École polytechnique fédérale de Lausanne

Bachelor's project

# Analysis of the Noninteracting-Boson Model of Computation for BosonSampling

*Autor*
Luca Carroz

*Responsible*
Prof. Nicolas Macris

*Supervisor*
Mr. Farzad Pourkamali

## Abstract

This report aims to analyze the noninteracting-boson model of computation and its implementation on a quantum computer operating on photons. With the rapid advancements in quantum computing, understanding the potential of the noninteracting-boson model and finding applications to photon-based quantum computers becomes increasingly interesting.

Through our analysis, we demonstrate that a quantum computer operating on photons, utilizing the noninteracting-boson model, can effectively approximate the permanent of a matrix. This breakthrough achievement offers a solution to the long-standing problem of approximating the permanent, which has eluded efficient classical algorithms. By leveraging the unique properties of quantum computing and the noninteracting-boson model, we showcase the significant computational advantage offered by photon-based quantum computers in solving this challenging problem.

June 9, 2023

# Contents

# 1 Introduction

The idea of quantum advantage was first proposed in the 1980s by physicist Richard Feynman, who believed there were some problems that could be solved notably faster by quantum computers compared to classical computers. The first quantum algorithm that showed such advantage was designed by David Deutsch and Richard Jozsa in 1992 [1], but unfortunately, this algorithm has no known practical use.

This report analyses the Boson Sampling problem and how a quantum computer can solve it efficiently with the absence of noise. Since solving this problem allows to approximate permanents of matrices, which is a difficult task for classical computing, proving that a quantum computer could solve this problem in polynomial time would also show quantum advantage (unless we discover some polynomial time classical algorithm to compute permanents).

We begin by giving a few notations in Section 2, after what we define our model in Section 3. We then give two more interpretations of our model in Section 4 and Section 5 that we link together to finally show the important results in Section 6. Finally, we wrap up the discussion in Section 7.

# 2 Notations

Throughout the report, we will denote the top-left submatrix of a matrix $M$ by $M_{n,n}$. We will also make use of the complex normal Gaussian distribution $\mathcal{G} = A + iB$, where $A, B \overset{i.i.d.}{\sim} \mathcal{N}(\mu = 0, \sigma^2 = \frac{1}{2})$, plotted in fig. 1.

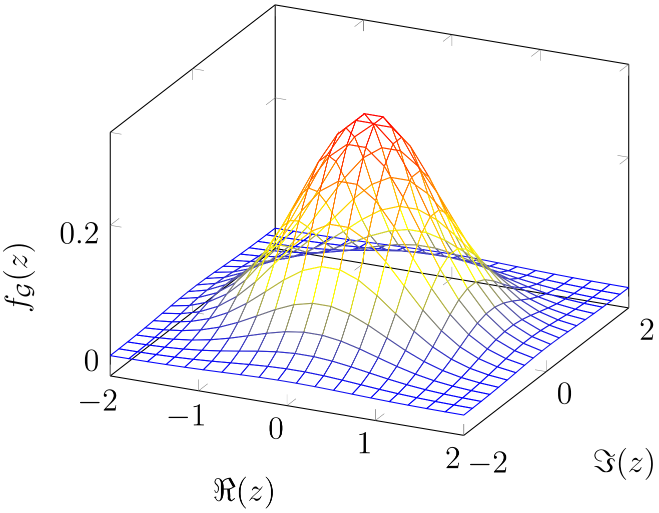

Figure 1: Complex Normal Gaussian Distribution

# 3 The Model

Our model considers $n$ identical and indistinguishable photons, that can each be in one of $m$ different modes (you can think of modes as positions). Those photons are then sent through a serie of optical elements having each a specific action on the photons, depending on the mode they are in. Finally, the photons are measured to determine their location (modes). Assuming that photons behave according to the laws of quantum physics, a photon can be in any superposition of modes, meaning that it can be at "several positions" at once, and measuring its position returns one of the superposed positions at random, with varying probabilities for each position.
The classical analogue of this model would be the following model:
with $m = 2$, we consider a circuit that has n bits for input (stored in registers), on which we apply a set of gates (AND, OR, etc.), and that we finally measure (we simply measure the current in the wires of our circuit to determine the final value of each of the $n$ bits). Note that in the classical case, those observed values are deterministic whereas they are not (in the general case) in the quantum model. With $m > 2$, we just use $n$ $m$-ary bits instead of bits.

For practical reasons, we will restrain ourselves to the case $n \leq m$. Assuming that each photon behaves according to the laws of quantum physics and that the number of photons stays fixed (i.e. no photon gets absorbed or emitted throughout the experiment), we can write the computational basis states of our system as $|S\rangle = |s_1, s_2, ..., s_m\rangle$, where $s_i$ represents the number of photons in the $i^{th}$ mode, for $i = 1, 2, .., m$ and $\sum_m^{i=1} s_i = n$ which ensures that the number of photons stays constant. We also note that the $s_i$'s cannot be negative, but that they can be greater than 1, which intuitively means that several photons are in the same mode (or position). We denote the set of computational basis state by $\Phi_{m,n}$ and its size by $M = |\Phi_{m,n}|$, where the value of $M$ is the following:

**Lemma 1** $M = |\Phi_{m,n}|= \binom{m+n-1}{n}$
**Proof.** We first observe that $M$ is equal to the number of ways we can distribute $n$ indistinguishable elements in $m$ boxes. We can think of it as if we had $m+n-1$ slots where we either have to put an element or a fence, where a fence delimits two different boxes (see fig. 2 for example). There are $m+n-1$ slots because we have to place $n$ elements and $m-1$ fences to delimit the $m$ boxes. Since elements and fences are indistinguishable, we can first chose where to place the $n$ elements and then put the fences in the remaing $m-1$ slots. Since there is $\binom{m+n-1}{n}$ ways to place $n$ indistinguishable elements in $m+n-1$ slots, we get the expected result.
□
In the example in fig. 2, the distribution on the right represents the state $|0,1,0,0,2,1\rangle$. As always in quantum mechanics, a general state of our system is of the form

$$|\psi\rangle = \sum_{S\in\Phi_{m,n}} \alpha_S \, |S\rangle$$

where $\alpha_S \in \mathbb{C}$, $\forall S \in \Phi_{m,n}$ and the $\alpha_S$'s satisfy $\sum_{S\in\Phi_{m,n}}|\alpha_S|^2= 1$. We call the infinite set of such $|\psi\rangle$'s the Hilbert space $H_{m,n}$.
In our analysis of this model, we will always set the initial state to be $|1_n\rangle$, where

$$|1_n\rangle := |\underbrace{1,1,...,1}_{n},\underbrace{0,0,...,0}_{m-n}\rangle\,,$$

which is the state in which we have exactly one photon in each of the first $n$ modes, and zero photons in the remaining $m-n$ modes. Since we set $m \geq n$, this state is well defined.
We will then apply a set of transformations on this state, by means of phaseshifters and beamsplitters (which we will define in Section 3.1.1), whose action can be described by a unitary matrix $U$, which leaves the initial state $|1_n\rangle$ in the state $U\,|1_n\rangle$.
Finally, we measure the state in the computational basis $\Phi_{m,n}$ which returns an element $S \in \Phi_{m,n}$ with probability $\mathbb{P}[S] = |\langle S|\, U\,|1_n\rangle\,|^2 = |\beta_S|^2$, where $U\,|1_n\rangle = \sum_{S\in\Phi_{m,n}} \beta_S\,|S\rangle$.

