Optics Communications 382 (2017) 237–240

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Linear optics only allows every possible quantum operation for one photon or one port

Julio José Moyano-Fernández [a], Juan Carlos Garcia-Escartin [b,*]

[a] Universitat Jaume I, Departamento de Matemáticas and IMAC-Institut Universitari de Matemàtiques i Aplicacions de Castelló, 12071 Castellón de la Plana, Spain

[b] Dpto. de Teoría de la Señal y Comunicaciones e Ingeniería Telemática, ETSI de Telecomunicación, Universidad de Valladolid, Campus Miguel Delibes, Paseo Belén 15, 47011 Valladolid, Spain

ARTICLE INFO

Article history:
Received 29 June 2016
Received in revised form
27 July 2016
Accepted 30 July 2016

Keywords:
Quantum optics
Linear optics multiports
No-go theorems

ABSTRACT

We study the evolution of the quantum state of n photons in m different modes when they go through a lossless linear optical system. We show that there are quantum evolution operators U that cannot be built with linear optics alone unless the number of photons or the number of modes is equal to one. The evolution for single photons can be controlled with the known realization of any unitary proved by Reck, Zeilinger, Bernstein and Bertani. The evolution for a single mode corresponds to the trivial evolution in a phase shifter. We analyze these two cases and prove that any other combination of the number of photons and modes produces a Hilbert state too large for the linear optics system to give any desired evolution.

1. Quantum optics in photon-preserving linear systems

There are many optical elements that can affect the quantum state of light. Elements that preserve the number of photons are particularly interesting in quantum optics and in applications to quantum information [1–3]. Linear, lossless, passive systems have received a great deal of attention since the demonstration that, combined with measurement, they can be used to build a universal quantum computer [4]. Recently there has been a revived interest kindled by the result that the output statistics of linear optics multiports cannot be accurately predicted in a classical computer efficiently unless several well-founded computational complexity hypothesis are false [5].

In this paper, we study the behavior of optical systems that act on n photons in m different modes. We call $m\times m$ multiport to a linear optical system that conserves the number of photons (it is lossless and passive). The evolution of the state of the photons can be characterized from the scattering matrices S used to describe m-ports in classical electromagnetism [6]. The simplest example is a system with photons traveling in different paths, but we can also imagine photons in orthogonal polarization states or which have orthogonal orbital angular momentum states. We stick to the port denomination for the intuitive picture it gives, but it is enough that the photons can be in different orthogonal modes. The key is that two photons in different modes are perfectly distinguishable and do not interfere.

The inputs to our system are a combination of states with n_i photons in a mode with index i, denoted by $|n_i\rangle_i$. For a system with a total number of photons n, all the possible input states can be described as a linear combination of states

$$|\Psi\rangle = |n_1\rangle_1|n_2\rangle_2\cdots|n_m\rangle_m \quad (1)$$

with $n_1+n_2+\cdots+n_m=n$. Linear optics multiports present at their output a linear combination of states of the same form.

The evolution of a photonic quantum state in our system can be specified from a unitary matrix U so that $|\Psi_{out}\rangle = U|\Psi_{in}\rangle$. The classical scattering matrix S is enough to characterize the evolution of any number of photons entering the multiport. Both S and U must be unitary matrices as they describe systems that conserve energy and the total probability, respectively.

The step from S to U depends on the number of photons. If we take the basis composed of the number states of Eq. (1), the element of U that describes the transition from $|\Psi_{in}\rangle = |n_1\rangle_1|n_2\rangle_2\cdots|n_m\rangle_m$ to $|\Psi_{out}\rangle = |n_1'\rangle_1|n_2'\rangle_2\cdots|n_m'\rangle_m$ can be determined from $\langle n_1'|_1\langle n_2'|_2\cdots\langle n_m'|_m U|n_1\rangle_1|n_2\rangle_2\cdots|n_m\rangle_m$, which has a value

$$\frac{\mathrm{Per}(S_{in,out})}{\sqrt{n_1'!\cdot n_2'!\cdots n_m'!\cdot n_1!\cdot n_2!\cdots n_m!}}. \quad (2)$$

* Corresponding author.
E-mail addresses: moyano@uji.es (J.J. Moyano-Fernández), juagar@tel.uva.es (J.C. Garcia-Escartin).

http://dx.doi.org/10.1016/j.optcom.2016.07.085
0030-4018/

In Eq. (2), $\text{Per}(S_{\text{in,out}})$ is the permanent of a matrix $S_{\text{in,out}}$ with elements $S_{i,j}$ from S such that each row index i appears exactly n_i' times and each column index j is repeated exactly n_j times [5,7].

