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

Julio José Moyano-Fernández*
Universitat Jaume I, Departamento de Matemáticas and IMAC-Institut Universitari de Matemàtiques i Aplicacions de Castelló, 12071 Castellón de la Plana, Spain.

Juan Carlos Garcia-Escartin†
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.

(Dated: February 5, 2016)

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.

PACS numbers: 42.50.-p, 42.79.-e, 02.10.Ox

I. 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 behaviour of optical systems that act on n photons in m different modes. We call $m \times m$ multiports to the optical systems of interest. The evolution of the state of the photons can be characterized from the scattering matrices S used to describe m-ports in classical electromagnetism. We stick to the port denomination for the intuitive picture it gives, but the photons can really be in different orthogonal modes. The key is that two photons in different modes are perfectly distinguishable and do not interfere. The simplest example is a system with photons travelling in different paths, but we can also imagine photons in orthogonal polarization states or which have orthogonal orbital angular momentum states.

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

$$|\Psi\rangle = |n_1\rangle_1 |n_2\rangle_2 \dots |n_m\rangle_m \tag{1}$$

with $n_1 + n_2 + \ldots + n_m = n$. 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 $|\Psi_{\text{out}}\rangle = U|\Psi_{\text{in}}\rangle$. 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 $|\Psi_{\text{in}}\rangle = |n_1\rangle_1 |n_2\rangle_2 \dots |n_m\rangle_m$ to $|\Psi_{\text{out}}\rangle = |n'_1\rangle_1 |n'_2\rangle_2 \dots |n'_m\rangle_m$ can be determined from $\langle n'_1|_1 \langle n'_2|_2 \dots \langle n'_m|_m U |n_1\rangle_1 |n_2\rangle_2 \dots |n_m\rangle_m$, which has a value

$$\frac{\text{Per}(S_{\text{in,out}})}{\sqrt{n_1!' \cdot n'_2! \cdots n'_m! \cdot n_1! \cdot n_2! \cdots n_m!}}. \tag{2}$$

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, 6].

Alternatively, we can write our number states from their creation operators so that $|n_i\rangle_i = \frac{\hat{a}_i^\dagger}{\sqrt{n_i!}}|0\rangle_i$ and see how the operators transform. For a linear optics multi-

* moyano@uji.es
† juagar@tel.uva.es

port, we know [7] the creation operator $\hat{a}_i^\dagger$ evolves into

$$\sum_{j=1}^{m} S_{ji}\hat{a}_j^\dagger. \tag{3}$$

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

$$M = \binom{m+n-1}{n} = \frac{(m+n-1)!}{(m-1)!\ n!}. \tag{4}$$

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.

II. 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 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 [8], 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.

III. 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.

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) we can define an homomorphism $\varphi : S \to U$ which maps $U(m^2)$ to $U(M^2)$ [5]. We can only reach all the matrices in $U(M^2)$ if φ is surjective, which for our unitary groups is equivalent to ask 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. 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

$$m \geq \binom{m+n-1}{n}. \tag{5}$$

■

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 the following sections, we show that in all the cases where necessary condition 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.

A. 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. (5). Our Hilbert space has a dimension

$$M = \binom{m+n-1}{n} = \binom{m-1}{0} = 1 \tag{6}$$

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.

B. Systems with one port are equivalent to a phase shifter and trivially give universality for any number of photons

When $m = 1$ we have a similar situation. For any number of photons n

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

and the necessary condition of Eq. (5) is met with $m = 1 = M$. The interpretation is also clear. If we have only one mode, the only allowed physical operation is a phase shift which is equivalent to a 1×1 unitary matrix $S = (e^{i\phi})$ whose only element is a root of unity. The linear optics system can only be a phase shifter. The evolution for n photons is then a phase term $e^{in\phi}$. We can use our degree of freedom ϕ to give any output phase shift we want and we have universality.

However, in a quantum state we cannot observe a global phase shift. Phase can only be determined when compared to a reference, like in interference between states. This is similar to the definition of voltage, where only differences of voltage have a physical meaning. The output state $e^{in\phi}\left|n\right\rangle_1$ is equivalent to the input state $\left|n\right\rangle_1$. There is no measurement that can distinguish between these two states. For a set of measurement operators $\{E_o\}$, we obtain outcome o with probability $p(o) = \left\langle n\right|_1 E_o^\dagger E_o \left|n\right\rangle_1$ for $\left|n\right\rangle_1$, which is the same result we get for $\left\langle n\right|_1 e^{-i\phi} E_o^\dagger E_o e^{i\phi} \left|n\right\rangle_1$. In this case, any unitary matrix U is, really, equivalent to the identity matrix I.

Notice that the equivalence disappears if we have a reference state. If we had one photon in a reference path, the effect of the phase shifter could be observed with a well designed measurement. But then we would be in a different case with $m > 1$.

