity quantum state evolution in imperfect photonic integrated circuits. *Phys. Rev. A*, 92:032322, 2015.

[34] 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(6249):711, 2015.

[35] N. C. Harris, G. R. Steinbrecher, M. Prabhu, Y. Lahini, J. Mower, D. Bunandar, C. Chen, F. N. C. Wong, T. Baehr-Jones, M. Hochberg, S. Lloyd, and D. Englund.

Quantum transport simulations in a programmable nanophotonic processor. *Nature Photonics*, 11:447, 2017.

[36] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson. Multidimensional quantum entanglement with large-scale integrated optics. *Science*, 360(6386):285, 2018.

[37] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto. Indistinguishable photons from a single-photon device. *Nature*, 419:594, 2002.

[38] A. B. U'Ren, C. Silberhorn, K. Banaszek, and I. A. Walmsley. Efficient conditional preparation of high-fidelity single photon states for fiber-optic quantum networks. *Phys. Rev. Lett.*, 93:093601, 2004.

[39] A. Faraon, I. Fushman, D. Englund, N. Stoltz, P. Petroff, and J. Vučković. Dipole induced transparency in waveguide coupled photonic crystal cavities. *Opt. Express*, 16(16):12154, 2008.

[40] A. Sipahigil, M. L. Goldman, E. Togan, Y. Chu, M. Markham, D. J. Twitchen, A. S. Zibrov, A. Kubanek, and M. D. Lukin. Quantum interference of single photons from remote nitrogen-vacancy centers in diamond. *Phys. Rev. Lett.*, 108:143601, 2012.

[41] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski. Picosecond superconducting single-photon optical detector. *Applied Physics Letters*, 79(6):705, 2001.

[42] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A*, 71:061803, 2005.

[43] E. J. Gansen, M. A. Rowe, M. B. Greene, D. Rosenberg, T. E. Harvey, M. Y. Su, R. H. Hadfield, S. W. Nam, and R. P. Mirin. Photon-number-discriminating detection using a quantum-dot, optically gated, field-effect transistor. *Nature Photonics*, 1:585, 2007.

[44] A. E. Lita, A. J. Miller, and S. W. Nam. Counting near-infrared single-photons with 95% efficiency. *Opt. Express*, 16(5):3032, 2008.

[45] 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. On-chip detection of non-classical light by scalable integration of single-photon detectors. *Nature Communications*, 6:5873, 2015.

[46] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X. 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. Boson sampling on a photonic chip. *Science*, 339(6121):798, 2013.

[47] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White. Photonic boson sampling in a tunable circuit. *Science*, 339(6121):794, 2013.

[48] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther. Experimental boson sampling. *Nat. Photon.*, 7:540, 2013.

[49] N. Spagnolo, C. Vitelli, M. Bentivegna, D. J. Brod, A. Crespi, F. Flamini, S. Giacomini, G. Milani, R. Ramponi, P. Mataloni, R. Osellame, E. F. Galvão, and F. Sciarrino. Experimental validation of photonic boson sampling. *Nat. Photon.*, 8:615, 2014.

[50] 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. Osellame, and F. Sciarrino. Experimental scattershot boson sampling. *Sci. Adv.*, 1(3), 2015.

[51] M. Tillmann, S. Tan, S. E. Stoeckl, B. C. Sanders, H. de Guise, R. Heilmann, S. Nolte, A. Szameit, and P. Walther. Generalized multiphoton quantum interference. *Phys. Rev. X*, 5:041015, 2015.

[52] R. Valivarthi, M. l. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel. Quantum teleportation across a metropolitan fibre network. *Nature Photonics*, 10:676, 2016.

[53] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33, 2011.

[54] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481, 2007.

[55] H. Fearn and R. Loudon. Quantum theory of the lossless beam splitter. *Opt. Commun.*, 64(6):485 , 1987.

[56] H. Fearn and R. Loudon. Theory of two-photon interference. *J. Opt. Soc. Am. B*, 6(5):917, 1989.

