Method to determine which quantum operations can be realized with linear optics with a constructive implementation recipe

Juan Carlos Garcia-Escartin*
Universidad de Valladolid, Dpto. Teoría de la Señal e Ing. Telemática, Paseo Belén No. 15, 47011 Valladolid, Spain

Vicent Gimeno† and Julio José Moyano-Fernández‡
Universitat Jaume I (UJI), Campus de Riu Sec, Institut Universitari de Matemàtiques i Aplicacions de Castelló, 12071 Castellón de la Plana, Spain.

(Received 18 January 2019; revised manuscript received 17 June 2019; published 2 August 2019)

The evolution of quantum light through linear optical devices can be described by the scattering matrix S of the system. For linear optical systems with m possible modes, the evolution of n input photons is given by a unitary matrix $U = \varphi_{m,M}(S)$, derived from a known homomorphism, $\varphi_{m,M}$, which depends on the size of the resulting Hilbert space of the possible photon states, M. We present a method to decide whether a given unitary evolution U for n photons in m modes can be achieved with linear optics or not and the inverse transformation $\varphi_{m,M}^{-1}$ when the transformation can be implemented. Together with previous results, the method can be used to find a simple optical system which implements any quantum operation within the reach of linear optics. The results come from studying the adjoint map between the Lie algebras corresponding to the Lie groups of the relevant unitary matrices.

DOI: 10.1103/PhysRevA.100.022301

I. INTRODUCTION

The action of a linear optical device can be described for classical (coherent) light fields as well as for single photon states using unitary matrices. The unitary transformations induced by linear optical devices for generic n-photon states of m modes are difficult to compute due to the indistinguishability of photons. Our paper studies the evolution of states of light through a linear optical interferometer acting on n photons in m different modes. These devices are also called linear optics multiports and conserve the total number of photons.

More precisely, we provide a prescription to assess whether a particular unitary U acting on the space of n-photon states distributed on m modes can be realized by a linear optical setup, cf. Theorem 1, and, if it can, give a recipe to build a device implementing it, cf. Theorem 2. Throughout the text, we will provide two worked examples of the method.

We will work in the Hilbert space $\mathscr{H}_{m,n}$ of the quantum states $|\psi\rangle$ of n photons in m modes, with superpositions of the form

$$|\psi\rangle = \sum_{n_1+\cdots+n_m=n} \alpha_{n_1,\ldots,n_m} |n_1 \cdots n_m\rangle,$$

where $|n_1 \cdots n_m\rangle$ is a state with n_k photons in the kth mode. This space is isomorphic to $\mathbb{C}^M$, where

$$M = \dim_{\mathbb{C}} \mathscr{H}_{m,n} = \binom{m+n-1}{n},$$

since each photon number state is orthogonal to the rest:

$$\langle n_1' \cdots n_m' | n_1 \cdots n_m \rangle = \delta_{n_1' n_1} \cdots \delta_{n_m' n_m}.$$

Linear interferometers are described by $m \times m$ unitary matrices $S \in \mathrm{U}(m)$ (the unitary group of $m \times m$ unitary matrices). The interferometer characterized by S naturally induces a transformation $\varphi_{m,M}(S)$ of arbitrary input states

$$|\psi\rangle \to \varphi_{m,M}(S)|\psi\rangle.$$

To understand the action of the interferometer S on multiple photon states we need to study the underlying transformation $\varphi_{m,M}$ from $\mathrm{U}(m)$ to the $\mathrm{U}(M)$, the group containing the unitary matrix U which gives the evolution of the n-photon state in $\mathscr{H}_{m,n}$. Aaronson and Arkhipov [1] give a nice algebraic description of the resulting one-to-one correspondence, which turns out to be a group homomorphism we call the (m, M)-*photonic homomorphism* (see also Refs. [2–4] for alternative descriptions).

This paper gives the inverse transformation $\varphi_{m,M}^{-1}(S)$, providing a way to implement any possible linear interferometer. Apart from being interesting in itself, this result also has applications to linear optics quantum computing [5,6] and in boson sampling, a problem which could prove quantum systems can outperform classical computers [1,7].

Organization of the paper

In Sec. II, we give an informal overview of the results. First, Secs. II A and II B introduce the basic concepts we need. Then, in Sec. II C, we give a general explanation of our results. Section II D presents the concept of the adjoint representation, which is fundamental in our method. Section II E describes our preferred basis when working with unitary algebras and

*juagar@tel.uva.es
†gimenov@mat.uji.es
‡moyano@uji.es

Sec. II F introduces the state space we will use for our guided examples in the rest of the paper.

Section III gives a necessary and sufficient condition for a unitary to be implemented with linear optics and Secs. III A and III B show concrete examples of operations which cannot and can be implemented with linear optics, respectively.

Section IV shows the method that finds the scattering matrix of the linear system which gives a given unitary operation U (if it exists). Section IV A shows the necessary steps, which are illustrated for an example in Sec. IV B.

Section V gives the detailed proofs of the theorems on which our results are based.

Finally, Sec. VI discusses the importance of our results and their limitations.

II. OUTLINE OF THE RESULTS AND DEFINITIONS

A. Optical realizations and their implementation

Any linear interferometer with m modes is completely described by an $m \times m$ unitary scattering matrix S which has a limited number of degrees of freedom, $2m^2 - 1$. This means that, except for trivial cases when $n = 1$ or $m = 1$, linear multiports can only provide a limited subset of all the possible operations over n photons in m modes, which are described by $M \times M$ unitary matrices U with $2M^2 - 1$ degrees of freedom [8].

The scattering matrices S are elements of the unitary group $\mathrm{U}(m)$ and any general evolution U on $\mathscr{H}_{m,n}$ is an element of the unitary group $\mathrm{U}(M)$. The subgroup of all the operations which can be implemented with linear optics is described by the image subgroup of $\varphi_{m,M}$, $\mathrm{im}\varphi_{m,M} = \{B \in \mathrm{U}(M) : \exists A \in \mathrm{U}(m) \text{ such that } \varphi_{m,M}(A) = B\}$.

Definition 1. A matrix $U \in \mathrm{U}(M)$ is an (m, n)-optical realization if $U \in \mathrm{im}\varphi_{m,M}$.

In this paper, we relate these groups to give a decision criterion that checks if any particular operator U is in $\mathrm{im}\varphi_{m,M}$ (it is an (m, n)-optical realization) and, if it is possible, compute the inverse $\varphi^{-1}_{m,M}(U)$ and recover the unitary matrix S of the linear interferometer which gives the desired evolution. Once we find S, we can use previous known results which tell us how to build any desired multiport with a fixed scattering matrix using only beam splitters and phase shifters [9] or only beam splitters [10,11], closing the full circle for the experimental implementation of U.

