MASTER DEGREE IN COMPUTATIONAL MATHEMATICS

MASTER THESIS

Unitary groups, quantum operations and linear optics

Author:
Joan BALAGUER OSUNA

Advisors:
Vicent GIMENO GARCÍA
Julio José MOYANO FERNÁNDEZ

2016/2017

This is to certify that the present document entitled

"Unitary groups, quantum operations and linear optics"

constitutes the Master thesis of the student Joan Balaguer Osuna, and is the result of his own work under our supervision.

Vicent Gimeno
Assistant Professor of Geometry
Universitat Jaume I de Castelló

Julio José Moyano Fernández
Assistant Professor of Algebra
Universitat Jaume I de Castelló

Abstract

This master thesis deals with the implementation of an algorithm which simulates the evolution of an optical system based on (quantum) linear optics; more specifically, we consider the evolution of n photons which are to be distributed in m modes. The procedure under consideration provides also a method which allows us to recreate the implemented optical system in the laboratory. The algorithm is based on the decomposition of the evolution matrix in optical elements which are easy to handle in the laboratory. The output of the algorithm coincides with the expected data according to the already existing theoretical models. However, the algorithm turns out to have a high computational complexity.

Keywords

- Special unitary groups
- Quantum computation
- Linear optics
- Hamiltonian evolution
- Algorithms in quantum linear optics

Contents

Chapter 1

Introduction

From the point of view of quantum physics, the electromagnetic field (including the light) is composed by elemental particles called photons. According to the postulates of quantum mechanics, each physical system is associated with a complex Hilbert space, and therefore the state of a photon is described by a one dimensional subspace of some Hilbert space.

In this work, we will study the evolution of n photons in m modes when they cross a linear optical network S. A linear optical network (consisting of optical elements) with m modes is modeled by an $m \times m$-unitary matrix which is called scattering matrix.

When the photons go through this network, their quantum states are modified. Thus, all possible arrangements of n photons in m modes correspond to $M := \binom{m+n-1}{n}$ pure states which turn out to build a suitable basis of the relevant Hilbert space. The evolution of quantum states of light is again given by a linear transformation; more precisely, by an $M \times M$-unitary matrix whenever a basis of H is chosen. Observe that this matrix coincides with S in the case of one single photon. The hypothesis of "unitarity" must be made due to quantum physical reasons which will be explained later.

The purpose of our work is to find out the final quantum state when a scattering matrix S which acts linearly and preserving the photon number is given.

To reach this goal, we need first of all to prove that any unitary matrix (i.e. an allowed operator in quantum physics) can be decomposed as a product of unitary block matrices, where the blocks are either 2×2 matrices or the identity matrix of a suitable size; those unitary block matrices represent optical elements between two modes. We also implement an algorithm, which computes the decomposition matrices from a given unitary matrix.

This procedure has practical consequences as well, because it let us reproduce in the laboratory any physical system of this type (we only have to build the decomposed matrix) if the initial state and the scattering matrix S are given.

Once we have computed the decomposed matrices, the next step is to make evolve these matrices. In order to show how these matrices evolve, we implement another algorithm. In this case, the input

will be the output of the previous algorithm, and the output is the final evolved system, i.e., the final evolution matrix. Also, we will interpret physically this resulting matrix.

Let us make a last remark: the algorithms we are describing are (unfortunately) computationally expensive; this means that our implementation will work in practice only when both the number n of photons and the number m of modes are relatively small.

Chapter 2

Mathematical preliminaries

The method which we will describe in the next chapters is based on a group homomorphism, so we will start by describing the foundations of group theory. In particular, we will go deep into special unitary groups because this is an extra requirement of physics. Besides, Hilbert spaces are the natural environment in quantum physics, so we will also introduce them.

2.1 Groups

A *group* is a set G, together with a binary operation $\circ$ that combines any two elements $a, b \in G$ in a certain manner; indeed, to qualify as a group, the pair $(G, \circ)$ must satisfy four requirements, known as the group axioms:

1. **Closure**

   For all a, b in G, the result of the operation $a \circ b$ is in G.

2. **Associativity**

   For all a, b and c in G, it holds that $(a \circ b) \circ c = a \circ (b \circ c)$.

3. **Identity element**

   There exists an element e in G such that, for every element $a \in G$, the equalities $a \circ e = e \circ a = a$ hold.

4. **Inverse element**

   For each a in G, there exists an element b, commonly denoted by a^{-1}, such that $a \circ b = b \circ a = e$.

Moreover, if any two elements in a group G commute, i.e. $a \circ b = b \circ a$ for all $a, b \in G$, then G is said to be **abelian**.

A subset of a group G which inherits its group structure is called a *subgroup* of G.

A *group homomorphism* is a map between two groups that preserves the group operations. This means, it is a map $f : (G, \circ) \to (H, *)$ between two groups $(G, \circ), (H, *)$ with identity elements e_G resp. e_H satisfying

$$f(e_G) = e_H$$
$$f(a \circ b) = f(a) * f(b)$$

for any $a, b \in G$.

Examples of abelian groups are $(\mathbb{Z}, +)$, or $(\mathbb{Q} \setminus \{0\}, \cdot)$. The usual matrix multiplication endows the set of all invertible matrices of size $n \times n$ with entries in a field K with the structure of group. This is called the general linear group, denoted by $\mathrm{GL}(n, K)$. We will always consider $K = \mathbb{C}$, therefore we will simply write $\mathrm{GL}(n)$ instead of $\mathrm{GL}(n, \mathbb{C})$. Observe that the general linear group is not abelian.

Let f be a homomorphism between $(G, \circ)$ and $(H, *)$. If e_H is the identity element of H, and we define the *kernel* of f to be

$$\ker(f) := \{g \in G \,|\, f(g) = e_H\},$$

then $\ker(f)$ is a subgroup of G.

Proposition 1. *Let $f : (G, \circ) \to (H, *)$ be a group homomorphism, then $(\ker(f), \circ)$ is a subgroup of G.*

Proof. We have to check that $(\ker(f), \circ)$ satisfies the group axioms. Obviously, associativity holds for $\circ$. Moreover, e_G belongs to $\ker(f)$ since $f(e_G) = e_H$ (recall that f is a group homomorphism).

Observe, moreover, that the closure axiom follows: given $g_1, g_2 \in \ker(f)$, then $f(g_1) = f(g_2) = e_H$, and so $g_1 \circ g_2 \in \ker(f)$ since $f(g_1 \circ g_2) = f(g_1) * f(g_2) = e_H * e_H = e_H$.

Finally, we only need to see that inverse element we must take is just e_G: if g^{-1} is the inverse of g, $f(g \circ g^{-1}) = f(e_G)$ implies $f(g) * f(g^{-1}) = e_H$, hence

$$f(g^{-1}) * e_H = e_H \Rightarrow f(g^{-1}) = e_H \Rightarrow g^{-1} \in \ker(f).$$

□

2.2 Hilbert spaces

A *Hilbert space H* is a complex inner product space that is also a complete metric space with respect to the distance function induced by the inner product.

Recall that a complex inner product space is a vector space H over the complex field on which there is an inner product $\langle x|y\rangle$ associating a complex number to each pair of elements $|x\rangle$,$|y\rangle$ of H that satisfies the following properties:

1. The inner product of a pair of elements is equal to the complex conjugate of the inner product of the swapped elements:
$$\langle x|y\rangle = \langle y|x\rangle^*$$
.

2. The inner product is linear in its first argument: for every $a, b \in \mathbb{C}$ it holds that
$$\langle x|ay_1 + by_2\rangle = a\langle x|y_1\rangle + b\langle x|y_2\rangle.$$

3. The inner product of an element with itself is positive definite:
$$\langle x|x\rangle \geq 0,$$
where the case of equality holds precisely when $|x\rangle = 0$.

