universität wien

# MASTERARBEIT | MASTER'S THESIS

Titel | Title

## Loss Purification in Linear-Optical Quantum Circuits with Measurement-Induced Nonlinearity


verfasst von | submitted by

Michael Hans Hüttenbrenner BSc


angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien | Vienna, 2026

| | |
|---|---|
| Studienkennzahl lt. Studienblatt \| Degree programme code as it appears on the student record sheet: | UA 066 876 |
| Studienrichtung lt. Studienblatt \| Degree programme as it appears on the student record sheet: | Masterstudium Physics |
| Betreut von \| Supervisor: | Assoz. Prof. Mag. Dr. Borivoje Dakic |

# Acknowledgments

This thesis and project would not exist without the exceptional commitment of its initiator, Patrik Sund. Most of the directions we explored began with his ideas, and I'm very grateful for his guidance and expertise throughout. I especially appreciated his enthusiasm for physics, his intuition for quantum optics, and his ability to continuously generate and pursue new ideas alongside his work as an experimental researcher.

I would also like to thank my supervisor, Borivoje Dakić, for bringing me into this project and for his time, feedback, patience, and trust in our progress. I learned a great deal from him, and I particularly appreciate his way of approaching the abstract mathematics behind quantum information and quantum optics.

When I came to Vienna for my master's degree, I didn't know anyone at the University, and I'm very thankful to Markus Arndt for the time and support he gave me. Beyond his guidance and teaching, he also welcomed me into his group for an internship, which made this experience genuinely special. I'm excited to keep following the work of his group.

Finally, I want to thank my mother for her constant support. Without her, I would not have been able to pursue my studies in this way.

# Abstract

Photonic quantum information processing is impaired by photon loss and partial distinguishability, and many practical on-demand sources (e.g., quantum dots) emit photons whose coupling into circuits cannot be reliably heralded and is susceptible to loss. This thesis investigates purification schemes that aim to suppress vacuum components and improve effective state quality using linear optics, ancilla photons, and measurement-induced nonlinearities. We show numerically that a KLM-style CNOT circuit does not act as a loss or indistinguishability purifier. We then prove a general no-go theorem for state-agnostic loss-purification: within this resource model, the heralded presence probability cannot be improved beyond what is achievable by simply using the lowest-loss photon resource available. For state-preserving purification, we present a dual-rail qubit loss-purification scheme based on entangled resources and compare it to a protocol relying only on two separable ancilla photons. Finally, we study two-photon indistinguishability purification and show that, for two-photon linear-optical circuits with no-click heralding, the attainable improvement is bounded and is saturated by a balanced beam splitter (Hadamard) operation.

# Zusammenfassung

Die photonische Quanteninformationsverarbeitung wird durch Photonenverluste und partielle Unterscheidbarkeit beeinträchtigt, und viele On-Demand-Quellen wie Quantenpunkte emittieren Photonen, die nur unter möglichen Verlusten in Schaltungen eingespeist werden können. Diese Arbeit beschäftigt sich mit Purifikationsschemata, die darauf abzielen Vakuumanteile zu unterdrücken und die effektive Qualität der Zustände zu erhöhen. Dabei stehen Quantenschaltungen basierend auf linearer Optik, Ancilla-Photonen, und messungsinduzierter Nichtlinearität zur Verfügung. Es wird durch numerische Analyse gezeigt, dass eine KLM CNOT-basierte Schaltung nicht zu diesem Zweck verwendet werden kann, da sie weder gegen Verluste wirkt noch signifikant die Ununterscheidbarkeit der Photonen verbessert. Daraufhin wird ein allgemeines No-Go-Theorem für zustandsagnostische Purifikation der Photonenpräsenz bewiesen: Innerhalb des genannten Ressourcenmodells kann die Anwesenheitswahrscheinlichkeit eines Photons nicht über das hinaus verbessert werden, was bereits durch die Verwendung der jeweils verlustärmsten verfügbaren Photonenressource erreichbar ist. Für zustandserhaltende Verlustreduktion wird ein Protokoll, welches verschränkte Ressourcen benötigt, vorgestellt, und mit einem Protokoll, das lediglich zwei separable Ancilla-Photonen verwendet verglichen. Abschließend wird die Purifikation der Ununterscheidbarkeit zweier Photonen untersucht, mit dem Resultat, dass ein symmetrischer Strahlteiler (Hadamard-Gatter) die gefundene Schranke erfüllt, und somit von keiner Schaltung die auf linearer Optik und dem Ausbleiben von Detektor-Klicks (No-Click-Heralding) beruht übertroffen werden kann.

# Contents

# 1 Introduction and summary

This thesis began as an investigation into ways to improve single-photon sources. Quantum dots (QDs) can emit photons on demand, but sometimes these photons will not make it to the circuit where they are needed due to the challenges involved in coupling the output of a QD into a circuit [1]. Another common source architecture is a heralded source, such as SPDC. Such sources emit multiple photons upon successful operation, and one of them can be used to herald the presence of the others. SPDC crystals can be placed such that photon delivery into the circuit can often be made highly reliable. Upon successful heralding, a photon can be assumed to have entered the circuit. The drawback of SPDC is that it is not on demand: it operates probabilistically [2]. QD-based sources exist within lossy platforms. Therefore, it would be of high relevance if the successful delivery of photons from on-demand sources into a circuit could be heralded.

The original motivation of this work was to combine several on-demand sources (such as quantum dots) and feed their photons into a linear-optical circuit. At the end of the circuit, detectors are placed, and upon observing a specific click pattern (potentially assuming perfect photon-number-resolving detection) one would like to be certain that all sources fired as expected, the coupling of these photons into the circuit worked, and that a photon leaves the circuit. Crucially, if any photon did not make it into the circuit, the heralding pattern should never occur. Throughout this thesis, we often use "loss" and "absence of a photon at the beginning of a protocol" interchangeably; the on-demand source setting is the reason for this identification. Furthermore, sometimes we speak of ancilla photons, although all involved photons are treated symmetrically in the same context. The reason for this is that the on-demand sources we always have in the back of our minds are interchangeable, but formally the concept of an ancilla photon is well established and known to enhance the range of possible operations in quantum information processing [3]. Since our desired protocol destroys all but one photon by detecting them, we can effectively think of the non-surviving photons as

used-up ancillae.

Achieving the functionality above would effectively implement a source that is both on-demand and heralded with respect to successful coupling. Motivated by the inner workings of the CNOT gate proposed by Knill, Laflamme, and Milburn [4], we initially believed that it might be a viable candidate for this task. We therefore begin by numerically investigating its behavior.

Besides photon absence, partial distinguishability of photons is also undesirable [5]. For this reason, we also study whether the same CNOT scheme can be used for indistinguishability purification.

Our numerical results show that this CNOT scheme cannot be used for either task. As we will expand on later, it is perhaps surprising that the CNOT does not help with photon-presence purification, and we therefore explored modifications and alternative circuits. After all attempts failed, we turned to the theoretical backbone of the problem and proved a no-go result: the desired circuit functionality is incompatible with the laws of physics within our model. In other words, the task cannot be achieved in the way we initially aimed for.

With a general theorem in hand, we then connect our findings to related work in the literature. In particular, we consider the closely related task of heralded state amplification, where one aims to herald the presence of a photon that is in a coherent superposition while preserving that superposition. Here, the involved photons are no longer fully interchangeable, because there will be one special incoming photon in a superposition, in contrast to the set of ancilla photons one prepares. We show that the loss of the involved ancilla photons determines how effective such protocols can be. Furthermore, we present our own protocol based on entangled resources, which implements a teleportation-style operation to achieve state amplification. We also discuss a scheme that has been proposed previously [6], which in principle does not rely on an entangled resource, in order to provide a comparison.

Finally, since the CNOT did not significantly improve photon indistinguishability, we investigate a general approach to indistinguishability purification for two photons. We find that a well-known Hadamard-based scheme [5] cannot be surpassed by adding additional modes and detectors that herald on the absence of a click.

# 2 Theory

With the advent of quantum mechanics, it became apparent that the electromagnetic field must consist of quantum particles [7], which are known as photons today. Photonic quantum states can be used in a multitude of applications for information processing, many of which have the potential to surpass non-quantum solutions in various metrics [8, 9]. These protocols, however, all require sources that can produce the required photonic quantum states reliably [1], or they are susceptible to imperfections of the involved quantum states [10]. This thesis investigates a set of schemes to improve the usefulness of photonic signals by purifying them. In this section, a brief overview of quantum optics and quantum information is given, such that the results of the thesis can be discussed in a self-contained manner.

## 2.1 Quantization of the EM field

The proper mathematical formulation that is used today in quantum optics was developed over many years, starting with canonical quantization [11, 12] and advancing to second quantization introduced by Dirac [13]. In second quantization the mathematical objects used to describe the behavior of a quantum state are no longer vectors, but operators. These can be associated with excitations in a quantum field. The time evolution or any transformation of a system is then determined by a transformation acting on the aforementioned operators. Let us investigate the quantization procedure for photonic quantum states, which will be the center of this thesis. A more detailed derivation can be found in many textbooks, the argument that is briefly presented here is taken from [14].

To extend a classical theory to a quantum theory, one needs to express the Hamiltonian function $H$ of the system in terms of a set of conjugate variables $\{q_i\}, \{p_i\}$. These

determine the dynamics through Hamilton's equations of motion.

$$\dot{q}_i = \frac{\partial H}{\partial p_i}, \qquad \dot{p}_i = -\frac{\partial H}{\partial q_i} \tag{2.1}$$

One then promotes these variables to operators, which fulfill the canonical commutation relation

$$[\hat{q}_i, \hat{p}_j] = i\hbar\,\delta_{ij}, \tag{2.2}$$

and can be used to form the Hamiltonian operator $\hat{H}$ in analogy to the classical case. The Hamiltonian may be interpreted as the total energy of a system. There are a multitude of caveats to this approach, but we will focus on the most striking: The stated objective is to find a quantum theory of light, but starting from Maxwell's equations

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0}, \qquad \nabla \cdot \mathbf{B} = 0, \qquad \nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}, \qquad \nabla \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t} \tag{2.3}$$

it is not so obvious how one could arrive at a Hamiltonian function, or which canonical variables one must choose. We start by considering the energy stored in the free classical EM field, expressed as the integral over an energy density.

$$H_R = \frac{\varepsilon_0}{2} \int_V d^3r \left[\mathbf{E}^2(\mathbf{r}, t) + c^2 \mathbf{B}^2(\mathbf{r}, t)\right]. \tag{2.4}$$

This expression gives the total energy, so we assume it must be equal to the Hamiltonian function of the system. It is common in this quantization approach to limit the fields to a box of volume $L^3$, which can be chosen arbitrarily large. This has the advantage that Fourier expansion can be used to express the fields.

$$\mathbf{E}(\mathbf{r}, t) = \sum_\ell \boldsymbol{\epsilon}_\ell \, \mathcal{E}_\ell^{(1)} \left[ i\,\alpha_\ell(t) e^{i\mathbf{k}_\ell \cdot \mathbf{r}} - i\,\alpha_\ell^*(t) e^{-i\mathbf{k}_\ell \cdot \mathbf{r}} \right] \tag{2.5}$$

$$\mathbf{B}(\mathbf{r}, t) = \sum_\ell \boldsymbol{\epsilon}'_\ell \, \frac{\mathcal{E}_\ell^{(1)}}{c} \left[ i\,\alpha_\ell(t) e^{i\mathbf{k}_\ell \cdot \mathbf{r}} - i\,\alpha_\ell^*(t) e^{-i\mathbf{k}_\ell \cdot \mathbf{r}} \right] \tag{2.6}$$

This expansion might seem cumbersome, but the individual constituents have simple interpretations. The index

$$\ell = (n_x, n_y, n_z;\, s) = (\mathbf{n};\, s), \tag{2.7}$$

specifies the direction and polarization of a field component. It is used to label the mode of radiation, as these numbers differentiate the individual components of the fields. It

is important to point out that $n_i$ are integer numbers and thus this encompasses all frequencies of light compatible with the boundary conditions, because

$$(\mathbf{k_n})_x = n_x \frac{2\pi}{L}, \qquad (\mathbf{k_n})_y = n_y \frac{2\pi}{L}, \qquad (\mathbf{k_n})_z = n_z \frac{2\pi}{L}. \tag{2.8}$$

Since the fields are transverse, any component can be specified by two basis vectors $\boldsymbol{\epsilon}_{\mathbf{n},s}$ orthogonal to the wave vector

$$\boldsymbol{\epsilon}_{\mathbf{n},s} \cdot \mathbf{k_n} = 0; \ s = 1, 2. \tag{2.9}$$

Notice that we denote the wave vector $\mathbf{k}_\ell$ also by index $\ell$, although it is only associated with a direction $\mathbf{n}$ but no polarization $s$. The coefficients $\alpha_\ell(t)$ and their complex conjugate are introduced ad hoc because the aim is to decouple the differential equations that govern the dynamics of electric and magnetic fields which one can obtain from manipulating Maxwell's equations. $\mathcal{E}_\ell^{(1)}$ is a constant, which can later be associated with the energy of a single photon with frequency $\omega_\ell$.

This expansion allows us to explicitly solve the integral from Eq. 2.4 obtaining

$$H_R = 2\varepsilon_0 L^3 \sum_\ell \left[\mathcal{E}_\ell^{(1)}\right]^2 |\alpha_\ell|^2. \tag{2.10}$$

Furthermore, considering only one mode of radiation $\ell$, the dynamics of the time-dependent components $\alpha_\ell(t)$ and $\alpha_\ell^*(t)$ can be used to identify a set of equations that resembles Hamilton's equations of motion in their abstract structure

$$\frac{dQ_\ell}{dt} = \frac{\partial H_\ell}{\partial P_\ell}, \qquad \frac{dP_\ell}{dt} = -\frac{\partial H_\ell}{\partial Q_\ell}, \tag{2.11}$$

where

$$H_\ell = 2\varepsilon_0 L^3 \left|\mathcal{E}_\ell^{(1)}\right|^2 |\alpha_\ell|^2. \tag{2.12}$$

For this, one introduces the canonical variables

$$Q_\ell = \sqrt{\frac{4\varepsilon_0 L^3}{\omega_\ell}\, \mathcal{E}_\ell^{(1)}\, \Re\{\alpha_\ell\}}, \qquad P_\ell = \sqrt{\frac{4\varepsilon_0 L^3}{\omega_\ell}\, \mathcal{E}_\ell^{(1)}\, \Im\{\alpha_\ell\}}. \tag{2.13}$$

These are now promoted to operators with the canonical commutation relation

$$\left[\hat{Q}_\ell, \hat{P}_{\ell'}\right] = i\hbar\, \delta_{\ell\ell'}, \qquad \left[\hat{Q}_\ell, \hat{Q}_{\ell'}\right] = \left[\hat{P}_\ell, \hat{P}_{\ell'}\right] = 0. \tag{2.14}$$

In analogy to the quantum harmonic oscillator, $\alpha_\ell(t)$ and $\alpha_\ell^*(t)$ can also be promoted to operators. These are called creation and annihilation operators or simply ladder operators, and by choosing

$$\mathcal{E}_\ell^{(1)} = \sqrt{\frac{\hbar\omega_\ell}{2\varepsilon_0 L^3}}, \tag{2.15}$$

they fulfill the commutation relations

$$\left[\hat{a}_\ell, \hat{a}_{\ell'}^\dagger\right] = \delta_{\ell\ell'}, \qquad [\hat{a}_\ell, \hat{a}_{\ell'}] = 0 \tag{2.16}$$

and relate to the field quadratures $\hat{Q}_\ell$ and $\hat{P}_\ell$ via

$$\hat{a}_\ell = \frac{1}{\sqrt{2\hbar}}\left(\hat{Q}_\ell + i\hat{P}_\ell\right), \qquad \hat{a}_\ell^\dagger = \frac{1}{\sqrt{2\hbar}}\left(\hat{Q}_\ell - i\hat{P}_\ell\right). \tag{2.17}$$

In much of the literature and parts of this thesis $\hat{a}, \hat{a}^\dagger$ are denoted without the operator symbol, just as $a, a^\dagger$.

The total Hamiltonian for the quantized EM field is then given by

$$\hat{H}_R = \sum_\ell \frac{\omega_\ell}{2}\left(\hat{Q}_\ell^2 + \hat{P}_\ell^2\right) = \sum_\ell \hbar\omega_\ell\left(\hat{a}_\ell^\dagger\hat{a}_\ell + \frac{1}{2}\right). \tag{2.18}$$

Additionally, one defines the number operator $\hat{N}_\ell$, which, for a given photonic state, returns the total number of photons. It can be expressed via

$$\hat{N}_\ell = \hat{a}_\ell^\dagger\hat{a}_\ell. \tag{2.19}$$

The names of $\hat{a}_\ell^\dagger, \hat{a}_\ell$ and $\hat{N}_\ell$ stem from their action on photonic states, which can be derived by using their respective behavior in commutators.

$$\hat{N}_\ell\,|n_\ell\rangle = n_\ell\,|n_\ell\rangle, \qquad \text{with} \qquad n_\ell = 0, 1, 2, \ldots \tag{2.20}$$

$$\hat{a}_\ell|n_\ell\rangle = \sqrt{n_\ell}\,|n_\ell - 1\rangle \quad \text{if} \quad n_\ell > 0, \qquad \hat{a}_\ell|0_\ell\rangle = 0, \qquad \hat{a}_\ell^\dagger|n_\ell\rangle = \sqrt{n_\ell + 1}\,|n_\ell + 1\rangle \tag{2.21}$$

The formalism used to describe a general photon state across arbitrary modes is called Fock-space formalism. It makes use of an infinite-dimensional product space, where each mode corresponds to an individual Hilbert space, while multiple photons across multiple modes are expressed as tensor product states [15]. The tensor product between

any two states between modes $a$ and $b$ is abbreviated as

$$|n_a\rangle_a \otimes |n_b\rangle_b \equiv |n_a, n_b\rangle_{a,b}. \tag{2.22}$$

For the quantized EM field, a general state will thus be of the form

$$|\psi\rangle = \sum_{n_1=0}^{+\infty} \sum_{n_2=0}^{+\infty} \cdots \sum_{n_\ell=0}^{+\infty} \cdots C_{n_1 n_2 \cdots n_\ell \cdots} |n_1, n_2, \cdots, n_\ell, \cdots\rangle, \tag{2.23}$$

where normalization demands $|\langle\psi\,|\,\psi\rangle|^2 = 1$, and $C_{n_1 n_2 \cdots n_\ell \cdots}$ will be complex numbers. The special state $|0, \ldots, 0, \ldots\rangle \equiv |0\rangle$ which has no photons in any mode, is referred to as vacuum. In general, if any mode is empty, we say it contains vacuum, which is represented as $|0\rangle_\ell$. Notice that this is not the zero vector of the underlying space, as $\langle 0\,|\,0\rangle = 1$. The actual zero vector is never used in these considerations, but would be denoted differently, often just as 0.