## 3.1 Unitary transformations

In standard quantum computing, we work with a number $n$ of differentiable qubits in a Hilbert space $H_n = (\mathbb{C}^2)^{\otimes n}$, and operations on the qubits are done via quantum gates. We know that any unitary $U_{2^n\times 2^n}$ in this hilbert space can be decomposed as a product of gates $U_{2^n\times 2^n} = U_k U_{k-1} ... U_2 U_1$, where each $U_i$ acts non-trivially on at most 2 qubits,

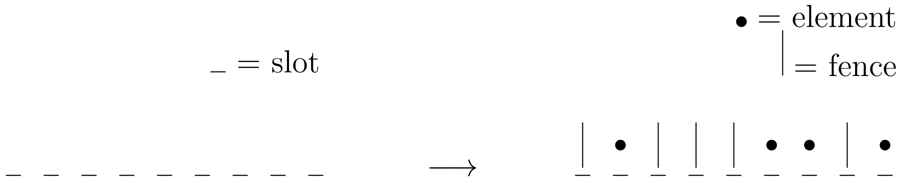

Figure 2: Example distribution ($n = 4, m = 6$)

and is the identity on the other qubits.
Similarly, in the linear optic model, any unitary $U_{M\times M}$ can be decomposed as a product of optical elements $U_{M\times M} = U_k U_{k-1} ... U_2 U_1$, where each $U_i$ acts non-trivially on at most 2 modes, and is the identity on the other modes.

### 3.1.1 Linear optics for $n = 1$

Let's first define the two best-known elements for $n = 1$ (which implies $M = m$):

- The *phaseshifter* : A phaseshifter multiplies the amplitude $\alpha_S$ of a single mode $m_1$ by $e^{i\phi}$, for some angle $\phi \in [0, 2\pi[$, and acts trivially on the remaining $m-1$ amplitudes of the remaining modes. The unitary matrix describing the effect of a phaseshifter can be written as

$$\begin{array}{cc} \begin{matrix} \quad & \quad & m_1 & \quad & \quad \end{matrix} & \\ \begin{pmatrix} 1 & & & & \\ & \ddots & & 0 & \\ & & e^{i\phi} & & \\ & 0 & & \ddots & \\ & & & & 1 \end{pmatrix} & \begin{matrix} \\ \\ m_1 \\ \\ \\ \end{matrix} \end{array}$$

- The *beamsplitter* : A beamsplitter modifies two amplitudes $\alpha_S$ and $\alpha_T$ from two different modes $m_1$ and $m_2$, for some $\theta \in [0, 2\pi[$. It can be written in matrix form as

$$\begin{array}{cc} \begin{matrix} \quad & \quad & m_1 & m_2 & \quad & \quad \end{matrix} & \\ \begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & \cos\theta & -\sin\theta & & \\ & & \sin\theta & \cos\theta & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{pmatrix} & \begin{matrix} \\ \\ m_1 \\ m_2 \\ \\ \\ \end{matrix} \end{array}$$

**Lemma 2** *Any $m \times m$ unitary matrix $U$ can be decomposed as a product $U = U_k U_{k-1} ... U_2 U_1$, where each $U_i$ is an optical element (i.e. either a phaseshifter or a beamsplitter)* [2].
**Proof.** We will prove this lemma by induction on the size $m$ of $U$.

- **Base step ($m = 1$):** $U = (c)$, where $c \in \mathbb{C}$. Since $U$ is unitary, $U^\dagger U = \bar{c}c = \mathbb{I}_{1\times 1} = 1 \implies |c|^2 = 1 \implies c = e^{i\phi}$, $\phi \in [0, 2\pi[$.
Thus, $U = (e^{i\phi})$ is already decomposed as a product of optical elements, since $U$ is a phaseshifter.

- **Hypothesis:** Assume that any $(m-1)\times(m-1)$ unitary matrix U can be decomposed as a product of optical elements $U_k U_{k-1} ... U_2 U_1$.

- **Induction step:** Let $V$ be an $m \times m$ unitary matrix, and let us write a few elements of the last row and last column of $V$: $V = \begin{pmatrix} & & & \vdots \\ & \mathrm{V}_{m-1,\, m-1} & & v_{m-2,m} \\ & & & v_{m-1,m} \\ \dots & v_{m,m-2} & v_{m,m-1} & v_{m,m} \end{pmatrix}$.

  Let $T_{m,q}(\theta_{m,q}, \phi_{m,q})$ for $q = m-1, m-2, ..., 1$ be unitary matrices describing the effect of a beamsplitter on modes $m$ and $q$ of paramter $\theta_{m,q}$ followed by a phaseshifer on mode $q$ of parameter $\phi_{m,q}$: $T_{m,q}(\theta_{m,q}, \phi_{m,q}) =$

$$\begin{array}{cc} \begin{matrix} \phantom{1} & \phantom{0} & q & & m \end{matrix} & \\ \begin{pmatrix} 1 & 0 & \dots & & \\ 0 & \ddots & & & \\ \vdots & & e^{i\phi_{m,q}} \cos\theta_{m,q} & \dots & -e^{i\phi_{m,q}} \sin\theta_{m,q} \\ & & \vdots & \ddots & \vdots \\ & & \sin\theta_{m,q} & \dots & \cos\theta_{m,q} \end{pmatrix} & \begin{matrix} \\ \\ q \\ \\ m \end{matrix} \end{array}$$

  We observe that $VT_{m,m-1}(\theta_{m,m-1,)}, \phi_{m,m-1}) = \begin{pmatrix} & & & \vdots \\ & \mathrm{V}'_{m-1,\, m-1} & & v'_{m-2,m} \\ & & & v'_{m-1,m} \\ \dots & v'_{m,m-2} & v'_{m,m-1} & v'_{m,m} \end{pmatrix}$, where $v'_{m,m-1} = e^{i\phi_{m,m-1}} \cos\theta_{m,m-1} v_{m,m-1} + \sin\theta_{m,m-1} v_{m,m} = 0$ by choosing $\phi_{m,m-1}$ and $\theta_{m,m-1}$ appropriately (see Appendix A for the proof). We can then multiply by $T_{m,m-2}(\theta_{m,m-2}, \phi_{m,m-2})$ and again, by choosing $\theta_{m,m-2}$ and $\phi_{m,m-2}$ correctly, we will zero out the component $(m, m-2)$ of $V$. Note that the component $(m, m-1)$ of $V$ will still be zero, independently of $\theta_{m,m-2}$ and $\phi_{m,m-2}$, since this component will be the result of the multiplication of the $m^{th}$ row of $V'$ and the $(m-1)^{th}$ column of $T_{m,m-1}$, and the $(m-1)^{th}$ column of $T_{m,m-1}$ has only null components except for the component $m-1$, and $V'$'s $(m-1)^{th}$ element of $m^{th}$ row is $v'_{m,m-1}$ which is zero.