B. Linear optical evolution from the unitary (group) and Hermitian (algebra) matrices point of view

The map $\varphi_{m,M}$ is a differentiable group homomorphism [1] and it induces an algebra homomorphism, $d\varphi_{m,M}$, as described by the commutative diagram,

$$\begin{array}{ccc} \mathrm{u}(m) & \xrightarrow{d\varphi_{m,M}} & \mathrm{u}(M) \\ {\scriptstyle \exp}\downarrow & & \downarrow{\scriptstyle \exp} \\ \mathrm{U}(m) & \xrightarrow[\varphi_{m,M}]{} & \mathrm{U}(M) \end{array},$$

which relates the unitary groups $\mathrm{U}(m)$ and $\mathrm{U}(M)$ containing the scattering matrix S and the n-photon evolution operator U, respectively, to the algebras $\mathrm{u}(m)$ and $\mathrm{u}(M)$, whose elements correspond to anti-Hermitian matrices iH_S and iH_U which give an equivalent description of the evolution through exponentiation of the Hamiltonians H_S and H_U ($S = e^{iH_S}$ and $U = e^{iH_U}$) [12,13].

Both the homomorphism $\varphi_{m,M}$ and the differential $d\varphi_{m,M}$ can be described in terms of the the photon creation, $\hat{a}^\dagger_k$, and annihilation, $\hat{a}_k$, operators for mode k [14], which act on states with n_k photons in the kth mode following

$$\begin{aligned} &\hat{a}^\dagger_k |n_k\rangle_k = \sqrt{n_k + 1}|n_k + 1\rangle_k, \\ &\hat{a}_k |n_k\rangle_k = \sqrt{n_k}|n_k - 1\rangle_k, \quad n \geqslant 1, \ \hat{a}_k|0\rangle_k = |0\rangle_k. \end{aligned} \tag{1}$$

The homomorphism $\varphi_{m,M}$ can be understood from studying the evolution of the creation operators $\hat{a}^\dagger_k$ in the Heisenberg picture under the action of a unitary U, $\hat{a}^\dagger_k \longrightarrow U\hat{a}^\dagger_k U^\dagger$. For an n-photon input state,

$$|n_1 n_2 \ldots n_m\rangle = \prod_{k=1}^{m} \left(\frac{\hat{a}^{\dagger n_k}_k}{\sqrt{n_k!}} \right) |00\ldots0\rangle, \tag{2}$$

the output state after a linear interferometer is described from the elements of S as [2–4]

$$U|n_1 n_2 \ldots n_m\rangle = \prod_{k=1}^{m} \frac{1}{\sqrt{n_k!}} \left(\sum_{j=1}^{m} S_{jk} \hat{a}^\dagger_j \right)^{n_k} |00\ldots0\rangle. \tag{3}$$

We can also write the elements of U from the permanent of different submatrices of S [4].

From the differential $d\varphi_{m,M}$ [13], we can write the effective Hamiltonian H_U of a linear optical transformation as

$$\langle p|iH_U|q\rangle = \langle p| \sum_{l=1}^{m} \sum_{j=1}^{m} iH_{Sjl} \hat{a}^\dagger_j \hat{a}_l |q\rangle, \tag{4}$$

where $|p\rangle$ and $|q\rangle$ are the photon number states in our Hilbert space. The same results can be reached from alternative points of view [12,15–18].

C. Summary of the results

The main design procedure is based on a simple basis decomposition in the image subalgebra of the Hamiltonian, with a detour due to the complications that appear when finding matrix logarithms.

If we know the desired final Hamiltonian, H_U, we can check if it can be implemented with linear optics by looking for a linear combination,

$$iH_U = \sum_i X_i b_i, \tag{5}$$

of elements of the basis $\{b_i\}$ of the image subalgebra $\mathfrak{d} \subseteq \mathrm{u}(M)$ for $i = 1, \ldots, m^2$. The elements $b_i = \varphi_{m,M}(a_i)$ are the image of the elements of a basis $\{a_i\}$ of $\mathrm{u}(m)$. H_U can be implemented with linear optics if Eq. (5) has a solution. Since $\varphi_{m,M}$ is a linear transformation, the effective Hamiltonian in $\mathrm{u}(m)$ is

$$iH_S = \sum_i X_i a_i \tag{6}$$

for the same coefficients X_i. Now, $S = e^{iH_S}$ is the unitary matrix of the desired linear interferometer, for which there are known methods for an experimental implementation [9–11].

The problem reduces to solving Eq. (5), which can be expressed as a system of $M \times M$ linear equations, one for each matrix element, and m^2 indeterminates (the size of the basis). If the system is not consistent, we know H_U cannot be implemented exactly using only linear optics.

Unfortunately, finding whether a given unitary $U \in \mathrm{U}(M)$ is an optical realization is more involved. In principle, it seems we could just take $iH_U = \log U$ and proceed as before, but, unlike the exponential map, the matrix logarithm is a multivalued function. Computing the matrix logarithm of a unitary numerically presents some challenges, particularly if it has degenerate eigenvalues, as many interesting operations, such as the quantum Fourier transform, do. However, there are reliable methods to obtain a Hamiltonian matrix from a unitary [19].

The greatest obstacle is choosing the correct branch when we are restricted to a subgroup. For a unitary in the image subgroup, we need to guarantee that the logarithm branch we choose is in the image subalgebra $iH_U \in \mathfrak{d}$. Otherwise, we will not be able to find a decomposition in terms of the basis of the image subalgebra, even if U can really be implemented.

We need a method to find a Hermitian matrix in the form given by Eq. (4). These matrices have a strong structure. The only nonzero elements are in positions which correspond to transitions between states that are, at most, one photon away from each other (for input states $|p\rangle$ and $|q\rangle$ that only differ in the photon number in two positions, one mode giving the photon to the other [13]).

The main contribution of our method is giving an alternative way of finding a suitable basis decomposition, when there is one, by using the adjoint representation. The method avoids using the usual matrix logarithm calculations. There is no need to compute any eigenvalues and we mostly use simple linear algebra methods (matrix multiplication and Gaussian elimination to solve linear systems). If the operation U cannot be implemented, we prove it and, if it can, we give a complete description in terms of a linear interferometers.

D. The adjoint representation

We will find the inverse of $\varphi_{m,M}$ using the adjoint representation, which gives an alternative way of describing linear interferometers and can help to study the evolution of unitary operators [20].

Let $\mathrm{Ad}_U : \mathrm{u}(M) \to \mathrm{u}(M)$ be the adjoint map defined by $\mathrm{Ad}_U(iH_U) = U iH_U U^\dagger$ [21]. We can also define $\mathrm{Ad}_S : \mathrm{u}(m) \to \mathrm{u}(m)$ for the scattering matrix so $\mathrm{Ad}_S(iH_S) = SiH_S S^\dagger$.

When U is an optical realization, the group of linear interferometers can be equally described by $m \times m$ unitaries S, by $M \times M$ unitaries U in the image subgroup or by the Hermitian matrices H_S and H_U with iH_S and iH_U in the associated unitary algebra and image subalgebra. Additionally, if U is in the image subalgebra, the adjoint will also describe the same physical system. Finding the inverse in this representation is easier and this is the path we choose.

The adjoint map is conceptually similar to computing the evolution in the Heisenberg picture. The terms $\hat{a}_j^\dagger \hat{a}_l$ in the effective Hamiltonian given by Eq. (4) evolve under the action of the adjoint as

$$U\hat{a}_j^\dagger \hat{a}_l U^\dagger = U\hat{a}_j^\dagger U^\dagger U \hat{a}_l U^\dagger, \tag{7}$$

which, for the definition we use of the adjoint, is the product of the evolutions of the corresponding creation and destruction operators under $U^{-1} = U^\dagger$ in the Heisenberg picture.