## 2.2 Transformation of multi-photon quantum states

From now on, we restrict ourselves to indistinguishable photons of identical polarization and frequency that are confined to distinct spatial modes. The formalism remains the same, with the only required label specifying which spatial mode the photon is in. This approach is used, for example, for photons that go through a circuit of optical fibres connected by different optical elements.

The space considered is infinite-dimensional, because it is always possible (mathematically) to create additional photons in mode $i$ by applying the creation operator $a_i^\dagger$. However, if we only consider states of a fixed photon number, the space will be contained in $\mathbb{C}^D$, where $D$ can be obtained via the Bose-Einstein statistics [16] as

$$D = \Omega_B(N, M) = \binom{N+M-1}{N} = \frac{(N+M-1)!}{N!\,(M-1)!}. \tag{2.24}$$

As a simple example, for two photons across two modes, we have the three possible states

$$|2,0\rangle_{1,2},\ |0,2\rangle_{1,2},\ |1,1\rangle_{1,2}, \tag{2.25}$$

which we can identify with the standard $\mathbb{C}^3$ basis-vectors. Furthermore, instead of denoting a state by the number of photons $n_i$ in each mode $i$, it is in principle possible

to denote it by the mode $m(\gamma_j)$ that each photon $\gamma_j$ is in.

$$|n_1, n_2, n_3, \ldots, n_M\rangle_{1,2,3,\ldots,M} \equiv [m(\gamma_1), m(\gamma_2), \ldots, m(\gamma_N)] \tag{2.26}$$

Since the photons are indistinguishable, one chooses by convention that the mode index must increase or stay the same when traversing the array from left to right. This way of denoting states is referred to as index notation, and is particularly helpful in applications that require explicit transition-amplitude calculation and involve coding, as will be shown in this section. To provide an example, the states from Eq. 2.25 are given in index notation as

$$[1,1],\ [2,2],\ [1,2]. \tag{2.27}$$

Since photonic states are described by vectors, we expect that a transformation that leaves the photon number untouched but maps the input Fock vector onto a new one is described by a matrix. In fact, as long as the photon number is preserved, we speak of linear optics [17], although it is important to point out that there exist photon-number-preserving transformations that cannot be realized with linear optics alone. [18]. The laws of quantum physics demand that this matrix must be a unitary matrix, in order to preserve the normalization of the state [14]. These transformations are realized by quantum circuits, which will be described in more detail later. Here, we only want to put emphasis on the following: Transforming a large Fock vector into a new one is mathematically convoluted because the space has, in general, such a high number $D$ of dimensions as Eq. 2.24 suggests. For this reason the matrix that does

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1D} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2D} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3D} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{D1} & a_{D2} & a_{D3} & \cdots & a_{DD} \end{pmatrix}}_{\text{Circuit}} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_D \end{pmatrix}}_{\text{Input}} = \underbrace{\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_D \end{pmatrix}}_{\text{Output}}, \tag{2.28}$$

is usually not calculated explicitly.

So how does one go about solving the problem depicted in Fig. 2.1?

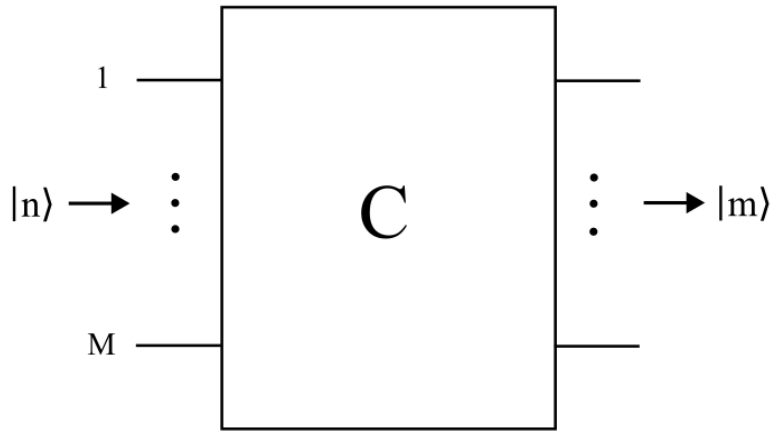


**Figure 2.1:** A general linear quantum optics circuit $C$ with $M$ modes transforms the $N$ photon input state $|n\rangle$ to an output-state $|m\rangle$, while photon number is preserved. In practice, input and output can be superpositions.

The aim is to find the output state $|m\rangle$ that is obtained by sending the input state $|n\rangle$ into the circuit $C$ with $M$ modes. We know that there will be some unitary operation $\hat{U}$ that encodes the action of this circuit on the input state. Notice, that input and output will in general be superpositions of basis states, but due to linearity finding the transition amplitude between two basis states suffices.

Consider a simpler problem: If just a single photon is incoming to the circuit, using linear algebra and vector-matrix products is the optimal approach, as the number of dimensions is limited to the number of modes $M$. The single-photon state $|x\rangle$ is described by a column vector

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_M \end{pmatrix}, \quad \langle 0,\ldots,0,1,0,\ldots,0\,|\,x\rangle_{1,\ldots,m,\ldots,M} = x_m, \quad \|\mathbf{x}\|^2 = \sum_{m=1}^{M} |x_m|^2 = 1, \quad (2.29)$$

where each entry specifies the amplitude of the photon being in the corresponding mode. The matrix that transforms such single-photon states is referred to as single-photon or mode transfer matrix. This unitary matrix will be called $U$ in the following considerations. It encodes the behavior of a quantum gate or circuit and is either already known or easy to calculate, as will be explained in Sec. 2.3. The transformation of $|x\rangle$

by the circuit to yield the output state $|y\rangle$ is thus simply given by a matrix product [19]

$$|y\rangle = \hat{U}|x\rangle \rightarrow \mathbf{y} = U\mathbf{x}. \tag{2.30}$$

Now, we could also rewrite this by using creation operators acting upon vacuum to describe the single-photon state.

$$\hat{U}|x\rangle = |y\rangle = \hat{U}\sum_{m=1}^{M} x_m a_m^\dagger|0\rangle = \sum_{m=1}^{M} x_m \hat{U} a_m^\dagger \hat{U}^\dagger|0\rangle \tag{2.31}$$

Here we made use of the linear nature of $\hat{U}$ and the fact that no linear-optics transformation will alter the vacuum state, so $|0\rangle = \hat{U}^\dagger|0\rangle$. What this hints at is that instead of transforming single-photon states as vectors, one can think of transforming the creation operators $a_m^\dagger$ instead, via some transformation $D(U)$. Indeed, doing a comparison of coefficients, one can show from here that the creation operators transform as row vectors with the same matrix $U$ that transforms single-photon states [17].

$$(\tilde{a}_1^\dagger, \ldots, \tilde{a}_M^\dagger) = (a_1^\dagger, \ldots, a_M^\dagger) \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1M} \\ u_{21} & u_{22} & \cdots & u_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ u_{M1} & u_{M2} & \cdots & u_{MM} \end{pmatrix} \tag{2.32}$$

The operators $\tilde{a}_m^\dagger$ will be comprised of a linear combination of the original operators $a_m^\dagger$, where the weights of the individual summands are given by the elements of column $m$ taken from the mode transfer matrix $U$. One can now think of the unitary that does the mode transformation in the following way: The elements of the matrix yield the final amplitudes of the resulting superposition for an incoming photon. If we just consider a single photon incoming in mode $m$, we have to multiply the row vector of creation operators with column $m$ of $U$. The result will in general be a sum over creation operators, and the photon will exit the circuit in a superposition. The coefficients in that superposition are given by the matrix elements $u_{im}$. Here $m$ is the input mode, and the row index $i$ corresponds to an output mode where we might find the photon now after the circuit.

This tangent into the abstract allows us to formulate the expression for the transition amplitude between general multi-photon Fock-basis states, which is used to determine the behavior of complex quantum circuits in practice. Since any state can be expanded as a superposition of basis states, our aim of finding a way to calculate how a circuit

transforms a general input reduces to finding the amplitude

$$\langle m|\hat{U}|n\rangle = \langle m_1, \ldots, m_M|\hat{U}|n_1, \ldots, n_M\rangle \tag{2.33}$$

for two Fock-space basis states $|n\rangle, |m\rangle$. Since multi-photon states can also be expressed via creation operators, we can consider transforming a general multi-photon Fock-basis state with $\hat{U}$.

$$\hat{U}|n_1, \ldots, n_M\rangle = \hat{U}\prod_{i=1}^{M}\frac{1}{\sqrt{n_i!}}(a_i^\dagger)^{n_i}|0\rangle \tag{2.34}$$

Since it is an $N$ photon basis state, it will be specified by a product of $N$ creation operators, where each mode can appear multiple times. Inserting the identity operator $\hat{\mathbb{1}}$, making use of unitarity $\hat{\mathbb{1}} = \hat{U}\hat{U}^\dagger$ and using once more the immutability of $|0\rangle$, one finds

$$\hat{U}|n_1, \ldots, n_M\rangle = \prod_{i=1}^{M}\frac{1}{\sqrt{n_i!}}(\hat{U}a_i^\dagger\hat{U}^\dagger)^{n_i}|0\rangle. \tag{2.35}$$

This means that, to transform any multi-photon quantum state, one only needs to consider how individual creation operators transform, which is precisely what Eq. 2.32 already tells us.

Now, if such a multi-photon state is transformed, the result will be a polynomial of creation operators which comes from combining the results of Eq. 2.32 and Eq. 2.35. If we are interested in the transition amplitude, we have to evaluate

$$\langle m_1, \ldots, m_M|\prod_{i=1}^{M}\frac{1}{\sqrt{n_i!}}(\hat{U}a_i^\dagger\hat{U}^\dagger)^{n_i}|0\rangle = \langle m_1, \ldots, m_M|\prod_{i=1}^{M}\frac{1}{\sqrt{n_i!}}(\sum_{j=1}^{M}u_{ji}a_j^\dagger)^{n_i}|0\rangle. \tag{2.36}$$

There exists a way to reduce complexity in this equation [17]. The photon distribution of $|n\rangle$ decides which columns of the single-photon transfer matrix $U$ will be picked, and how many times ($n_i$) the resulting weighted sum of creation operators will be multiplied with itself. On the other hand, notice how applying $\langle m|$ from the left will, by orthogonality of the Fock basis, remove all states with combinations of creation operators not matching the photon distribution of $|m\rangle$. The remaining parts are terms with permutations of creation operators that match the output state $|m\rangle$ and have coefficients determined by the input state $|n\rangle$ and the matrix $U$. Finally, the expression can be simplified using the multinomial theorem. The transition amplitude between two Fock-basis states $|n\rangle, |m\rangle$ of photon number $N$ for an $M$ mode circuit described by

$\hat{U}$ is given by

$$\boxed{\langle m \,|\, \hat{U} \,|\, n \rangle \;=\; \frac{\mathrm{perm}(U[m|n])}{\sqrt{\prod_{i=1}^{M} n_i! \prod_{j=1}^{M} m_j!}}.} \tag{2.37}$$

The permanent is calculated from a modified version of the single-photon transfer matrix $U$. The notation $U[m|n]$ specifies which rows and columns of $U$ are used to make this altered matrix. To be formally correct, for the states $|n_1, n_2, \ldots, n_M\rangle$ and $|m_1, m_2, \ldots, m_M\rangle$, the matrix is obtained via

$$\begin{aligned} &U[\Omega'|\Omega] \\ &\Omega = (1^{n_1}, 2^{n_2}, \ldots, M^{n_M}) \\ &\Omega' = (1^{m_1}, 2^{m_2}, \ldots, M^{m_M}) \end{aligned} \tag{2.38}$$

where $\Omega$ specifies which columns to use and $\Omega'$ which rows. The photon numbers $n_i, m_i$ specify the multiplicity of a column/row. In other words, $k^{n_i}/k^{m_i}$ means that the corresponding column/row $k$ will be stacked $n_i/m_i$ times [17].

$$U[\Omega'|\Omega] = \begin{bmatrix} \overbrace{U_{1,1} \cdots U_{1,1}}^{n_1} & \overbrace{U_{1,2} \cdots U_{1,2}}^{n_2} & \cdots & \overbrace{U_{1,M} \cdots U_{1,M}}^{n_M} & \\ \vdots & \vdots & & \vdots & \Big\}m_1 \\ U_{1,1} \cdots U_{1,1} & U_{1,2} \cdots U_{1,2} & \cdots & U_{1,M} \cdots U_{1,M} & \\ \vdots & \vdots & & \vdots & \\ \vdots & \vdots & & \vdots & \\ U_{x,1} \cdots U_{x,1} & U_{x,2} \cdots U_{x,2} & \cdots & U_{x,M} \cdots U_{x,M} & \\ \vdots & \vdots & & \vdots & \Big\}m_i \\ U_{x,1} \cdots U_{x,1} & U_{x,2} \cdots U_{x,2} & \cdots & U_{x,M} \cdots U_{x,M} & \\ \vdots & \vdots & & \vdots & \end{bmatrix} \tag{2.39}$$

In Eq. 2.37, the index notation introduced in the beginning of this section is used

for $[n], [m]$, since it already conveys what one needs to do in practice. Each mode index appearing just specifies a row/column to pick (see Eq. 2.39). If an index appears multiple times in sequence inside $[n]$ or $[m]$, the corresponding row / column will be used multiple times accordingly. If a certain mode is missing from the index state, the matching row/column is skipped. This method of indexing is similar to how advanced indexing and slicing of arrays works in many programming languages, including Python [20].

## 2.3 Optical quantum circuits and quantum information

Quantum information has developed as a wide and versatile field over the last decades. In principle, a plethora of physical mechanisms can be used to process quantum information [21, 22]. Even for photons, one can for example encode the information in modes that correspond to physical wires in a circuit, or via the photons' polarization. An in-depth introduction to the concepts in quantum information can be found in [23]. Here only the necessary basics are introduced.

Regardless of the underlying physical system, in quantum information one attempts to implement states referred to as qubits. A single qubit

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1 \quad \text{and} \quad \alpha, \beta \in \mathbb{C} \tag{2.40}$$

can be seen as being in a superposition between the logical states $|0\rangle$ and $|1\rangle$. Since the coefficients are arbitrary complex numbers that satisfy the normalization constraints of quantum physics, a qubit has the same degrees of freedom as the surface of a sphere [24]. This continuous freedom together with entanglement and interference allows quantum information procedures to surpass their classical counterparts in theory, with prominent examples ranging from the efficient factorization of prime numbers [25] to theoretically secure communication [26]. Similar to how classical information is represented in strings of bits, in practice multiple qubits are used together to process information. Generating and preserving a set of logical qubits is one of the primary challenges in modern quantum information science [27].

Similar to classical information processing, logic gates can be used to manipulate information. Quantum gates are described by matrices, which act upon the states to transform them. There exist a plethora of gates with one of the most important gates

being the Hadamard gate $H$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.41}$$

The Hadamard gate $H$ acts on the computational basis state $|0\rangle$ as follows:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.42}$$

This means the state is put in an even superposition between $|0\rangle$ and $|1\rangle$. In our considerations, a qubit is implemented by a photon that is in a superposition between two modes $a$ and $b$

$$\alpha|1,0\rangle_{a,b} + \beta|0,1\rangle_{a,b} \equiv \alpha|0\rangle + \beta|1\rangle. \tag{2.43}$$

This encoding of photonic quantum information is named dual-rail encoding. Quantum circuits usually consist of multiple gates. One can multiply together the matrices corresponding to individual quantum gates to obtain the single-photon transfer matrix of the circuit they comprise. Of course, these matrices will have to be expanded to match the total dimensionality of the circuit given by the number of modes. But this can easily be done by inserting 1s on the diagonal and 0s elsewhere in the correct spots, such that the matrix extends to the correct dimensionality.

In addition to regular quantum information processing, photons offer additional ways of manipulating quantum states with logic gates. The Hadamard gate is usually implemented with a beam splitter. If two indistinguishable photons are incident from the two input arms of a beam splitter $|1,1\rangle_{a,b}$, they will exhibit non-classical behavior called the Hong-Ou-Mandel effect [28]. Due to their indistinguishability, interference can take place, which only yields the two bunched states after the beam splitter, assuming perfect indistinguishability.

$$\begin{aligned} |\psi_{\text{in}}\rangle = a^\dagger b^\dagger |0,0\rangle \xrightarrow{H} |\psi_{\text{out}}\rangle &= \frac{1}{2}\Big((a^\dagger + b^\dagger)(a^\dagger - b^\dagger)\Big)|0,0\rangle \\ &= \frac{1}{\sqrt{2}}\Big((a^\dagger)^2 - (b^\dagger)^2\Big)|0,0\rangle \\ &= \frac{1}{\sqrt{2}}\Big(|2,0\rangle - |0,2\rangle\Big) \end{aligned} \tag{2.44}$$

The anti-bunched state $|1,1\rangle_{a,b}$ one would also expect classically will not be present. This illustrates that the nature of boson sampling [16] is quite different from what one would expect from classical particles.

## 2.4 Mixed states, entanglement and measurement

Quantum physics is inherently probabilistic. Quantum states are capable of non-classical interference which can influence the probability amplitude associated with a certain measurement outcome [28]. There exists, however, the possibility that, in addition to the quantum nature of a system, a classical statistical mixture has to be considered. To provide an example, consider a circuit that expects a certain two-photon state $|\psi_2\rangle$. Due to imperfect photon sources, sometimes the circuit will, however, receive only one photon or none. It is clear that these instances should not interfere in a quantum sense, yet they must be described mathematically with some probabilistic nature attached to them.