  We can keep proceeding like this to zero out every component (except the last one) of the last row of $V$, which results in a matrix $W = VT_{m,m-1}T_{m,m-2}...T_{m,2}T_{m,1} = \begin{pmatrix} & & & \vdots \\ & \mathrm{W}_{m-1,\, m-1} & & w_{m-2,m} \\ & & & w_{m-1,m} \\ \dots & 0 & 0 & w_{m,m} \end{pmatrix}$.

  Since $W$ is the result of a multiplication of unitary matrices, $W$ is also unitary. In particular, this implies that the norm squared of the last row is equal to 1, which in turn implies that $|w_{m,m}|^2 = 1$, and also that the norm of the last column is equal to 1, which in turn implies that $\sum_{i=1}^{m} |w_{i,m}|^2 = 1 \implies \underbrace{|w_{m,m}|^2}_{=1} + \sum_{i=1}^{m-1} |w_{i,m}|^2 = 1 \implies \sum_{i=1}^{m-1} |w_{i,m}|^2 = 0 \implies w_{i,m} = 0, i = 1, 2, ..., m-1$.

And thus, $W = \begin{pmatrix} & & & \vdots \\ & \text{W}_{m-1,\, m-1} & & 0 \\ & & & 0 \\ \dots & 0 & 0 & e^{i\omega} \end{pmatrix}$, with $\omega \in [0, 2\pi[$.

By multiplying $W$ by a phaseshifter P on mode $m$, with parameter $-\omega$, we get $X := WP = \begin{pmatrix} & & & \vdots \\ & \text{X}_{m-1,\, m-1} & & 0 \\ & & & 0 \\ \dots & 0 & 0 & 1 \end{pmatrix}$

Note that since $X$ is the product of unitary matrices, $X$ is also unitary, which implies that

$$\begin{aligned} &X^\dagger X = XX^\dagger = \mathbb{I}_{n\times n} \\ &\quad \iff X^\dagger_{(m-1)\times(m-1)} X_{(m-1)\times(m-1)} = X_{(m-1)\times(m-1)} X^\dagger_{(m-1)\times(m-1)} = \mathbb{I}_{(m-1)\times(m-1)} \\ &\quad \iff X_{(m-1)\times(m-1)} \text{ is unitary.} \end{aligned}$$

Since $X_{(m-1)\times(m-1)}$ is a unitary matrix of dimension $(m-1)\times(m-1)$, we have from our hypothesis that $X_{(m-1)\times(m-1)}$ can be written as a product of optical elements: $X_{(m-1)\times(m-1)} = U_k U_{k-1} ... U_2 U_1$.

By defining $U_i' = \begin{pmatrix} & & \vdots \\ & \text{U}_i & 0 \\ & & 0 \\ \dots & 0 & 0 \quad 1 \end{pmatrix}$, for $i = 1, 2, ..., k$, we see that each $U_i'$ is also an optical element (by adding 1 row and 1 column we just added 1 mode on which nothing happens), and also that $X = U_k' U_{k-1}' ... U_2' U_1'$, and thus that $X$ can be written as a product of optical elements. We conclude by observing that:

$W = VT_{m,m-1}T_{m,m-2}...T_{m,2}T_{m,1} \implies X = WP = VT_{m,m-1}T_{m,m-2}...T_{m,2}T_{m,1}P \overset{2}{\Rightarrow}$
$V = XP^\dagger T^\dagger_{m,1}T^\dagger_{m,2}...T^\dagger_{m,k-1}T^\dagger_{m,k} = U_k' U_{k-1}' ... U_2' U_1' P^\dagger T^\dagger_{m,1}T^\dagger_{m,2}...T^\dagger_{m,k-1}T^\dagger_{m,k}$.
Which means that $V$ can be written as a product of optical elements, and thus that any $m \times m$ unitary matrix can be written as a product of optical elements, given the hypothesis.

- **Conclusion:** We proved every step of the induction and hence, we just proved that any unitary matrix can be written as a product of optical elements.
  □

[2] Since the inverse of a unitary matrix is its Hermitian conjugate. Note that the Hermitian conjugate of an optical element is the same optical element with the same parameter multiplied by $-1$.

### 3.1.2 Linear optics for $n \geq 1$

When changing the number of photons in the system, the unitaries describing the action of the phaseshifters and beamsplitters change. It turns out there exist a natural homomorphism $\varphi$ which maps an $m \times m$ unitary $U$ acting on a single photon to the correcsponding $M \times M$ unitary $\varphi(U)$ acting on $n$ photons.
Since $\varphi(U)$ preserves photon number, we know that the following must always hold whenever $s + t \neq u + v$ (i.e. when the number of photon in the input is different from the number of photons in the output)

$$\langle s, t| \, \varphi(U) \, |u, v\rangle = 0$$

When $s + t = u + v$, we claim that the correct formula for the entry of $\varphi(U)$ is

$$\langle s, t| \, \varphi(U) \, |u, v\rangle = \sqrt{\frac{u! \, v!}{s! \, t!}} \sum_{k+l=u, \, k \leq s, \, l \leq t} \binom{s}{k} \binom{t}{l} a^k b^{s-k} c^l d^{t-l}$$

We provide an intuitional reasoning of why this formula is true in Appendix B.

# 4 Polynomial definition

Instead of thinking of our model as being a computer that acts on photons, we will take an alternative representation where the "states" become multivariate complex-valued polynomials of degree $n$, optical elements become unitary changes of variable, and a "measurement" becomes a sampling from a probability distribution over monomials (weighted by their coefficients). Note that we still enforce $m \geq n$. A multivariate complex-valued polynomial of degree $n$ is defined as

$$p(x_1, x_2, ..., x_m) = \sum_{S \in \Phi_{m,n}} a_S x^{s_1} x^{s_2} ... x^{s_m}, \text{ where}$$

$$\Phi_{m,n} = \{S = (s_1, s_2, ..., s_m) : s_i \geq 0 \, \forall i, \sum_{i=1}^{m} s_i = n\}, \text{ and } a_S \in \mathbb{C}, \; \forall S \in \Phi_{m,n}.$$

In this definition, instead of writing the state of our computer as a superposition of a subset of the $m$ different modes, we define our state to be a multivariate complex-valued polynomial $p(x_1, x_2, ..., x_m)$ of degree $n$ . Our previously defined initial state $|1_n\rangle$ corresponds to the degree-$n$ multivariate monomial

$$J_{m,n}(x_1, x_2, ..., x_m) := \prod_{i=1}^{n} x_i = x_1 x_2 ... x_n.$$

To transform the state, we can apply any $m \times m$ unitary change of variables $U$ we like to the variables $x_1, x_2, ..., x_m$:

$$U = \begin{pmatrix} u_{11} & \dots & u_{1m} \\ \vdots & \ddots & \vdots \\ u_{m1} & \dots & u_{mm} \end{pmatrix}, \; x_i \to u_{i1} x_1 + u_{i2} x_2 + ... + u_{im} x_m, \; i = 1, 2, ..., m$$