Here we have used the bra-ket notation, also known as Dirac's notation. The notation uses angle brackets "⟨" and "⟩" and vertical bars "|". In such terms, the vectors of H are represented by "kets", $|x\rangle$, the scalar product between the vectors $|x\rangle \in H$ and $|y\rangle \in H$ is denoted by the "bracket", $\langle x|y\rangle$. Moreover, the "bra", $\langle x|$, stands here for the dual element to $|x\rangle \in H$, namely $\langle x|$ is the following linear map:
$$\langle x| : H \to \mathbb{C}, \quad |y\rangle \to \langle x|\,(|y\rangle) = \langle x|y\rangle.$$

This inner product induces a distance function $d : H \times H \to \mathbb{R}$ on H given by
$$d : H \times H \to \mathbb{R}, \quad d\,(|x\rangle, |y\rangle) := \|\,|x\rangle - |y\rangle\,\| = \sqrt{(\langle x| - \langle y|)\,(|x\rangle - |y\rangle)}$$

It is easy to check that d is a distance function, *i.e.*, a function such that for any $|x\rangle, |y\rangle, |z\rangle \in H$, the following holds:

1. Non-negativity: $d(|x\rangle, |y\rangle) \geq 0$ and $d(|x\rangle, |y\rangle) = 0$ if and only if $|x\rangle = |y\rangle$.

2. It is symmetric: $d(|x\rangle, |y\rangle) = d(|y\rangle, |x\rangle)$

3. It satisfies the triangle inequality: $d(|x\rangle, |z\rangle) \leq d(|x\rangle, |y\rangle) + d(|y\rangle, |z\rangle)$

With the distance function, the complex inner product space becomes a metric space. Finally, we recall that a complete metric space is a metric space where any Cauchy sequence is a convergent sequence.

We will work in finite dimensional spaces, i.e., we will assume $\dim(H) < \infty$. This means, the Hilbert space H is isomorphic to $\mathbb{C}^n$.

2.2.1 Linear operators in Hilbert spaces

Let H be a Hilbert space of dimension n. Let $\{|i\rangle\}_{i=1}^{n}$ be an orthogonal basis of H so that a vector $v \in H$ can be written as

$$v = \sum_{i=1}^{n} v^i |i\rangle.$$

We can describe the action of a linear map $U : H \to H$ on a vector v as

$$U(v) = \sum_{i=1}^{n} v^i U(|i\rangle).$$

On the other hand, since $U(v) \in H$, one may write

$$U(v) = \sum_{j=1}^{n} U(v)^j |j\rangle.$$

Taking into account that $\{|k\rangle\}_{k=1}^{n}$ is an orthonormal basis, one has

$$U(v)^k = \langle k|U(v) = \sum_{j=1}^{n} v^i \langle k|U|j\rangle = \sum_{j=1}^{n} U_{k,j} v^j.$$

We will use therefore $\langle k|U|j\rangle$ to describe the elements $U_{k,j}$ of the matrix associated to the linear map $U : H \to H$ with respect to the basis $\{|k\rangle\}_{k=1}^{n}$.

2.3 Special unitary groups

In quantum mechanics, special unitary groups play a key role, as already mentioned in the Introduction. Here we present the basics on unitary and special unitary groups with the hope of a better understanding of the main results of this master thesis.

2.3.1 Unitary group

The unitary group is the following subgroup of $\mathrm{GL}(n)$:

$$U(n) = \{U \in \mathrm{GL}(n) : U^\dagger U = U U^\dagger = I\},$$

where $U^\dagger$ is the conjugate transpose of U. Observe the following:

1. $U(n)$ is a subgroup of $\mathrm{GL}(n)$:
   (a) Each element of $U(n)$ has inverse $U^{-1} = U^\dagger \in U(n)$
   (b) The identity element satisfies the property

$$I = I^{-1} = I^\dagger \Longrightarrow I^\dagger I = I$$

(c) Closure and associativity: if A and $B \in U(n)$, then $AB \in U(n)$: indeed,

$$(AB)(AB)^\dagger = ABB^\dagger A^\dagger = AIA^\dagger = I$$

$$(AB)^\dagger(AB) = B^\dagger A^\dagger AB = I$$

Therefore $AB \in U(n)$.

2. The columns of a unitary matrix form an orthonormal basis.

   Indeed, since any $U \in U(n)$ is an invertible matrix, the columns of U are linearly independent when they are considered as vectors of $\mathbb{C}^n$. Moreover, if U_i stands for the i-th column of U, then we have

$$[U^\dagger U]_{ij} = \sum_k u_{ik}^* u_{kj} = \langle U_i, U_j \rangle = \delta_{ij}.$$

   The same argument applies to the rows.

3. $U(1) = \{e^{i\theta} : \theta \in \mathbb{R}\}$, because

$$(e^{i\theta})(e^{i\theta})^\dagger = (e^{i\theta})(e^{-i\theta}) = 1$$

$$(e^{i\theta})^\dagger(e^{i\theta}) = 1$$

4. If $u \in U(n)$, then $det(U) \in U(1)$:

$$det(UU^\dagger) = det(I) = 1 \Leftrightarrow det(U)det(U^\dagger) = 1$$

$$det(U)det(U)^* = 1 \Leftrightarrow |det(U)|^2 = 1 \Leftrightarrow \exists\theta / det(U) = e^{i\theta}$$

5. $det : U(n) \Leftrightarrow U(1)$ is group homomorphism. It is easy to show:

$$det(I) = 1$$

$$det(AB) = det(A)det(B)$$

   Hence, by Proposition 1 the kernel of the determinant is a subgroup of $U(n)$. This subgroup is called the special unitary group.

2.3.2 Special unitary group

The special unitary group is defined as

$$SU(n) := \{U \in U(n) \,/\, det(U) = 1\}$$

Proposition 2. *Given $U \in U(n)$, there exist $U_0 \in SU(n)$ and $\theta \in \mathbb{R}$ such that $U = e^{i\theta}U_0$*

Proof. We have already seen that $det(U) = e^{i\beta}$ for some $\beta \in \mathbb{R}$. This means that $\frac{det(U)}{e^{i\beta}} = 1$, therefore we can obtain $det(e^{-i\beta/n}U) = 1$, where n is the size of the matrix. Setting $U_0 = e^{-i\beta/n}U$, it is then clear that $U_0 \in SU(n)$. Moreover, we can "isolate" U, namely we can write $U = (e^{i\beta/n})U_0$. Now, by taking $\theta = \beta/n$ the statement follows. □

We have thus seen that we can decompose the unitary group as a product of $U(1)$ and the special unitary group:

$$U(n) = U(1) \times SU(n).$$

In quantum physics, unitarity is a restriction on the allowed evolution of quantum systems that ensures that the sum of probabilities of all possible outcomes of any event always equals 1. Let us put an example.

Example 3. Let be $|\varphi(t_1)\rangle$ the state of a quantum system at the moment $t = t_1$. Let $\hbar$ denote the reduced Planck constant, i.e., the quantum of action. In other words, the minimum amount of action involved in an interaction. We need to consider the evolution operator $U(t) = e^{-iHt/\hbar}$ to compute the evolved state, namely

$$|\varphi(t_2)\rangle = U(t)|\varphi(t_1)\rangle$$

As $U(t)$ is unitary, we have the equalities

$$\langle\varphi(t_2)|\varphi(t_2)\rangle = \langle U(t)\varphi(t_1)|U(t)\varphi(t_1)\rangle = \langle\varphi(t_1)|U(t)^* U(t)\varphi(t_1)\rangle = \langle\varphi(t_1)|\varphi(t_1)\rangle.$$

It is therefore clear that the probability is preserved.