Alternatively, we can write our number states from their creation operators [8] so that

$$|n_i\rangle_i = \frac{\hat{a}_i^{\dagger}}{\sqrt{n_i!}}|0\rangle_i \tag{3}$$

and see how the operators transform. For a linear optics multiport, we know [9] the creation operator $\hat{a}_i^{\dagger}$ evolves into

$$\sum_{j=1}^{m} S_{ji}\hat{a}_j^{\dagger}. \tag{4}$$

The size of the scattering matrix is a function of the number of inputs and outputs of the optical system. S is an $m \times m$ matrix, whereas U is an $M \times M$ matrix, with M the size of the Hilbert space that contains all the possible configurations of n photons divided into m modes. These different states form a complete basis of the state space and their number is equivalent to the number of ways of placing n indistinct balls in m different boxes, which is the combinatorial number

$$M = \binom{m+n-1}{n} = \frac{(m+n-1)!}{(m-1)!n!}. \tag{5}$$

We can generate all the possible states recursively if we assign a photon number i from 0 to n to the first mode and then generate all the possible states for the $n-i$ remaining photons in the rest of the modes. By the time we arrive to the last mode the assignment is trivial and we can repeat the procedure until we have a complete list.

2. Universal quantum transformations

We say we have universality if, for our number of photons n and the number of modes m of our system, we can generate any desired quantum evolution U in the state space of all the possible distributions of the n photons in the m modes.

In this paper, we show that there are limitations to the quantum transformations U we can create from a linear optics multiport. While we can implement any desired unitary scattering matrix S using only beam splitters and phase shifters [10], a tailored S can only produce any arbitrary U in a limited set of cases.

This is a problem different from finding a universal set of gates for quantum computation. In most linear optics implementations of quantum computing we restrict ourselves to only a subset of all the possible quantum states and there is some kind of postselection.

3. Degrees of freedom and universality

The main result of the paper is a proof that there is a necessary condition for universality which is only satisfied in a limited number of cases for which there are explicit ways to describe how we can generate any desired U.

The basic argument is that the degrees of freedom we have when we build the multiport must be at least equal to the degrees of freedom in the photonic Hilbert space. Otherwise, there will be transformations that are impossible to perform.

This intuitive argument becomes clear from the combinatorial growth of M with the size of the problem, which rapidly overtakes the available degrees of freedom in S. While it is obvious that for an increasing size this must be the case and this limitation is commonly taken for granted [11], in this paper we provide an explicit proof of impossibility and give an exhaustive analysis of the number of photons and ports for which we can build any wanted unitary.

First we formalize the degrees of freedom argument in terms of group theory.

Lemma 1. *A linear optics multiport with m inputs cannot be used to give all the possible quantum evolutions in the state space of n photons in m distinct modes unless $m \geq M$, where M is the dimension of the Hilbert space of the photonic states.*

Proof. The unitary group $U(m^2)$ contains the $m \times m$ matrices S that describe the linear optics system and the unitary group $U(M^2)$ contains the $M \times M$ matrices U that describe the quantum evolution of the photons' state. Using the expression of Eq. (2) or Eq. (4) we can define a group homomorphism $\varphi: S \to U$ which maps $U(m^2)$ to $U(M^2)$ preserving the group structure [5]. We can only reach all the matrices in $U(M^2)$ if φ is surjective, which for our unitary groups is equivalent to asking for φ to be an epimorphism. The homomorphism can only be surjective if the dimension of the domain of φ is at least as large as its codomain (the image). In our problem, the condition is $m^2 \geq M^2$, which, for the ranges we are interested in, reduces to the necessary condition for universality

$$m \geq \binom{m+n-1}{n}. \quad \square \tag{6}$$

The intuition behind this result is that we have only a limited number of degrees of freedom when we build the linear optics system. If the target state space is too big, we cannot reach all the possible matrices U.

In terms of matrices, we can give a more relaxed argument pointing out that an $m \times m$ unitary matrix has m^2 real degrees of freedom. Any unitary matrix U can be written as the exponential of a Hermitian matrix $H = H^{\dagger}$ where we can only choose m real values for the main diagonal of H and $(m^2 - m)/2$ free complex parameters for the upper (or lower) triangular matrix excluding the main diagonal. This makes a total of m^2 real parameters. If $M > m$, there are only m^2 real parameters that cannot give all the possible variations of the M^2 real parameters of an $M \times M$ unitary matrix.

In the following sections, we show that in all the cases where necessary condition of Eq. (6) is met ($n=0$, $n=1$ and $m=1$), there is also an explicit way to find any desired unitary. For $n > 1$ and $m > 1$ we prove it is impossible to implement all possible unitary matrices U using linear optics alone.

3.1. The vacuum state is always taken to the vacuum

The first trivial result is that linear optics preserves the vacuum state with zero photons. This is obvious as a passive linear optics multiport cannot create photons, but can also be deduced from the necessary condition of Eq. (6). For $n=0$, our Hilbert space has a dimension

$$M = \binom{m+n-1}{n} = \binom{m-1}{0} = 1 \tag{7}$$

and $m \geq 1$ for any linear optics system, which will have, at least, one input. There can be many unused degrees of freedom. With no photons the exact configuration of the linear optics multiport is irrelevant and we can choose different scattering matrices.