This changes our multivariate monomial to the complex-valued multivariate polynomial:

$$U[J_{m,n}](x_1, x_2, ..., x_m) = \prod_{i=1}^{n} (u_{i1}x_1 + u_{i2}x_2 + ... + u_{im}x_m).$$

To simplify the notations, we will now write $U[J_{m,n}]$ instead of $U[J_{m,n}](x_1, x_2, ..., x_m)$ After having applied an arbitrary number of such changes of variables, we measure the final polynomial $p$, that can be writen in its general form as:

$$p(x_1, x_2, ..., x_m) = \sum_{S \in \Phi_{m,n}} a_S x_1^{s_1} x_2^{s_2} ... x_m^{s_m},$$

where $\Phi_{m,n}$ is the set of all $s_i \geq 0$ such that $\sum_{i=1}^{m} s_i = n$. Then, measuring the polynomial $p$ returns a state $S \in \Phi_{m,n}$ with probability:

$$\mathbb{P}[S] := |a_S|^2 s_1!\, s_2! ... s_m!\,.$$

We can already see that when measuring the initial state $J_{m,n}$, the probability of observing the result $S = (\underbrace{1, 1, ..., 1}_{n}, \underbrace{0, 0, ..., 0}_{m-n})$ is $\mathbb{P}[S] = |1|^2 \underbrace{1!\, 1! ... 1!}_{n} \underbrace{0!\, 0! ... 0!}_{m-n} = 1$, and we will prove later on that this probability remains equal to 1 after any unitary change of variable.

To further simplify the notations, let $x := x_1, x_2, ..., x_m$, $x^S := x_1^{s_1} x_2^{s_2} ... x_m^{s_m}$, $S! := s_1!\, s_2! ... s_m!$ and let us define two arbitrary polynomials $q(x) = \sum_{S \in \Phi_{m,n}} a_S x^S$, $r(x) = \sum_{S \in \Phi_{m,n}} b_S x^S$. We define the so called *Fock-space inner product* between two polynomials as:

$$\langle q, r \rangle := \sum_{S \in \Phi_{m,n}} \bar{a}_S b_S S!\,.$$

We notice that this inner product has the following property:

**Lemma 3 (Fock-Space Inner Product Identity)** $\langle q, r \rangle = \mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(x) r(x)]$ *where* $\mathcal{G}$ *is the Gaussian distribution* $\mathcal{N}(0, 1)_{\mathbb{C}}$

**Proof.** We begin by observing that since the expectation and the Fock-space inner product are linear, it is enough to prove the lemma for monomials with coefficient equal to 1. So, let $q(x) = x^S$ and $r(x) = x^T$, for some $S, T \in \Phi_{m,n}$.

- **If** $q(x) \neq r(x)$**:** $\langle q, r \rangle = 0$, since $q$ and $r$ are orthogonal and $\mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(x) r(x)] = \mathbb{E}_{x \sim \mathcal{G}^m}[x^S x^T] \overset{a)}{=} \prod_{i=1}^{m} \mathbb{E}_{x_i \sim \mathcal{G}}[\bar{x}_i^{s_i} x_i^{t_i}]$. Since $q(x) \neq r(x)$, $\exists i : s_i \neq t_i$ and the term $\mathbb{E}_{x_i \sim \mathcal{G}}[\bar{x}_i^{s_i} x_i^{t_i}] = 0$ since the Gaussian distribution is uniform over phases $\implies \langle q, r \rangle = \mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(x) r(x)] = 0$. The a) equality holds since the $m$ random variables from the Gaussian distribution $\mathcal{G}^m$ are independent.

- **If** $q(x) = r(x)$**:** $\langle q, r \rangle = S! = T!$ and $\mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(x) r(x)] = \prod_{i=1}^{m} \mathbb{E}_{x_i \sim \mathcal{G}}[\bar{x}_i^{s_i} x_i^{t_i}] \overset{b)}{=} \prod_{i=1}^{m} \mathbb{E}_{x_i \sim \mathcal{G}}[|x_i|^{2s_i}]$.
  $\mathbb{E}_{x_i \sim \mathcal{G}}[|x_i|^{2s_i}]$ is the $s_i^{th}$ moment of the norm squared of a complex Gaussian random variable. Note that $\mathcal{G}$ can be written as $\mathcal{G} = A + iB$, where $A, B \overset{i.i.d.}{\sim} \mathcal{N}(\mu = 0, \sigma^2 = \frac{1}{2})$, which implies that $\mathbb{E}_{x_i \sim \mathcal{G}}[|x_i|^{2s_i}] = \mathbb{E}[(|\mathcal{G}|^2)^{s_i}] = \mathbb{E}[(|A + iB|^2)^{s_i}] = \mathbb{E}[(A^2 + B^2)^{s_i}]$.

Since $\frac{A}{\sigma} = N_1 \sim \mathcal{N}(0,1)$ and $\frac{B}{\sigma} = N_2 \sim \mathcal{N}(0,1)$, with $N_1 \perp\!\!\!\perp N_2$, we can further simplify the above equation to $\mathbb{E}[((\sigma N_1)^2 + (\sigma N_2)^2)^{s_i}] = \sigma^{2s_i}\mathbb{E}[(N_1^2 + N_2^2)^{s_i}]$. Now note that $N_1^2 + N_2^2$ follows a chi-square distribution with parameter $k = 2$, whose $n^{th}$ moment is well known to be equal to $\frac{2^n\Gamma(\frac{k}{2}+n)}{\Gamma(\frac{k}{2})}$ [3]. In our case with $k = 2$ and $n = s_i$, we get that $\sigma^{2s_i}\mathbb{E}[(N_1^2 + N_2^2)^{s_i}] = \sigma^{2s_i}\frac{2^{s_i}\Gamma(1+s_i)}{\Gamma(1)} \overset{a)}{=} \frac{1}{2}^{s_i} 2^{s_i} s_i! = s_i!$, where a) comes from the fact that the gamma function $\Gamma(n)$ is equal to $(n-1)!$ when $n \in \mathbf{N}$. Thus, $\mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(x)r(x)] = \prod_{i=1}^m \mathbb{E}_{x_i \sim \mathcal{G}}[|x_i|^{2s_i}] = \prod_{i=1}^m s_i! = s_1!\, s_2! \ldots s_m! = S! = \langle q, r\rangle$.
□

This Lemma allows us to prove the two following theorems:

**Theorem 1 (Unitary Invariance of Fock Inner product)** $\langle U[q], U[r]\rangle = \langle q, r\rangle$ *for all polynomials* $q, r$ *and all unitary changes of variables* $U$.