We must here say that in a quantum state we cannot observe a global phase shift. Phase can only be determined when compared into to a reference. Same concept applies to the voltage, where only differences of voltage has physical meaning. The output state $e^{in\theta}|n\rangle_1$ is equivalent to the output state $|n\rangle_1$. There is no measurement that can distinguish that two states. For an operator E, we have the outcome 0 with probability $p(0) = \langle n|_1 E_0^* E_0 |n\rangle_1$, which is the same result we get for

$$p(0) = \langle e^{i\varphi} n|_1 E_0^* E_0 |n e^{i\varphi}\rangle_1 = \langle n|_1 e^{-i\varphi} E_0^* E_0 e^{i\varphi} |n\rangle_1.$$

Chapter 3

Physical preliminaries

We will study the behavior of optical systems that act on n identically photons in m different modes (intuitively, the modes are the places in which a photon can be or can go through). For a system with a total number of photons n, all the possible input states can be described as a linear combination of states:

$$|\Psi\rangle = |n_1\rangle_1 |n_2\rangle_2 \cdots |n_m\rangle_m,$$

with $n_1 + n_2 + \cdots + n_m = n$. The total number of basis states is then $M := \binom{m+n-1}{n}$.

The evolution of the quantum state in our system can be specified from a unitary matrix U so that $|\Psi_{out}\rangle = U|\Psi_{in}\rangle$.

In the linear optics model, any unitary transformation in m modes can be decomposed into a product of optical elements. The two best-known optical elements are called **phase shifters** and **beam splitters**. We will refer to these two types of elements together as **BOE** (Basic Optical Elements). Each of these two optical elements acts as an element $S \in U(M)$, i.e., its behaviour is modeled by a $M \times M$-unitary (complex) matrix;

3.1 One photon in two modes $(n = 1, m = 2)$

We start with the simplest system, namely one photon and two modes; we will see now how this can be done.

In this case, our Hilbert basis is

$$|1\rangle = |1,0\rangle$$
$$|2\rangle = |0,1\rangle$$

A **phase shifter** multiplies a single amplitude by $e^{i\theta}$. We can represent the evolution matrix as

$$\begin{pmatrix} \alpha'_S \\ \alpha'_T \end{pmatrix} := \begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_S \\ \alpha_T \end{pmatrix}$$

Figure 3.1: Beam splitter and phase shifter

if the phase shifter acts on the first mode, and as

$$\begin{pmatrix} \alpha'_S \\ \alpha'_T \end{pmatrix} := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} \alpha_S \\ \alpha_T \end{pmatrix}$$

if the phase shifter acts on the second mode.

A **beam splitter** modifies two amplitudes α_S and α_T as follows:

$$\begin{pmatrix} \alpha'_S \\ \alpha'_T \end{pmatrix} := \begin{pmatrix} \sin\alpha & \cos\alpha \\ \cos\alpha & -\sin\alpha \end{pmatrix} \begin{pmatrix} \alpha_S \\ \alpha_T \end{pmatrix}.$$

We can combine both elements to "create" the general BOE matrix

$$T = \begin{pmatrix} e^{i\theta}\sin\alpha & e^{i\theta}\cos\alpha \\ \cos\alpha & -\sin\alpha \end{pmatrix}$$

3.2 One photon in m modes $(n = 1, m$ free$)$

In the case of an arbitrary number m of modes and one single photon, the BOE acts as an element of $S \in U(m)$. Each BOE acts non-trivially on at most two modes, and it is the identity on the other $m-2$ modes.

Definition 4. A matrix $T_{i,j} \in U(n)$ is called a *Basic Optical Element acting between modes i and j* if $T_{i,j}$ is the identity except the submatrix

$$\begin{pmatrix} [T_{i,j}]_{i,i} & [T_{i,j}]_{i,j} \\ [T_{i,j}]_{j,i} & [T_{i,j}]_{j,j} \end{pmatrix}$$

which is a BOE matrix.

As an example, if we put a beam splitter $T_{4,2}$ that acts on the second and forth modes, the evolution matrix is

$$\begin{pmatrix} \alpha_1' \\ \alpha_2' \\ \alpha_3' \\ \alpha_4' \end{pmatrix} := T_{4,2} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sin\alpha & 0 & \cos\alpha \\ 0 & 0 & 1 & 0 \\ 0 & \cos\alpha & 0 & -\sin\alpha \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix}$$

The next step is the following, if we have a succession of N optical networks, the first with a matrix S_1 and the last with S_n, the total system has a scattering $S = S_N \cdots S_2 S_1$. Conversely, we will prove in theorem 5 that that any $m \times m$-unitary matrix S can be decomposed as a product $S = S_T \cdots S_1$, where each S_t is a BOE (that is, unitary matrix that acts non trivially on at most 2 modes and as the identity on the remaining $m-2$ modes)

3.3 n photons in m modes

We have n identical photons on m modes and they have to go through the BOEs. Now, we are going to explain how those elements act on the states.

The phase shifter adds a local phase θ in the i^{th} mode, so we multiply the amplitude by $e^{i\theta}$ once for each of the n_i photons on the mode i, which yields a (unitary) transformation that can be described in the form

$$|s_1\rangle \cdots |s_m\rangle \to e^{i\theta_1}|s_1\rangle \cdots e^{i\theta_m}|s_m\rangle.$$

The action of the beam splitter is more complex. There is an homomorphism φ, which maps a $m \times m$ unitary transformation U acting on a single photon to the corresponding $M \times M$-unitary transformation $\varphi(U)$ acting on n photons. Remember that we will prove we can decompose the $m \times m$-matrix U into a product $U = U_T \cdots U_1$. So we can write $\varphi(U)$ as

$$\varphi(U_T \cdots U_1) = \varphi(U_T) \cdots \varphi(U_1),$$

where each U_t is an optical element. So let

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be any 2×2 unitary matrix, which acts on the Hilbert space spanned by $|1,0\rangle$ and $|0,1\rangle$. Then, since $\varphi(U)$ preserves photon number, we know that it must be a block-diagonal matrix that satisfies

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

whenever $s+t \neq u+v$. Otherwise, when $s+t = u+v$, the formula is a bit more complicated (see [**?**]):

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

One can verify by (tedious) calculations that $\varphi(U)$ is unitary (see again [1]).

Chapter 4

Results

In this chapter we have two goals. First, we have decomposed any unitary matrix $m \times m$ into N BOEs. We have provided an algorithm that the input is the unitary matrix and the algorithm does the decomposition. And second, we need to evolve all these optical matrices. Again, we have compute other algorithm that the input is each BOE matrix which decomposed the unitary matrix. Basically, with the first goal, we can recreate in the laboratory any similar experiment if we know the unitary matrix. And the second goal tell us the theoretical results. So we can contrast both results.

4.1 The decomposition algorithm

We need to prove that any unitary matrix can be decomposed into N BOEs. We define a matrix T_{pq} which is an N-dimensional identity matrix with the elements I_{pp}, I_{pq} ,I_{qp} and I_{qq} replaced by the corresponding BOE matrix. The function if this matrix is to perform a unitary transformation in the two nodes affected and leaving the other $N-2$ unaffected. The experiment is build up by successively attaching the corresponding BOE. Once all elements of the last column except the one on the diagonal are zero, this row will not be affected by later transformations. After the final BOE transformation, one obtains a diagonal matrix with elements of modulus 1, we can make the resulting matrix equal to the identity,

$$D^{\dagger} T_{2,1}^{\dagger} \cdots T_{N,N-1}^{\dagger} U(N) = I(N)$$

The experimental set up is equivalent to the inverse (remember that we are working with unitary matrices) of the original $N \times N$ unitary matrix.

$$U(N) = T_{N,N-1} ... T_{2,1} D$$

Finally it is the time when the homomorphism shines. We do not know how to evolve $U(N)$, however, we know how to evolve each BOE.

$$\varphi(U(N)) = \varphi(T_{N,N-1}) ... \varphi(T_{2,1}) \varphi(D)$$

Besides, we can build this system in the laboratory in order to compare both results.