To describe such situations, one must move from state vectors to density operators. For a pure state $|\psi\rangle$, the corresponding density operator $\hat{\rho}_{\text{pure}}$ is

$$\hat{\rho}_{pure} = |\psi\rangle\langle\psi|. \tag{2.45}$$

Now consider a probabilistic source that selects states from a set $\{|\phi_i\rangle\}_i$, emitting $|\phi_i\rangle$ with probability $p_i$. In general, the resulting state cannot be expressed as $|\phi'\rangle\langle\phi'|$ with some $|\phi'\rangle$. Instead, it must be described as a mixed state [29],

$$\hat{\rho}_{mix} = \sum_i p_i |\phi_i\rangle\langle\phi_i|, \quad \text{where } \mathrm{Tr}\Big[\hat{\rho}_{mix}\Big] \stackrel{!}{=} 1. \tag{2.46}$$

The unit-trace condition ensures normalization. Because pure states are orthogonal projections, one can define the following measure of the purity of a quantum state $\hat{\rho}$ [30]:

$$P = \mathrm{Tr}\Big[\hat{\rho}^2\Big] \tag{2.47}$$

with $P = 1$ for pure states and $1/d \leq P < 1$ for mixed states in a $d$-dimensional Hilbert space. This criterion therefore allows one to determine whether a given state is pure.

In a finite-dimensional vector space, any density operator can be represented by a density matrix with the elements $\rho_{ij} = \langle i|\hat{\rho}|j\rangle$ [29]. Due to the linearity of quantum mechanics, one can apply any transformation on each part of the mixture separately and collect the terms afterwards [31].

We have touched upon earlier that mathematically, two systems $|\phi\rangle$ and $|\psi\rangle$ can be combined by taking their tensor product $|\phi\rangle \otimes |\psi\rangle$. Consider, however, for example the

two-qubit state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \tag{2.48}$$

This state cannot be factorized into two distinct single-qubit states of the form $|\phi\rangle \otimes |\psi\rangle$. More interestingly, the state exhibits a perfect correlation between the two qubits, as observing $|0\rangle$ or $|1\rangle$ for one constituent would necessarily also produce the same outcome for the other. States that are not factorizable in this way are called entangled states [23, Ch. 2]. Quantum entanglement is a distinctive resource of quantum information with no identical classical counterpart. The collapse of the wave function of entangled states leads to peculiar philosophical questions about the nature of reality, which was famously pointed out by Einstein, Podolsky, and Rosen [32], and later further investigated by Bell [33]. For our purpose, it is important to point out that entanglement is a key resource in quantum information processing [34]. In photonic architectures, passive linear optics alone is insufficient for deterministic entangling gates; scalable schemes rely on ancillary photons and measurement-induced nonlinearities. The possible transformations of entangled states also go beyond the boson-sampling expression shown in Sec. 2.2; Eq. 2.37 gives Fock-to-Fock transition amplitudes. For general entangled/superposed input states, output amplitudes become coherent sums of these Fock basis amplitudes. We will investigate some schemes that make use of entanglement in the next sections. The generation of entangled photonic states requires nonlinearities and can, for example, be achieved using special crystals and a process called spontaneous parametric down-conversion (SPDC) [2].

In addition to entanglement, another feature of quantum physics that distinguishes it from classical physics is the special role of observation. Quantum measurement theory provides the mathematical tools to evaluate expected outcomes and probabilities for experiments. As an introduction, a qubit $\alpha|0\rangle + \beta|1\rangle$ is in a superposition between either $|0\rangle$ or $|1\rangle$. If one measures in the correct basis, one can implement a projective measurement with the projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ which are orthogonal projections. They have the effect of projecting the qubit onto either computational basis state, by collapsing the wave function, yielding the outcomes with probabilities $|\alpha|^2$ and $|\beta|^2$ [23, Ch. 2].

In general, the expectation value of an observable $\hat{A}$ which can be decomposed into projective constituents $\hat{P}_m$ via the spectral theorem

$$\hat{A} = \sum_m a_m \hat{P}_m, \tag{2.49}$$

is given by

$$\langle\psi|\hat{A}|\psi\rangle \tag{2.50}$$

for pure states and

$$\mathrm{Tr}\left[\hat{A}\hat{\rho}\right] \tag{2.51}$$

for mixed states [23, Ch. 2]. Post-measurement, the state will furthermore be left in one of the possible outcomes

$$|\psi_m\rangle = \frac{\hat{P}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_m|\psi\rangle}} \qquad \text{or} \qquad \hat{\rho}_m = \frac{\hat{P}_m\hat{\rho}\hat{P}_m}{\mathrm{Tr}\left[\hat{P}_m\hat{\rho}\right]} \tag{2.52}$$

Assume now, for example, that instead of measuring the state $|\psi\rangle$ one interacts the state in a unitary way with a number of ancilla photons and then measures only the ancillae. It can be shown that in this case measurements on the state $|\psi\rangle$ that go beyond simple projective measurements can be implemented [3]. In general, measurements only have to correspond to a set of Kraus operators $\{\hat{M}_m\}$ [31] that fulfill

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = \hat{\mathbb{1}} \tag{2.53}$$

and will leave the state post-measurement in

$$|\psi_m\rangle = \frac{\hat{M}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_m^\dagger\hat{M}_m|\psi\rangle}} \qquad \text{or} \qquad \hat{\rho}_m = \frac{\hat{M}_m\hat{\rho}\hat{M}_m^\dagger}{\mathrm{Tr}\left[\hat{M}_m^\dagger\hat{M}_m\hat{\rho}\right]} \tag{2.54}$$

The probability of a general measurement outcome can be written formally as

$$p(m) = \langle\psi|\hat{E}_m|\psi\rangle \qquad \text{or} \qquad p(m) = \mathrm{Tr}\left[\hat{E}_m\hat{\rho}\right] \tag{2.55}$$

and thus a set of operators that satisfies

$$\hat{E}_m \succeq 0 \qquad \text{and} \qquad \sum_m \hat{E}_m = \hat{\mathbb{1}} \tag{2.56}$$

suffices. These are called POVM elements [23, Ch. 2].

## 2.5 Circuits with measurement-induced nonlinearity

In the previous section, Sec. 2.4, it was shown that measurement can be used to influence quantum states in a non-trivial way. There are many schemes in quantum information processing that rely on measurement for this reason. The type of circuit that is central to this thesis uses a set of detectors placed at the end of certain modes, and only those outcomes are considered where a well-defined pattern of detector clicks and no-clicks appears. Such a pattern is called a heralding pattern. This procedure allows one to perform a measurement without destroying the relevant state, in contrast to true post-selection. Of course, that means the scheme only succeeds probabilistically, as there will exist cases where the desired heralding pattern does not show.

The first circuit we shall consider, which is actually often summarized as a single gate, is a type of Bell-state measurement. As a gate, this circuit is called a Type-II fusion gate and can be used to implement teleportation [35] or entanglement swapping [36]; it is used in many areas of photonic quantum information [37, 35, 36]. The gate itself is depicted in Fig. 2.2.

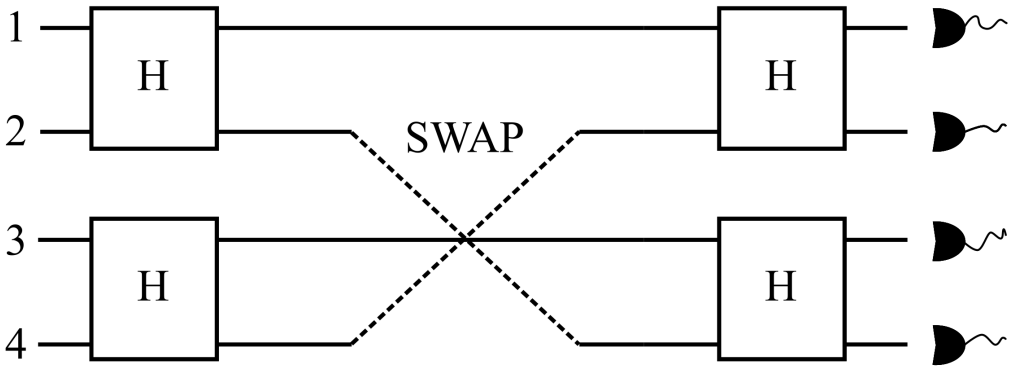


**Figure 2.2:** A Type-II fusion gate for dual-rail encoded qubits. The gate uses four Hadamards and a SWAP operation between modes 2 and 4 to implement a partial Bell-state measurement on two incoming dual-rail encoded qubits [38]. In the process, all photons entering the gate will be destroyed via measurement.
(Qubit encoding: modes 1 & 2 and 3 & 4.)

It acts on four modes, and uses four Hadamard gates and a SWAP / Pauli X operation

between modes 2 and 4. The SWAP operation simply forces a photon to change modes.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.57}$$

If the gate is implemented in the way Fig. 2.2 suggests, it expects dual-rail encoded qubits. Furthermore, by observing the detector click pattern, one can distinguish two out of the four entangled Bell states

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left( |1,0\rangle_{1,2}|1,0\rangle_{3,4} \pm |0,1\rangle_{1,2}|0,1\rangle_{3,4} \right), \tag{2.58}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left( |1,0\rangle_{1,2}|0,1\rangle_{3,4} \pm |0,1\rangle_{1,2}|1,0\rangle_{3,4} \right). \tag{2.59}$$

This succeeds with a probability of 50 % [39]. There are four possible heralding patterns that consist of exactly one click between mode 1 and 2, and exactly one click between mode 3 and 4 [38].

Since a variation of the protocol will be presented later in this thesis, let us next consider quantum teleportation via the use of a Type-II fusion gate. To that end, consider the setup depicted in Fig. 2.3.

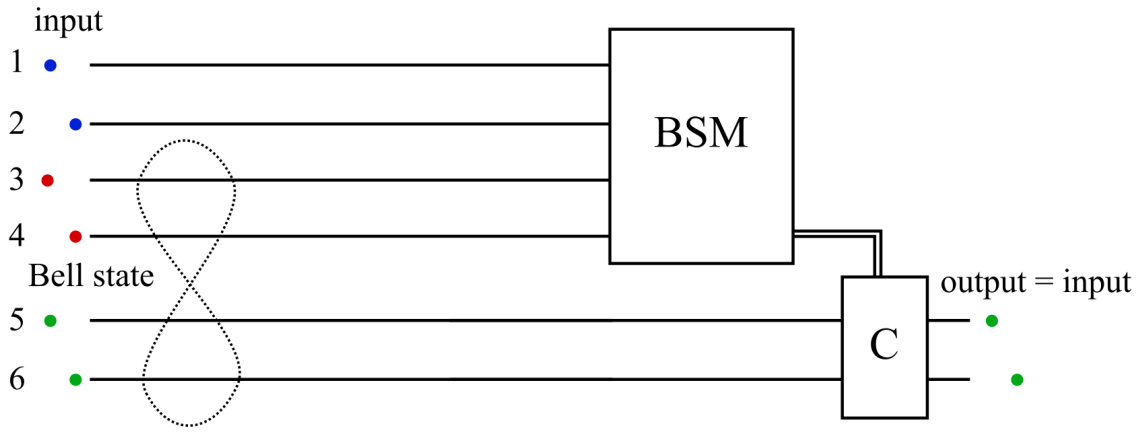


**Figure 2.3:** Quantum teleportation implemented with a Bell state measurement (BSM) and a feedforward correction (C) to boost the success probability. The circuit moves an unknown dual-rail encoded qubit $|\psi\rangle_{1,2}$ to different output modes, while preserving the superposition $|\psi\rangle_{5,6}$. The required resource is a Bell state, for example the maximally entangled two-photon state $|\Phi^+\rangle_{3,4,5,6}$. The different colors are used to showcase that the three photons involved in the protocol enter in superpositions across two modes each.

A dual-rail encoded qubit is incoming in modes 1 and 2

$$|\psi\rangle_{1,2} = \alpha|1,0\rangle_{1,2} + \beta|0,1\rangle_{1,2}. \tag{2.60}$$

As a resource, one uses the Bell state $|\Phi^+\rangle$, encoded between modes 3, 4, 5 and 6

$$|\Phi^+\rangle_{3,4,5,6} = \frac{1}{\sqrt{2}}\left(|1,0\rangle_{3,4}|1,0\rangle_{5,6} + |0,1\rangle_{3,4}|0,1\rangle_{5,6}\right). \tag{2.61}$$

The initial state will be a tensor product of the two. It is easy to show that after the fusion gate, and discarding all outcomes that did not yield the heralding pattern [click, no click, click, no click]$_{1,2,3,4}$ there will now be the same qubit encoded between modes 5 and 6

$$|\psi\rangle_{1,2} \otimes |\Phi^+\rangle_{3,4,5,6} \overset{\text{teleportation}}{\longrightarrow} |\psi\rangle_{5,6}. \tag{2.62}$$

Notice that it is necessarily comprised of a different photon that might even have a

spacelike separation from the original qubit photon. Yet, the qubit is moved onto new modes, while completely preserving the, in general, unknown coefficients $\alpha$ and $\beta$. For this reason, the described protocol is called quantum teleportation [40]. It is important to point out that since one needs to select on receiving a certain heralding pattern, this cannot be used to transmit information faster than light. Furthermore, the original state is destroyed, which is in line with the no-cloning theorem [41, 42], which says that quantum information cannot be copied. Finally, there exist four possible heralding patterns that have the potential to implement teleportation, but three require a feedforward correction operation on the output. The overall success probability will then be 50 % [37].

The concept of quantum teleportation requires entangled photons, which can only be made by overcoming a plethora of challenges. If we take a step back and assume that we only have standard single-photon sources and linear-optical elements, non-trivial operations are still possible by using ancillary modes and heralded measurement. A central example introduced by Knill, Laflamme, and Milburn (KLM) [4] is the nonlinear-sign (NS) gate, which implements

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \xrightarrow{\text{NS}} \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle. \tag{2.63}$$

Thus, it applies a $\pi$ phase shift only to the two-photon component. The gate is probabilistic and works by interfering the signal mode with ancilla modes prepared using single photons (and vacuum) and conditioning on a specific photon-counting outcome (heralding). Using NS gates as building blocks, one can construct probabilistic two-qubit entangling gates such as controlled-phase (CZ) and hence CNOT. This forms the basis for the first circuit investigated in this thesis (see Sec. 3 for details). More broadly, KLM showed that universal quantum computation is possible using only linear optics, single-photon sources, photon counting, and feedforward, with overhead that can be made polynomial in the problem size [43].

## 2.6 Loss and indistinguishability of photons

The technical implementation of any quantum information device will run into the challenge of imperfections in the underlying information carriers [39]. In the context of photons, one such issue is the potential loss of any photon. There are multiple reasons for photon loss, from imperfect sources, where a photon will not be produced in the

first place, to simple imperfections in the signal chain. In this thesis, loss-purification is investigated as a way to mitigate any of these cases. The emphasis of this consideration will be on protocols that use ancilla photons and measurement-induced nonlinearities. Unless explicitly mentioned otherwise, the detectors are assumed to be photon-number-resolving. Although the modeling of imperfect detectors is an important issue, where both false positives and false negatives can play a significant role in worsening the outcome of a given protocol [44, 45], we will focus mainly on the theoretical implications and limitations given by the quantum circuits themselves while assuming flawless detection.

The umbrella term of *loss-purification* is used to label distinct applications. Usually, the main interest lies in the purification of quantum states [6]. Existing schemes can also be found under the label of state amplification [6, 46]. Formally, this means that the state one wishes to purify will be a mixed state, which in the case of a qubit is given by

$$\hat{\rho}_{\text{in}} = (1 - P_{\text{signal loss}})\hat{\rho}_{\text{qubit}} + P_{\text{signal loss}}|0\rangle\langle 0| \tag{2.64}$$

Here $\hat{\rho}_{\text{qubit}}$ is the term describing the case where the photon is present, and the information is encoded correctly. On the other hand, $|0\rangle\langle 0|$ is a contribution where the photon used to encode the information is lost. What one tries to achieve in this context is to either suppress or remove $|0\rangle\langle 0|$ from the mixed state that will be the output of the protocol.

One could also consider the possibility of making the state robust against loss in the first place. Any such measures are, however, not the focus of this work. We refer to various schemes of error-correction and similar protocols that ensure that the information is robust against loss [47, 48]. For our consideration, we assume that the loss has already taken place.

In addition to state purification, one can also consider the task of purifying the simple presence of a photon against loss [49]. This is primarily relevant for photonic sources. The idea is similar to before, but will just be a single-photon state in a single mode. At first glance, one might point out that state purification completely encompasses this state-agnostic purification, because of this observation. There is however a crucial difference between the two when one considers the requirements for the resources: The schemes we consider will make use of ancilla photons, as they expand the range of theoretical possibilities. Since state-agnostic purification only purifies the presence of a photon, there would be no use in sacrificing lossless ancillae, as these could just be used

as signal photons in the first place. So any scheme that aims to achieve this (we will show that this is actually physically impossible) must also be robust against ancilla-loss. For state purification, this is not the case. Although it is definitely desirable to have a protocol that is robust against the loss of internal ancillae, there is still merit in a scheme that relies on lossless ancillae, as the aim is more than just the mere presence of a photon [6]. It is important to point out that by loss of ancilla photons we primarily mean that the photons are missing at the very start of the protocol. Although it is worthwhile to consider the effects of losing a photon during the protocol, we are mostly interested in the protocol's robustness against the full absence of any involved photon.

In addition to loss, another factor that determines the behavior of photons in an optical quantum circuit is their indistinguishability [5]. For fundamental particles to show any type of interference of their wave function, it is presupposed that they exhibit indistinguishability in any internal degree of freedom [50]. One can, even classically, demonstrate that photons of orthogonal polarization will not show interference fringes in a Michelson interferometer [51]. In addition to polarization, the indistinguishability of photons depends for example on their relative frequency and time of arrival at a certain optical element [52]. If one varies the relative time of arrival of two incoming photons, one can illustrate the Hong–Ou–Mandel dip, which stems from the fact that the anti-bunched terms only destructively interfere fully in the perfectly indistinguishable case. Photons with different times of arrival will not fully show this behavior [28].