In our derivation, we use the fact that, for linear transformations, we can relate the adjoint representations of S and $U = \varphi_{m,M}(S)$ so

$$\mathrm{Ad}_S(v) = d\varphi_{m,M}^{-1}(\mathrm{Ad}_U(d\varphi_{m,M}(v))) \tag{8}$$

for any $v \in \mathrm{u}(m)$.

E. Bases for the u(m) algebra and the image subalgebra

Consider the canonical basis $\{|1\rangle = |1, 0, \ldots, 0\rangle, |2\rangle = |0, 1, \ldots, 0\rangle, \ldots, |m\rangle = |0, \ldots, 0, 1\rangle\}$ of $\mathbb{C}^m$. The matrices

$$\begin{aligned} e_{jk} &:= \frac{i}{2}(|j\rangle\langle k| + |k\rangle\langle j|), \\ f_{jk} &:= \frac{1}{2}(|j\rangle\langle k| - |k\rangle\langle j|), \end{aligned} \tag{9}$$

give a basis of $\mathrm{u}(m)$. The real linear combinations of the matrices

$$\begin{aligned} &e_{jk} \quad \text{for } k \leqslant j = 1, \ldots, m, \\ &f_{jk} \quad \text{for } k < j = 1, \ldots, m, \end{aligned} \tag{10}$$

give any desired antihermitian matrix in the algebra.

Observe that $e_{jk} = e_{kj}$ and $f_{jk} = -f_{kj}$. From Eq. (4), we see the basis of $\mathrm{u}(m)$ transforms into

$$\begin{aligned} d\varphi_{m,M}(e_{jk}) &= \frac{i}{2}(\hat{a}_j^\dagger \hat{a}_k + \hat{a}_k^\dagger \hat{a}_j) \neq 0, \\ d\varphi_{m,M}(f_{jk}) &= \frac{1}{2}(\hat{a}_j^\dagger \hat{a}_k - \hat{a}_k^\dagger \hat{a}_j) \neq 0, \end{aligned}$$

and therefore the map $d\varphi_{m,M}$ is injective and gives a basis of the image subalgebra.

F. Example space: Five photons in two modes

To illustrate our results, we will give a few examples using linear interferometers with $m = 2$ modes and $n = 5$ input photons, for which we have a Hilbert space of dimension $M = \binom{2+5-1}{5} = 6$. We choose the basis

$$\{|5, 0\rangle, |4, 1\rangle, |3, 2\rangle, |2, 3\rangle, |1, 4\rangle, |0, 5\rangle\} \tag{11}$$

of $\mathbb{C}^6$. For our reference bases, the ith basis element corresponds to a column vector filled with zeros except for a single 1 in the ith row.

The (2,6)-photonic homomorphism will be denoted as $\varphi_{2,6} : U(2) \to U(6)$. The basis for $\mathbb{C}^2$ will be

$$\{|1, 0\rangle, \quad |0, 1\rangle\}. \tag{12}$$

We study how Ad_U acts on $\mathfrak{d} = d\varphi_{2,6}(\mathrm{u}(2))$ using the basis $\{e_{11}, e_{12}, e_{22}, f_{12}\}$ of u(2),

$$e_{11} = i\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \quad e_{12} = \frac{i}{2}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$
$$e_{22} = i\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} \quad f_{12} = \frac{1}{2}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}. \tag{13}$$

The U and iH_U matrices in these examples are given for the state order of the basis in Eq. (11), i.e., $U_{11} = \langle 1|U|1\rangle = \langle 50|U|50\rangle$, ..., $U_{32} = \langle 3|U|2\rangle = \langle 32|U|41\rangle$, ..., $U_{66} = \langle 6|U|6\rangle = \langle 05|U|05\rangle$. The same applies to S and iH_S and the basis in Eq. (12).

For a given $iH_S \in \mathrm{u}(2)$, the corresponding element in the image subalgebra $\mathfrak{d}$, $iH_U = d\varphi_{2,6}(iH_S)$, is given by [13]

$$\langle p|iH_U|q\rangle = \langle p|\sum_{l=1}^{m}\sum_{j=1}^{m} iH_{Sjl}\hat{a}_j^\dagger \hat{a}_l|q\rangle. \tag{14}$$

The matrices $\{a_i\}$ in the basis of u(2), ordered as in Eqs. (13), give us a basis $\{b_1, b_2, b_3, b_4\}$ of the image subspace $\mathfrak{d} \subseteq \mathrm{u}(M)$, with $b_i = d\varphi_{2,6}(a_i)$, where

$$b_1 := d\varphi_{2,6}(e_{11}) = i\hat{a}_1^\dagger\hat{a}_1 = i\hat{n}_1$$
$$= i\begin{pmatrix}5&0&0&0&0&0\\0&4&0&0&0&0\\0&0&3&0&0&0\\0&0&0&2&0&0\\0&0&0&0&1&0\\0&0&0&0&0&0\end{pmatrix}, \tag{15}$$

$$b_2 := d\varphi_{2,6}(e_{12}) = \frac{i}{2}(\hat{a}_1^\dagger\hat{a}_2 + \hat{a}_2^\dagger\hat{a}_1)$$
$$= \frac{i}{2}\begin{pmatrix}0&\sqrt{5}&0&0&0&0\\\sqrt{5}&0&2\sqrt{2}&0&0&0\\0&2\sqrt{2}&0&3&0&0\\0&0&3&0&2\sqrt{2}&0\\0&0&0&2\sqrt{2}&0&\sqrt{5}\\0&0&0&0&\sqrt{5}&0\end{pmatrix}, \tag{16}$$

$$b_3 := d\varphi_{2,6}(e_{22}) = i\hat{a}_2^\dagger\hat{a}_2 = i\hat{n}_2$$
$$= i\begin{pmatrix}0&0&0&0&0&0\\0&1&0&0&0&0\\0&0&2&0&0&0\\0&0&0&3&0&0\\0&0&0&0&4&0\\0&0&0&0&0&5\end{pmatrix}, \tag{17}$$

$$b_4 := d\varphi_{2,6}(f_{12}) = \frac{1}{2}(\hat{a}_1^\dagger\hat{a}_2 - \hat{a}_2^\dagger\hat{a}_1)$$
$$= \frac{1}{2}\begin{pmatrix}0&\sqrt{5}&0&0&0&0\\-\sqrt{5}&0&2\sqrt{2}&0&0&0\\0&-2\sqrt{2}&0&3&0&0\\0&0&-3&0&2\sqrt{2}&0\\0&0&0&-2\sqrt{2}&0&\sqrt{5}\\0&0&0&0&-\sqrt{5}&0\end{pmatrix}. \tag{18}$$

III. EXISTENCE OF A UNITARY EVOLUTION VIA LINEAR OPTICS

The adjoint representation gives us a necessary and sufficient condition for the implementation of any given unitary operator U with linear interferometers.

Theorem 1. $U \in \mathrm{im}\varphi_{m,M} \iff \mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism.

Theorem 1 gives a criterion to decide whether a matrix $U \in \mathrm{U}(M)$ is an (n, m)-optical realization or not. A quantum operation U can be implemented with linear optics if and only if $\mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism (for any v in the image subalgebra $\mathfrak{d}$, the adjoint $UvU^\dagger$ remains in the subalgebra). We only need to see this is the case for a basis of $\mathfrak{d}$, which can be obtained by transforming the elements of a basis of u(m) by the algebra homomorphism $d\varphi_{m,M}$.