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

[58] V. Tamma and S. Laibacher. Multiboson correlation interferometry with arbitrary single-photon pure states. *Phys. Rev. Lett.*, 114:243601, 2015.

[59] V. S. Shchesnovich. Partial indistinguishability theory for multiphoton experiments in multiport devices. *Phys. Rev. A*, 91:013844, 2015.

[60] M. C. Tichy. Sampling of partially distinguishable bosons and the relation to the multidimensional permanent. *Phys. Rev. A*, 91:022316, 2015.

[61] V. Shchesnovich. Partial distinguishability and photon counting probabilities in linear multiport devices. *ArXiv e-prints*, 2017.

[62] V. S. Shchesnovich. Sufficient condition for the mode mismatch of single photons for scalability of the boson-sampling computer. *Phys. Rev. A*, 89:022333, 2014.

[63] V. S. Shchesnovich. Tight bound on the trace distance between a realistic device with partially indistinguishable bosons and the ideal bosonsampling. *Phys. Rev. A*, 91:063842, 2015.

[64] A. J. Menssen, A. E. Jones, B. J. Metcalf, M. C. Tichy, S. Barz, W. S. Kolthammer, and I. A. Walmsley. Distinguishability and many-particle interference. *Phys. Rev. Lett.*, 118:153603, 2017.

[65] I. Dhand and S. K. Goyal. Realization of arbitrary discrete unitary transformations using spatial and internal modes of light. *Phys. Rev. A*, 92:043813, 2015.

[66] S.-H. Tan, Y. Y. Gao, H. de Guise, and B. C. Sanders. SU(3) quantum interferometry with single-photon input pulses. *Phys. Rev. Lett.*, 110:113603, 2013.

[67] H. de Guise, S.-H. Tan, I. P. Poulin, and B. C. Sanders. Coincidence landscapes for three-channel linear optical networks. *Phys. Rev. A*, 89:063819, 2014.

[68] J. Chen, J. Ping, and F. Wang. *Group Representation Theory for Physicists*, volume 7. World Scientific, Singapore, 1989.

[69] S. Scheel. Permanents in linear optical networks. *eprint arXiv:quant-ph/0406127*, 2004.

[70] P. Bürgisser. The computational complexity of immanants. *SIAM J. Comput.*, 30(3):1023, 2000.

[71] J.-L. Brylinski and R. Brylinski. Complexity and Completeness of Immanants. *eprint arXiv:cs/0301024*, 2003.

[72] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky. Complete characterization of quantum-optical processes. *Science*, 322(5901):563, 2008.

[73] A. Laing and J. L. O'Brien. Super-stable tomography of any linear optical device. *ArXiv e-prints*, 2012.

[74] S. Rahimi-Keshari, M. A. Broome, R. Fickler, A. Fedrizzi, T. C. Ralph, and A. G. White. Direct characterization of linear-optical networks. *Opt. Express*, 21(11):13450, 2013.

[75] R. Heilmann, M. Gräfe, S. Nolte, and A. Szameit. A novel integrated quantum circuit for high-order w-state generation and its highly precise characterization. *Science Bulletin*, 60(1):96, 2015.

[76] M. Poot, C. Schuck, X. song Ma, X. Guo, and H. X. Tang. Design and characterization of integrated components for sin photonic quantum circuits. *Opt. Express*, 24(7):6843, 2016.

[77] K. Valson Jacob, A. E. Mirasola, S. Adhikari, and J. P. Dowling. Quantum process tomography of linear and quadratically nonlinear optical systems. *ArXiv e-prints*, 2018.

[78] M. Tillmann, C. Schmidt, and P. Walther. On unitary reconstruction of linear optical networks. *Journal of Optics*, 18(11):114002, 2016.

[79] N. Spagnolo, E. Maiorino, C. Vitelli, M. Bentivegna, A. Crespi, R. Ramponi, P. Mataloni, R. Osellame, and F. Sciarrino. Learning an unknown transformation via a genetic approach. *Scientific Reports*, 7(1):14316, 2017.

[80] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino. Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nat. Photon.*, 7:545, 2013.