To quantify indistinguishability independently of the degrees of freedom from which any distinguishability may arise, one constructs the distinguishability matrix $S$ which is defined as the wave function overlap between any two photons in the mode assignment list $[d_1, d_2, \ldots, d_N]_{1,2,\ldots,N}$, which specifies each photon's mode:

$$S_{ij} = \langle \psi_{d_i} \,|\, \psi_{d_j} \rangle \tag{2.65}$$

Heuristically, this can be understood by considering that $\langle \psi_i \,|\, \psi_j \rangle = 0$ if the two photons with indices $i$ and $j$ were perfectly distinguishable. In the case of a set of only distinguishable photons, $S$ reduces to the identity matrix. In contrast, for fully indistinguishable photons, $S_{ij} = 1 \; \forall i, j$. Numbers in between 0 and 1 quantify partial distinguishability between any two photons. It is important to note that not any such $S$ will be physical; it needs to be Hermitian, positive-semidefinite with ones on the diagonal [53, 54]. The introduction of $S$ serves a computational purpose. The transition

amplitude from Eq. 2.37 can be generalized by using a tensor permanent [53]:

$$\mathrm{perm}(W) = \sum_{\sigma,\rho \in S_N} \prod_{j=1}^{N} W_{\sigma_j,\rho_j,j} \tag{2.66}$$

Here, $W$ is given by

$$W_{k,l,j} = B_{kj} B^*_{lj} S_{lk} \tag{2.67}$$

and $B$ is simply the matrix obtained from the mode transfer matrix $U$ by choosing rows and columns corresponding to the input and output state, as specified in Sec. 2.2

$$B = U[m|n] \tag{2.68}$$

One then obtains the transition probability for partially distinguishable photons by taking

$$\mathrm{P}(m|n) \;=\; \frac{\mathrm{perm}(W)}{\prod_{i=1}^{M} n_i! \prod_{j=1}^{M} m_j!}. \tag{2.69}$$

The quantity that is obtained by Eq. 2.69 is not a complex transition amplitude anymore. It is a regular probability, because it encodes any combination of photons for the output state. In other words, although the photons have a fundamental distinguishability, it is assumed here implicitly in the formalism that we cannot distinguish between different configurations of them for practical reasons. There is no reason to assume that we care about distinguishing the photons at the output of the circuit. Distinguishability is something to be avoided, as we wish to purify against it. In successful indistinguishability purification, outcomes with the heralding pattern have an increased probability to correspond to indistinguishable photons. This can, for example, be done by making use of the HOM effect and using a cascade of Hadamard gates [5].

Finally, it should be pointed out exactly how indistinguishability affects the outcome statistics in boson sampling. The mere fact that the particles are indistinguishable means that terms containing creation operators can be combined beyond what is possible if each photon has a clear index [55, Ch. 2].

## 2.7 Existing purification schemes to mitigate photon loss

In this section, an overview of existing protocols is given that aims at clarifying terms and describing the similarities and differences between schemes that use ancilla photons and heralding to reduce the lossy component of an incoming mixed quantum state. In this context, loss is modeled as the absence of a photon prior to the protocol, which means it was already lost or never produced in the first place.

### 2.7.1 Loss-purification

The aim of perfect loss-purification is that for $N$ incoming photons, a certain heralding pattern is observed, where a single photon is left in an output mode and can now be assumed to be present for sure. For this reason, the term photon presence purification is used synonymously in this thesis. Loss-purification does not prefer any photon involved in the protocol. The heralding pattern must (in the case of perfect loss-purification) show if and only if all photons are present. This will be shown to be impossible. Imperfect loss-purification would just reduce the probability that the output photon is lossy. For this to be meaningful, it must be reduced below the value for the lowest-loss-photon present in the protocol, as otherwise we could just use said photon. The aim of true loss-purification is to use a set of lossy incoming photons to create a single photon that is either for sure present, if the flag given by the heralding pattern is shown, or at least present with truly improved probability. Since this essentially implements a heralded photonic source, it is of high interest for source architectures like quantum dots [56, 57]. The investigation of such schemes is the main focus of this thesis.

### 2.7.2 Quantum non-demolition measurement / detection

Quantum non-demolition measurement (QND) is, in general, used to obtain information about a quantum system without destroying some of the information that is stored in the system [6]. It can be used to signal the presence of a photon with the help of ancillae and a heralding pattern, without destroying the photon [49]. We will name these schemes state-agnostic QND protocols. These QND protocols are designed for specific photons entering the circuit in a certain mode, where a mixed state with loss is expected. All ancilla photons, however, are usually considered to be perfectly free of

loss in the literature when presenting how the protocol works in theory, although the impact of such lossy ancilla photons is sometimes also investigated.

Any practical implementation will suffer from ancilla loss, because ancilla loss can never be mitigated fully [49]. It is worth adding that some QND protocols also aim to remove higher photon-number states; this functionality is called quantum scissors [58].

### 2.7.3 Heralded state amplification / purification

Heralded state amplification (HA) or purification uses again ancilla photons and a heralding pattern to purify a state against loss [6]. The state, however, is now not just the $|1\rangle\langle 1|$ component of a mixed state, but rather a qubit state. If this state is encoded in single-rail, like in some proposed schemes, there is a natural limit coming from the fact that perfectly removing $|0\rangle\langle 0|$ from the incoming mixed state would destroy the qubit, since the logical 0 is encoded in the vacuum [59].

Usually, dual-rail qubits are considered where the presence of a photon in mode $A$ encodes the logical 0, and the presence of a photon in mode $B$ encodes the logical 1, such that

$$\alpha|0\rangle + \beta|1\rangle \equiv \alpha|1,0\rangle_{A,B} + \beta|0,1\rangle_{A,B}. \tag{2.70}$$

It is possible to build a state amplifier from two identical QND devices, if the QND device does not have ancilla leakage into the output mode in the absence of a heralding pattern. To achieve this, one must remove the which-path information of the two QNDs by introducing connections between the two. This has been proposed already, and shown to be possible with only two auxiliary photons [6].

State amplification treats the photons involved in the protocol asymmetrically. The incoming qubit photon is permitted to have a lossy component, while any auxiliary photons are assumed to be perfectly free of loss when presenting how the protocol works in principle. It is possible to make a perfect state purifier (i.e. one that completely removes the vacuum component from a dual-rail encoded single-qubit state part of a mixed state) with only two ancilla photons [6], assuming those are free of loss.

It is worth pointing out that QND and state amplification, if hypothetically achieved despite lossy ancillae, would mean that true loss-purification was possible. This is obvious for QND as the only difference is that the ancillae are allowed to be lossy in

QND, in contrast to general loss-purification. For state purification, the input qubit state $|1,0\rangle_{A,B}$ with $\beta = 0$ and $\alpha = 1$ corresponds to just a single photon in a mode that is purified against loss. Obviously, in this case heralded state amplification will become QND, and if done perfectly despite lossy ancillae, will imply true loss-purification. It thus follows by contraposition that if true loss-purification is impossible, the same is true for QND and heralded state amplification with lossy ancillae.

## 2.8 Numerical methods for optical quantum circuits

The problem of boson sampling is computationally expensive. If one aims to predict the workings of any linear-optics quantum circuit, one needs to calculate matrix permanents efficiently. Boson sampling is believed to be classically hard because its output probabilities are proportional to $|\operatorname{perm}(A)|^2$, and computing the permanent exactly is #P-hard. Aaronson and Arkhipov showed that if a classical computer could sample exactly from the boson sampling distribution in polynomial time, then the polynomial hierarchy would collapse to a low level, which is considered extremely unlikely. The polynomial hierarchy is a layered family of complexity classes that generalizes **P**, **NP**, and **coNP** by allowing polynomial-time algorithms to make a bounded number of alternations of existential and universal quantifiers (equivalently, access to **NP** oracles at increasing levels) [16].

The approach chosen in this thesis, which is considered among the fastest approaches [60], uses Ryser's algorithm implemented with Gray code ordering. Ryser's algorithm is used for permanent calculation of an $n \times n$ matrix $A$. It is based on inclusion–exclusion, where one calculates the product of sums of rows, where certain columns are deleted, specified by a set of indices $S$ that labels the columns which are kept

$$\operatorname{perm}(A) = (-1)^n \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} a_{ij}. \tag{2.71}$$

One then sums over these possible subsets of $\{1, \ldots, n\}$ while giving the terms a prefactor of 1 or -1, depending on the parity of the cardinality of $S$ [61]. If the sets $S$ are processed in an order where the difference between two consecutive sets can be specified by only one bit, the algorithm can be sped up further. This method of ordering binary numbers is referred to as Gray code [62]. The just presented version of the algorithm will take $\mathcal{O}(2^n n)$ operations to calculate the permanent $\operatorname{perm}(A)$ [63, 60].

# 3 Initial numerical considerations

In this work, we will arrive at a general theorem about loss-purification. To introduce the topic, the numerical results that motivated said theorem will be presented in this section. To perform the calculations, an object-oriented simulation package for Python was developed. Within this framework, one can test arbitrary circuits by passing matrices corresponding to the gates involved in the scheme and specifying the connections. Then, input/output states and post-selection conditions can be specified and the transition amplitudes will be calculated. The package can also be used to work with mixed states or partial distinguishability. The code alongside a more detailed description of its inner workings is available at [64]. It is based on an optimized permanent calculation with Ryser's algorithm and Gray-code ordering, as introduced in Sec. 2.8. To improve computational performance, a many functions are compiled directly in C using the numba framework [65, 66].

## 3.1 Investigation of a CNOT-based purification scheme

The initial hypothesis was that the circuit depicted in Fig. 3.1 might be potentially useful for loss or indistinguishability purification.

The circuit itself presents a possibility to implement a CNOT gate in the context of the KLM approach to quantum optical information processing. Here, measurement is used to herald a successful operation of the gate. Outcomes that do not include the desired heralding pattern are discarded. At the heart of this circuit are two nonlinear-sign gates (NS gates) each of which facilitates an operation that flips the sign of a two-photon state, while leaving the 0- and 1-photon state untouched.

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \xrightarrow{\text{NS}} \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle \tag{3.1}$$

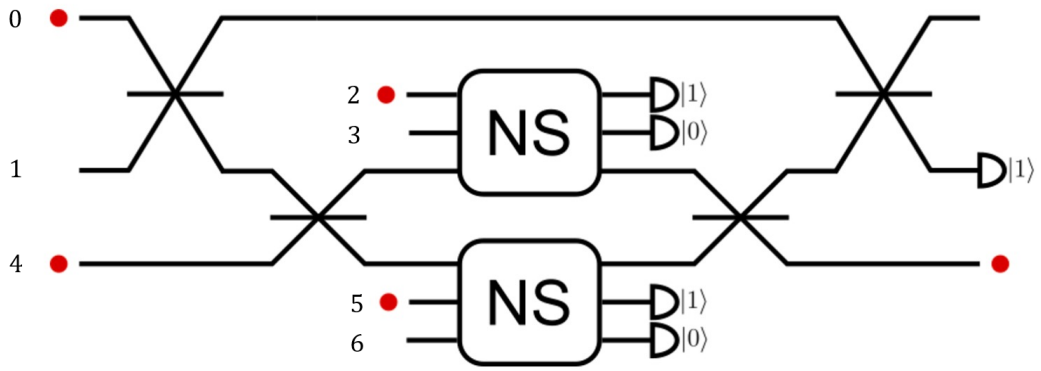


**Figure 3.1:** A KLM CNOT gate made using two NS gates [4]. All beam splitters are assumed to function as Hadamard gates. The circuit uses two ancilla photons in addition to a control and a target qubit photon. The target photon's logical states are encoded through its presence in either mode 0 or 1. For the control qubit, mode 4 corresponds to the logical 1 state. The control qubit's logical 0 state is the absence of the control photon, which can be modeled by moving it to an additional mode with mode label 7 (not shown in this illustration). The heralding pattern is given by the expected number of detector clicks, denoted by either $|0\rangle$ or $|1\rangle$. The detector at the end of mode 1 is not used in the CNOT gate, but will be used for the proposed purifier.

The NS gate does this by the use of ancilla photons and heralding [4].

To see why one might have hopes to use this setup for purification, it is instructive to consider how it implements a CNOT gate in the first place. For this, take the NS gates as black-box operations to obtain the result from Eq. 3.1. If the target and control photon are in their corresponding logical states 0 and 1 (modes 0 and 4), the Hadamard gates (simple beam splitters) will first put the target qubit in a superposition between modes 0 and 1, and the control qubit between modes 1 and 4. Now, due to the Hong–Ou–Mandel effect these photons bunch at the Hadamard gate right before the NS gates. The NS gates now invert the sign of the bunched states' phase. Because of this, the Hadamard following the NS gates does not conclude an identity operation, but rather a phase of $-1$ is left on this part of the superposition.

Now, since the target qubit is first put into a superposition where only a part goes to the NS gates, upon recombining these two parts, a photon will now be present in mode 1 and not the initial mode 0, because of the added phase. Thus, the target is moved to the logical state 1. If the target starts out in mode 1, a photon will end up in mode 0, by the same argument if the control is present. Now, if the control is not present / in it's logical 0 state, the NS gates will not impose a phase shift, and thus the lower

part of the circuit will become an identity operation. From this it immediately follows that the target qubit will just remain in whatever mode / logical state it was before the circuit. This is precisely what a CNOT gate does.

Next, we will move to purification: Consider the effect of adding a detector to mode 1, and only ever sending in target and control in modes 0 and 4. Assume the target and control qubit are potentially lossy, but the NS gates function perfectly as a black-box operation. If either target or control qubit was missing in the input, the detector in mode 1 would never click. This is because only if both photons are present at the same time, can they experience the phase shift that allows the superposition to recombine in such a way at the final Hadamard that a photon goes to the detector mode. Since the proper workings of the circuit require the HOM effect, one might find it desirable to investigate if this could be used for indistinguishability purification. Distinguishable photons will necessarily produce the anti-bunched outcome at the beam splitters, as they do not interfere with each other.

All this relies on the major assumption that the NS gates will not fail, neither if ancillae are lost nor if they have a degree of distinguishability to them. Notice however, that only a very specific type of failure would render this scheme undesirable: If an ancilla is lost, one of the photons must find a way into the ancilla detector, while at the same time another photon makes it to the detector in mode 1. A simulation of the circuit showed, however, that precisely this will indeed happen.

At first, the CNOT property of the circuit was probed. It showed the expected transmission amplitudes, which are depicted in Tab. 3.1.

| | $\|0,1\rangle$ | $\|0,0\rangle$ | $\|1,1\rangle$ | $\|1,0\rangle$ |
|---|---|---|---|---|
| $\|0,1\rangle$ | 0 | 0 | 0.25 | 0 |
| $\|0,0\rangle$ | 0 | 0.25 | 0 | 0 |
| $\|1,1\rangle$ | 0.25 | 0 | 0 | 0 |
| $\|1,0\rangle$ | 0 | 0 | 0 | 0.25 |

**Table 3.1:** Computationally obtained transition amplitudes of a KLM CNOT circuit for the four logical states spanned by the target and control qubit. The first bit is the target qubit, the second the control qubit.

Notice that we post-select on states that come with the correct heralding pattern at the NS gates' detectors.

Now, loss can be introduced by simply removing one photon after the other from the

calculation. Since the heralding pattern contains three clicks now (the detector in mode 1 is added for this attempt), the only possible states that could physically trigger the heralding pattern are those with either all four photons present, or any three of them. We are thus interested in the amplitudes $\langle \text{heralding pattern} \,|\, \text{one photon missing} \rangle$.

The obtained transition amplitudes are listed in Tab. 3.2. Some of the lossy states (the states where an ancilla photon, which are used for the NS gates, is missing) do indeed trigger the heralding pattern. This means that the circuit is not a viable candidate for (perfect) loss-purification.

| | $\lvert\text{heralding pattern}\rangle$ |
|---|---|
| $\lvert\text{target missing}\rangle$ | 0 |
| $\lvert\text{ancilla 1 missing}\rangle$ | -0.21 |
| $\lvert\text{control missing}\rangle$ | 0 |
| $\lvert\text{ancilla 2 missing}\rangle$ | 0.21 |

**Table 3.2:** Computationally obtained transition amplitudes for a KLM CNOT based loss-purification circuit. The heralding pattern consists of three clicks and two no-clicks. The original input state contains four photons, and for this calculation the results are obtained by leaving out either of those four.

Additionally, the circuits capabilities with respect to indistinguishability purification were probed. Numerically, one needs to resort to the formalism described in Sec. 2.6, with a generalized tensor permanent, in order to accurately represent (partial) distinguishability. One then obtains true probabilities instead of transition amplitudes.

If the matrix $S$ that quantifies how distinguishable any pair of photons are, is chosen to be the identity, it means that all photons are perfectly distinguishable. For this, one obtains the transition probabilities listed in Tab. 3.3.

A comparison between the values in Tab. 3.1 (taking the absolute value squared) and Tab. 3.3 shows that the circuit actually produces the heralding pattern with similar likelihood if the photons are distinguishable. Most importantly, the relevant element, we need for purification $[0,1] \longrightarrow [1,1] = 0.055$, while $|\langle 1,1 \,|\, 0,1 \rangle|^2 = 0.0625$ is only marginally larger. We can thus conclude that the circuit also fails as an indistinguishability purifier.

| | $[0,1]$ | $[0,0]$ | $[1,1]$ | $[1,0]$ |
|---|---|---|---|---|
| $[0,1]$ | 0.025 | 0 | 0.055 | 0 |
| $[0,0]$ | 0 | 0.021 | 0 | 0.047 |
| $[1,1]$ | 0.055 | 0 | 0.025 | 0 |
| $[1,0]$ | 0 | 0.047 | 0 | 0.021 |

**Table 3.3:** Computationally obtained transition probabilities of a KLM CNOT circuit for perfectly distinguishable photons. Inputs and outputs are the four logical states spanned by the target and control qubit. The first bit is the target qubit, the second the control qubit. While the photons are distinguishable fundamentally and will not interfere, we do not differentiate them when considering the outputs. Hence the numbers given in this table will be probabilities that encapsulate all arrangements of photons for a given output state and not complex valued amplitudes.

## 3.2 Additional attempts

Since the failure of the CNOT-based circuit as loss-purifier can be reduced to an issue with lossy ancillae, a plethora of enhancements and additional circuits were tested to mitigate this issue. None showed the desired behavior. It is not of any value to go deeper into the considerations regarding these additional circuits. There is, however, one peculiar property that always emerged, which is closely related to the general theorem we will derive in the next section and already hints at why such a circuit can never be constructed.

Many of these circuits featured tunable beam splitters, for which the settings to destructively interfere the problematic lossy state(s) away from at least one detector mode were analytically calculated. Curiously, at the exact settings where no lossy photonic state could trigger the heralding pattern, the heralding pattern would also disappear for the desired full photon state. This strongly hints at the fact that the transition amplitude of the full state's heralding pattern can be expressed as a weighted sum over something that is proportional to the lossy states' transition amplitudes. If all of these need to be 0, then so will the full, desired transition amplitude. In the next section, it will be shown that precisely this is the reason why all circuits that were considered had to fail.