We can choose a basis of u(m) $\{a_1, \cdots, a_m\}$ following Eqs. (9) and (10) so any element in the algebra can be expressed as a real linear combination of the a_i matrices. For that basis, the matrices $b_i = d\varphi_{m,M}(a_i)$ form a basis for $\mathfrak{d}$.

U is an optical realization if and only if, for any v that is a real linear combination of the computed b_i, we can also write $UvU^\dagger$ in the same basis. There must exist real coefficients X_{ij} such that

$$Ub_iU^\dagger = \sum_{j=1}^{m^2} X_{ij}b_j, \quad i = 1, \ldots, m^2. \tag{19}$$

To check whether a given U can be realized with linear optics, we need to satisfy m^2 equations with $M \times M$ complex matrices, one for each element of the basis, for a total of m^2M^2 independent real equations [22] with m^4 indeterminates. If the system is consistent, U is an (n, m)-optical realization.

A. Example 1: An impossible operation

In our example state space, see Sec. II F, to decide whether a matrix U is a (2,6)-optical realization or not, by Theorem 1, we have to compute Ad_U and see if $\mathrm{Ad}_U(v) \in \mathfrak{d}$ for any $v \in \mathfrak{d}$.

The adjoint is linear and it is enough to verify the property for the vectors in the basis $\{b_1, b_2, b_3, b_4\}$ of $\mathfrak{d}$. This leads to a real linear system with $2^2 \cdot 6^2$ equations,

$$\mathrm{Ad}_U(b_j) = \sum_{k=1}^{4} X_{jk}b_k, \quad j = 1, \ldots, 4, \tag{20}$$

in the 2^4 indeterminates X_{jk} belonging to $\mathbb{R}$. If the system is consistent, then U is a (2,6)-photonic realization.

First, we are going to use Theorem 1 to show that not every unitary 6×6 matrix is a (2,6)-optical realization. If we take the matrix

$$U = \begin{pmatrix}0&0&0&1&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\1&0&0&0&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{pmatrix}, \tag{21}$$

the system Eqs. (20) is inconsistent. Consider, for instance, Eqs. (20) for b_2,

$$Ub_2U^\dagger = X_{21}b_1 + X_{22}b_2 + X_{23}b_3 + X_{24}b_4, \tag{22}$$

which, in matrix form, is

$$\begin{pmatrix} 0 & 0 & \frac{3i}{2} & 0 & \sqrt{2}i & 0 \\ 0 & 0 & \sqrt{2}i & \frac{\sqrt{5}i}{2} & 0 & 0 \\ \frac{3i}{2} & \sqrt{2}i & 0 & 0 & 0 & 0 \\ 0 & \frac{\sqrt{5}i}{2} & 0 & 0 & 0 & 0 \\ \sqrt{2}i & 0 & 0 & 0 & 0 & \frac{\sqrt{5}i}{2} \\ 0 & 0 & 0 & 0 & \frac{\sqrt{5}i}{2} & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 5iX_{21} & \frac{iX_{22}}{2}\sqrt{5} + \frac{\sqrt{5}X_{24}}{2} & 0 & 0 & 0 & 0 \\ \frac{iX_{22}}{2}\sqrt{5} - \frac{\sqrt{5}X_{24}}{2} & 4iX_{21} + iX_{23} & \sqrt{2}iX_{22} + \sqrt{2}X_{24} & 0 & 0 & 0 \\ 0 & \sqrt{2}iX_{22} - \sqrt{2}X_{24} & 3iX_{21} + 2iX_{23} & \frac{3i}{2}X_{22} + \frac{3X_{24}}{2} & 0 & 0 \\ 0 & 0 & \frac{3i}{2}X_{22} - \frac{3X_{24}}{2} & 2iX_{21} + 3iX_{23} & \sqrt{2}iX_{22} + \sqrt{2}X_{24} & 0 \\ 0 & 0 & 0 & \sqrt{2}iX_{22} - \sqrt{2}X_{24} & iX_{21} + 4iX_{23} & \frac{iX_{22}}{2}\sqrt{5} + \frac{\sqrt{5}X_{24}}{2} \\ 0 & 0 & 0 & 0 & \frac{iX_{22}}{2}\sqrt{5} - \frac{\sqrt{5}X_{24}}{2} & 5iX_{23} \end{pmatrix}. \tag{23}$$

The system is clearly inconsistent. In the first row, we see two constants, $\frac{3i}{2}$ and $\sqrt{2}i$, which should be equal to zero, which is impossible.

Therefore, since Ad_U is not an automorphism of $\mathfrak{d}$, we have that $U \notin \mathrm{Im}(\varphi_{2,6})$ by Theorem 1 and U is not a (2,6)-optical realization.

Another way to show that inconsistency is noticing that, if $v \in \mathfrak{d}$, then $\langle n_1', n_2'|v|n_1, n_2\rangle \neq 0$ implies that the input state $|n_1, n_2\rangle$ is, at most, one photon away from the output state $|n_1', n_2'\rangle$ (cf. Eq. (4) and Ref. [13]).

This is not the case for the given U and our basis order in Eq. (11): Notice that $|2, 3\rangle$ is two photons away from $|4, 1\rangle$, but

$$\langle 4, 1|\mathrm{Ad}_U(b_2)|2, 3\rangle = \langle 4, 1|Ub_2U^\dagger|2, 3\rangle = \langle 4, 1|b_2|5, 0\rangle = \frac{\sqrt{5}}{2}i \neq 0. \tag{24}$$

B. Example 2: An optical realization

Continuing with Sec. III A, let us show that for the operator,

$$U = \begin{pmatrix} \frac{\sqrt{2}}{8} & \frac{\sqrt{10}}{8} & \frac{\sqrt{5}}{4} & \frac{\sqrt{5}}{4} & \frac{\sqrt{10}}{8} & \frac{\sqrt{2}}{8} \\ \frac{\sqrt{10}}{8} & \frac{3\sqrt{2}}{8} & \frac{1}{4} & -\frac{1}{4} & -\frac{3\sqrt{2}}{8} & -\frac{\sqrt{10}}{8} \\ \frac{\sqrt{5}}{4} & \frac{1}{4} & -\frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} & \frac{1}{4} & \frac{\sqrt{5}}{4} \\ \frac{\sqrt{5}}{4} & -\frac{1}{4} & -\frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} & \frac{1}{4} & -\frac{\sqrt{5}}{4} \\ \frac{\sqrt{10}}{8} & -\frac{3\sqrt{2}}{8} & \frac{1}{4} & \frac{1}{4} & -\frac{3\sqrt{2}}{8} & \frac{\sqrt{10}}{8} \\ \frac{\sqrt{2}}{8} & -\frac{\sqrt{10}}{8} & \frac{\sqrt{5}}{4} & -\frac{\sqrt{5}}{4} & \frac{\sqrt{10}}{8} & -\frac{\sqrt{2}}{8} \end{pmatrix}, \tag{25}$$

there exists a matrix S in $U(2)$ such that $\varphi_{2,6}(S) = U$.