C. Linear optics multiports can give any possible quantum transformation for one input photon

The next interesting case is the evolution of a single photon in an arbitrary multiport with $m \geq 1$ ports. Here

$$M = \binom{m+n-1}{n} = \binom{m}{1} = m \tag{8}$$

and we fulfill the necessary condition with $m = M$. One basis of the Hilbert space of the photon states is the basis of elements $\left|i\right\rangle$ where $i = 1, \ldots, m$ is the index of the mode our only photon is in. State $\left|i\right\rangle$ corresponds to a column vector filled with zeros and a 1 entry in row i. From the definition in Eq. (2) we can see that, for one photon, $\left\langle j\right| U \left|i\right\rangle = S_{j,i}$. The permanent $\mathrm{Per}(S_{\mathrm{in,out}})$ is exactly the only element of the matrix $S_{\mathrm{in,out}} = (S_{j,i})$ and $U = S$.

We can then implement any desired unitary directly by choosing the appropriate matrix S. There are constructive methods to implement any unitary S using only beam splitters and phase shifters [8] or only one kind of beam splitter for $m \geq 3$ [9, 10].

This result cannot be used to build a scalable universal quantum computer. If we want to implement an algorithm acting on q qubits, we need to use 2^q paths to generate all the possible states. This exponential growth prevents a generalized use of linear optics with one photon for quantum computation.

D. Linear optics alone cannot give any desired quantum transformation for more than one input photon in more than one mode

Apart from the limited results of the previous sections, in general, linear optics multiports cannot give any desired unitary evolution.

Theorem 1 *A linear optics multiport with $m > 1$ inputs cannot be used to give all the possible quantum evolutions in the state space of $n > 1$ photons in m distinct modes.*

Proof We consider all the cases with $m > 1$ and $n > 1$. From Eq. (4)

$$M = \binom{m+n-1}{n} = \frac{(m+n-1)\cdots(m+1)\cdot m}{n!} = m\frac{(m+1)\cdots(m+n-1)}{2\cdot 3\cdots n}. \tag{9}$$

We can write the dimension of the photons' Hilbert space as

$$M = m\cdot\frac{m+1}{2}\cdot\frac{m}{3}\cdots\frac{m+n-1}{n} = m\prod_{k=2}^{n}\left(\frac{m-1+k}{k}\right), \tag{10}$$

with a product of terms $1+\frac{m-1}{k} > 1$ if $m > 1$. For $n > 1$ and $m > 1$ there is at least one such term in the product and it is immediate to prove $M > m$ which violates the necessary condition of Eq. (5). ■

IV. COMMENTS AND EXAMPLES

We have shown that, except for a few restricted cases, linear optical systems cannot be used to give any desired quantum evolution for n photons divided into m optical modes. We have given a necessary condition for universality and proved that when the condition is satisfied there are explicit constructions for any unitary evolution U we require.

It is still open how severe this restriction is. In the condition $m \geq M$, the growth of M as $\binom{m+n-1}{n}$ suggests a smaller number of achievable operators U for higher values of n and m. However, there can be important limitations even for small state spaces. We can show that in a simple example with two input ports and two photons.

The linear optics system is determined by the unitary matrix

$$S = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix}. \tag{11}$$

From Eq. (3), we can see an input state $|n_1\rangle_1 |n_2\rangle_2$ has an output

$$\frac{1}{\sqrt{n_1! n_2!}} (S_{11}\hat{a}_1^\dagger + S_{21}\hat{a}_2^\dagger)^{n_1} (S_{12}\hat{a}_1^\dagger + S_{22}\hat{a}_2^\dagger)^{n_2} |0\rangle_1 |0\rangle_2 . \tag{12}$$

For the basis $\{|2\rangle_1 |0\rangle_2 , |0\rangle_1 |2\rangle_2 , |1\rangle_1 |1\rangle_2\}$ and defining

$$|2\rangle_1 |0\rangle_2 = |20\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |0\rangle_1 |2\rangle_2 = |02\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

$$|1\rangle_1 |1\rangle_2 = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

the unitary matrix that gives the evolution of the photons' state is

$$U = \begin{pmatrix} S_{11}^2 & S_{12}^2 & \sqrt{2}S_{11}S_{12} \\ S_{21}^2 & S_{22}^2 & \sqrt{2}S_{21}S_{22} \\ \sqrt{2}S_{11}S_{21} & \sqrt{2}S_{12}S_{22} & S_{11}S_{22} + S_{12}S_{21} \end{pmatrix}. \tag{13}$$

We can review many interesting known phenomena from this description. Take for instance the Hadamard matrix that corresponds to a balanced beam splitter

$$S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{14}$$

For an input state $|11\rangle$, if we substitute the relevant terms in Eq. (13) and operate, we get the evolution

$$U|11\rangle = \frac{|20\rangle - |02\rangle}{\sqrt{2}}. \tag{15}$$

This is the simplest example of quantum interference between indistinguishable photons and it is described in the famous Hong-Ou-Mandel experiment [11].