# 4 Theoretical considerations for loss-purification

In state-agnostic loss-purification, the goal is to use a resource of lossy photons to obtain one photon in a heralded way. This photon must then either be present with certainty (perfect case) or with improved probability (imperfect case). In this section, it will be shown that both versions are impossible. We model loss as the absence of a photon before entering the circuit, and we assume all detectors to work flawlessly and are photon-number-resolving if necessary. We will show that even with these perfect resources such a circuit cannot be built.

## 4.1 Special case

To build up to a general theorem, let us consider a special case inspired by the circuit described in Sec. 3. In this special case, both input and heralding pattern consist of exactly one photon per mode. This allows us to illustrate both why such an attempt must fail, and also provides insights into how the boson-sampling amplitudes are calculated. Let us consider a formalized version of the circuit that was investigated numerically, which is depicted in Fig. 4.1.

This is described by $U$, a unitary $(m+n) \times (m+n)$ matrix. The relevant part with photon detection and photon input occurs in the upper $m$ modes. In the lower $n$ modes heralding on $|0\rangle$ may take place for any mode. The photons may have paths that lead through the lower $n$ modes, but no photons are directly input into these. The upper part of the circuit will be represented by a, in general, non-unitary $m \times m$ matrix $M$,

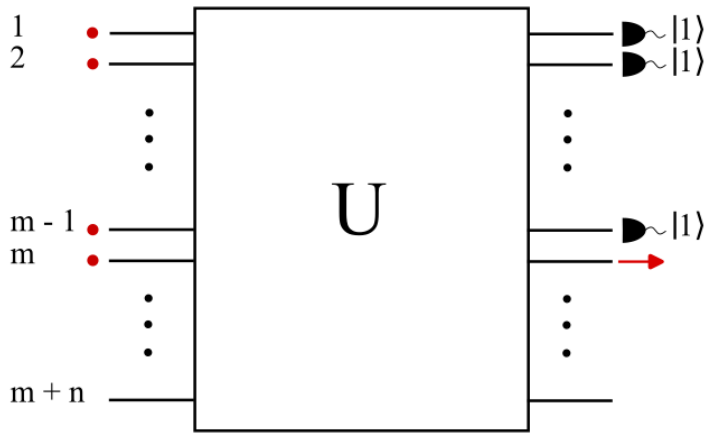


**Figure 4.1:** Loss-purification setup with a heralding pattern consisting of $m-1$ detector clicks, and a single signal photon exiting mode $m$. There are a total of $m$ photons used as input, and if all detectors click, there must be a photon in mode $m$. Conversely, if any photon goes missing, the heralding pattern must never show.

which must be a contraction on $\mathbb{C}^m$, such that it can be extended to a unitary [67, 68].

$$M = \begin{pmatrix} m_{11} & \cdots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{m1} & \cdots & m_{mm} \end{pmatrix} \tag{4.1}$$

If the circuit uses any measurement-induced nonlinearities, the measurements are moved to the end of the circuit and part of the $m-1$ detectors that signal the heralding pattern.

Let us consider ways in which a circuit might differ. One can always reorder the modes such that the click-modes are on top like in the setup we want to use, given that each input mode has a detector at the end. If, however, a photon would end up in a mode that does not have a detector, we can always deflect the photon with a Pauli X operation such that it goes from the original end position to the desired end position with detector. Modes without clicks or $|0\rangle$-detection can just be moved towards the bottom and are not relevant. Additionally, one can always place the mode that will contain the signal photon and no detector at position $m$. Finally, this allows us to only consider the upper $m \times m$ matrix that connects the input photons to the detectors.

This circuit can be thought of as providing the means to connect $m$ non-heralded sources to one heralded source by feeding them into a linear-optics circuit and using up $m-1$ photons for heralding. Furthermore, one could think of it as a conditioned demultiplexer that demultiplexes $m$ photons to a single photon, but only signals success if all photons were present.

**Claim: It is impossible to make the circuit from Fig. 4.1.**

With the setup established, we can ask the question of what loss-purification should do. We arrive at two statements that we will use in this proof:

1) If any of the $m$ photons went missing, the heralding pattern must be missing at least one detector click. This is equivalent to saying that if any photon is missing, you cannot have a photon in each of the $m-1$ upper modes in the end.

2) If all photons are present, it should be possible that all $m-1$ detectors click, and a photon must be in the lowest mode, mode $m$, if they do so. This is equivalent to saying that if all photons are present, there exists a possible outcome where one photon ends up in each of the $m$ modes.

The goal is now to express statements 1) and 2) in terms of the matrix $M$ and show that they cannot possibly be true at the same time. We will start by considering statement 1).

If any photon is missing, the output state with one photon in each of the upper $m-1$ modes must have a zero amplitude prior to detection. Otherwise the circuit can fail. Let us determine the amplitude of that state. The state itself is given by the sum of all products of creation operators where each mode is mentioned exactly once, because it must be equal to the heralding pattern up to a factor.

$$|\text{out}\rangle = c\,|\text{heralding pattern}\rangle = c\left(\prod_{i=1}^{m-1} a_i^\dagger\right)|0\rangle \tag{4.2}$$

Let us determine the coefficient $c$, which can be used to obtain the transition amplitude as $|c|^2$. The circuit acts upon the input in a linear way and transforms the creation operators as row vectors under $M$. The column $j$ of $M$ determines what happens to a

single photon / creation operator in mode $j$.

$$\left(a_1^\dagger, a_2^\dagger, \ldots, a_m^\dagger\right) \xrightarrow{M} \left(a_1^\dagger, a_2^\dagger, \ldots, a_m^\dagger\right) \begin{pmatrix} m_{11} & \cdots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{m1} & \cdots & m_{mm} \end{pmatrix} = \tag{4.3}$$
$$= \left(m_{11}a_1^\dagger + m_{21}a_2^\dagger + \cdots + m_{m1}a_m^\dagger,\ \ldots,\ m_{1m}a_1^\dagger + m_{2m}a_2^\dagger + \cdots + m_{mm}a_m^\dagger\right)$$

Since one of the photons is missing and we are interested in the amplitude of the state where all detectors would click, we can omit the last row of the matrix, because this row is responsible for sending photons to the lowest mode of $M$ (mode $m$) where no detector sits / where the signal should come out in the full input state case. If a photon is missing, it is impossible to have $m-1$ clicks and also a photon in this mode, as we only have $m-1$ photons in total.

We are thus left with an $(m-1) \times m$ matrix, without said last row. We will call that matrix $M'$. If photon $k$ is missing, it means that the corresponding input mode starts out empty. Hence, we can also ignore column $k$, which describes what happens to a photon as input in mode $k$. This leaves us with a square $(m-1) \times (m-1)$ matrix $M'_{-k}$, which written in terms of $M$'s original elements $m_{ij}$ looks like this:

$$M'_{-k} = \begin{pmatrix} m_{11} & \cdots & m_{1,k-1} & m_{1,k+1} & \cdots & m_{1m} \\ m_{21} & \cdots & m_{2,k-1} & m_{2,k+1} & \cdots & m_{2m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ m_{m-1,1} & \cdots & m_{m-1,k-1} & m_{m-1,k+1} & \cdots & m_{m-1,m} \end{pmatrix} \equiv (h_{ij})_{i,j \in \{1,\ldots,m-1\}} \tag{4.4}$$

Then, the amplitude of the unwanted pattern-compatible state is given by the sum of all products of creation operators, where each operator appears exactly once. The coefficients will be the products of matrix elements: Since each operator appears exactly once, we can only pick one number from each matrix column as we go down the rows. Example: if $M$ is $4 \times 4$, the reduced matrix $M'_{-k} \equiv (h_{ij})$ will be $3 \times 3$, and the element product $h_{12}h_{21}h_{33}$ would be a valid choice for the coefficient of one of the summands that lead to the final amplitude of the heralding pattern-state. $h_{12}h_{21}h_{32}$ would not be, because it contains the same column index, index 2, twice. Since these are permutations of the column index, the general expression is

$$|\text{out}\rangle = c \left( \prod_{i=1}^{m-1} a_i^\dagger \right) |0\rangle, \quad \text{where } c = \sum_{\sigma \in S_{m-1}} \prod_{i=1}^{m-1} h_{i,\sigma(i)} = \text{perm}(M'_{-k}) \tag{4.5}$$

The sum runs over the elements of the symmetric group $S_{m-1}$, to account for all permutations [69]. Notice that this is by definition $\mathrm{perm}(M'_{-k})$. If the amplitude to obtain the heralding pattern-state must be zero, then so must this permanent. One should mention that this is exactly what Eq. 2.37 yields, but motivated explicitly for the example we are currently considering. Our findings can be expressed more concisely:

**Theorem 1** *For loss-purification to be possible with the given m-photon setup described by the matrix $M$, the permanent* $\mathrm{perm}(M'_{-k})$ *must equal 0, regardless of which column $k$ is removed from $M'$. $M'$ is obtained from $M$ by removing the final row and $M'_{-k}$ is obtained from $M'$ by removing column $k$.*

Now we can move on to statement 2), which focuses on a loss-free input. In order to get each detector to click with a photon in the signal mode $m$, the output state with one photon in each of the $m$ modes must have a nonzero amplitude. Again, this is the sum of all products of creation operators where each mode appears exactly once. This time, we use the full matrix, as all photons are present and all modes must be reached. Now we want the amplitude to be nonzero to get the heralding pattern and the signal photon. In complete analogy to before, we find:

**Theorem 2** *For loss-purification to be possible with the given m-photon setup described by the matrix $M$, the permanent* $\mathrm{perm}(M)$ *must be nonzero.*

We will now show that Theorem 1 can never be fulfilled if Theorem 2 is fulfilled and vice versa. To that end, consider the Laplace expansion rule for permanent calculation [70]:

**Theorem 3 (Laplace expansion)** *Let $M \equiv (m_{ij})_{i,j\in\{1,\dots,m\}}$ be an $m \times m$ matrix.* $\mathrm{perm}(M)$ *can be calculated by expanding via any row $i$:*

$$\mathrm{perm}(M) = \sum_{j=1}^{m} m_{ij}\,\mathrm{perm}(M_{-i,-j}) \tag{4.6}$$

*Here $M_{-i,-j}$ is the matrix obtained from $M$ by removing row $i$ and column $j$.*

This means that we can expand $\mathrm{perm}(M)$ via the last row $m$ of $M$, where we need to

use the submatrices $M'_{-k}$ which miss the final row and column $k$.

$$\mathrm{perm}(M) = \sum_{k=1}^{m} m_{mk}\,\mathrm{perm}(M'_{-k}) \tag{4.7}$$

The permanent of $M$ must not be zero (Theorem 2), but the permanent of each of these submatrices $M'_{-k}$ must be zero (Theorem 1). It is impossible to have both at the same time, and thus loss-purification with 100% success probability is impossible for any circuit equivalent to the one depicted in Fig. 4.1.

□

## 4.2 General no-go theorem

The main objection to the previous result is that the heralding pattern could include some bunching. This would mean that at one or more of the detectors, multiple photons are incident, while at some other detector(s) no photons are present. Notice that this would still be a viable heralding pattern, and satisfy all criteria for a working loss-purification circuit. The outcome would be of the form represented in Fig. 4.2.

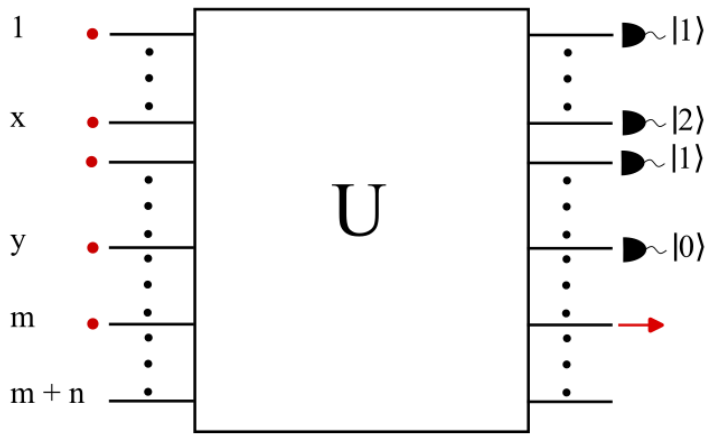


**Figure 4.2:** Illustration of a loss-purification circuit that produces a heralding pattern with bunching in mode $x$ and no photons in mode $y$. All other detector modes have a single photon in them. This is the simplest version of a circuit that has a possible heralding pattern that differs from the anti-bunched state. Bunching in more than one mode with more than two photons is also a possibility.

With the state being of the form

$$|\psi_{\text{herald}}\rangle = |1, \cdots, 2, \cdots, 0, \cdots, 1\rangle_{1,\cdots,x,\cdots,y,\cdots,m}. \tag{4.8}$$

Here, horizontal dots represent single-photon states for the remaining detectors. This state has a non-zero amplitude if it is indeed a possible outcome. It is important to add that this might not be the only possible heralding pattern. There could be a superposition of outcomes that would all be a viable heralding pattern. In this case, we just focus on one part of the superposition. We do not need to consider superpositions as ancillary inputs separately, because any superposition that is made with linear optics and measurement can be thought of as being made during the circuit operation.

Feedforward operations can be thought of as a larger circuit with many sub-circuits, where the particular sub-circuit that corresponds to the correct feedforward for a given measurement is chosen via post-selection [4]. In that sense, the argument presented here also covers such schemes.

Finally, it should be reiterated that the considerations in this section focus on all opportunities offered by linear optics and measurement-induced nonlinearities with ancilla photons, when we have a single state that might include some bunching in certain modes as input.

We will now build on the previous argument to obtain a general theorem that accounts for all feasible input states and heralding patterns. In general, the heralding pattern $|h\rangle$ may include any ordering of photons, with multiple photons in one mode and none in others. The same holds for the loss-free input state $|n\rangle$. The state $|h\rangle$ specifies the heralding pattern and one special mode where the signal photon is expected to exit the circuit.

Now, the transition amplitude that should be non-vanishing is given by

$$\langle h \,|\, \hat{U} \,|\, n \rangle \;=\; \frac{\operatorname{perm}(B)}{\sqrt{\prod_{i=1}^{m} h_i! \prod_{j=1}^{m} n_j!}} = N(h,n)\operatorname{perm}(B) \overset{!}{\neq} 0 \tag{4.9}$$

where $B$ is obtained by choosing certain rows and columns from the mode transfer matrix $M$, according to Eq. 2.37. This expression is nonzero if and only if the permanent is nonzero.

If the photon $l$ is lost, the input state $|n'_l\rangle$ and the matrix will be modified. The heralding pattern $|h'\rangle$ is still the same, but now there can no longer be a photon in the output mode. This means that the corresponding row can be removed from $B$, yielding $B'$. Additionally, if photon $l$ is missing, the number of times the corresponding column is selected to form $B$ decreases by one. We are thus left with a new matrix $B'_{-l}$, which also misses the column $l$ corresponding to the lost photon. The expression for the transition amplitude changes to

$$\langle h' \,|\, \hat{U} \,|\, n'_l \rangle \;=\; \frac{\mathrm{perm}(B'_{-l})}{\sqrt{\prod_{i=1}^{m} h'_i! \prod_{j=1}^{m} n'_j!}} = N'(h', n'_l)\,\mathrm{perm}(B'_{-l}) \overset{!}{=} 0,\ \forall l. \tag{4.10}$$

As a reminder, this must be zero to ensure the heralding pattern cannot show if any photon was missing. Since the normalization factor will always be greater than zero, this is zero if and only if $\mathrm{perm}(B'_{-l}) = 0,\ \forall l$. However, using Laplace expansion one obtains again

$$\mathrm{perm}(B) = \sum_{l=1}^{m} b_{m,l}\,\mathrm{perm}(B'_{-l}) \tag{4.11}$$

Here, the individual permanents $\mathrm{perm}(B'_{-l}) \overset{!}{=} 0,\ \forall l$, while $\mathrm{perm}(B) \overset{!}{\neq} 0$. These conditions cannot be fulfilled at the same time, and hence perfect loss-purification with linear optics, ancilla photons, and measurement-induced nonlinearities is impossible.

□

## 4.3 Bound

In the previous section, it was established that perfect loss-purification by means of linear optics, ancilla photons, and measurement-induced nonlinearities cannot be achieved. To gauge the potential usefulness of imperfect or partial loss-purification, a bound must be found that specifies how much a lossy mixed state could be purified in principle by using these resources. If it were possible for a circuit that achieves imperfect loss-purification to exist, there would still be merit in attempting to design one.