[81] A. Kent. A no-summoning theorem in relativistic quantum theory. *Quantum Inf. Process.*, 12(2):1023, 2013.

[82] P. Hayden and A. May. Summoning information in spacetime, or where and when can a qubit be? *J. Phys. A*, 49(17):175304, 2016.

[83] P. Hayden, S. Nezami, G. Salton, and B. C. Sanders. Spacetime replication of continuous variable quantum information. *New J. Phys.*, 18(8):083043, 2016.

[84] E. Adlam and A. Kent. Quantum paradox of choice: More freedom makes summoning a quantum state harder. *Phys. Rev. A*, 93:062327, 2016.

[85] J. L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23, 1970.

[86] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[87] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271 , 1982.

[88] J. Ortigoso. Twelve years before the quantum no-cloning theorem. *American Journal of Physics*, 86(3):201, 2018.

[89] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648, 1999.

[90] D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, 2000.

[91] D. Markham and B. C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78:042309, 2008.

[92] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[93] R. F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, 2001.

[94] A. Cross, G. Smith, J. A. Smolin, and B. Zeng. Codeword stabilized quantum codes. *IEEE Transactions on Information Theory*, 55(1):433, 2009.

[95] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[96] S. Homer and A. L. Selman. *Computability and complexity theory*. Springer Science & Business Media, 2011.

[97] A. Montanaro and R. de Wolf. A Survey of Quantum Property Testing. *ArXiv e-prints*, 2013.

[98] E. Adlam and A. Kent. Knowledge-concealing evidencing of knowledge about a quantum state. *Phys. Rev. Lett.*, 120:050501, 2018.

[99] B. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54:2614, 1996.

[100] M. A. Nielsen. The entanglement fidelity and quantum error correction. *eprint arXiv:quant-ph/9606012*, 1996.

[101] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996.

[102] A. Steane. Multiple-particle interference and quantum error correction. *Proc. Royal Soc. A*, 452(1954):2551, 1996.

[103] R. Diestel. *Graph Theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Heidelberg, 2016.

[104] H. Bombin and M. A. Martin-Delgado. Homological error correction: Classical and quantum codes. *J. Math. Phys.*, 48(5):052105, 2007.

[105] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, 2011.

[106] P. P. Rohde and T. C. Ralph. Modelling photo-detectors in quantum optics. *Journal of Modern Optics*, 53(11):1589, 2006.

[107] Z.-Y. J. Ou. *Multi-photon quantum interference*, volume 43. Springer, 2007.

[108] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[109] J. Preskill. *Lecture Notes for Physics 229: Quantum Information and Computation*. CreateSpace Independent Publishing Platform, North Charleston, 2015.

[110] M. Grassl, T. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56:33, 1997.

[111] S. Roman. *Advanced Linear Algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer Science+Business Media, New York, 2005.

[112] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge university press, Cambridge, 1997.

[113] `https://github.com/abdullahkhalids/sakht-e-kiran`.

[114] H. Weyl. *The theory of groups and quantum mechanics*. Courier Corporation, New York, 1950.

[115] A. Brauer and H. Rohrbach. *Issai Schur/Gesammelte Abhandlungen*. Springer, Berlin, 1973.

[116] D. J. Rowe, M. J. Carvalho, and J. Repka. Dual pairing of symmetry and dynamical groups in physics. *Rev. Mod. Phys.*, 84:711, 2012.

[117] A. Bunse-Gerstner, R. Byers, and V. Mehrmann. Numerical methods for simultaneous diagonalization. *SIAM Journal on Matrix Analysis and Applications*, 14(4):927, 1993.

[118] `https://github.com/ishdhand/Simulation-of-characterization-procedure`.

[119] F. James. *Statistical methods in experimental physics*. World Scientific Publishing Company, 2006.

[120] T. Strutz. *Data fitting and uncertainty: A practical introduction to weighted least squares and beyond*. Vieweg and Teubner, 2010.

[121] M. G. Akritas and I. Van Keilegom. Non-parametric estimation of the residual distribution. *Scandinavian Journal of Statistics*, 28(3):549, 2001.