We start by solving the system in Eqs. (20). We write one matrix identity for each element in the $\{b_i\}$ basis. For instance, for b_1,

$$Ub_1U^\dagger = X_{11}b_1 + X_{12}b_2 + X_{13}b_3 + X_{14}b_4 \tag{26}$$

becomes

$$\begin{pmatrix} \frac{5i}{2} & \frac{\sqrt{5}i}{2} & 0 & 0 & 0 & 0 \\ \frac{\sqrt{5}i}{2} & \frac{5i}{2} & \sqrt{2}i & 0 & 0 & 0 \\ 0 & \sqrt{2}i & \frac{5i}{2} & \frac{3i}{2} & 0 & 0 \\ 0 & 0 & \frac{3i}{2} & \frac{5i}{2} & \sqrt{2}i & 0 \\ 0 & 0 & 0 & \sqrt{2}i & \frac{5i}{2} & \frac{\sqrt{5}i}{2} \\ 0 & 0 & 0 & 0 & \frac{\sqrt{5}i}{2} & \frac{5i}{2} \end{pmatrix}$$

$$= \begin{pmatrix} 5iX_{11} & \frac{iX_{12}}{2}\sqrt{5} + \frac{\sqrt{5}X_{14}}{2} & 0 & 0 & 0 & 0 \\ \frac{iX_{12}}{2}\sqrt{5} - \frac{\sqrt{5}X_{14}}{2} & 4iX_{11} + iX_{13} & \sqrt{2}iX_{12} + \sqrt{2}X_{14} & 0 & 0 & 0 \\ 0 & \sqrt{2}iX_{12} - \sqrt{2}X_{14} & 3iX_{11} + 2iX_{13} & \frac{3i}{2}X_{12} + \frac{3X_{14}}{2} & 0 & 0 \\ 0 & 0 & \frac{3i}{2}X_{12} - \frac{3X_{14}}{2} & 2iX_{11} + 3iX_{13} & \sqrt{2}iX_{12} + \sqrt{2}X_{14} & 0 \\ 0 & 0 & 0 & \sqrt{2}iX_{12} - \sqrt{2}X_{14} & iX_{11} + 4iX_{13} & \frac{iX_{12}}{2}\sqrt{5} + \frac{\sqrt{5}X_{14}}{2} \\ 0 & 0 & 0 & 0 & \frac{iX_{12}}{2}\sqrt{5} - \frac{\sqrt{5}X_{14}}{2} & 5iX_{13} \end{pmatrix}, \tag{27}$$

from which we see $X_{11} = \frac{1}{2}$, $X_{12} = 1$, $X_{13} = \frac{1}{2}$ and $X_{14} = 0$. If we repeat the same operation for each b_i in the basis, we see the system Eqs. (20) is consistent and its solutions are given by the matrix

$$X = (X_{jk}) = \begin{pmatrix} 1/2 & 1 & 1/2 & 0 \\ 1/2 & 0 & -1/2 & 0 \\ 1/2 & -1 & 1/2 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{28}$$

Therefore, since Ad_U is a linear map so $\mathrm{Ad}_U : d\varphi_{2,6}(\mathfrak{u}(2)) \to d\varphi_{2,6}(\mathfrak{u}(2))$, we know (by Theorem 1) that there exists at least one $S \in U(2)$ such that $\varphi_{2,6}(S) = U$.

IV. IMPLEMENTATION OF THE POSSIBLE OPERATIONS USING LINEAR OPTICS

When the operation can be implemented, we can give an explicit implementation which uses the solution to the system of equations. Let $U \in \mathrm{U}(M)$, then Theorem 1 shows that, if $\mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism, there exists an $S \in \mathrm{U}(m)$ such that $\varphi_{m,M}(S) = U$. The goal is to obtain an algorithm which provides this S.

Theorem 2. For some $S = \sum_{\ell j} S_{\ell j}|\ell\rangle\langle j| \in \mathrm{U}(m)$, let $\mathrm{Ad}_S : \mathfrak{u}(m) \to \mathfrak{u}(m)$ be the adjoint map; then there exist ℓ_0, j_0 such that $-i\langle\ell_0|\mathrm{Ad}_S(e_{j_0 j_0})|\ell_0\rangle = |S_{\ell_0 j_0}|^2 \neq 0$ and

$$S = e^{i\theta} \sum_{\ell,j} \frac{\langle\ell|\mathrm{Ad}_S(f_{jj_0})|\ell_0\rangle - i\langle\ell|\mathrm{Ad}_S(e_{jj_0})|\ell_0\rangle}{\sqrt{-i\langle\ell_0|\mathrm{Ad}_S(e_{j_0 j_0})|\ell_0\rangle}} |\ell\rangle\langle j|, \tag{29}$$

with $\theta \in \mathbb{R}$.

All the relevant adjoint operators can be written from $\mathrm{Ad}_S(a_i)$ for the elements a_i of the basis of $\mathfrak{u}(m)$ and the desired U.

Notice that

$$d\varphi_{m,M}(\mathrm{Ad}_S(a_i)) = \mathrm{Ad}_U(d\varphi_{m,M}(a_i)) = \sum_{j=1}^{m^2} X_{ij} d\varphi_{m,M}(a_i) \tag{30}$$

for the X_{ij} from the system in Eq. (19), which must be consistent (otherwise we know the operation cannot be realized). Both $d\varphi_{m,M}$ and $d\varphi_{m,M}^{-1}$ are linear and

$$\mathrm{Ad}_S(a_i) = d\varphi_{m,M}^{-1}\left(\sum_{j=1}^{m^2} X_{ij} d\varphi_{m,M}(a_i)\right) = \sum_{j=1}^{m^2} X_{ij} a_i \tag{31}$$

where all the X_{ij} and a_i are known.

A. Implementation recipe

Given an operator U, we first solve the system in Eq. (19) (or say it cannot be realized if it is inconsistent).

Then, we try different integer pairs ℓ, j in

$$|S_{\ell j}|^2 = -i\langle\ell|\mathrm{Ad}_S(e_{jj})|\ell\rangle. \tag{32}$$

If the chosen $|S_{\ell j}|^2 = 0$, we have one element of S. We continue until we find a pair ℓ_0, j_0 which gives a nonzero element of S. This $S_{\ell_0 j_0} = e^{i\theta}|S_{\ell_0 j_0}|$ will be our reference.

We can only compute the modulus, but, if we use the same $S_{\ell_0 j_0}$ for all the ℓ, j pairs, all the elements of S will have the same global phase, which can be ignored. Using Eq. (31) and Theorem 2, we can compute all the elements of a scattering matrix S which realizes the desired operator U. The scattering matrix, in turn, can be used to build the desired device with linear optical elements [9–11].

B. Implementation example

In Sec. III B, we proved the existence of a matrix $S \in U(2)$ such that $\varphi_{2,6}(S) = U$ for the unitary operation U in Eq. (25). To find this matrix S up to global phase, we apply Theorem 2.