This first part of the algorithm makes use of the following theorem:

Theorem 5. *Let $U \in U(n)$ be a unitary matrix, then it can be decomposed as a product of at most $\frac{n(n-1)}{2}$ BOEs and a diagonal matrix D,*

$$U = T_{n,n-1} \cdots T_{2,1} D. \tag{4.1.1}$$

The proof of this theorem is based on the following lemma:

Lemma 6. *Let U_0 be a matrix in $U(n)$. Then there exist at most $n-1$ BOEs, namely $T^\dagger_{n,n-1}, \ldots, T^\dagger_{n,1}$, such that*

$$T^\dagger_{n,1} \cdots T^\dagger_{n,n-2} \cdot T^\dagger_{n,n-1} U_0 = \begin{pmatrix} a'_{1,1} & a'_{1,2} & \cdots & a'_{1,n-1} & 0 \\ a'_{2,1} & \ddots & & a'_{2,n-1} & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ a'_{n-1,1} & a'_{n-1,2} & \cdots & a'_{n-1,n-1} & 0 \\ 0 & 0 & \cdots & 0 & \alpha_1 \end{pmatrix} \tag{4.1.2}$$

where we call

$$U_1 := \begin{pmatrix} a'_{1,1} & a'_{1,2} & \cdots & a'_{1,n-1} \\ a'_{2,1} & \ddots & & a'_{2,n-1} \\ \vdots & & \ddots & \vdots \\ a'_{n-1,1} & a'_{n-1,2} & \cdots & a'_{n-1,n-1} \end{pmatrix} \in U(n-1),$$

and α_1 belongs to $U(1)$, i.e. $|\alpha_1| = 1$.

Proof. Given the matrix

$$U_0 = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & \ddots & & a_{2,n} \\ \vdots & & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

we can prove that there exists $T^\dagger_{n,n-1}$ such that

$$T^\dagger_{n,n-1} U_0 = \begin{pmatrix} a'_{1,1} & a'_{1,2} & \cdots & a'_{1,n} \\ a'_{2,1} & \ddots & & a'_{2,n} \\ \vdots & & \ddots & \vdots \\ a'_{n-1,1} & a'_{n-1,2} & \cdots & 0 \\ a'_{n,1} & a'_{n,2} & \cdots & a'_{n,n} \end{pmatrix} \tag{4.1.3}$$

The matrix $T^\dagger_{n,n-1}$ is completely determined by two variables: θ of the phase shifter and α of the beam splitter. These two variables depend on the specific values of the elements of U_0, $a_{n,n}$ and $a_{n-1,n}$. We choose

$$\alpha = \arctan\left(-\frac{|a_{n,n}|}{|a_{n-1,n}|}\right), \quad \theta = \arg(a_{n-1,n}) - \arg(a_{n,n})$$

when $a_{n,n} \neq 0$ and $a_{n-1,n} \neq 0$. We will choose $\theta = 0$ if $a_{n,n} = 0$ or $a_{n-1,n} = 0$ (or both) and we will choose $\alpha = \pi/2$ if $a_{n-1,n} = 0$. Observe, that in any case

$$\left(a_{n-1,n}\, e^{-i\theta} \sin\alpha + a_{n,n} \cos\alpha\right) = 0$$

hence,

$$\begin{aligned}
T^{\dagger}_{n,n-1}U|n\rangle =& T^{\dagger}_{n,n-1}\left(a_{1,n}|1\rangle + a_{1,n}|2\rangle + \cdots + a_{n-1,n}|n-1\rangle + a_{n,n}|n\rangle\right)\\
=& a_{1,n}|1\rangle + a_{2,n}|2\rangle + \cdots + a_{n-2,n}|n-2\rangle + a_{n-1,n}\left(e^{-i\theta}\sin\alpha|n-1\rangle + e^{-i\theta}\cos\alpha|n\rangle\right)\\
&+ a_{n,n}\left(\cos\alpha|n-1\rangle - \sin\alpha|n\rangle\right)\\
=& a_{1,n}|1\rangle + a_{2,n}|2\rangle + \cdots + a_{n-2,n}|n-2\rangle + \left(a_{n-1,n}\,e^{-i\theta}\sin\alpha + a_{n,n}\cos\alpha\right)|n-1\rangle\\
&+ \left(a_{n-1,n}\,e^{-i\theta}\cos\alpha - a_{n,n}\sin\alpha\right)|n\rangle\\
=& a_{1,n}|1\rangle + a_{2,n}|2\rangle + \cdots + a_{n-2,n}|n-2\rangle + \left(a_{n-1,n}\,e^{-i\theta}\cos\alpha - a_{n,n}\sin\alpha\right)|n\rangle\\
=& a'_{1,n}|1\rangle + a'_{2,n}|2\rangle + \cdots + a'_{n-2,n}|n-2\rangle + a'_{n,n}|n\rangle
\end{aligned}$$

and therefore equation (4.1.3) is fulfilled. Likewise, we can obtain $T^{\dagger}_{n,n-2}$ with θ' and α' depending on $a'_{n-2,n}$ and $a'_{n,n}$ such that

$$T^{\dagger}_{n,n-2}T^{\dagger}_{n,n-1}U|n\rangle = a''_{1,n}|1\rangle + a''_{2,n}|2\rangle + \cdots + a''_{n-3,n}|n-3\rangle + a''_{n,n}|n\rangle$$

Aplying this proceed we obtain

$$T^{\dagger}_{n,1}\cdots T^{\dagger}_{n,n-2}T^{\dagger}_{n,n-1}U|n\rangle = \alpha_1|n\rangle$$

which implies (4.1.2) because the columns and the rows of a unitary matrix are orthonormal vectors. □

Proof of Theorem 5. We are going to prove the theorem recursively. The first step is just the content of Lemma6. An inductive argument columnwise finishes the proof: taking into account that the matrix U_1 in the statement of the lemma belongs to $U(n-1)$, we can obtain a matrix $U_2 \in U(n-2)$ and a complex number $\alpha_2 \in U(1)$ by using some of the BOEs $T^{\dagger}_{n-1,n-2}, T^{\dagger}_{n-1,n-3}, \ldots, T^{\dagger}_{n-1,1}$. By repeating the process at most $\frac{n(n-1)}{2}$ BOEs, we obtain

$$T^{\dagger}_{n,1}\cdots T^{\dagger}_{2,1}U = \begin{pmatrix} \alpha_n & 0 & \ldots & 0 & 0\\ 0 & \alpha_{n-1} & & 0 & 0\\ \vdots & & \ddots & \vdots & \vdots\\ 0 & 0 & \ldots & \alpha_2 & 0\\ 0 & 0 & \ldots & 0 & \alpha_1 \end{pmatrix} = D,$$

which obviously implies equation (4.1.1). □

Observe that this proof is constructive. Hence, we can construct an algorithm (Algorithm [**?**]) to

implement the decomposition of a unitary matrix into BOEs.

Algorithm 7: Computing the matrix decomposition

Input: A unitary matrix $S = (s_{i,j})$

- - Size of the scattering matrix:
$m :=$ size of S;
$k := m$;
$j := k - 1$;
$B := S$;
repeat
  $k := k - 1$;
  $j := j - k$;
  if $s_{k,k} = 0$ **then**
    if $s_{k-j,k} = 0$ **then**
      Do nothing;
    else
      $\theta := 0$;
      $\alpha := 0$;
    end
  else
    if $s_{k-j,k} = 0$ **then**
      $\theta := 0$;
      $\alpha := \frac{\pi}{2}$;
    else
      $\theta := -\big(\mathrm{Arg}(s_{k,k}) - \mathrm{Arg}(s_{k-j,k})\big)$;
      $\alpha := \arctan\Big(-\frac{|s_{k,k}|}{|s_{k-j,k}|}\Big)$;
    end
  end
  Compute the matrix $T_{j,k} := T_{j,k}(\alpha, \theta)$;
  Compute the matrix $T_{j,k}^{\dagger}$;
  $B := T_{j,k}^{\dagger} \cdot B$;
until $k = 2,\ j = 1$;
- - Extract the angles of the beam splitters and phase shifters into lists:
$A := [\alpha_{m,m-1}, \alpha_{m,m-2}, \ldots, \alpha_{2,1}]$;
$Z := [\theta_{m,m-1}, \theta_{m,m-2}, \ldots, \theta_{2,1}]$;
- - Extract the diagonal matrix and the BOEs:
$D := B$;
BOE $:= [T_{m,m-1}, T_{m,m-2}, \ldots, T_{2,1}]$;

Output: list of numbers A and Z, a list of matrices BOE, a diagonal matrix D

In Chapter 7 we present a Mathematica program for implementing this algorithm.