[122] X. Chen, O. Linton, and I. Van Keilegom. Estimation of semiparametric models when the criterion function is not smooth. *Econometrica*, 71(5):1591, 2003.

[123] T. Kailath. *Linear systems*, volume 156. Prentice-Hall Englewood Cliffs, NJ, 1980.

[124] J. B. Keller. Closest unitary, orthogonal and hermitian operators to a given operator. *Mathematics Magazine*, 48(4):192, 1975.

[125] T. Tao. *Topics in random matrix theory*, volume 132. American Mathematical Soc., 2012.

[126] B. Efron. Bootstrap methods: Another look at the jackknife. *Ann. Statist.*, 7(1):1, 1979.

[127] P. Diaconis and B. Efron. Computer-intensive methods in statistics. *Scientific American*, 248(5):116, 1983.

[128] C. J. Willmott, S. G. Ackleson, R. E. Davis, J. J. Feddema, K. M. Klink, D. R. Legates, J. O'Donnell, and C. M. Rowe. Statistics for the evaluation and comparison of models. *Journal of Geophysical Research: Oceans*, 90(C5):8995, 1985.

[129] B. Efron and R. Tibshirani. Bootstrap methods for standard errors, confidence intervals, and other measures of statistical accuracy. *Statist. Sci.*, 1(1):54, 1986.

[130] B. F. Manly. *Randomization, bootstrap and Monte Carlo methods in biology*. Chapman and Hall/CRC, 2006.

[131] T. J. DiCiccio and B. Efron. Bootstrap confidence intervals. *Statist. Sci.*, 11(3):189, 1996.

[132] A. C. Davison, D. V. Hinkley, et al. *Bootstrap methods and their application*, volume 1. Cambridge university press, 1997.

[133] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph. Boson sampling from a gaussian state. *Phys. Rev. Lett.*, 113:100502, 2014.

[134] 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. Osellame, and F. Sciarrino. Experimental scattershot boson sampling. *Science Advances*, 1(3), 2015.

[135] N. Gisin and S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.*, 79:2153, 1997.

[136] D. Bruss, A. Ekert, and C. Macchiavello. Optimal universal quantum cloning and state estimation. *Phys. Rev. Lett.*, 81:2598, 1998.

[137] R. F. Werner. Optimal cloning of pure states. *Phys. Rev. A*, 58:1827, 1998.

[138] J. Bae and A. Acín. Asymptotic quantum cloning is state estimation. *Phys. Rev. Lett.*, 97:030402, 2006.

[139] G. Chiribella and G. M. D'Ariano. Quantum information becomes classical when distributed to many users. *Phys. Rev. Lett.*, 97:250503, 2006.

[140] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Cambridge, 2010.

[141] P. Kok, H. Lee, and J. P. Dowling. Single-photon quantum-nondemolition detectors constructed with linear optics and projective measurements. *Phys. Rev. A*, 66:063814, 2002.

[142] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White. Linear optical controlled-not gate in the coincidence basis. *Phys. Rev. A*, 65:062324, 2002.

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

[144] M. Mitzenmacher and E. Upfal. *Probability and computing: Randomized algorithms and probabilistic analysis*. Cambridge university press, 2005.

[145] M. C. Tichy and K. Mølmer. Extending exchange symmetry beyond bosons and fermions. *Phys. Rev. A*, 96:022119, 2017.

[146] P. M. Alsing and G. J. Milburn. Teleportation with a uniformly accelerated partner. *Phys. Rev. Lett.*, 91:180404, 2003.

[147] N. Friis, A. R. Lee, K. Truong, C. Sabín, E. Solano, G. Johansson, and I. Fuentes. Relativistic quantum teleportation with superconducting circuits. *Phys. Rev. Lett.*, 110:113602, 2013.

[148] M. Ahmadi, Y.-D. Wu, and B. C. Sanders. Relativistic (2,3)-threshold quantum secret sharing. *Phys. Rev. D*, 96:065018, 2017.