We first look for a nonzero element of S from Eq. (32):

$$|S_{\ell j}|^2 = -i\langle \ell|\mathrm{Ad}_S(e_{jj})|\ell\rangle. \tag{33}$$

We start with $\ell = j = 1$

$$|S_{11}|^2 = -i\langle 1|\mathrm{Ad}_S(e_{11})|1\rangle. \tag{34}$$

We also need to use Eq. (31)

$$\mathrm{Ad}_S(a_i) = d\varphi_{m,M}^{-1}\left(\sum_{j=1}^{m^2} X_{ij} d\varphi_{m,M}(a_i)\right) = \sum_{j=1}^{m^2} X_{ij} a_i, \tag{35}$$

which, for $a_1 = e_{11}$ and the matrix with the coefficients of the solution in Eq. (28), gives

$$\begin{aligned}\mathrm{Ad}_S(e_{11}) &= X_{11}e_{11} + X_{12}e_{12} + X_{13}e_{22} + X_{14}f_{12}\\ &= \frac{i}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix},\end{aligned}$$

so that

$$|S_{11}|^2 = \tfrac{1}{2}. \tag{36}$$

We obtain $S_{11} = e^{i\theta}\frac{1}{\sqrt{2}}$. From Theorem 2, we see the remaining $S_{\ell j}$ are

$$S_{\ell j} = \sqrt{2}\exp(i\theta)(\langle \ell|\mathrm{Ad}_S(f_{j1})|1\rangle - i\langle \ell|\mathrm{Ad}_S(e_{j1})|1\rangle). \tag{37}$$

We use the same reference S_{11} to find the rest of the entries in S:

$$S_{12} = \sqrt{2}\exp(i\theta)(\langle 1|\mathrm{Ad}_S(f_{21})|1\rangle - i\langle 1|\mathrm{Ad}_S(e_{21})|1\rangle), \tag{38}$$

$$S_{21} = \sqrt{2}\exp(i\theta)(\langle 2|\mathrm{Ad}_S(f_{11})|1\rangle - i\langle 2|\mathrm{Ad}_S(e_{11})|1\rangle), \tag{39}$$

$$S_{22} = \sqrt{2}\exp(i\theta)(\langle 2|\mathrm{Ad}_S(f_{21})|1\rangle - i\langle 2|\mathrm{Ad}_S(e_{21})|1\rangle). \tag{40}$$

All the elements can be computed from the basis $\{e_{11}, e_{12}, e_{22}, f_{12}\}$ (remembering $f_{ii} = 0$, $e_{jk} = e_{kj}$, and $f_{jk} = -f_{kj}$). Apart from $\mathrm{Ad}_S(e_{11})$, we need the matrices

$$\begin{aligned}\mathrm{Ad}_S(f_{21}) &= -\mathrm{Ad}_S(f_{12})\\ &= -(X_{41}e_{11} + X_{42}e_{12} + X_{43}e_{22} + X_{44}f_{12})\\ &= f_{12} = \frac{1}{2}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\end{aligned} \tag{41}$$

$$\begin{aligned}\mathrm{Ad}_S(e_{21}) &= \mathrm{Ad}_S(e_{12})\\ &= X_{21}e_{11} + X_{22}e_{12} + X_{23}e_{22} + X_{24}f_{12}\\ &= \frac{1}{2}e_{11} - \frac{1}{2}e_{22} = \frac{i}{2}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\end{aligned} \tag{42}$$

which give the solution

$$S_{12} = \sqrt{2}\exp(i\theta)\left(0 - i\frac{i}{2}\right) = e^{i\theta}\frac{1}{\sqrt{2}}, \tag{43}$$

$$S_{21} = \sqrt{2}\exp(i\theta)\left(0 - i\frac{i}{2}\right) = e^{i\theta}\frac{1}{\sqrt{2}}, \tag{44}$$

$$S_{22} = \sqrt{2}\exp(i\theta)\left(-\frac{1}{2} - 0\right) = e^{i\theta}\frac{-1}{\sqrt{2}}. \tag{45}$$

We can ignore the global phase θ and obtain the scattering matrix

$$S = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{46}$$

If we compute $\varphi_{2,6}(S)$ using Eq. (3), we can check we get the desired evolution U.

Notice that, had we tried to simply take the matrix logarithm of the unitary in Eq. (25), we could have obtained results such as

$$iH_U = \begin{pmatrix}
1.293i & -0.621i & -0.878i & -0.878i & -0.621i & -0.278i\\
-0.621i & 0.738i & -0.393i & 0.393i & 0.833i & 0.621i\\
-0.878i & -0.393i & 2.126i & 0.555i & -0.393i & -0.878i\\
-0.878i & 0.393i & 0.555i & 1.015i & -0.393i & 0.878i\\
-0.621i & 0.833i & -0.393i & -0.393i & 2.404i & -0.621i\\
-0.278i & 0.621i & -0.878i & 0.878i & -0.621i & 1.848i
\end{pmatrix}, \tag{47}$$

which was computed numerically and is presented rounded to three decimal places. While this is a valid logarithm ($U = e^{iH_U}$), the matrix is not in the image subspace (it has nonzero elements for transitions between states which are more than one photon away). As a result, this logarithm is not compatible with our approach using the basis of $\mathfrak{d}$ to check whether U can be implemented or not.

V. PROOFS OF THE MAIN RESULTS

In this section, we prove Theorems 1 and 2, which lay the foundations for our results.

Let $\mathrm{Ad}_U : \mathrm{u}(M) \to \mathrm{u}(M)$ be the adjoint map defined by $\mathrm{Ad}_U(iH_S) = UiH_SU^\dagger$ [21].

We denote by $\mathfrak{d}$ the subalgebra $d\varphi_{m,M}(\mathrm{u}(m)) \subseteq \mathrm{u}(M)$, and by $\mathfrak{sd}$ the subalgebra $d\varphi_{m,M}(\mathfrak{su}(m)) \subseteq \mathrm{u}(M)$ where $\mathfrak{su}(m)$ is the special unitary algebra of dimension m which gives by exponentiation the matrices in the special unitary group which describe any quantum evolution for a quantum state up to an unobservable global phase shift. Notice that $d\varphi_{m,M} : \mathrm{u}(m) \to \mathfrak{d}$ is a bijection.

A. Proof of Theorem 1

Lemma 1. Let $iH_U = d\varphi_{m,M}(iH_S) \in \mathfrak{d}$ for $iH_S \in \mathrm{u}(m)$, then,

$$\mathrm{tr}(iH_U) = \binom{n+m-1}{n-1}\mathrm{tr}(iH_S).$$

Therefore, $v \in \mathfrak{sd}$ if and only if $\mathrm{tr}(v) = 0$. Moreover,

$$\mathfrak{d} = \mathfrak{sd} \oplus \mathrm{span}_{\mathbb{R}}(iI_M).$$

Proof. $\mathrm{tr}(iH_U) = \mathrm{tr}(d\varphi_{m,M}(iH_S)) = \sum_\ell^M \sum_{j,k}^m \langle \ell | iH_{Sjk} \hat{a}_j^\dagger \hat{a}_k | \ell \rangle = \sum_{\ell jk} iH_{Sjk} \langle \ell | \hat{a}_j^\dagger \hat{a}_k | \ell \rangle = \sum_{\ell jk} iH_{Sjk} \delta_{jk} \langle \ell | \hat{n}_j | \ell \rangle = \sum_{\ell j} iH_{Sjj} \langle \ell | \hat{n}_j | \ell \rangle = \sum_j iH_{Sjj} \sum_\ell \langle \ell | \hat{n}_j | \ell \rangle = \sum_j iH_{Sjj} \frac{nM}{m} = \binom{n+m-1}{n-1} \mathrm{tr}(iH_S)$, taking into account that the sum for the average of the photon number operator $\hat{n}_j = \hat{a}_j^\dagger \hat{a}_j$ in mode j, $\sum_\ell \langle \ell | \hat{n}_j | \ell \rangle$, must be the same for every mode (we cover all the permutations for photon occupation). For n total photons and M possible states, the total sum is nM, which is divided by m for each position.