4.1.1 Examples of application of the decomposition algorithm

To illustrate the method, we are going to show some examples. We start with a 2×2–Hadamard matrix, we will use this matrix in the second part of this paragraph:

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

We give this input to our algorithm and it returns the following matrix. Note that we only need to do one 0 (first row, second column) to get the diagonal matrix

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

In this particular case, we obtain the same matrix. It is not a good example of decomposition algorithm but it will be a very good example of the evolution matrix. If we multiple both matrix we get:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which is already diagonal.

Now, we are going to do an example with complex numbers. The matrix is simple, so we can obtain the diagonal matrix easily:

$$\begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}.$$

The matrices obtained by our algorithm are (remember that these matrices are the complex conjugate, the inverse, of the BOEs)

$$\begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ i & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} i & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Finally, we are going to do a more challenging case

$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

We can decompose this matrix as follows. First of all, we need to do the last column equals to 0 except the last element:

$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ -1/2 & 1/2 & -1/2 & 1/2 \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ -1/2 & 1/2 & -1/2 & 1/2 \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -\sqrt{\frac{2}{3}} & 0 & \frac{1}{\sqrt{3}} \\ 0 & 0 & 1 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ \frac{1}{\sqrt{6}} & -\sqrt{\frac{2}{3}} & \frac{1}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & -\frac{1}{2\sqrt{3}} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

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

the following step will be getting the zeros in the third column and so on.

4.2 The evolution algorithm

The second algorithm that we present in this work is the evolution algorithm. Once, we have decomposed the scattering matrix $S \in U(m)$ using the the decomposition algorithm (Algorithm 7) we can compute the evolution matrix by using the optical homomorphism $\varphi : U(m) \to U(N)$ on the BOEs (see section 3.3). More precisely, the first algorithm transforms the scattering matrix S as a product of BOEs,

$$S = T_{m,m-1} \cdots T_{2,1} \cdot D$$

and the second algorithm evolves the BOEs given by the first algorithm

$$\varphi(S) = \varphi(T_{m,m-1}) \cdots \varphi(T_{2,1}) \cdot \varphi(D)$$

This algorithm can be provided as follows:

Algorithm 8: Computing the evolution matrix

Input: A unitary matrix $S = (s_{i,j})$, the number of photons n

- - Size of the scattering matrix:
$m :=$ size of S;
- - Compute the dimension of the Hilbert space:
$M := \binom{m+n-1}{n}$;
- - Take angles of BOEs from Algorithm 7:
$A :=$ Algorithm7[1];
$Z :=$ Algorithm7[2];
$\ell :=$ length(A);
– Identity matrix of size M:
V:=I(M);
k:=1;
repeat
  $V = V \cdot \varphi(Z[k]) \cdot \varphi(A[k])$;
until $k = \ell$;
;
$D :=$ Algorithm7[3];
$V := V \cdot \varphi(D)$;

Output: the evolution matrix $V \in SU(M)$

Here we have assumed that we have algorithms computing the evolutions $\varphi(Z[k]), \varphi(A[k])$ resp. $\varphi(D)$ of the BOEs $Z[k]$ and $A[k]$ resp. the diagonal matrix D, where $Z[k], A[k]$ are the kth components of the first two lists A, Z which are outputs of Algorithm 7, and D is its third output.

In Chapter 7 we present a Mathematica program for implementing this algorithm.

4.2.1 Example of application of the algorithm of evolution

Suppose we have 2 photons and 2 modes in the Hadamard matrix

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

which can be represented as

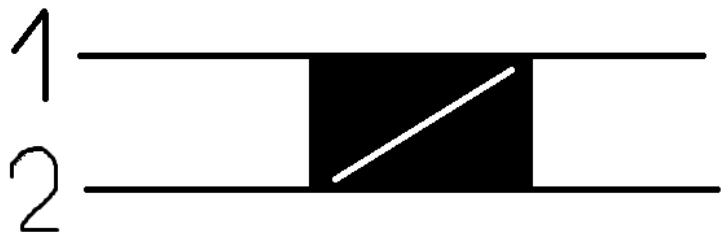


Figure 4.1: First example

The suitable basis is $|2,0\rangle$ (first row), $|1,1\rangle$ (second row) and $|0,2\rangle$ (last row). Remember that the decomposition matrix is

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

We can decomposed this BOE in the phase shifter matrix and the beam splitter matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The phase shifter matrix is the identity, so the evolution matrix is also the identity. We are going to verify this, the phase shifter is acting in the first row of the matrix, the evolution matrix is calculated raising the first element of the phase shifter matrix to the number of photons on each state($|2,0\rangle$ has two photons on the first mode, $|1,1\rangle$) has one photon and $|0,2\rangle$ has no photons)

$$\varphi(T_p) = \begin{pmatrix} 1^2 & 0 & 0 \\ 0 & 1^1 & 0 \\ 0 & 0 & 1^0 \end{pmatrix}$$

Using the beam splitter evolution formula, we can calculate the evolution matrix of the beam splitter. In this case, we have:

$$\varphi(T_b) = \begin{pmatrix} 1/2 & 1/\sqrt{2} & 1/2 \\ -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/2 & -1/\sqrt{2} & 1/2 \end{pmatrix}$$

Remember that we have ordered previously this matrix. The first element is then $\langle 2,0|\varphi(T)|2,0\rangle$, and the element of the second row, third column as $\langle 1,1|\varphi(T)|0,2\rangle$. You may change this order. If you multiply the Hadamard matrix by the BOE matrix you get:

$$D^{\dagger} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Now, we have to evolve the matrix D. The method is very similar to the phase shifter, but now you have to evolve each element instead of only the first element. The evolution of the first element (1) is:

$$\begin{pmatrix} 1^2 & 0 & 0 \\ 0 & 1^1 & 0 \\ 0 & 0 & 1^0 \end{pmatrix}$$

Again, we have ordered the rows: $|2,0\rangle$(first) , $|1,1\rangle$ (second), $|0,2\rangle$ (third). The second element (1):

$$\begin{pmatrix} 1^0 & 0 & 0 \\ 0 & 1^1 & 0 \\ 0 & 0 & 1^2 \end{pmatrix}$$

Look at the exponent, now the mode $|2,0\rangle$ has 0 photons in the second mode. The evolution of the phase shifter is

$$\varphi(D) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

And finally $\varphi(U) = \varphi(T_p)\varphi(T_b)\varphi(D)$:

$$\varphi(U) = \begin{pmatrix} 1/2 & 1/\sqrt{2} & 1/2 \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/2 & -1/\sqrt{2} & 1/2 \end{pmatrix}$$

Chapter 5

Interpretation of the results

In this chapter we will interpret the results in Chapter 4 from the point of view of the Physics. Thus, once we have the evolved matrix, we want to find out its physical meaning. For the sake of clarity, let us continue with the previous example (two photons in two modes). Then we consider again the initial matrix

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

As we already know, this matrix can be represented as a beam splitter as

Figure 5.1: Beam splitter representation of the matrix U

We have seen that its evolution matrix is

$$\varphi(U) = \begin{pmatrix} 1/2 & 1/\sqrt{2} & 1/2 \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/2 & -1/\sqrt{2} & 1/2 \end{pmatrix}.$$

Now, it is time to interpret this matrix. Recall that in our example there are three different initial states, namely $|2,0\rangle$, $|1,1\rangle$ and $|0,2\rangle$ (in this ordering!).

First of all, each column represents an initial state $|\Psi_{in}\rangle$ of the system, and each row is a final state $|\Psi_{out}\rangle$. The square of the element that intersects a row and a column is the probability that the given

initial state $|\Psi_{in}\rangle$ evolves to the final state $|\Psi_{out}\rangle$. For example, if the initial state is $|2,0\rangle$, i.e., the first column, then there is a 25% that the final state is $|2,0\rangle$ (the first row).