We can also use this simple example to show there are forbidden operations. For instance, the evolution

$$U = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \tag{16}$$

is impossible as we cannot, among others, make $S_{21}^2 = 0$ and $\sqrt{2}S_{11}S_{21} = 1$ at the same time.

We can go a bit further and give bounds to how close we can get to a given state when we start with a fixed input. If we use the general expression in Eq. (13), we can see the output state for an input $|11\rangle$ is

$$|\Phi_{\text{out}}\rangle = \begin{pmatrix} \sqrt{2}S_{11}S_{12} \\ \sqrt{2}S_{21}S_{22} \\ S_{11}S_{22} + S_{12}S_{21} \end{pmatrix}. \tag{17}$$

Imagine we want to obtain the output state $|20\rangle$. We know this is impossible because it would require the matrix of Eq. (16), up to a global phase. We can, instead, search for the closest possible state, as measured from the overlap

$$|\langle 20| U |11\rangle|^2 = 2|S_{11}|^2|S_{12}|^2 = 2|S_{11}|^2(1-|S_{11}|^2), \tag{18}$$

where we use S is unitary and therefore $|S_{11}|^2 + |S_{12}|^2 = 1$. We would like to get $|\sqrt{2}S_{11}S_{12}| = 1$, but we must settle with maximizing $2|S_{11}|^2(1-|S_{11}|^2)$. The entry is maximized for $|S_{11}|^2 = \frac{1}{2}$ with a maximum overlap $\frac{1}{2}$, which is exactly the case in the Hong-Ou-Mandel experiment. This example shows the limitations can be severe even for values of M slightly above m, like our example with $M = 3$ and $n = 2$.

We can also wonder if the results are valid outside Fock states. However, other states, like coherent states

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle \tag{19}$$

can always be written as a linear superposition of number states. Linear optics preserves the number of photons and we can study separately the evolution for different photon numbers. For most of the terms in the superposition we cannot achieve any arbitrary evolution. Unless we only have superpositions of states for which universal evolution is possible there will be forbidden operations.

The restrictions of the achievable evolutions U does not mean we cannot produce any desired output state. We can always introduce the desired state $|\Psi\rangle$ in a linear system with a scattering matrix S and measure the output $|\Phi\rangle$. The inverse system, with matrix $S^\dagger$, will produce an output $|\Psi\rangle$ for an input $|\Phi\rangle$. Trivially, if $S = I$ we can generate any output by choosing that state at the input. This only shows that arbitrary state preparation is equivalent to preparing a known state and being able to perform an arbitrary evolution.

The interest of the presented result lies in the realization that certain states cannot be achieved from certain inputs. Determining which states can be reached for any given input state is left as an open problem that will require different methods that the ones presented here.

ACKNOWLEDGMENTS

The first author has been partially supported by the Spanish Government Ministerio de Economía y Competitividad (MINECO), grant MTM2012-36917-C03-03, and by Universitat Jaume I, grant P1-1B2015-02.

[1] R.A. Campos, B.E.A. Saleh, and M.C. Teich, "Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statistics," Phys. Rev. A **40**, 1371–1384 (1989).

[2] U. Leonhardt, "Quantum physics of simple optical instruments," Reports on Progress in Physics **66**, 1207 (2003).

[3] P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J.P. Dowling, and G.J. Milburn, "Linear optical quantum computing with photonic qubits," Reviews of Modern Physics **79**, 135 (2007).

[4] E. Knill, R. Laflamme, and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46–52 (2001).

[5] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," in *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, STOC '11 (ACM, New York, NY, USA, 2011) pp. 333–342.

[6] S. Scheel, "Permanents in linear optical networks," quant-ph/0406127 (2004).

[7] J. Skaar, J.C. Garcia-Escartin and H. Landro, "Quantum mechanical description of linear optics," American Journal of Physics **72**, 1385–1391 (2004).

[8] M. Reck, A. Zeilinger, H.J. Bernstein and P. Bertani, "Experimental realization of any discrete unitary operator," Physical Review Letters **73**, 58 (1994).

[9] A. Bouland and S. Aaronson, "Generation of universal linear optics by any beam splitter," Physical Review A **89**, 062316 (2014).

[10] A. Sawicki, "Universality of beamsplitters," Quantum Information and Computation **16, 3&4**, 0291–0312 (2016).

[11] C.K. Hong, Z.Y. Ou and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," Physical Review Letters **59**, 2044–2046 (1987).