Observe that $\mathrm{span}_{\mathbb{R}}(iI_M)$ is a subalgebra of $\mathfrak{d}$, since

$$d\varphi_{m,M}(\beta I_m) = \beta \sum_{jk} \delta_{jk} \hat{a}_j^\dagger \hat{a}_k = \beta \sum_j \hat{n}_j = \beta n I_M.$$

Let $iH_U \in \mathfrak{d}$ and $v = \frac{\mathrm{tr}(iH_U)}{M} I_M \in \mathrm{span}_{\mathbb{R}}(iI_M)$, since $\mathrm{Re}(\mathrm{tr}(iH_U)) = 0$. Then $iH_U - v \in \mathfrak{sd}$ as $\mathrm{tr}(iH_U - v) = 0$, hence $iH_U = (iH_U - v) + v \in \mathfrak{sd} + \mathrm{span}_{\mathbb{R}}(iI_M)$. The result follows from the fact that $\mathfrak{sd} \cap \mathrm{span}_{\mathbb{R}}(iI_M) = 0$. ■

Lemma 2. Let $U \in \mathrm{U}(M)$, then $\mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism if and only if $\mathrm{Ad}_U|_{\mathfrak{sd}}$ is an automorphism.

Proof. We first assume that $\mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism, then for any $v \in \mathfrak{sd}$,

$$\mathrm{tr}(\mathrm{Ad}_U(v)) = \mathrm{tr}(UvU^\dagger) = \mathrm{tr}(v) = 0,$$

therefore $\mathrm{Ad}_U(v) \in \mathfrak{sd}$ by Lemma 1. This proves that Ad_U is an endomorphism. Moreover, the kernel is trivial, since $\|\mathrm{Ad}_U(v)\| = 0$ implies $\|v\| = 0$ for any v, as can be checked for the trace norm: $\|\mathrm{Ad}_U(v)\| = \sqrt{\mathrm{tr}(\mathrm{Ad}_U(v)(\mathrm{Ad}_U(v))^\dagger)} = \sqrt{\mathrm{tr}(UvU^\dagger (UvU^\dagger)^\dagger)} = \sqrt{\mathrm{tr}(UvU^\dagger UvU^\dagger)} = \sqrt{\mathrm{tr}(vv^\dagger)} = \|v\|$.

Conversely, let us assume that $\mathrm{Ad}_U|_{\mathfrak{sd}}$ is an automorphism. By Lemma 1, since $\mathfrak{d} = \mathfrak{sd} \oplus \mathrm{span}_{\mathbb{R}}(iI_M)$ and $\mathrm{Ad}_U : \mathrm{span}_{\mathbb{R}}(iI_M) \to \mathrm{span}_{\mathbb{R}}(iI_M)$ is the identity, then $\mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism. ■

We can now prove Theorem 1.

Proof. $\Longrightarrow$) Let $U \in \mathrm{im}\varphi_{m,M}$, then there exists $iH_U \in \mathfrak{d}$ such that $U = \exp(iH_U)$, hence for any $v \in \mathfrak{d} \mathrm{Ad}_U(iH_U) = \exp(iH_U) v \exp(-iH_U) = v + [iH_U, v] + \frac{1}{2}[iH_U, [iH_U, v]] + \frac{1}{3!}[iH_U, [iH_U, [iH_U, v]]] + \cdots$ and clearly $\mathrm{Ad}_U(v) \in \mathfrak{d}$, since $iH_U, v \in \mathfrak{d}$ and the Lie bracket is closed in $\mathfrak{d}$. This proves that Ad_U is an endomorphism. Moreover, the kernel is trivial, since $\|\mathrm{Ad}_U(v)\| = 0$ implies $\|v\| = 0$ for some v (see proof of Lemma 2).

$\Longleftarrow$) Let $U \in \mathrm{U}(M)$ such that $\mathrm{Ad}_U|_{\mathfrak{d}}$ is an automorphism. There exists $\theta \in \mathbb{R}$ such that $\exp(i\theta)U \in SU(M)$. Moreover, for any $W \in \varphi_{m,M}(SU(m))$, there exists $w \in \mathfrak{sd}$ with $W = \exp(w)$, and $\exp(i\theta)UW(\exp(i\theta)U)^\dagger = U\exp(w)U^\dagger = \exp(UwU^\dagger) = \exp(\mathrm{Ad}_U(w))$, by Lemma 2, $\mathrm{Ad}_U(w) \in \mathfrak{sd}$, and so $\exp(\mathrm{Ad}_U(w)) \in \varphi_{m,M}(SU(m))$. Finally, by Lemma 9 of Ref. [23],

$$\exp(i\theta)U = \exp(i\beta)U',$$

for some $\beta \in \mathbb{R}$ and $U' \in \varphi_{m,M}(SU(m))$. Hence

$$U = \exp(i(\beta - \theta))U' = \exp(i(\beta - \theta)I_M)\exp(w'),$$

with $w' \in \mathfrak{sd}$. Since $[I_M, w'] = 0$, then

$$U = \exp(i(\beta - \theta)I_M + w').$$

Since $i(\beta - \theta)I_M + w' \in \mathfrak{sd} \oplus \mathrm{span}_{\mathbb{R}}(iI_M)$, by Lemma 1 $i(\beta - \theta)I_M + w' \in \mathfrak{d}$, therefore $\exp(i(\beta - \theta)I_M + w') \in \mathrm{im}\varphi_{m,M}$. ■

B. Proof of Theorem 2

Proof. Let $S = \sum_{jk} S_{jk} |j\rangle\langle k|$. The adjoint map acting on the tangent vectors e_{jk}, f_{jk} of $\mathrm{u}(m)$ gives

$$\begin{aligned}
\langle \ell | \mathrm{Ad}_S(e_{jk}) | h \rangle &= \langle \ell | S e_{jk} S^\dagger | h \rangle \\
&= \sum_{s,t,\mu,\nu} \langle \ell | S_{st} | s \rangle \langle t | e_{jk} S^*_{\mu\nu} | \nu \rangle \langle \mu | h \rangle \\
&= \frac{i}{2} \sum_{s,t,\mu,\nu} S_{st} S^*_{\mu\nu} \langle \ell | s \rangle \langle t | (|j\rangle\langle k| + |k\rangle\langle j|) | \nu \rangle \langle \mu | h \rangle \\
&= \frac{i}{2} \sum_{s,t,\mu,\nu} S_{st} S^*_{\mu\nu} (\delta_{\ell s}\delta_{tj}\delta_{k\nu}\delta_{\mu h} + \delta_{\ell s}\delta_{tk}\delta_{j\nu}\delta_{\mu h}) \\
&= \frac{i}{2} (S_{\ell j} S^*_{hk} + S_{\ell k} S^*_{hj}),
\end{aligned}$$

and, similarly,

$$\langle \ell | \mathrm{Ad}_S(f_{jk}) | h \rangle = \tfrac{1}{2} (S_{\ell j} S^*_{hk} - S_{\ell k} S^*_{hj}).$$