If the initial state $|\Psi_{in}\rangle$ is $|2,0\rangle$, the the final state $|\Psi_{out}\rangle$ has a probability 25% to be $|2,0\rangle$, 50% to be $|1,1\rangle$ and 25% to be $|0,2\rangle$. In other words, we can explain this result in classic physics as follows: there is a probability of 25% that the two photons remain in the same mode, a probability of 50% that one of the two photons changes to the other mode, and a probability of 25% that both photons change their mode. The case in which the initial state $|\Psi_{in}\rangle$ is $|0,2\rangle$ can be interpreted analogously, with the only difference that the photons are in the second mode instead of in the first mode.

However, the most interesting case is when the initial state $|\Psi_{in}\rangle$ is $|1,1\rangle$. We observe that $|\Psi_{out}\rangle$ has a probability of 50% to be $|2,0\rangle$, and 50% to be $|0,2\rangle$. Classically, we might think that the most probable final state will be $|1,1\rangle$, but contrary to this intuition, this state occurs with a probability of 0%, it means, it never ever happens. This is a famous effect in quantum optics called the **Hong-Ou-Mandel Effect**, see [7].

This phenomenon happens only when the two identical photons, *one in each mode*, enter to a beam splitter built in such a form that the photons have the same probability (i.e., 50%) to remain or change their mode. The result is that both photons leave the beam splitter in the same mode; this means, the state $|1,1\rangle$ is forbidden. This is a good example showing that quantum physics sometimes contradicts the intuition inherited from classical physics.

Now we are ready to do a more challenging example. Suppose we have 2 photons and 3 modes with the following scattering matrix:

$$S = \begin{pmatrix} -1/\sqrt{2} & -1/2 & 1/2 \\ 1/\sqrt{2} & -1/2 & 1/2 \\ 0 & 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

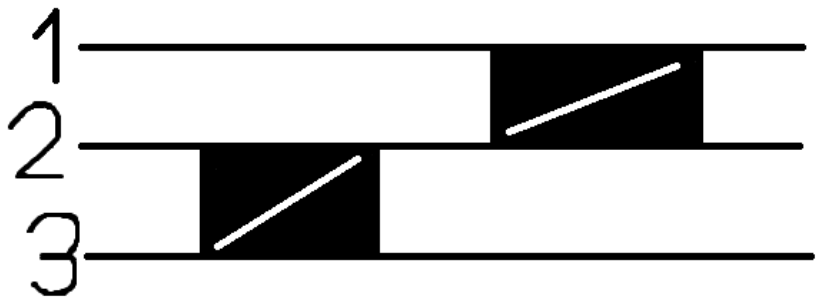


Figure 5.2: Beam splitter representing the scattering matrix S

The evolution matrix $\varphi(S)$ will be given with respect to the basis

$$|1\rangle = |2,0,0\rangle$$

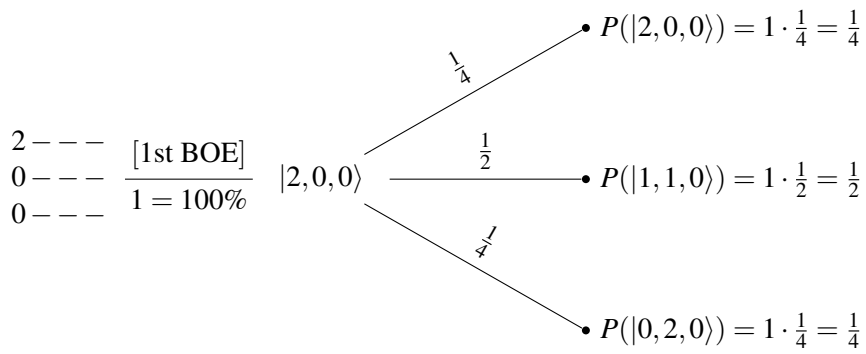
$$|2\rangle = |1,1,0\rangle$$
$$|3\rangle = |1,0,1\rangle$$
$$|4\rangle = |0,2,0\rangle$$
$$|5\rangle = |0,1,1\rangle$$
$$|6\rangle = |0,0,2\rangle$$

By using our Mathematica program we can compute the final evolution matrix:

$$\varphi(S) = \begin{pmatrix} 1/2 & 1/2 & -1/2 & 1/4 & -\frac{1}{2\sqrt{2}} & 1/4 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{2\sqrt{2}} & -1/2 & -\frac{1}{2\sqrt{2}} \\ 0 & -1/2 & -1/2 & -1/2 & 0 & 1/2 \\ 1/2 & -1/2 & -1/2 & 1/4 & -\frac{1}{2\sqrt{2}} & 1/4 \\ 0 & 1/2 & 1/2 & -1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 1/2 & \frac{1}{\sqrt{2}} & 1/2 \end{pmatrix}$$

We will start with the easy cases (basically, the cases corresponding to columns of $\varphi(S)$ containing zeros):

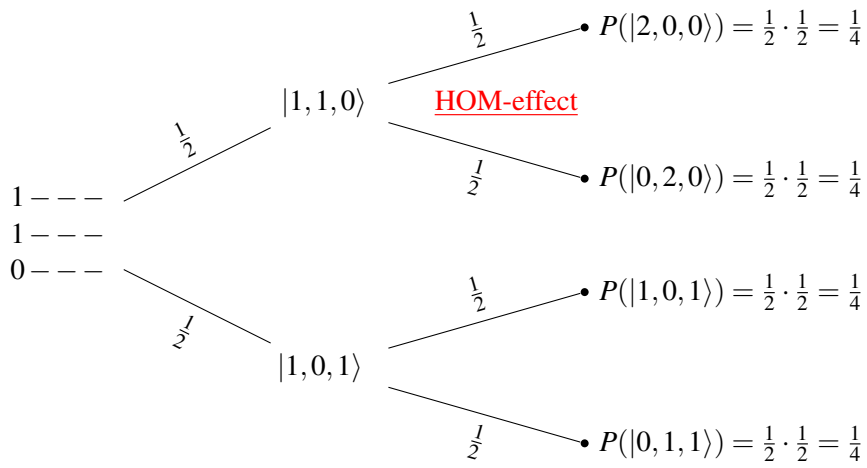
◇ The first column of the matrix $\varphi(S)$ represents the state with both photons in the first mode. We see in Figure 5.2 that the first BOE only affects the second and the third mode. At the beginning of the second BOE, both photons are in the first mode. We can explain this evolution classically: there is a probability of 25% that both photons remain in the first mode, 25% that both photons move to the second mode, and a probability of 50% that one photon remains in the first mode and the other photon changes to the second mode. This can be easily summarized in a probability tree:



Where here $P(|0,2,0\rangle)$, for instance, stands for the probability of transcition from the state $|2,0,0\rangle$ to the state $|0,2,0\rangle$.

◇ For the second column, i.e., the state $|1,1,0\rangle$, the evolution of the first BOE is easy: there is a probability of 50% that the state evolves in $|1,0,1\rangle$ and of 50% that it remains in the same state $|1,1,0\rangle$.

If the state $|1,0,1\rangle$ enters to the second BOE, then the third mode cannot change, and two cases arise: either the photon has a probability of 50% to remain in the first mode, which results in the final state $|1,0,1\rangle$, or the photon has a probability of 50% to change to the second mode, with final state $|0,1,1\rangle$. On the other hand, if the state $|1,1,0\rangle$ enters to the second BOE, Hong-Ou-Mandel Effect appears again, and this state can only evolve in $|2,0,0\rangle$ and $|0,2,0\rangle$. Altogether there are four equiprobable possibilities (i.e. 25% each one).