**Proof.** $\langle U[q], U[r]\rangle = \mathbb{E}_{x \sim \mathcal{G}^m}[\overline{U[q]}(x)U[r](x)] = \mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(Ux)r(Ux)] \overset{c)}{=} \mathbb{E}_{x \sim \mathcal{G}^m}[\bar{q}(x)r(x)] = \langle q, r\rangle$, where c) follows from the fact that the Gaussian distribution is invariant over rotations.
□

**Theorem 2 (Linear Transformation Identity of Fock Inner Product)** $\langle q, L[r]\rangle = \left\langle L^\dagger[q], r\right\rangle$ *for all polynomials* $q, r$ *and all linear transformations* $L$.
**Proof.** For $q(x) = \sum_{S \in \Phi_{m,n}} \bar{a}_S x^S, r(x) = \sum_{S \in \Phi_{m,n}} \bar{b}_S x^S$, we will first prove that the theorem holds when $L$ is a diagonal matrix, and then use this result to prove that the thorem holds for any linear transformation $L$:

- **If** $L = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_m \end{pmatrix} = \text{diag}(\lambda)$, where $\lambda = (\lambda_1, \lambda_2, ..., \lambda_m)$, then $\langle q, L[r]\rangle = \sum_{S \in \Phi_{m,n}} \bar{a}_S (b_S \lambda^S) S! = \sum_{S \in \Phi_{m,n}} \bar{a}_S b_S \bar{\bar{\lambda}}^S S! = \sum_{S \in \Phi_{m,n}} (\overline{a\bar{\lambda}^S}) b_S S! = \left\langle L^\dagger[q], r\right\rangle$.
- **If $L$ is not diagonal,** then we can use the singular value decomposition theorem [4] to decompose $L$ as $U\Sigma V^\dagger$, where $U$ and $V$ are unitary (and thus, $V^\dagger$ is also unitary) and $\Sigma$ is a diagonal matrix. Then, we have the following equalities: $\langle q, L[r]\rangle \overset{a)}{=} \left\langle q, U\Sigma V^\dagger[r]\right\rangle \overset{b)}{=} \left\langle U^\dagger[q], U^\dagger U\Sigma V^\dagger[r]\right\rangle = \left\langle U^\dagger[q], \Sigma V^\dagger[r]\right\rangle \overset{c)}{=} \left\langle \Sigma^\dagger U^\dagger[q], V^\dagger[r]\right\rangle \overset{b)}{=} \left\langle V\Sigma^\dagger U^\dagger[q], r\right\rangle = \left\langle (U\Sigma V^\dagger)^\dagger[q], r\right\rangle = \left\langle L^\dagger[q], r\right\rangle$, where a) comes from the SV decomposition, b) from Theorem 1, and c) from what we just proved when $L$ is diagonal.

□

We showed before that the probabilities of the various measurement outcomes sum up to 1 for the initial state $J_{m,n}$, but we still need to show that this property holds after applying unitary changes of variables to the initial state. For $q(x) = \sum_{S \in \Phi_{m,n}} a_S x^S$, we observe that the sum of probabilities of the various measurement outcomes $\sum_{S \in \Phi_{m,n}} |a_S|^2 S!$ is equal to $\langle q, q\rangle$. Thus, we just need to show that $\langle U[J_{m,n}], U[J_{m,n}]\rangle = 1$, for any unitary $U$:

$$\langle U[J_{m,n}], U[J_{m,n}]\rangle \overset{a)}{=} \langle J_{m,n}, J_{m,n}\rangle \overset{b)}{=} 1,$$

where a) follows from Theorem 1, and b) follows from the fact that the initial state $J_{m,n}$ is normalized.

## 4.1 Equivalence of the polynomial definition and the linear-optics model

In this subsection, we will prove that the polynomial definition is isomorphic to the linear-optics model:
**Theorem 3 (Equivalence of Physical and Polynomial Definitions)** *Let $P_{|\psi\rangle}$ be the complex-valued multivariate polynomial associated to the linear-optics state $|\psi\rangle = \sum_{S\in\Phi_{m,n}} \alpha_S |S\rangle$ as follows*

$$P_{|\psi\rangle} := \sum_{S\in\Phi_{m,n}} \frac{\alpha_S x^S}{\sqrt{S!}}.$$

*Then, $|\psi\rangle$ and $P_{|\psi\rangle}$ are isomorphic, where inner products and unitary transformations commute as follows*

$$\begin{aligned} \langle\psi|\phi\rangle &= \left\langle P_{|\psi\rangle}, P_{|\phi\rangle} \right\rangle, \\ P_{\varphi(U)|\psi\rangle} &= U[P_{|\psi\rangle}] \end{aligned}$$

**Proof.** We will first show that $\langle\psi|\phi\rangle = \left\langle P_{|\psi\rangle}, P_{|\phi\rangle}\right\rangle$, with $|\psi\rangle = \sum_{S\in\Phi_{m,n}} \alpha_S |S\rangle$ and $|\phi\rangle = \sum_{S\in\Phi_{m,n}} \beta_S |S\rangle$:

$\langle\psi|\phi\rangle = \sum_{S\in\Phi_{m,n}} \bar{\alpha}_S\beta_S = \sum_{S\in\Phi_{m,n}} \frac{\bar{\alpha}_S}{\sqrt{S!}}\frac{\beta_S}{\sqrt{S!}}S! = \langle q, r\rangle$, where $q(x) = \sum_{S\in\Phi_{m,n}} \frac{\alpha_S}{\sqrt{S!}}x^S$ and $r(x) = \sum_{S\in\Phi_{m,n}} \frac{\beta_S}{\sqrt{S!}}x^S$. We directly see that $q(x) = P_{|\psi\rangle}$ and $r(x) = P_{|\phi\rangle}$, and thus that $\langle\psi|\phi\rangle = \left\langle P_{|\psi\rangle}, P_{|\phi\rangle}\right\rangle$.

We will now show that $P_{\varphi(U)|\psi\rangle} = U[P_{|\psi\rangle}]$, with $|\psi\rangle = \sum_{S\in\Phi_{m,n}} \alpha_S |S\rangle$:
We proved in Lemma 2that any unitary $U$ can be decomposed as a product of optical elements acting on 2 modes at most. Thus, we only need to prove the above equality for a $2\times 2$ unitary $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, since the isomorphism will trivially generalize the theorem for any bigger matrix. Also, since the isomorphism is linear, we can restrict ourselves to the action of $\varphi(U)$ (resp. $U$) on computational states $|s, t\rangle$ (resp. on monomials $x^s y^t$):