This allows us to obtain

$$S_{\ell j} S^*_{hk} = \langle \ell | \mathrm{Ad}_S(f_{jk}) | h \rangle - i \langle \ell | \mathrm{Ad}_S(e_{jk}) | h \rangle \tag{48}$$

for all ℓ, j, h, k and, for $\ell = h$ and $j = k$:

$$|S_{\ell j}|^2 = -i \langle \ell | \mathrm{Ad}_S(e_{jj}) | \ell \rangle. \tag{49}$$

Since the matrix S is unitary, there exists $S_{\ell_0 j_0} \neq 0$ and there is $\theta \in \mathbb{R}$ with $S_{\ell_0 j_0} = |S_{\ell_0 j_0}| e^{i\theta}$. By Eqs. (48) and (49),

$$S_{\ell j} = e^{i\theta} \frac{\langle \ell | \mathrm{Ad}_S(f_{jj_0}) | \ell_0 \rangle - i \langle \ell | \mathrm{Ad}_S(e_{jj_0}) | \ell_0 \rangle}{\sqrt{-i \langle \ell_0 | \mathrm{Ad}_S(e_{j_0 j_0}) | \ell_0 \rangle}}. \tag{50}$$

■

VI. CONCLUSIONS

In this paper, we give a way to check whether any given linear operator U on n photons in m modes can be implemented with linear optics or not and, if it can, provide a explicit method to find the multiport S which gives the desired operator.

The method tries to write the Hamiltonian corresponding to the desired operator in terms of a linear combination of a basis of the subalgebra of all the possible Hamiltonians.

In principle, the same analysis with a decomposition in the basis of the image subalgebra could be directly applied to the H_U coming from computing the logarithm of the desired operator matrix U. However, computing a suitable matrix logarithm is far from trivial. By using the adjoint representation, we guarantee a simple and flexible method for any operator U. The computation only involves matrix multiplications and solving a linear system and avoids computing eigenvalues.

This method solves the problem completely for any given U.

There are some limitations to this result worth mentioning. First, it applies only to systems which can be exactly implemented, which, as n and m grow, become a smaller subset of the possible matrices U. In many cases, we are more

concerned with finding the best approximation. In a future work, we will present a different method which finds the linear optics evolution which is locally closest to the desired operator in terms of some operator distance.

Second, that a particular operation cannot be implemented has limited implications to the related quantum information problem of whether a given quantum gate can be implemented with linear optics or not. Apart from encoding issues (a gate might be realized using only a subspace of the possible states), notice that, in linear interferometers, permutations are not trivial. For instance, the quantum Fourier transform matrix might be realizable for some mapping of the logical states to the photon states but not for others.

Taking into account these precautions, the inverse method we have given can be used in quantum optics and quantum information to search for particular quantum tasks or primitives which can be implemented with linear optics, such as particular instances of quantum cloning machines [24] or simple quantum algorithms showing quantum advantage. In general, the framework provided from group theory helps us to understand better the connections between classical and quantum evolution in linear optics.

ACKNOWLEDGMENTS

J.C.G.-E. has been funded by the Spanish Ministerio de Economía y Competitividad, Project No. TEC2015-69665-R, MINECO/FEDER, UE. V.G. has been partially supported by the Spanish Government Ministerio de Economía y Competitividad (MINECO-FEDER), Grant No. MTM2017-84851-C2-2-P, and by Universitat Jaume I, Grant No. UJI-B2018-35. J.J.M.-F. was partially supported by the Spanish Government Ministerio de Economía, Industria y Competitividad (MINECO), Grant No. PGC2018-096446-B-C22, as well as by Universitat Jaume I, Grants No. P1-1B2015-02 and No. UJI-B2018-10.

[1] 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, 2011), pp. 333–342.

[2] E. R. Caianiello, On quantum field theory—I: Explicit solution of Dyson's equation in electrodynamics without use of Feynman graphs, Nuovo Cimento **10**, 1634 (1953).

[3] J. Skaar, J. C. García Escartín, and H. Landro, Quantum mechanical description of linear optics, Am. J. Phys. **72**, 1385 (2004).

[4] S. Scheel, Permanents in linear optical networks, Acta Phys. Slovaca **58**, 675 (2008).

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

[6] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn, Linear optical quantum computing with photonic qubits, Rev. Mod. Phys. **79**, 135 (2007).

[7] S. Aaronson, A linear-optical proof that the permanent is #P-hard, Proc. R. Soc. London A: Math. Phys. Sci. **467**, 3393 (2011).

[8] J. J. Moyano-Fernández and J. C. Garcia-Escartin, Linear optics only allows every possible quantum operation for one photon or one port, Opt. Commun. **382**, 237 (2017).

[9] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Experimental Realization of Any Discrete Unitary Operator, Phys. Rev. Lett. **73**, 58 (1994).

[10] A. Bouland and S. Aaronson, Generation of universal linear optics by any beam splitter, Phys. Rev. A **89**, 062316 (2014).

[11] A. Sawicki, Universality of beamsplitters, Quantum Inf. Comput. **16**, 0291 (2016).

[12] U. Leonhardt and A. Neumaier, Explicit effective Hamiltonians for general linear quantum-optical networks, J. Opt. B: Quantum Semiclass. Opt. **6**, L1 (2004).

[13] J. C. Garcia-Escartin, V. Gimeno, and J. J. Moyano-Fernández, Multiple photon effective Hamiltonians in linear quantum optical networks, Opt. Commun. **430**, 434 (2019).

[14] R. Loudon, *The Quantum Theory of Light*, 3rd ed. (Oxford University Press, Oxford, UK, 2000)

[15] H. Y. Fan and M. Xiao, Construction of optical networks by virture of the IWOP technique, Quantum Semiclassi, Quantum Semiclass. Opt. **9**, 53 (1997).

[16] P. Aniello and R. Coen Cagli, An algebraic approach to linear-optical schemes for deterministic quantum computing, J. Opt. B **7**, S711 (2005).

[17] L. C. Biedenharn and J. D. Louck, *Angular Momentum in Quantum Physics: Theory and Application* (Addison-Wesley, Reading, MA, 1981).

[18] P. Aniello, C. Lupo and M. Napolitano, Exploring representation theory of unitary groups via linear optical passive devices, Open Syst. Inform. Dyn. **13**, 415 (2006).

[19] T. A. Loring, Computing a logarithm of a unitary matrix with general spectrum, Numerical Linear Algebra Appl. **21**, 744 (2014).

[20] A. Sawicki and K. Karnas, Criteria for universality of quantum gates, Phys. Rev. A **95**, 062303 (2017).

[21] B. C. Hall, Lie algebras, in *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction* (Springer International Publishing, Switzerland, 2015), pp. 49–75.

[22] Each of the $M \times M$ matrices has $2M^2$ real parameters, but they are anti-Hermitian, leaving only M^2 independent real values.

[23] M. Oszmaniec and Z. Zimborás, Supplemental Material in Universal Extensions of Restricted Classes of Quantum Operations, Phys. Rev. Lett. **119**, 220502 (2017).

[24] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Quantum cloning, Rev. Mod. Phys. **77**, 1225 (2005).