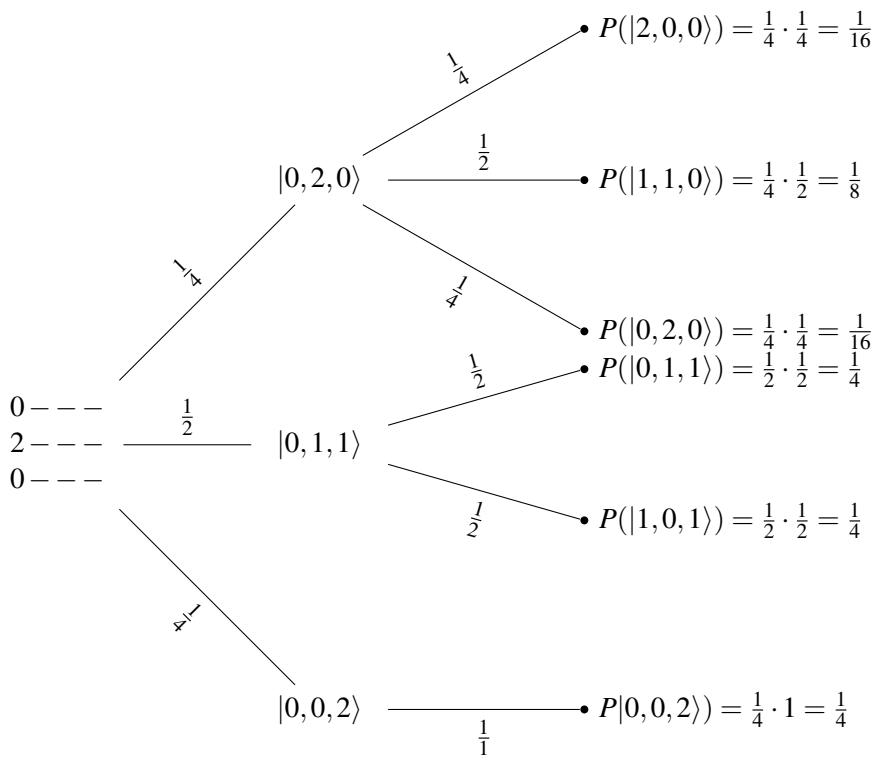


◇ The evolution of the state $|1,0,1\rangle$ is similar to that of $|1,1,0\rangle$, since the first BOE only affects the second and third modes, and both states have the same number of photons in these modes.

◇ The fifth column corresponds to the state $|0,1,1\rangle$. Again the Hong-Ou-Mandel Effect does occur when entering the first BOE, and the evolved state has a probability of 50% to be $|0,2,0\rangle$, and of 50% to be $|0,0,2\rangle$. Now the second BOE only affects the first and second mode, so the state $|0,0,2\rangle$ cannot evolve. On the contrary, the state $|0,2,0\rangle$ does evolve as expected: with a probability of 25% that both photons remain in the first mode, a probability of 25% that both photons move to the second mode, and a probability of 50% that one photon changes to the first mode and the other photon stays in the second one.

Let us go now to study of the more intricate cases (corresponding to thw forth and sixth columns of the evolution matrix $\varphi(S)$):

◇ We start with the forth column, $|0,2,0\rangle$. This state can evolve in three: $25\%|0,2,0\rangle$, $50\%|0,1,1\rangle$ and $25\%|0,0,2\rangle$. The last state can't evolve because it has no photons in the modes 1 and 2. The first state can evolve in $25\%|2,0,0\rangle$, $50\%|1,1,0\rangle$ and $50\%|0,2,0\rangle$. Finally, take care with the second state $|0,1,1\rangle$, it is similar to the Hong-Ou-Mandel Effect, however the modes affected are the first and the second, so this effect will not happen. The right evolved states are $50\%|1,0,1\rangle$, and $50\%|0,1,1\rangle$. One can verify that these probabilities agree with the elements of the matrix.



◇ Finally the last state, $|0,0,2\rangle$. The evolution is similar to $|0,2,0\rangle$, the only difference is that the photon is now on the third mode, but the evolution of the first BOE has the same probability.

Chapter 6

Conclusion

We have achieved the main purpose of this work, namely we have described an algorithm whose output gives the final evolution matrix of the linear optical systems under considerations. This algorithm has been split into two parts:

- ◇ The first part deals with the linear optical network S. We have shown that one may decompose the scattering matrix S, as a product of unitary block matrices; in particular, as a combination of beam splitters and phase shifters.
- ◇ The second part works out these decomposed matrices in the following manner: once we have calculated them, we have to evolve those matrices; at this point the group homomorphism φ is useful in order to evolve the matrices.

Again, we must say that this algorithm is handy. Given the scattering matrix S, the algorithm gives you the decomposed matrices and the evolve state. With both results, somebody can recreate the experiment in the laboratory and he can also contrast the theoretical results with the experimental results.

However, as already mentioned, the algorithm is computationally expensive. This means that it will only work efficiently for the case of simple systems, i.e., systems with a rather small number of photons and modes.

Chapter 7

Code

The input of this algorithm is the scattering matrix S and the photon number n. The first step is to calculate the dimension of S and the important basis of H, we save this basis as F in the algorithm.

```
(* Introduce la matriz S (unitaria) *)
S = {{-1/Sqrt[2], -1/2, 1/2}, {1/1/Sqrt[2], -1/2, 1/2}, {0, 1/Sqrt[2], 1/Sqrt[2]}};
UnitaryMatrixQ[S]
(* Una vez tenemos la matriz introducida podemos calcular el número de modos mirando su dimensión *)
m = Dimensions[S][[1]];
(* Por último solo nos queda introducir el número de fotones n *)
n = 2;
(* Calculamos las combinaciones de n y m *)
Multisets[l_List, k_]:=Union[Sort/@Flatten[Outer[List, Sequence@@Table[l, {k}]], k - 1]]
Multisets[n_, k_]:=Multisets[Range[n], k]
F[m_, n_]:=Table[Table[Count[Multisets[m, n][[k]], j], {j, 1, m}], {k, 1, Binomial[n + m - 1, n]}]//MatrixForm
(* Guardamos los vectores en la matriz A que posteriormente utilizaremos *)
A = F[m, n]
```

Then, we start with the decomposition algorithm, i.e., we calculated each BOE needed

```
(* Primero vamos a separar la matriz S en submatrices diagonales con bloques 2x2 *)
(* La matriz S2 es una ayuda *)
```

```
CopiaS = S;
S2 = IdentityMatrix[Binomial[n + m - 1, n]];
(* Definimos la matriz del elemento óptico *)
T[t_, w_]:={{Exp[I * t] * Sin[w], Exp[I * t] * Cos[w]}, {Cos[w], -Sin[w]}};
(* Empezamos diagonalizando *)
(* i indica el elemento de la diagonal, j los elementos que hay por encima *)

For[i = m, i > 1, i--,
G = S[[i, i]];
For[j = i - 1, j > 0, j--,
Copia = IdentityMatrix[m];
Print["i ", i, " j ", j, " G ", G, " elemento matriz ", S[[j, i]]//Simplify]
If[G == 0&&S[[j, i]] == 0, 0,
If[G == 0, t = 0; w = 0, 0];
If[S[[j, i]] == 0, (* 1 sí *)t = 0;
(*1No, 2Sí*)w = π/2, If[Arg[G] == π||Arg[G] == 0&&Arg[S[[j, i]]] == π||Arg[S[[j, i]]] == 0, (*2.Sí *)t = 0;
w = ArcTan[-G/S[[j, i]]], (*2.No, 3.Sí*)w = ArcTan[-Abs[G]/Abs[S[[j, i]]]]; t = -(Arg[G] - Arg[S[[j, i]]])]];
T2 = T[t, w];
iT2 = ConjugateTranspose[T[t, w]];
Print["w vale ", w//Simplify, " t vale ", t, " La matriz queda ", T2//Simplify//MatrixForm];
G = S[[j, i]] * Exp[-I * t] * Cos[w] - G * Sin[w]//Simplify;
(* Para una mejor visualización de los modos afectados ampliamos la dimensión a la original,
la matriz del elemento óptico representado es la inversa *)
For[l = 1, l ≤ m, l++,
For[k = 1, k ≤ m, k++,
If[l == j&&k == j, Copia[[l, k]] = iT2[[1, 1]];, 0;];
If[l == j&&k == i, Copia[[l, k]] = iT2[[1, 2]];, 0;];
If[l == i&&k == j, Copia[[l, k]] = iT2[[2, 1]];, 0;];
If[l == i&&k == i, Copia[[l, k]] = iT2[[2, 2]];, 0;];
```

```
(*Columnas*)];
(*Filas*)];
Print["La matriz traspuesta conjugada ampliada es: ", Copia//Simplify//MatrixForm];
CopiaS = Copia.CopiaS;
Print["La nueva matriz S es ", CopiaS//Simplify//MatrixForm];
```

Once we have calculated the BOEs, we start evolving them.