Let $p(x,y) = \frac{x^s y^t}{\sqrt{s!t!}}$ be a normalized monomial. Then:

$$\begin{aligned}
U[p(x,y)] &= p(ax+by, cx+dy) \\
&= \frac{1}{\sqrt{s!\,t!}}(ax+by)^s(cx+dy)^t \\
&= \frac{1}{\sqrt{s!\,t!}} \left(\sum_{i=0}^{s} \binom{s}{i} a^i b^{s-i} x^i y^{s-i}\right) \left(\sum_{j=0}^{t} \binom{t}{j} c^j d^{t-j} x^j y^{t-j}\right) \\
&= \frac{1}{\sqrt{s!\,t!}} \sum_{i=0}^{s}\sum_{j=0}^{t} \binom{s}{i}\binom{t}{j} a^i b^{s-i} c^j d^{t-j} x^{i+j} y^{s+t-i-j} \\
&= \frac{1}{\sqrt{s!\,t!}} \sum_{u+v=s+t} \sum_{i+j=u,\ i\leq s,\ j\leq t} \binom{s}{i}\binom{t}{j} a^i b^{s-i} c^j d^{t-j} x^u y^v \\
&= \sum_{u+v=s+t} \underbrace{\sqrt{\frac{u!\,v!}{s!\,t!}} \sum_{i+j=u,\ i\leq s,\ j\leq t} \binom{s}{i}\binom{t}{j} a^i b^{s-i} c^j d^{t-j}}_{=\langle s,t|\varphi(U)|u,v\rangle} \underbrace{\frac{x^u y^v}{\sqrt{u!\,v!}}}_{|u,v\rangle} \\
&= \sum_{u+v=s+t} \langle s,t|\,\varphi(U)\,|u,v\rangle\,|u,v\rangle \\
&= \varphi(U)\,|s,t\rangle\,,
\end{aligned}$$

where we used the binomial expansion to get line 2.
□

# 5 Permanent definition

We will give a third and last interpretation of our model that will allow us to finally link the photonic model with the permanent. Recall that the permanent of an $n \times n$ complex matrix $A$ is defined as

$$\mathrm{Per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

where $S_n$ is the set of permutations of the elements $\{1, 2, ..., n\}$ and $a_{i,j} \in \mathbb{C}$ is the value of the $i^{th}$ row and $j^{th}$ column of $A$.

**Lemma 4 (Relation Between Permanents and Polynomials)**
$\mathrm{Per}(A_{n,n}) = \langle J_{m,n}, A[J_{m,n}]\rangle$ *, for any* $m \times m$ *matrix* $A$.
**Proof.** $A[J_{m,n}] = \prod_{i=1}^{n}(a_{i1}x_1 + a_{i2}x_2 + ... + a_{im}x_m)$ by definition. Then, $\langle J_{m,n}, A[J_{m,n}]\rangle$ is the sum of the coefficients of $A[J_{m,n}]$, for the monomials that are equal to $x_1x_2...x_n$. The coefficients of those monomials are constructed by taking any combination of $v_{ij}$'s in the sub matrix $A_{n,n}$ (since if we pick an element from $A$ that is not in this submatrix, the resulting monomial will contain a $x_k$, where $k > n$), and where the product of $a_{ij}$'s do not contain the same $i$ or $j$ twice (since picking two elements from the same column or row of $A_{n,n}$ will yield a monomial with an $x_k{}^p$, where $p > 1$). Thus, by picking a certain order $\sigma$ to choose the $n$ first columns of $A$, we find a monomial $\prod_{i=1}^{n} a_{i,\sigma(i)}x_i = x_1x_2...x_n \prod_{i=1}^{n} a_{i,\sigma(i)}$,

and by summing over all possible $\sigma$'s, we find:

$$\begin{aligned}\langle J_{m,n}, A[J_{m,n}]\rangle &= \sum_{\sigma\in S_n}\left\langle x_1x_2...x_n, x_1x_2...x_n\prod_{i=1}^{n}a_{i,\sigma(i)}\right\rangle\\ &= \sum_{\sigma\in S_n}\prod_{i=1}^{n}a_{i,\sigma(i)}1!\,1!\,...1!\\ &= \sum_{\sigma\in S_n}\prod_{i=1}^{n}a_{i,\sigma(i)}\\ &= \mathrm{Per}(A_{n,n})\end{aligned}$$

□

This important result implies the following Corollary:

**Corollary 1** $\mathrm{Per}\big((A^{\dagger}B)_{n,n}\big) = \langle A[J_{m,n}], B[J_{m,n}]\rangle$ *for any two $m\times m$ complex matrices $A, B$.*

**Proof.** $\mathrm{Per}\big((A^{\dagger}B)_{n,n}\big) \overset{a)}{=} \big\langle J_{m,n}, A^{\dagger}B[J_{m,n}]\big\rangle \overset{b)}{=} \langle A[J_{m,n}], B[J_{m,n}]\rangle$, where a) follows from Lemma 4 and b) follows from Theorem 2.

□

Let $S = (s_1, s_2, ..., s_m), T = (t_1, t_2, ..., t_m) \in \Phi_{m,n}$, and $U$ a $m\times m$ unitary matrix. We define the $n\times n$ matrix $U_{S,T}$ as follows:

- Construct the $m\times n$ matrix $U_T$ by repeating the $i^{th}$ column of $U$ $t_i$ times, for $i = 1, 2, ..., m$.
- Then, form $U_{S,T}$ by repeating the $j^{th}$ row of $U_T$ $s_j$ times, for $j = 1, 2, ..., m$.

**Example:**

$$\text{Let } U = \begin{pmatrix} 1 & 2 & 3 & 4\\ 5 & 6 & 7 & 8\\ 9 & 10 & 11 & 12\\ 13 & 14 & 15 & 16\end{pmatrix},\ |S\rangle = (1,1,0,1) \text{ and } |T\rangle = (2,0,1,0).$$

$$\text{Then, } U_T = \begin{pmatrix} 1 & 1 & 3\\ 5 & 5 & 7\\ 9 & 9 & 11\\ 13 & 13 & 15\end{pmatrix} \text{ and } U_{S,T} = \begin{pmatrix} 1 & 1 & 3\\ 5 & 5 & 7\\ 13 & 13 & 15\end{pmatrix}.$$

## 5.1 Equivalence of the Three Definitions

**Theorem 4** *for any two $m\times m$ complex matrices $A, B$ and any $S, T \in \Phi_{m,n}$,*

$$\langle S|\,\varphi(U)\,|T\rangle\sqrt{S!\,T!} = \big\langle x^S, U[x^T]\big\rangle = \mathrm{Per}(U_{S,T}).$$

**Proof.**
First of all, let us define an alternative way to construct the matrix $U_{S,T}$.
For $S \in \Phi_{n,m}$, let $I_S$ be a linear change of variables that maps the first $s_1$ variables to $x_1$,

the $s_2$ following variables to $x_2$, etc. If $n < m$, $I_S$ maps the remaining $m-n$ variables to 0. Note that $I_S[J_{m,n}] = x_1^{s_1} x_2^{s_2} ... x_m^{s_m} = x^S$, and also that (from Theorem 3) $\varphi(I_S) \left| 1_n \right\rangle =$, Then, we can check that

$$U_{S,T} = \left( I_S^\dagger U I_T \right)_{n,n}.$$

Let us first prove the first equality. We have:

$$\begin{aligned}
\left\langle S \right| \varphi(U) \left| T \right\rangle \sqrt{S!\,T!} &= \left\langle P_{|S\rangle}, P_{\varphi(U)|T\rangle} \right\rangle \sqrt{S!\,T!} \\
&= \left\langle P_{|S\rangle}, U[P_{|T\rangle}] \right\rangle \sqrt{S!\,T!} \\
&= \left\langle \frac{x^S}{\sqrt{S!}}, U\left[ \frac{x^T}{\sqrt{T!}} \right] \right\rangle \sqrt{S!\,T!} \\
&= \left\langle x^S, U\left[ x^T \right] \right\rangle,
\end{aligned}$$

where the three first equalities follow from Theorem 3.