To that end, consider the following problem: An imperfect photon source $S$ produces the mixed state

$$\hat{\rho}_S = P_{\mathrm{success}}|1\rangle\langle 1| + P_{\mathrm{fail}}|0\rangle\langle 0|, \tag{4.12}$$

where a photon is either provided or not. The absence of the photon can be traced back to either the source never producing it, or the photon being lost before it arrived at the point where it was needed. We summarize these events by assigning the probability $P_{\text{fail}} = P_{\text{loss}}$ to the state $|0\rangle\langle 0|$. Due to normalization of mixed states, the ratio of successful photon provision to failed provision is given by

$$\frac{P_{\text{success}}}{P_{\text{fail}}} = \frac{1 - P_{\text{loss}}}{P_{\text{loss}}} = \frac{1}{P_{\text{loss}}} - 1. \tag{4.13}$$

If imperfect loss-purification was possible, there must be a way to improve this ratio. Assume we have access to a total of $m$ identical sources $S_i$, which share the failure probability specified by Eq. 4.12 and 4.13. Is it possible to use these, in addition to a linear-optics setup with measurement-induced nonlinearities, to obtain a single photon, conditioned on a heralding pattern, such that the posterior odds that the output photon is present given heralding are truly improved?

$$\text{FOM} = \frac{P'_{\text{success}}}{P'_{\text{fail}}} \overset{?}{\geq} \frac{1}{P_{\text{loss}}} - 1\,? \tag{4.14}$$

To that end, let us consider the figure of merit (FOM) for loss-purification of a single signal photon, and ignore no-loss false heralds as well as detector imperfections, as we can assume that the existence of those would only make the FOM worse. For simplicity, we assume that we add $m - 1$ extra sources (ancillae), and $m - 1$ detector clicks are used for the heralding pattern in the end. So there will be a total of $m$ photons. One of these photons is obtained as signal and should have an improved probability to be present. The updated figure of merit arises from the consideration of a mixed state that has a lossy part and a full photon part. The lossy part can be split up into $m$ contributions with exactly one photon missing (can potentially trigger the heralding pattern) and higher order (HO)-loss (physically impossible to trigger heralding pattern).

$$\hat{\rho}_{\text{total}} = P_{\text{full}}\hat{\rho}_{\text{full}} + P_{\text{lossy}}\hat{\rho}_{\text{lossy}} + P_{\text{HO-loss}}\hat{\rho}_{\text{HO-loss}} \tag{4.15}$$

Initially the probabilities are (ignoring higher order loss terms and normalization) given by

$$P_{\text{full}} = (1 - P_{\text{loss}})^m;\ P_{\text{lossy}} = P_{\text{loss}} \cdot (1 - P_{\text{loss}})^{m-1}. \tag{4.16}$$

After the circuit and disregarding all instances where the heralding pattern did not show, the state is

$$\hat{\rho}_{\text{out}} = P'_{\text{success}}|1\rangle\langle 1| + P'_{\text{fail}}|0\rangle\langle 0| \tag{4.17}$$

where

$$P'_{\text{success}} \propto P(\text{heralding pattern}|\text{ full input}) \cdot (1 - P_{\text{loss}})^m \tag{4.18}$$

and

$$P'_{\text{fail}} \propto P(\text{heralding pattern}|\text{ any lossy input}) \cdot P_{\text{loss}} \cdot (1 - P_{\text{loss}})^{m-1}. \tag{4.19}$$

The ratio of these can again be used to express the figure of merit, which should be maximized:

$$\text{FOM} = \frac{P'_{\text{success}}}{P'_{\text{fail}}} \tag{4.20}$$

Notice how building this ratio gets rid of any global factors of renormalization.

Consider what happens if the input state and the heralding pattern consist of general, in some modes bunched, input states. We will have to work with the matrix $B$ from Sec. 4.2. Furthermore, we still assume that the signal photon will exit the final mode alone, so it only contributes a factor of 1 in the normalization of Eq. 2.37. The inputs, however, can yield a different normalization factor depending on which photon is lost. This factor will be proportional to the loss-free case. In general

$$\langle h \,|\, \hat{U} \,|\, n \rangle \;=\; \frac{\text{perm}(B)}{\sqrt{\prod_{i=1}^{m} h_i! \prod_{j=1}^{m} n_j!}} = N(h,n)\,\text{perm}(B) \tag{4.21}$$

If any input photon from a bunched mode is missing, the normalization factor $N(h,n)$ changes to $N'(h,n') = N(h,n)\sqrt{n_l^{(\max)}}$ where $n_l^{(\max)}$ is the original occupation number of the mode with loss. The FOM can then be investigated by using again Laplace expansion of the permanent:

$$\begin{aligned}
\text{FOM} = \frac{P'_{\text{success}}}{P'_{\text{fail}}} &= \frac{P(\text{heralding pattern}|\text{ full input}) \cdot (1 - P_{\text{loss}})^m}{P(\text{heralding pattern}|\text{ any lossy input}) \cdot P_{\text{loss}} \cdot (1 - P_{\text{loss}})^{m-1}} \\
&= \frac{|N(h,n)\,\text{perm}(B)|^2 \cdot (1 - P_{\text{loss}})^m}{\sum_{k\in H} \left|N'(h,n_{-k})\,\text{perm}(B'_{-k})\right|^2 \cdot P_{\text{loss}} \cdot (1 - P_{\text{loss}})^{m-1}} = \\
&= \frac{\left|\sum_{k=1}^{m} m_{mk} (n_k^{(\max)})^{-\frac{1}{2}} N'(h,n_{-k})\,\text{perm}(B'_{-k})\right|^2}{\sum_{k=1}^{m} \left|N'(h,n_{-k})\,\text{perm}(B'_{-k})\right|^2} \cdot \left(\frac{1}{P_{\text{loss}}} - 1\right)
\end{aligned} \tag{4.22}$$

Here $H$ is the set of all lossy outcomes that can trigger the heralding pattern. If a certain lossy outcome cannot lead to the heralding pattern, the corresponding permanent will

be zero. However, since adding 0 to a sum does not change it, we can include these permanents to obtain the full sum over all $k$. Furthermore, we expanded the original normalization factor to write it via the $N'(h, n_{-k})$ from the lossy cases.

The factor on the right-hand side is a constant independent of the photon number $m$, only depending on the loss probability. We will ignore it for now. The permanents multiplied by $N'(h, n_{-k})$ will be some complex numbers $h_k$. The same holds for the elements $m_{mk}(n_k^{(\max)})^{-1/2}$ that appear as weights $w_k$ in this equation. We can make this a lot simpler:

Suppose we consider

$$R(h) \;=\; \frac{\left|\sum_{i=1}^{m} w_i\, h_i\right|^2}{\sum_{i=1}^{m} |h_i|^2}, \tag{4.23}$$

with fixed weights $w = (w_1, \ldots, w_m) \in \mathbb{C}^m$. This is the special case of a well-studied mathematical expression referred to as Rayleigh quotient [71].

Using the Cauchy–Schwarz inequality [72] (with the standard inner product $\langle x, y\rangle = \sum_i x_i \overline{y_i}$), we obtain

$$\left|\sum_{i=1}^{m} w_i h_i\right| = \left|\langle h, \overline{w}\rangle\right| \;\leq\; \|h\|_2\, \|\overline{w}\|_2 = \left(\sum_{i=1}^{m} |h_i|^2\right)^{1/2} \left(\sum_{i=1}^{m} |w_i|^2\right)^{1/2}. \tag{4.24}$$

Squaring both sides and dividing by $\sum_{i=1}^{m} |h_i|^2$ gives

$$R(h) \;\leq\; \sum_{i=1}^{m} |w_i|^2. \tag{4.25}$$

Therefore, the maximum is

$$\max_{h \neq 0} R(h) \;=\; \sum_{i=1}^{m} |w_i|^2. \tag{4.26}$$

Equality is attained precisely when $h$ is proportional to $\overline{w}$ [72], i.e.

$$h_i \;=\; \lambda\, \overline{w_i}, \qquad \lambda \in \mathbb{C}. \tag{4.27}$$

We know that the vector $h$ cannot be zero as we require at least one $h_i$ to be nonzero for the heralding pattern to show up in the lossless case (for this reason we are allowed to take the maximum over $h \neq 0$). If the matrix $M$ were required to be unitary, then

$$\max_{h \neq 0} R(h) \;=\; \sum_{i=1}^{m} |w_i|^2 \leq 1 \tag{4.28}$$

Because the $w_i$ are the elements of the matrix' last row multiplied by factors $(n_k^{(\max)})^{-1/2} \leq 1$, and the sum of absolute value squares of the elements in any given row must be 1 for unitary matrices. But $M$ must merely be a contraction on $\mathbb{C}^m$. To show that this does not change anything, let $A \in \mathbb{C}^{m\times m}$ be a contraction on $\mathbb{C}^m$, i.e. its operator norm satisfies [73]

$$\|A\|_2 \;\leq\; 1, \tag{4.29}$$

where the operator norm is defined as

$$\|A\|_2 \;:=\; \sup_{x\neq 0} \frac{\|Ax\|_2}{\|x\|_2}. \tag{4.30}$$

Denote the $j$-th row of $A$ by

$$r_j^\intercal \;=\; (a_{j1}, \ldots, a_{jm}). \tag{4.31}$$

For any $x \in \mathbb{C}^m$ with $\|x\|_2 = 1$, we have by definition of the operator norm

$$|r_j x| \;=\; |\sum_k a_{jk} x_k| \;=\; |(Ax)_j| \;\leq\; \|Ax\|_2 \;\leq\; \|A\|_2\, \|x\|_2 \;\leq\; 1. \tag{4.32}$$

Taking the supremum over all such $x$ gives

$$\|r_j\|_2 \;=\; \sup_{\|x\|_2=1} |r_j x| \;\leq\; 1. \tag{4.33}$$

Hence the squared $\ell^2$-norm of the $j$-th row satisfies (by using again the Cauchy–Schwarz inequality)

$$\sum_{k=1}^{m} |a_{jk}|^2 \;=\; \|r_j\|_2^2 \;\leq\; 1. \tag{4.34}$$

Therefore, the maximum possible value of the sum of squared absolute values in a row of a contraction matrix is

$$\max_j \sum_{k=1}^{m} |a_{jk}|^2 \;\leq\; 1. \tag{4.35}$$

From this it follows that the expression from Eq. 4.23 is bounded from above by 1. Finally, this means that the best possible loss-purification protocol can achieve a figure of merit independent of photon number of

$$\mathrm{FOM}_{\max} = \frac{1}{P_{\mathrm{loss}}} - 1 \tag{4.36}$$

This is equivalent to the initial ratio for just one imperfect source. It is thus shown that loss-purification, even done imperfectly, is not useful, as it cannot beat just leaving the photon alone. If the ancillae had a different (lower) probability $P_{\text{loss ancilla}}$ of being lost, the outcome would, by the same argument, be bounded by a new, better ratio obtained from ancillae with lower loss.

$$\text{FOM}_{\text{max}}^{\text{ancillae different}} = \frac{1}{P_{\text{loss ancilla}}} - 1 \tag{4.37}$$

But in such a case, one could just use the lowest-loss ancilla photon and not bother building a proper circuit.

## 4.4 Situating existing work on QND

In the literature, there exist proposals for circuits which perform state-agnostic QND using ancilla photons [49, 74]. Within the resource model considered here (linear optics & heralding, no state preservation required), a state-agnostic photonic QND does not increase the confidence of photon presence beyond what can be achieved by straightforward detect-and-reprepare using the same quality sources. If the ancillae are lossy with $P_{\text{loss ancilla}}$, one can be at best as sure about the photon being present upon successful herald, as one would be when just forwarding one of these ancillae upon registering a click associated incoming photon. However, it is important to point out that the preservation of coherence between multi-photon states [74], for example, could be of interest, making these protocols potentially relevant for different applications. Furthermore, under certain conditions (see Sec. 2.7.3) even true state-agnostic QND devices without additional functionality can be extended to perform state amplification [6].

Finally, the weakness of these schemes with respect to lossy ancilla photons can be mitigated by using an entangled resource. Kok, Lee, and Dowling pointed this out already, and proposed that using SPDC to generate ancilla photons will vastly improve the robustness of the protocol [49]. The reason for this is that the physical conservation laws underpinning SPDC forbid the source from only creating one out of two ancilla photons [2]. In the next section, we will provide a circuit that makes use of this exact property to achieve heralded state-amplification.

# 5 State amplification

Since the aim of state amplification is to purify a qubit state against loss, the theoretical conclusions about the state-agnostic protocols, which were the main focus of this work, do not fully carry over. The main difference is that even lossy ancillae can be of use, as long as they increase the relative contribution of the qubit against $|0\rangle\langle 0|$ in the mixed state. We begin this consideration by investigating the best possible improvement that state amplification with lossy ancilla photons can bring. In order not to violate the bound from Sec. 4.3, the purification can only improve the state up to the level of ancilla loss:

$$\begin{aligned}\hat{\rho}_{\text{in}} &= (1 - P_{\text{signal loss}})\hat{\rho}_{\text{qubit}} + P_{\text{signal loss}}|0\rangle\langle 0| \\ &\xrightarrow{\text{purify}} (1 - P_{\text{ancilla loss}})\hat{\rho}_{\text{qubit}} + P_{\text{ancilla loss}}|0\rangle\langle 0| = \hat{\rho}_{\text{out}}\end{aligned} \tag{5.1}$$

This will lift the loss to the level of the ancilla loss, so it can be potentially useful in practice if one can make low-loss ancillae and the qubit comes through lossy channels. In that sense, the main use of the schemes we investigated would be to restore a state that is passed through a lossy channel with the help of low-loss ancilla photons. It is possible to design a circuit that uses two ancillae to achieve purification [6]. A numerical analysis of this circuit, replicating the findings from the aforementioned paper, will be given in Sec. 5.2.

## 5.1 State amplification with entangled resources

If one is not restricted to separable ancilla photons and can use entangled resource states, it is indeed possible to make a perfect purifier that is not susceptible to missing ancillae. This assumes, however, that the modes for the ancillae do not add loss, a real constraint that can never be fully removed. It is easy to see that quantum teleportation / Type-II

fusion/ a Bell-state measurement (BSM) can be used to build a purifier. Assuming the resource $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$ is available, one can do a BSM on the first particle and the incoming state one wishes to purify against loss. Upon successful heralding, the remaining half of the EPR pair will be left in the original state by quantum teleportation. If the original photon is lost, an idealized BSM / fusion operation with perfect detectors fails, since it requires two clicks, and thus the heralding pattern can only ever show if all photons are present. The protocol can be considered robust against events where an ancilla is missing at the source, because physical conservation laws restrict photon generation to cases where both parts of the Bell pair (or higher order terms) are created [44]. The sole presence of only one part of the ancilla-pair is not compatible with conservation of energy and momentum. It is, however, important to reiterate that this assumes loss-free channels for the Bell-state resource and ideal coupling to the entangled-photon source. It should also be mentioned that this allows for additional flexibility that would not be possible in the linear-optics case: The output photon and the incoming photon can be spacelike separated as well as distinguishable (they can have a different frequency), since this is possible in quantum teleportation under appropriate resources [75].

Building upon this, one can design a state-purifier that is in principle robust against any mechanism that would lead to incorrect heralding. The entirety of the scheme is depicted in Fig. 5.1, and photon-number-resolving detectors are assumed.

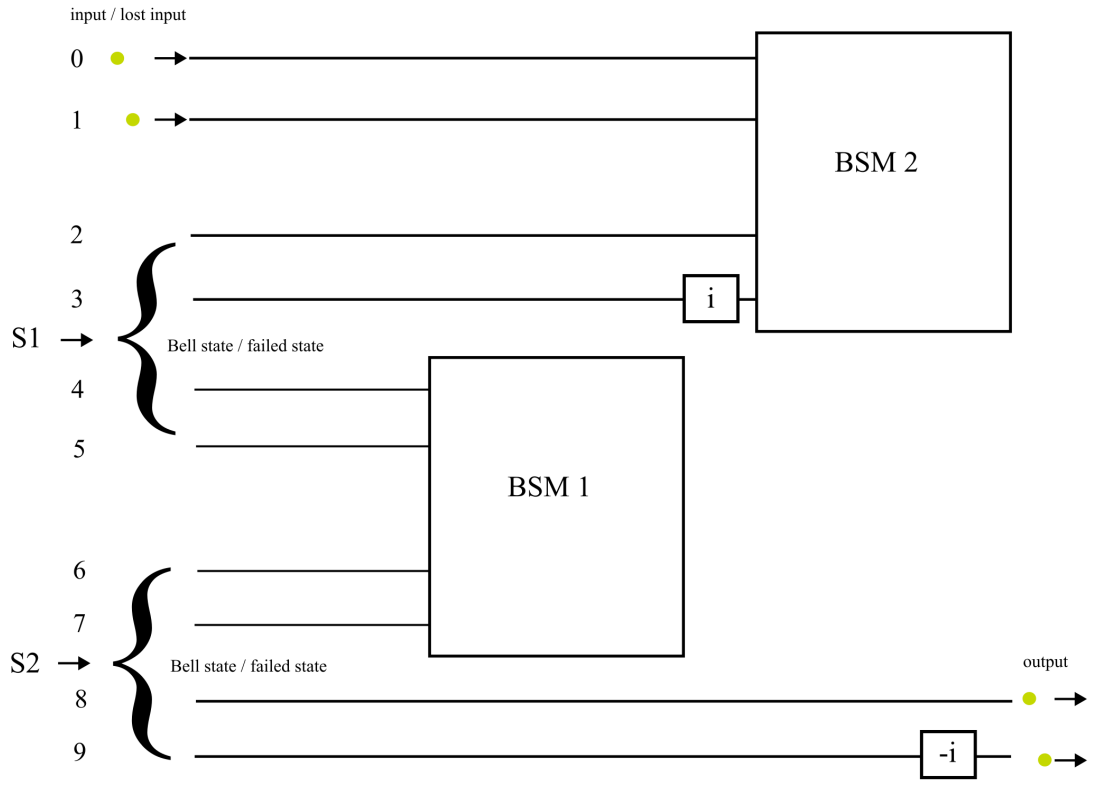


**Figure 5.1:** A state purifier which is in theory robust against any design-induced failure mechanism. The state is teleported from modes 1 & 2 to modes 8 & 9, by using two BSMs implemented via Type-II fusion gates. The sources S1 and S2 produce the Bell-state $|\Phi^+\rangle$. The construction with two BSMs and a phase shift in mode 3 ensures that a potential double pair generation can never trigger the heralding pattern. As a consequence a corrective phase shift is applied in mode 9. Potential feedforward operations to boost teleportation success are ignored.