First, we calculate the phase shifter matrix. The algorithm needs the phase shifter matrix and F.

```
(* Empezamos a transformar cada elemento óptico *)
```

```
(* Primero de todo evolucionamos el phase shifter *)
BOE1 = {{Exp[I * t], 0}, {0, 1}};
Print["La matriz del phaseshifter es ", BOE1//MatrixForm];
If[t == 0, Copia2 = IdentityMatrix[Binomial[n + m - 1, n]],
z = Exp[I * t];
For[s = 1, s ≤ Binomial[n + m - 1, n], s++,
Copia2[[s, s]] = z^A[[1, s, j]];
(* Nos indica en qué fila de A estamos *)];
(* Nos indica en qué lugar de la diagonal estamos y en qué columna de A *)];
Print["La matriz de evolución del phase shifter es ", Copia2//MatrixForm];
S2 = S2.Copia2//Simplify;
Print["La matriz evolución es ", S2//Simplify//MatrixForm];
```

Then, the beam splitter. The algorithm needs the beam splitter and F.

```
(* Creamos la matriz donde iremos guardando los resultados de la transformación del beamsplitter *)
Print["Evolucionamos el beamsplitter"];
BOE2 = {{Sin[w], Cos[w]}, {Cos[w], -Sin[w]}};
Print["La matriz del beamsplitter es ", BOE2//MatrixForm];
Copia2 = ConstantArray[0, {Binomial[n+m-1, n], Binomial[n+m-1, n]}];
(* Fórmula de evolución de un beam splitter *)
For[r = 1, r <= Binomial[n+m-1, n], r++,
For[s = 1, s <= Binomial[n+m-1, n], s++,
contador = 0;
For[q = 1, q<=m, q++,
If[q != i&&q != j&&A[[1, r, q]] == A[[1, s, q]], contador = contador + 1, 0];
(* Cerramos el for para movernos *)];
Print["El contador vale ", contador];

If[A[[1, r, j]] + A[[1, r, i]]==A[[1, s, j]] + A[[1, s, i]]&&contador == m - 2,

suma = 0;
Raiz = Sqrt[Factorial[A[[1, s, j]]] * Factorial[A[[1, s, i]]]/(Factorial[A[[1, r, j]]] * Factorial[A[[1, r, i]]])];

Print["La columna es:", r, " La fila es:", s];
Print["s es ", A[[1, r, j]], " t es ", A[[1, r, i]]];
Print["u es ", A[[1, s, j]], " v es ", A[[1, s, i]]];
l1 = A[[1, s, j]];
For[k1 = 0, k1<=A[[1, s, j]], k1++,
Print["l vale:", l1, " t vale:", A[[1, r, i]]];
Print["k vale:", k1, " s vale:", A[[1, r, j]]];
If[l1 > A[[1, r, i]], 0;,
If[k1 > A[[1, r, j]], 0;,
```

```
Print["l es más pequeño que t:",l1,"<",A[[1,r,i]]];
Print["k es más pequeño que s:",k1,"<",A[[1,r,j]]];
If[BOE2[[1,1]]==0&&k1==0,aa = 1,aa = BOE2[[1,1]]^(k1)];
If[BOE2[[1,2]]==0&&A[[1,r,j]] - k1==0,bb = 1,bb = BOE2[[1,2]]^(A[[1,r,j]] - k1)];
If[BOE2[[2,1]]==0&&l1==0,cc = 1,cc = BOE2[[2,1]]^(l1)];
If[BOE2[[2,2]]==0&&A[[1,r,i]] - l1==0,dd = 1,dd = BOE2[[2,2]]^(A[[1,r,i]] - l1)];
suma = suma + Binomial[A[[1,r,j]],k1] * Binomial[A[[1,r,i]],l1] * aa * bb * cc * dd;
suma = Raiz * suma;
Print["El sumatorio vale:",suma];
Copia2[[r,s]] = suma;
(* Cerramos el if para saber si k es más pequeño que s *)];
(* Cerramos el if para saber si l es más pequeño que t *)];
l1 = l1 - 1;
(* Cerramos el bucle for de k1 *)]
,(* Cerramos el if que nos dice si tienen los mismos fotones *)0;]
(* Cerramos el for de s*)]
(* Cerramos el for de r*)]

Print["La matriz evolución del beamsplitter es ",Copia2//Simplify//MatrixForm];
S2 = S2.Copia2//Simplify;
Print["La matriz evolución es ",S2//Simplify//MatrixForm];

(* Cerramos el if si los dos elementos son 0, no hacer nada *)];
(* Cerramos el for de j *)];
S = CopiaS//Simplify;
(* Cerramos el for de i *)];
```

Finally, we have only to deal with the diagonal matrix D. And we print out the evolution matrix

```
(* Falta arreglar la diagonal para que sea la matriz identidad *)
S4 = IdentityMatrix[Binomial[n + m - 1, n]];
S5 = ConjugateTranspose[S];
For[r = 1(* nos indica en qué fila estamos de la matriz diagonal*), r ≤ m, r++,
S3 = IdentityMatrix[Binomial[n + m - 1, n]];
z = S5[[r, r]];
For[s = 1, s ≤ Binomial[n + m - 1, n], s++,
S3[[s, s]] = z^A[[1, s, r]];

(* Nos indica en qué fila de A estamos *)];
Print["La matriz del elemento ", r, " es "];
Print[S3//Simplify//MatrixForm];
S4 = S4.S3//Simplify;
(* Nos indica en qué lugar de la diagonal estamos y en qué columna de A *)];
Print["La multipicación de las anteriores matrices vale:"];
Print[S4//Simplify//MatrixForm];
(* Finalmente *)
S2 = S2.S4//Simplify;
Print["La evolución del estado es "];
Print[S2//Simplify //MatrixForm];
```

Bibliography

[1] S. AARONSON and A. ARKHIPOV, *The Computational Complexity of Linear Optics*. In "Proceedings of the 43rd Annual ACM Symposium on Theory of Computing" (ACM, New York, NY, USA, 2011), STOC'11, pp. 333–342.

[2] J. C. GARCÍA-ESCARTÍN, V. GIMENO and J. J. MOYANO-FERNÁNDEZ, *Multiple photon Hamiltonian in linear quantum optical networks*. Preprint, arXiv:1605.02653.

[3] D. J. GRIFFITHS, *Introduction to Quantum Mechanics*. Prentice Hall, 1995.

[4] J. J. MOYANO-FERNÁNDEZ and J. C. GARCÍA-ESCARTÍN, *Linear optics only allows every possible quantum operation for one photon on one port*. Optics communications **382**, pp. 237–240.

[5] G. NAVARRO, *Un curso de álgebra*. Universitat de València, 2002.

[6] M. A. NIELSEN and I. L. CHUAN, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge U.P, 2010.

[7] C. K. HONG, Z. Y. OU, L. MANDEL, *Measurement of subpicosecond time intervals between two photons by interference*. Physical Review Letters **59**, no.18, 1987, pp. 2044–2046.

[8] M. RECK, A. ZEILLINGER, H. J. BERNSTEIN and P. BERTANI, *Experimental Realization of Any Discrete Unitary Operator*. Physical Review Letters **73**, no. 1, 1994, pp. 58–61.