The second equality follows from the above mentioned $I_S$ and $I_T$:

$$\begin{aligned}
\left\langle x^S, U\left[ x^T \right] \right\rangle &= \left\langle I_S[J_{m,n}], U I_T[J_{m,n}] \right\rangle \\
&= \mathrm{Per}\left( (I_S^\dagger U I_T)_{n,n} \right) \\
&= \mathrm{Per}(U_{S,T}).
\end{aligned}$$

□

# 6 Results

With Theorem 4, we have successfully linked the permanent of a matrix with a physical experiment using photons and optical elements. The problem that we can now solve efficiently by using those results is the following:

- **Input:** Two positive integers $n, m \in \mathbb{N}^*, m \geq n$ and an $m \times n$ column-orthonormal matrix $A$.
- **Circuit preparation:** Let $U$ be equal to the matrix $A$ completed with $m-n$ columns, such that the columns of $U$ are orthonormal. Note that $U$ is then unitary. From this $U$ and from Lemma 2, we can construct a circuit consisting of phaseshifters and beamsplitters such that the matrix describing the operation of the circuit is $U$. We do not prove it here, but the decomposition of U in optical elements takes a time polynomial in $m$, and the depth of the resulting circuit is also polynomial in $m$ [5]. Then, we prepare our photons in the initial state $\left| 1_n \right\rangle$ and we give them as input to our circuit, and we finally measure the output state in the computational basis $\Phi_{m,n}$.
- **Output:** From Theorem 4, we found that the probability of observing the state $\left| S \right\rangle \in \Phi_{m,n}$ is:

$$\mathbb{P}_A[S] = \left\langle S \right| \varphi(U) \left| 1_n \right\rangle = \frac{\mathrm{Per}(U_{S,1_n})}{\sqrt{S!\,1_n!}} = \frac{\mathrm{Per}(A_S)}{\sqrt{S!}}.$$

The problem of sampling from the distribution defined by $\mathbb{P}_A[S]$ is called a **Boson-Sampling** problem.

By running this circuit multiple times and recording the results, we would be able to approximate the permanents of those matrices $A_S$ with arbitrary precision, by increasing the number of runs.

# 7 Conclusion

We began by defining our model of computation and proving how we could efficiently build a circuit doing a given unitary operation. We then defined two new interpretations to help us link our model to the problem is computing permanents. We showed how those three models are linked to one another and ended up by showing in the last section how a quantum circuit operating on photons (or bosons to be more general) could solve in polynomial time the problem of approximating permanents of matrices or more generally of generating samples from a boson distribution. In classical computation, the Boson-Sampling problem is known to be hard, and our result implies that finding a classical algorithm able to solve this problem in polynomial time would imply a collapse to the third level in the polynomial hierarchy, on which we will not elaborate.

At first, some concrete realisations of BosonSampling with a few photons and modes have been implemented, but most of them were not that impressive, in the sense that with those small $m$ and $n$, even a classical computer could sample from those distributions in relatively little time. Recently however, Google, Xanadu (a canadian company) and a group of physicists in China have each constructed a quantum computer performing BosonSampling, and each of them claimed to have reached huge quantum advantages. Xanadu by example claimed that it would take around 9000 years for the best currently available supercomputer to generate one single sample from the probability distribution generated by their quantum compute [6].

We will conclude by noting that we did not take noise into account in our analysis. It has been shown that past a certain level of noise, the distribution generated by our quantum computer would "smooth out", such that it becomes possible for a classical computer to generate sample from this ditribution in polynomial time. Considering noise in the model makes the analysis considerably more complicated, and it is actually not exactly clear how one should model the noise in such experiment [7].

# 8 References

[1] Deutsch-Josza algorithm:
https://quantum-computing.ibm.com/composer/docs/iqx/guide/deutsch-jozsa-algorithm

[2] Experimental realization of any discrete unitary operator:
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.73.58

[3] Moments of the chi-squared distribution:
https://statproofbook.github.io/P/chi2-mom.html

[4] Singular value decomposition theorem:
https://en.wikipedia.org/wiki/Singular_value_decomposition

[5] The computational complexity of linear optics:
https://www.scottaaronson.com/papers/optics.pdf

[6] Quantum computational advantage with a programmable photonic processor (Xanadu):
https://www.nature.com/articles/s41586-022-04725-x

[7] Gaussian noise sensitivity and BosonSampling :
https://arxiv.org/abs/1409.3093

# A Appendix: Cancellation of Two Complex Numbers

Given $x, y \in \mathbb{C}$, we want to prove that the equation

$$xe^{i\phi}\cos\theta + y\sin\theta = 0$$

has always at least one solution, with $\phi, \theta \in [0, 2\pi[$. By writing $x, y$ as $x = r_1 e^{i\alpha_1}$ and $y = r_2 e^{i\alpha_2}$, $r_1, r_2 \in \mathbb{R}$, $\alpha_1, \alpha_2 \in [0, 2\pi[$, the equation becomes

$$r_1 e^{i\alpha_1} e^{i\phi}\cos\theta + r_2 e^{i\alpha_2}\sin\theta = 0.$$

By taking $\phi = \alpha_2 - \alpha_1$ we get

$$\begin{aligned} & r_1 e^{i\alpha_1} e^{i(\alpha_2-\alpha_1)}\cos\theta + r_2 e^{i\alpha_2}\sin\theta = 0 \\ \iff & r_1 e^{i\alpha_2}\cos\theta + r_2 e^{i\alpha_2}\sin\theta = 0 \\ \iff & r_1\cos\theta + r_2\sin\theta = 0 \end{aligned}$$

Then, if $r_1 = 0$, we pick $\theta = 0$ and if $r_2 = 0$, we pick $\theta = \frac{\pi}{2}$.
Otherwise, we get

$$\begin{aligned} & r_1\cos\theta + r_2\sin\theta = 0 \\ \iff & r_1\cos\theta = -r_2\sin\theta \\ \iff & \frac{-r_1}{r_2} = \frac{\sin\theta}{\cos\theta} = \tan\theta \\ \iff & \theta = \arctan\frac{-r_1}{r_2}, \end{aligned}$$

which is our general solution.
□

# B Appendix: Intuitional Reasoning on $\varphi(U)$

We will give some intuition to convince ourselves that the following formula is correct:

$$\langle s,t|\,\varphi(U)\,|u,v\rangle = \sqrt{\frac{u!\,v!}{s!\,t!}} \sum_{k+l=u,\,k\leq s,\,l\leq t} \binom{s}{k}\binom{t}{l} a^k b^{s-k} c^l d^{t-l},\ U=\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We will thus reason classically and show that the classical formula is very similar to the one above. Since we only used this formula when $U$ describes a beamsplitter, we will restrain ourselves to that case, by setting

$$U=\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

By considering only one photon, we see that the probability that a photon in the first mode stays in the first mode is $|\langle 1,0|\,U\,|1,0\rangle\,|^2{=}\,a^2$, the probability that the photon goes from the first mode to the second is $|\langle 0,1|\,U\,|1,0|^2{=}\,b^2\rangle$, the probability that the photon goes from the second mode to the first is $|\langle 1,0|\,U\,|0,1|^2{=}\,b^2\rangle$ and the probability that the photon stay the second mode is $|\langle 0,1|\,U\,|0,1|^2{=}\,a^2\rangle$.