Although this is in principle robust against the initial loss of the two ancilla photons that are used to make the resource state (two Bell pairs via SPDC [76]), it is important to note that there exists an additional way in which photon sources can behave in an undesired manner. If SPDC is used to generate a photon pair from either ancilla, there will be a non-zero probability that instead of two photons per ancilla, four will be created [77].

$$|\text{double pair}\rangle = \frac{1}{2}([2,2,4,4] + [3,3,5,5] + 2[2,3,4,5]) \tag{5.2}$$

These cases need to be considered since they may lead to incorrect heralding. Consider,

for example, that source 1 produces two pairs instead of one, while source 2 does not produce anything. The first BSM can be triggered by two of the photons, while the second BSM can be triggered by the other two. In this case, neither an initial state nor an output are present upon receiving the correct heralding pattern. To remove this failure mechanism, a $\frac{\pi}{2}$ phase shifter is added in mode 3. In the aforementioned case of source 1 generating a double pair, it will be left in the state

$$|\text{double pair}\rangle \overset{\text{BSM 1}}{\longrightarrow} \frac{1}{\sqrt{2}}([2,2]-[3,3]) \overset{\frac{\pi}{2}\text{phase shift}}{\longrightarrow} \frac{1}{\sqrt{2}}([2,2]+[3,3]) \tag{5.3}$$

after the initial BSM and the phase shifter. This state is now an eigenstate of the Hadamard gate. Because of this, it cannot trigger the heralding pattern in the second fusion gate, since both photons will either be swapped or none. The fusion gate requires exactly one photon in each half of the gate for one of the correct click patterns to occur (see Sec. 2.5). In order to correct the output state, a $-\frac{\pi}{2}$ phase shifter is added in mode 9. If source 2 were to produce the faulty two-pair state, it is not possible to get the heralding pattern. BSM 1 requires exactly two clicks, so source 1 cannot yield photons in this case. But then BSM 2 will be missing at least one click, as only the input state could be present. Thus, this protocol can be used to perform theoretically perfect state amplification against loss. The entanglement swapping stage BSM 1 can be implemented in a multiplexed fashion [78]. For the previously discussed reason, sometimes the heralding pattern will be triggered by a double-pair event. To obtain an estimate for the success probability of the entire protocol, consider that a single SPDC source approximately generates the state

$$|\text{SPDC}\rangle = Z|0,0\rangle + p|1,1\rangle + p^2|2,2\rangle + \mathcal{O}(p^3), \tag{5.4}$$

under perturbative expansion [79], where $p < 1$ and $Z$ can be obtained from normalization and the geometric series as

$$Z = \frac{2p-1}{p-1}. \tag{5.5}$$

Notice that we switch back to Fock-space formalism here, and only consider that there are two possible modes the newly generated photons can go to. When implementing this circuit, however, the setup must be chosen such that the photon-number state $|1,1\rangle$ produced by one of the sources is actually the Bell state we wish to use as a resource. There exist ways to achieve this [76]. As a consequence, one will find that the higher-order terms in Eq. 5.4 will also be in a superposition. For example, if the state associated with $|2,2\rangle$ were produced by source $S_1$, it would actually be given by the state $|\text{double pair}\rangle$ we presented using index notation in Eq. 5.2. Yet, to obtain the

success probability of the first BSM, it is sufficient to only consider photon number.

Assuming no coherence between the two sources and different photon-number states, the sources $S_1$ and $S_2$ will produce states of the form $\hat{\rho}_{N_1,N_2}$, where $N_i$ specifies the number of photons obtained from source $S_i$. The total state will thus be given by

$$\hat{\rho}_{S_1,S_2} = Z^2\hat{\rho}_{0,0} + Zp(\hat{\rho}_{0,2} + \hat{\rho}_{2,0}) + p^2(\hat{\rho}_{4,0} + \hat{\rho}_{0,4} + \hat{\rho}_{2,2}) + \mathcal{O}(p^3). \tag{5.6}$$

Notice that only terms belonging to $p^2$ can trigger the heralding pattern, as two photons have to enter the fusion gate to trigger the pattern, and because of the design of the circuit only half of the photons associated with a single source will enter the gate. This means that upon receiving the heralding pattern from stage BSM 1, there is a $33.\overline{3}\,\%$ probability that the sources produced the correct state. The other two cases will be removed by the second BSM stage. There exist four possible heralding patterns for the second fusion measurement with a success probability of 50 % (assuming phase correction) [80]. Together, this yields the maximal total success probability of $P_{\text{succ}} = 16.\overline{6}\,\%$ for the entire protocol. This bound can be approached by actively multiplexing the first BSM stage.

Finally, if the original state is part of a mixture with a two-photon-component [58], additional ways that would break the scheme exist, because it can also trigger the BSM on its own. Furthermore, photons might be lost at any stage of the circuit, which could be investigated further to gauge the robustness of this scheme against realistic loss mechanisms. Any two photons that are expected to enter a fusion gate together must be indistinguishable, otherwise teleportation will not work because the polynomial of creation operators does not simplify. Nevertheless, using entangled photons can potentially be more promising than regular single-photon sources due to the increased flexibility that comes with teleportation, and the heralded source behavior that mitigates the inevitable susceptibility to a missing ancilla photon.

## 5.2 State amplification without an entangled resource

In this section, a brief numerical investigation of a promising scheme to purify a photonic dual-rail qubit state against loss is given. Pitkanen et al. presented a circuit that uses two ancilla photons as well as an analysis of its performance [6]. Here, we repeated the analysis to replicate their findings and confirm the results numerically. The circuit is

depicted in Fig. 5.2.

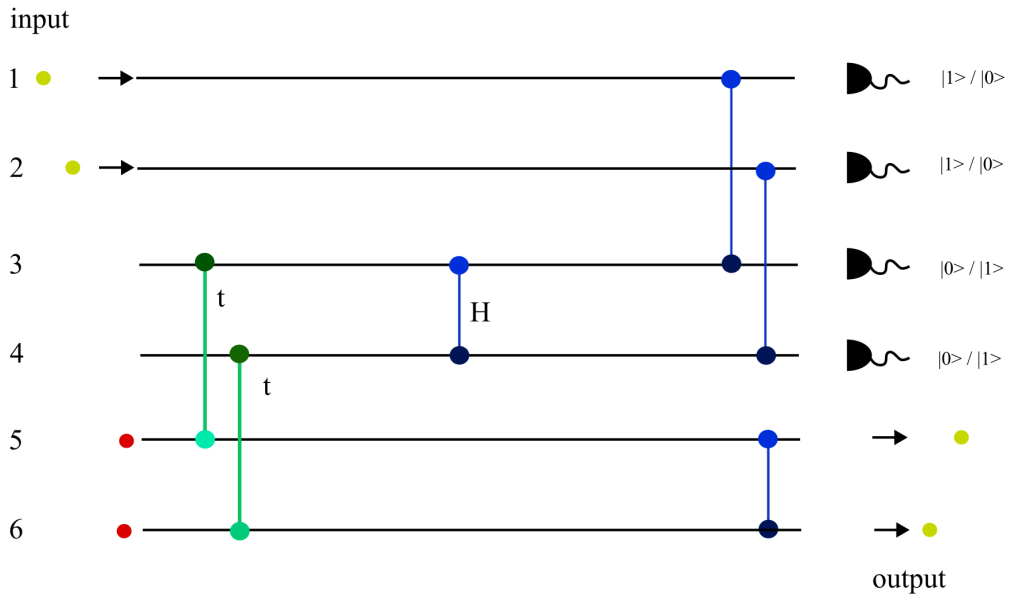


**Figure 5.2:** Heralded state amplification circuit proposed by Pitkanen et al. [6]. The circuit requires two ancilla photons in order to purify a dual-rail qubit against loss. It features two adjustable beam splitters with transmissivity $t$, and four beam spitters that are set to resemble a Hadamard gate. There exist four possible heralding patterns, three of which would require a feedforward correction to restore the state.

There are four heralding patterns which can be combined to give a total success probability of 25 % when the two tunable beam splitters are assumed to function as Hadamard gates. This assumes that one can perform the required phase correction on the output state. Furthermore, the circuit will remove HOM-type input states, but can fail for the anti-bunched two-photon input $|1,1\rangle_{1,2}$. This state can be asymptotically damped by tuning the beam splitters, at the cost of a vanishing success probability. Loss of either ancilla photon cannot be excluded by the heralding pattern. This circuit is a resource-efficient representative for loss-purification with linear optics, ancilla photons and measurement-induced nonlinearities. The two ancilla photons can be obtained from a simple single-photon source. Their states are simply $|1\rangle$. Ultimately, it is sensitive to ancilla loss. Pitkanen et al. propose, however, using SPDC sources in order to generate ancilla photons in a heralded way. This results in advantages similar to the ones described in Sec. 5.1.

# 6 Indistinguishability purification with two photons

It was experimentally demonstrated by Faurby et al. that a Hadamard gate can be used to purify the indistinguishability of two photons [5]. To that end, consider the following ratio of probabilities to obtain distinguishable / indistinguishable photons by post-selecting on events where both photons exit the same mode:

$$\frac{P(\psi_{dist})}{P(\psi_{indist})} = \frac{P(|1,0\rangle_{\gamma_1}|1,0\rangle_{\gamma_2})}{P(|2,0\rangle)} = \frac{\frac{1}{4}}{\frac{1}{2}} = 0.5 \tag{6.1}$$

A lower ratio would improve the scheme. Here, a brief analytical investigation of any circuit that uses two photons and potentially $|0\rangle$-detection is given, and it will be shown that one cannot improve beyond this.

## 6.1 Ratio for bunched states without post-selection

Consider any setup described by an $n \times n$ unitary transfer matrix $U$. We will only consider the effects on the first two modes, as the scheme for indistinguishability purification would send one photon into each of these input modes, and then also consider these as output modes. For that reason, the matrix $M$ acting on this reduced $2 \times 2$ subspace does not have to be unitary. It is only important that it can be extended to a unitary matrix by adding more dimensions. This is in general only possible if $M$ is a contraction on $\mathbb{C}^2$ [67]. Let $M$ be given by

$$M = \begin{pmatrix} k & l \\ m & n \end{pmatrix}, \; k,l,m,n \in \mathbb{C}. \tag{6.2}$$

We will look at the ratio $\frac{P(\psi_{dist})}{P(\psi_{indist})}$ which refers to the ratio of probabilities for a chosen output of indistinguishable photons and fully distinguishable photons. Concretely, the possible output states for a two-photon input after any two-mode interferometer are

$$|\Phi_{indist}\rangle = x_1|2,0\rangle + y_1|1,1\rangle + z_1|0,2\rangle \tag{6.3}$$

for the indistinguishable case, and

$$|\Phi_{dist}\rangle = x_2|1,0\rangle_{\gamma_1}|1,0\rangle_{\gamma_2} + y_{21}|1,0\rangle_{\gamma_1}|0,1\rangle_{\gamma_2} + y_{22}|0,1\rangle_{\gamma_1}|1,0\rangle_{\gamma_2} + z_2|0,1\rangle_{\gamma_1}|0,1\rangle_{\gamma_2} \tag{6.4}$$

for the perfectly distinguishable case with photons $\gamma_1$ and $\gamma_2$. Let us, without loss of generality, choose the state where both photons bunch in the upper mode to cover the case of bunching:

$$\frac{P(\psi_{dist})}{P(\psi_{indist})} = \left|\frac{x_2}{x_1}\right|^2 \tag{6.5}$$

The matrix $M$ transforms the modes as row vectors:

$$(a_0^\dagger, a_1^\dagger) \xrightarrow{M} (ka_0^\dagger + ma_1^\dagger,\, la_0^\dagger + na_1^\dagger) \tag{6.6}$$

The input states will thus be transformed according to

$$|1,1\rangle = a_0^\dagger a_1^\dagger|0\rangle \xrightarrow{M} (ka_0^\dagger + ma_1^\dagger)(la_0^\dagger + na_1^\dagger)|0\rangle \tag{6.7}$$

$$|1,0\rangle_{\gamma_1}|0,1\rangle_{\gamma_2} = a_0^\dagger b_1^\dagger|0\rangle \xrightarrow{M} (ka_0^\dagger + ma_1^\dagger)(lb_0^\dagger + nb_1^\dagger)|0\rangle. \tag{6.8}$$

This means

$$x_1|2,0\rangle = kl(a_0^\dagger)^2|0\rangle = \sqrt{2}kl|2,0\rangle \tag{6.9}$$

and

$$x_2|1,0\rangle_{\gamma_1}|1,0\rangle_{\gamma_2} = kla_0^\dagger b_0^\dagger|0\rangle = kl|1,0\rangle_{\gamma_1}|1,0\rangle_{\gamma_2}. \tag{6.10}$$

If $M$ is properly chosen, the full state will be normalized correctly when considering the full unitary $U$ and all additional modes. This allows us to not consider normalization at this point, because it is implicit in a proper choice of $M$ as contraction on $\mathbb{C}^2$, and we neglect any post-selection in this first section. So crucially,

$$\frac{P(\psi_{dist})}{P(\psi_{indist})} = \left|\frac{x_2}{x_1}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}, \tag{6.11}$$

because the only difference between $x_1$ and $x_2$ is that in the indistinguishable case the

same creation operator $a_0^\dagger$ appears for both photons, leading to an additional factor of $\sqrt{2}$, which does not appear in the distinguishable case. But since all other coefficients are exactly equal, this ratio will never depend on the matrix elements / beam-splitter settings.

## 6.2 Ratio for anti-bunched states without post-selection

The state with one photon in either mode is more interesting at first glance, because it holds for complex numbers [72] that

$$|kn + ml|^2 = |kn|^2 + |ml|^2 + 2\Re\{kn \cdot \overline{ml}\}. \tag{6.12}$$

If we cannot distinguish between $|1,0\rangle_{\gamma_1}|0,1\rangle_{\gamma_2}$ and $|0,1\rangle_{\gamma_1}|1,0\rangle_{\gamma_2}$, the ratio for this state will be

$$\frac{P(\psi_{dist})}{P(\psi_{indist})} = \frac{|y_{21}|^2 + |y_{22}|^2}{|y_1|^2} = \frac{|kn|^2 + |ml|^2}{|kn + ml|^2} = \frac{|kn|^2 + |ml|^2}{|kn|^2 + |ml|^2 + 2\Re\{kn \cdot \overline{ml}\}}. \tag{6.13}$$

This expression is minimized when the real part in the denominator is maximized. For this reason, the problem can be restated as

$$\begin{aligned} \min_{a,b\in\mathbb{R}}\{\frac{a^2+b^2}{(a+b)^2}\} &= \min_{a,k\in\mathbb{R}}^{a\neq 0}\{\frac{a^2+(ka)^2}{(a+(ka))^2}\} \\ &= \min_{a,k\in\mathbb{R}}^{a\neq 0}\{\frac{a^2(1+k^2)}{a^2(1+k)^2}\} \\ &= \min_{k\in\mathbb{R}}\{\frac{(1+k^2)}{(1+k)^2}\} = \frac{1}{2}. \end{aligned} \tag{6.14}$$

Thus we can conclude that using the anti-bunched state also cannot improve upon a simple Hadamard gate and bunched states.

## 6.3 With post-selection

Post-selection breaks one crucial step in the argument above. If we renormalize the states from Eq. 6.7, the distinguishable and indistinguishable case will get a different overall factor. This is due to the fact that we again have $|kn|^2 + |ml|^2$ vs $|kn + ml|^2$,

and also that parts of the indistinguishable probabilities get a factor of 2. So, the natural question to ask is whether this can be used to gain an advantage. In this context, post-selection means that we can use any linear-optics circuit and $|0\rangle$-detection (heralding on no-click events) such that the equivalence class of the two-photon quantum state is altered [18]. We investigate the ratio

$$\frac{P(\psi_{dist})}{P(\psi_{indist})} = \frac{\frac{P(|x,y\rangle_{\gamma_1}|y,x\rangle_{\gamma_2})}{N'^2}}{\frac{P(|a,b\rangle)}{N^2}};\ x,y \in \{0,1\},\ x+y=1 \text{ and } a,b \in \{0,1,2\}, a+b=2 \tag{6.15}$$

Here, the probabilities $P(|x,y\rangle_{\gamma_1}|y,x\rangle_{\gamma_2})$ and $P(|a,b\rangle)$ are taken from the transformed state without post-selection and renormalization. The normalization factors are thus obtained by ignoring the additional modes from the larger unitary $U$ and focusing on the $M$ subspace:

$$N = \sqrt{2|kl|^2 + |kn+ml|^2 + 2|mn|^2} \tag{6.16}$$

and

$$N' = \sqrt{|kl|^2 + |kn|^2 + |ml|^2 + |mn|^2} \tag{6.17}$$

The factor of 2 comes from the square of the creation operator. The question of whether post-selection can improve the ratios is then restated as whether

$$\left(\frac{N}{N'}\right)^2 = \frac{2|kl|^2 + |kn|^2 + |ml|^2 + 2|mn|^2 + 2\Re\{kn\cdot\overline{ml}\}}{|kl|^2 + |kn|^2 + |ml|^2 + |mn|^2} < 1 \tag{6.18}$$

is possible. This can, however, never be achieved for any $k,l,m,n \in \mathbb{C}$ . Recall

$$N^2 = 2|kl|^2 + |kn+ml|^2 + 2|mn|^2, \qquad N'^2 = |kl|^2 + |kn|^2 + |ml|^2 + |mn|^2. \tag{6.19}$$

Consider the difference

$$\begin{aligned} N^2 - N'^2 &= |kl|^2 + |mn|^2 + \left(|kn+ml|^2 - |kn|^2 - |ml|^2\right) \\ &= |kl|^2 + |mn|^2 + 2\Re\left\{kn\,\overline{ml}\right\}. \end{aligned} \tag{6.20}$$

Using $\Re\{z\} \geq -|z|$ for any $z \in \mathbb{C}$, we obtain

$$\begin{aligned} N^2 - N'^2 &\geq |kl|^2 + |mn|^2 - 2|kn|\,|ml| \\ &= |k|^2|l|^2 + |m|^2|n|^2 - 2|k||l||m||n| \\ &= \left(|k||l| - |m||n|\right)^2 \ \geq\ 0. \end{aligned} \tag{6.21}$$

Therefore $N^2 \geq N'^2$, i.e. $N \geq N'$, and consequently

$$\left(\frac{N}{N'}\right)^2 \geq 1. \tag{6.22}$$

Hence post-selecting on no clicks will only worsen the ratio in general. Generating random complex matrices and probing the ratios with the established numerical framework provides confirmation: Without post-selection, the bunched states' ratios are always 0.5. With post-selection, 0.5 is the lower bound. We can thus conclude that a simple Hadamard gate already saturates the bound for two-photon indistinguishability purification with the given resources.

# 7 Discussion and outlook

The theorem we found during this work provides a satisfying conclusion as to why it was impossible for us to design a circuit for photon presence purification with the considered resources. Nevertheless, real-world constraints can often go beyond the underlying assumptions of a model. In particular, we model loss as the absence of a photon at the start of the protocol. The effects of loss of any photon during operation might, however, also be of interest and could be investigated further, both in theory and for the circuits we considered. Furthermore, there exist many additional challenges when implementing quantum circuits. Detectors and optical elements have been assumed to function perfectly in these theoretical considerations, but one should also model imperfections of these technological components when fully evaluating the performance of a quantum circuit. It is, however, important to point out that any of these additional imperfections would only make the performance of a general loss-purifier we considered in Sec. 4 worse, and thus our theorem about the impossibility of constructing such a circuit is not weakened by real-world challenges. We were able to show that even in the ideal case there is no merit in building such a device.