Thus, we can say that we start with $u$ photons in the first mode and $v$ in the second, and we want to find the probability to find $s$ photons in the first mode and $t$ in the second, after having applied $\varphi(U)$.

Note that this probability is $\langle s,t|\,\varphi(U)\,|u,v\rangle\,|^2$. By reasoning classically, this value equals the probability that, given a subset of $k$ photons out of the $u$ photons in the first mode and a subset of $s-k$ photons out of the $v$ photons in the second mode, each of those $k+s-k=s$ photons stay or swap to the first mode, times the probability that the remaining $t$ photons in mode 1 and 2 all stay or swap to mode 2, and we need to sum this probability for every possible choice of $k$ (see fig. 3 below) .

This yields the following equality:

$$\langle s,t|\,\varphi(U)\,|u,v\rangle\,|^2 = \sum_{k+\ell=u,\,k\leq s,\,\ell\leq t} \binom{u}{k}\binom{v}{s-k}(a^2)^k(b^2)^{s-k}(b^2)^{\ell}(a^2)^{t-\ell} =$$

$$\sum_{k+\ell=u,\,k\leq s,\,\ell\leq t} \frac{u!\,v!}{k!\,(s-k)!\,(\underbrace{u-k}_{=\ell})!\,(\underbrace{v-(s-k)}_{=t-\ell})!}\left(a^{k-\ell+t}b^{\ell-k+s}\right)^2 =$$

$$\frac{u!\,v!}{s!\,t!}\sum_{k+\ell=u,\,k\leq s,\,\ell\leq t} \frac{s!\,t!}{k!\,(s-k)!\,\ell!\,(t-\ell)!}\left(a^{k-\ell+t}b^{\ell-k+s}\right)^2 =$$

$$\frac{u!\,v!}{s!\,t!}\sum_{k+\ell=u,\,k\leq s,\,\ell\leq t} \binom{s}{k}\binom{t}{\ell}\left(a^{k-\ell+t}b^{\ell-k+s}\right)^2,$$

which is very close to the square of the expected formula for the entries of $\varphi(U)$!

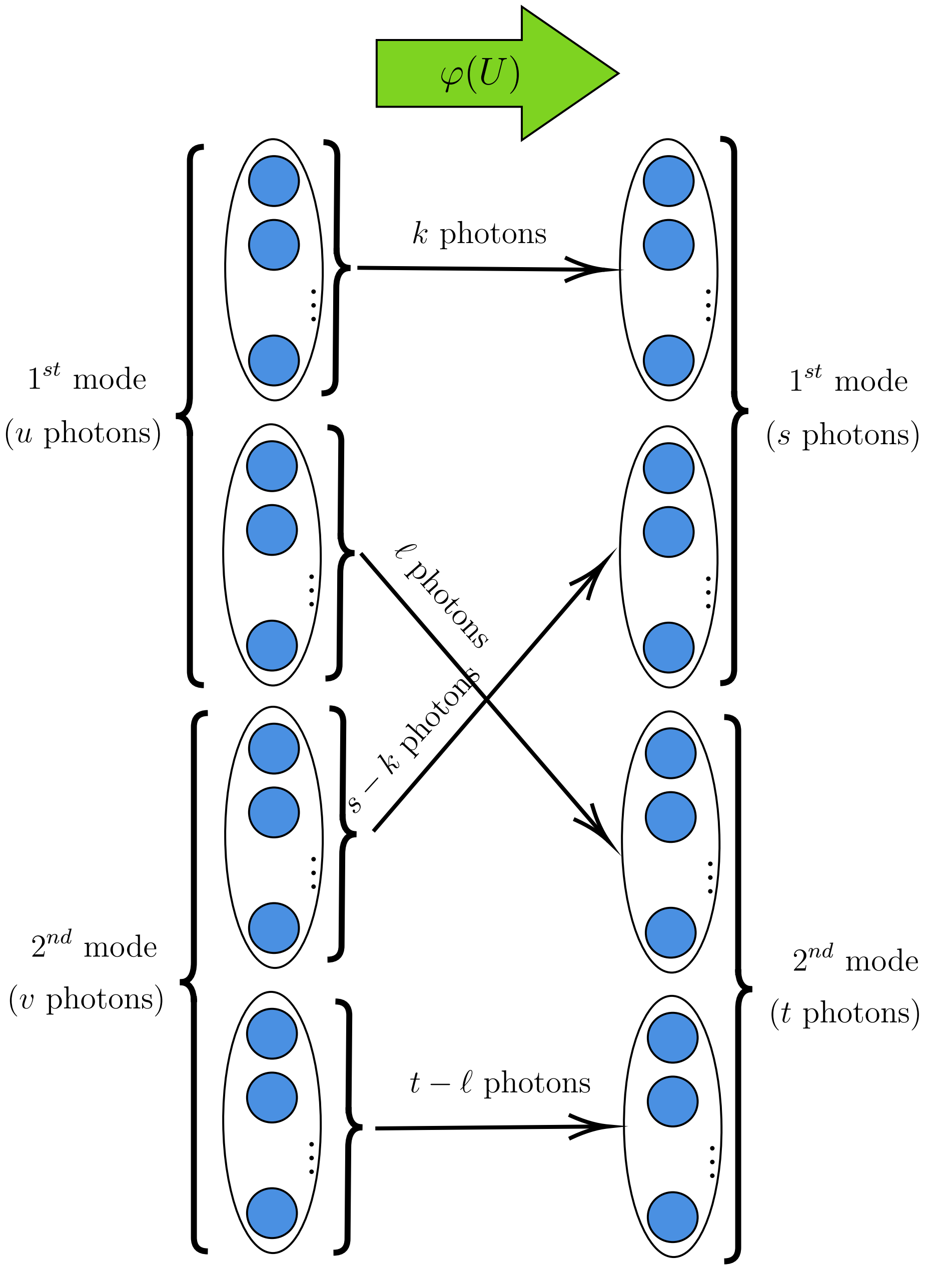

Figure 3: Visualisation of photons, modes and effect of $\varphi(U)$