The initial CNOT-based circuit was proposed in the context of quantum dots, for which it can be difficult to successfully feed photons into a circuit without loss, unlike SPDC. Therefore, throughout this work, we placed an emphasis on the problem of potentially lossy ancilla photons, which are not present at the very start of the protocol. It was proposed in multiple papers [49, 6] that the loss of ancilla photons can be mitigated by using SPDC to generate the ancilla photons. These sources can be advantageous when combating loss, since the absence of ancilla photons can be kept under better control, and we were able to show that this is the limiting factor in such protocols. It is crucial to point out that sources like quantum dots operate quasi-deterministically and on demand, which may appear similar to a heralded mode of operation at first glance. However, it is difficult to guarantee reliable photon delivery to the actual input of the circuit with these sources. This is often easier with SPDC, since one can place

the crystal such that failed coupling can be largely ruled out when heralding succeeds. This is precisely what is proposed in existing purification schemes that rely on ancilla photons [49, 6]. SPDC, however, brings its own drawbacks: It operates probabilistically and can generate higher-order terms, which we needed to deal with when designing the state-amplification protocol we proposed.

When presenting an estimate for the success probability of the proposed entanglement-based state amplifier, we relied upon a set of assumptions and approximations. First, we assumed that a single SPDC source approximately generates the state

$$|\mathrm{SPDC}\rangle = Z|0,0\rangle + p|1,1\rangle + p^2|2,2\rangle + \mathcal{O}(p^3). \tag{7.1}$$

Then, we assumed that the two sources are not driven coherently and there is no coherence between the different photon-number states, such that a mixed state can be used to express the joint state of the two sources. In practice, however, the sources can be driven coherently, for example by using the same laser as a pump for both crystals. If one aims to implement this protocol, there might be merit in repeating the analysis once a source architecture is specified. It might even be the case that modifications can be made to optimize the scheme for a given type of Bell-state source.

Finally, we provided a brief theoretical discussion about indistinguishability purification for two photons. One could build upon these considerations and establish a framework to arrive at general statements that situate potential circuits for indistinguishability purification.

# Bibliography


[1] M. D. Eisaman, J. Fan, A. Migdall, S. V. Polyakov. *Invited Review Article: Single-photon sources and detectors.* Review of Scientific Instruments **82** (2011) 071101.
doi:10.1063/1.3610677

[2] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, Y. Shih. *New High-Intensity Source of Polarization-Entangled Photon Pairs.* Physical Review Letters **75** (1995) 4337.
doi:10.1103/PhysRevLett.75.4337

[3] P. X. Chen, J. A. Bergou, S. Y. Zhu, G. C. Guo. *Ancilla dimensions needed to carry out positive-operator-valued measurement.* Physical Review A **76** (2007) 060303.
doi:10.1103/PhysRevA.76.060303

[4] E. Knill, R. Laflamme, G. J. Milburn. *A scheme for efficient quantum computation with linear optics.* Nature **409** (2001) 46.

[5] C. F. D. Faurby, L. Carosini, H. Cao, P. I. Sund, L. M. Hansen, F. Giorgino, A. B. Villadsen, S. N. van den Hoven, P. Lodahl, S. Paesani, J. C. Loredo, P. Walther. Purifying photon indistinguishability through quantum interference, 2025.
`https://arxiv.org/abs/2403.12866`

[6] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, N. Lütkenhaus. *Efficient heralding of photonic qubits with applications to device-independent quantum key distribution.* Phys. Rev. A **84** (2011) 022325.
doi:10.1103/PhysRevA.84.022325

[7] A. Einstein. *Zur Theorie der Lichterzeugung und Lichtabsorption.* Annalen der

Physik **325** (1906) 199.
doi:10.1002/andp.19063250613. Often cited as Ann. Phys. (4) 20 (1906) 199–206; EAP 259; CPE 2, 349

[8] F. Flamini, N. Spagnolo, F. Sciarrino. *Photonic quantum information processing: a review.* Reports on Progress in Physics **82** (2018) 016001.
doi:10.1088/1361-6633/aad5b2

[9] J. Wang, F. Sciarrino, A. Laing, M. G. Thompson. *Integrated photonic quantum technologies.* Nature Photonics **14** (2019) 273–284.
doi:10.1038/s41566-019-0532-1

[10] S. Slussarenko, G. J. Pryde. *Photonic quantum information processing: A concise review.* Applied Physics Reviews **6** (2019).
doi:10.1063/1.5115814

[11] M. Born, P. Jordan. *Zur Quantenmechanik.* Zeitschrift für Physik **34** (1925) 858.
doi:10.1007/BF01328531

[12] P. A. M. Dirac. *The Fundamental Equations of Quantum Mechanics.* Proceedings of the Royal Society of London. Series A **109** (1925) 642.
doi:10.1098/rspa.1925.0150

[13] P. A. M. Dirac. *The quantum theory of the emission and absorption of radiation.* Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character **114** (1927) 243.
doi:10.1098/rspa.1927.0039

[14] C. Fabre, G. Grynberg, A. Aspect. *Introduction to Quantum Optics: From the Semi-classical Approach to Quantized Light*, 2010.
doi:10.1017/CBO9780511778261

[15] C. C. Gerry, P. L. Knight. *Introductory Quantum Optics.* Cambridge University Press, 2005.

[16] S. Aaronson, A. Arkhipov. *The Computational Complexity of Linear Optics.* Theory of Computing **9** (2013) 143.
doi:10.4086/toc.2013.v009a004

[17] S. Scheel. Permanents in linear optical networks, 2004.
`https://arxiv.org/abs/quant-ph/0406127`

[18] A. P. Lund. *Classes of two-photon states defined by linear interactions and destructive two-photon quantum interference in a single mode.* Phys. Rev. A **92** (2015) 053844.
doi:10.1103/PhysRevA.92.053844

[19] A. M. Martins. Quantum Optics. `https://fenix.tecnico.ulisboa.pt/downloadFile/1689468335556599/Curso_OpticaQuantica_2014.pdf`, 2014. Lecture notes (Instituto Superior Técnico). Accessed: 2025-12-22.

[20] NumPy Developers. Indexing on ndarrays. `https://numpy.org/doc/stable/user/basics.indexing.html`. NumPy v2.4 Manual. Accessed: 2025-12-22.

[21] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O'Brien. *Quantum Computing* (2010).
doi:10.48550/arXiv.1009.2267. Early draft of Nature 464, 45–53 (2010), doi:10.1038/nature08812

[22] D. P. DiVincenzo. *The Physical Implementation of Quantum Computation* (2000).
doi:10.48550/arXiv.quant-ph/0002077. Published in Fortschritte der Physik (2000); related DOI: 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E

[23] M. A. Nielsen, I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[24] F. Bloch. *Nuclear Induction.* Physical Review **70** (1946) 460.
doi:10.1103/PhysRev.70.460

[25] P. W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM Journal on Computing **26** (1997) 1484–1509.
doi:10.1137/s0097539795293172

[26] C. H. Bennett, G. Brassard. *Quantum cryptography: Public key distribution and coin tossing.* Theoretical Computer Science **560** (2014) 7–11.
doi:10.1016/j.tcs.2014.05.025

[27] B. M. Terhal. *Quantum Error Correction for Quantum Memories.* Reviews of Modern Physics **87** (2015) 307.
doi:10.1103/RevModPhys.87.307. Free preprint: arXiv:1302.3428

[28] C. K. Hong, Z. Y. Ou, L. Mandel. *Measurement of subpicosecond time intervals between two photons by interference.* Physical Review Letters **59** (1987) 2044.
doi:10.1103/PhysRevLett.59.2044

[29] J. von Neumann. *Wahrscheinlichkeitstheoretischer Aufbau der Quantenmechanik.* Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1927** (1927) 245.

[30] F. A. Bovino, G. Castagnoli, A. Ekert, P. Horodecki, C. M. Alves, A. V. Sergienko. *Direct Measurement of Nonlinear Properties of Bipartite Quantum States.* Physical Review Letters **95** (2005) 240407.
doi:10.1103/PhysRevLett.95.240407

[31] K. Kraus. *General state changes in quantum theory.* Annals of Physics **64** (1971) 311.
doi:10.1016/0003-4916(71)90108-4

[32] A. Einstein, B. Podolsky, N. Rosen. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. **47** (1935) 777.
doi:10.1103/PhysRev.47.777

[33] J. S. Bell. *On the Einstein Podolsky Rosen paradox.* Physics Physique Fizika **1** (1964) 195.
doi:10.1103/PhysicsPhysiqueFizika.1.195

[34] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki. *Quantum entanglement.* Reviews of Modern Physics **81** (2009) 865.
doi:10.1103/RevModPhys.81.865

[35] A. Avanesov, A. Shurinov, I. Dyakonov, S. Straupe. *Building a fusion-based quantum computer using teleported gates.* Quantum **9** (2025) 1762.
doi:10.22331/q-2025-06-04-1762

[36] Y. Hasegawa, R. Ikuta, N. Matsuda, K. Tamaki, H.-K. Lo, T. Yamamoto, K. Azuma, N. Imoto. *Experimental time-reversed adaptive Bell measurement*

*towards all-photonic quantum repeaters*. Nature Communications **10** (2019) 378. doi:10.1038/s41467-018-08099-5

[37] A. Melkozerov, A. Avanesov, I. Dyakonov, S. Straupe. Analysis of optical loss thresholds in the fusion-based quantum computing architecture, 2024.

[38] D. Singh, A. P. Lund, P. P. Rohde. Optical cluster-state generation with unitary averaging, 2022.
`https://arxiv.org/abs/2209.15282`

[39] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, G. J. Milburn. *Linear optical quantum computing with photonic qubits*. Reviews of Modern Physics **79** (2007) 135.
doi:10.1103/RevModPhys.79.135. See discussion of the type-II fusion gate: projects onto one of two Bell states with success probability 1/2.

[40] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters. *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Phys. Rev. Lett. **70** (1993) 1895.
doi:10.1103/PhysRevLett.70.1895

[41] D. Dieks. *Communication by EPR devices*. Physics Letters A **92** (1982) 271.
doi:10.1016/0375-9601(82)90084-6

[42] W. K. Wootters, W. H. Zurek. *A Single Quantum Cannot be Cloned*. Nature **299** (1982) 802.
doi:10.1038/299802a0

[43] C. R. Myers, R. Laflamme. Linear Optics Quantum Computation: an Overview, 2005.
`https://arxiv.org/abs/quant-ph/0512104`

[44] R. H. Hadfield. *Single-photon detectors for optical quantum information applications*. Nature Photonics **3** (2009) 696.
doi:10.1038/nphoton.2009.230

[45] M. D. Eisaman, J. Fan, A. Migdall, S. V. Polyakov. *Invited Review Article: Single-photon sources and detectors*. Review of Scientific Instruments **82** (2011) 071101.

doi:10.1063/1.3610677

[46] N. Bruno, V. Pini, A. Martin, V. B. Verma, S. W. Nam, R. P. Mirin, A. E. Lita, F. Marsili, B. Korzh, F. Bussières, N. Sangouard, H. Zbinden, N. Gisin, R. Thew. *Heralded amplification of photonic qubits.* Optics Express **24** (2016) 125.
doi:10.1364/OE.24.000125

[47] M. Varnava, D. E. Browne, T. Rudolph. *Loss Tolerance in One-Way Quantum Computation via Counterfactual Error Correction.* Physical Review Letters **97** (2006) 120501.
doi:10.1103/PhysRevLett.97.120501

[48] T. C. Ralph, A. J. F. Hayes, A. Gilchrist. *Loss-tolerant optical qubits.* Physical Review Letters **95** (2005) 100501.
doi:10.1103/PhysRevLett.95.100501

[49] P. Kok, H. Lee, J. P. Dowling. *Single-photon quantum-nondemolition detectors constructed with linear optics and projective measurements.* Physical Review A **66** (2002).
doi:10.1103/physreva.66.063814

[50] L. Mandel. *Coherence and indistinguishability.* Optics Letters **16** (1991) 1882.
doi:10.1364/OL.16.001882

[51] F. Gori, M. Santarsiero, R. Borghi, E. Wolf. *Maximizing Young's fringe visibility through reversible optical transformations.* Optics Letters **32** (2007) 588.
doi:10.1364/OL.32.000588

[52] T. Legero, T. Wilk, M. Hennrich, G. Rempe, A. Kuhn. *Quantum Beat of Two Single Photons.* Physical Review Letters **93** (2004) 070503.
doi:10.1103/PhysRevLett.93.070503

[53] M. C. Tichy. *Sampling of partially distinguishable bosons and the relation to the multidimensional permanent.* Physical Review A **91** (2015) 022316.
doi:10.1103/PhysRevA.91.022316

[54] V. S. Shchesnovich. *Partial indistinguishability theory for multiphoton experiments in multiport devices.* Physical Review A **91** (2015) 013844.

doi:10.1103/PhysRevA.91.013844

[55] P. I. Sund. *Photonic Quantum Information Processing with Quantum Dot Single-Photon Sources*. Ph.d. thesis, Niels Bohr Institute, Faculty of Science, University of Copenhagen, 2023. Accessed: 2025-12-26.
`https://nbi.ku.dk/english/theses/phd-theses/patrik-isene-sund/patrik-isene-sund.pdf`

[56] P. Lodahl. Quantum-dot based photonic quantum networks, 2017.
`https://arxiv.org/abs/1707.02094`

[57] A. Kiraz, M. Atatüre, A. Imamoğlu. *Quantum-dot single-photon sources: Prospects for applications in linear optics quantum-information processing*. Physical Review A **69** (2004).
doi:10.1103/physreva.69.032305

[58] D. Pegg, L. Phillips, S. Barnett. *Optical State Truncation by Projection Synthesis*. Physical Review Letters - PHYS REV LETT **81** (1998) 1604.
doi:10.1103/PhysRevLett.81.1604

[59] S. Slussarenko, M. M. Weston, L. K. Shalm, V. B. Verma, S.-W. Nam, S. Kocsis, T. C. Ralph, G. J. Pryde. *Quantum channel correction outperforming direct transmission*. Nature Communications **13** (2022) 1832.
doi:10.1038/s41467-022-29376-4

[60] P. Clifford, R. Clifford. The Classical Complexity of Boson Sampling. *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2018)*. SIAM, 2018 S. 146–155.
doi:10.1137/1.9781611975031.10

[61] H. J. Ryser. *Combinatorial Mathematics*, Band 14 von *Carus Mathematical Monographs*. Mathematical Association of America, 1963.

[62] R. W. Doran. *The Gray Code*. Journal of Universal Computer Science **13** (2007) 1573. Accessed: 2025-12-26.

[63] A. Nijenhuis, H. S. Wilf. *Combinatorial Algorithms for Computers and Calculators*. Academic Press, 2 Auflage, 1978. Free download provided by the authors; accessed: 2025-12-26.

[64] M. H. Hüttenbrenner. Photonic-Quantum-Information-Simulator. `https://github.com/Michael-Huettenbrenner/Photonic-Quantum-Information-Simulator`, 2025. GitHub repository, accessed on 2026-01-04.

[65] Numba: A Just-In-Time Compiler for Numerical Functions in Python, 2025. PyPI package, accessed 2026-01-04.
`https://pypi.org/project/numba/`

[66] S. K. Lam, A. Pitrou, S. Seibert. Numba: A LLVM-based Python JIT Compiler. *Proceedings of the Second Workshop on the LLVM Compiler Infrastructure in HPC*, 2015
doi:10.1145/2833157.2833162
`https://dl.acm.org/doi/10.1145/2833157.2833162`

[67] B. Sz.-Nagy, C. Foiaş, H. Bercovici, L. Kérchy. *Harmonic Analysis of Operators on Hilbert Space*. Universitext. Springer, 2 Auflage, 2010.
doi:10.1007/978-1-4419-6094-8

[68] M. Reck, A. Zeilinger, H. J. Bernstein, P. Bertani. *Experimental realization of any discrete unitary operator*. Physical Review Letters **73** (1994) 58.
doi:10.1103/PhysRevLett.73.58

[69] T. W. Judson. Abstract Algebra: Theory and Applications. `https://scholarworks.sfasu.edu/ebooks/23/`, 2020. Open textbook. See the chapter/section introducing symmetric groups $S_n$ as permutations. ISBN: 9781944325091. Accessed: 2025-12-29.

[70] R. A. Brualdi, H. J. Ryser. *Combinatorial Matrix Theory*, Band 39 von *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1991.
doi:10.1017/CBO9781107325708

[71] R. A. Horn, C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 2 Auflage, 2013.

[72] E. Kreyszig. *Introductory Functional Analysis with Applications*. John Wiley & Sons, 1978.

[73] R. Bhatia. *Matrix Analysis*, Band 169 von *Graduate Texts in Mathematics*. Springer, 1997.
doi:10.1007/978-1-4612-0653-8

[74] L. Villegas-Aguilar, F. Ghafari, M. S. Winnel, V. B. Verma, L. K. Shalm, T. C. Ralph, G. J. Pryde, S. Slussarenko. A heralded quantum amplifier of multi-photon states, 2025.
https://arxiv.org/abs/2505.13992

[75] T. Strobel, *et al. Telecom-wavelength quantum teleportation using frequency-converted photons from remote quantum dots*. Nature Communications (2025).
doi:10.1038/s41467-025-65912-8

[76] P. Dhara, S. J. Johnson, C. N. Gagatsos, P. G. Kwiat, S. Guha. *Heralded Multiplexed High-Efficiency Cascaded Source of Dual-Rail Entangled Photon Pairs Using Spontaneous Parametric Down-Conversion*. Physical Review Applied **17** (2022).
doi:10.1103/physrevapplied.17.034071

[77] M. Eibl, N. Kiesel, J. Bouda, C. Kurtsiefer, K. Mattle, H. Weinfurter, A. Zeilinger. *Experimental Observation of Four-Photon Entanglement from Spontaneous Parametric Down-Conversion*. Physical Review Letters **90** (2003) 200403.
doi:10.1103/PhysRevLett.90.200403

[78] N. Sangouard, C. Simon, H. de Riedmatten, N. Gisin. *Quantum repeaters based on atomic ensembles and linear optics*. Reviews of Modern Physics **83** (2011) 33.
doi:10.1103/RevModPhys.83.33

[79] W. Wasilewski, C. Radzewicz, R. Frankowski, K. Banaszek. *Statistics of multiphoton events in spontaneous parametric down-conversion*. Phys. Rev. A **78** (2008) 033831.
doi:10.1103/PhysRevA.78.033831

[80] D. E. Browne, T. Rudolph. *Resource-Efficient Linear Optical Quantum Computation*. Physical Review Letters **95** (2005) 010501.
doi:10.1103/PhysRevLett.95.010501