Electronic Colloquium on Computational Complexity, Report No. 147 (2013)

Any Beamsplitter Generates Universal Quantum Linear Optics

Adam Bouland* Scott Aaronson†

Abstract

In 1994, Reck et al. showed how to realize any linear-optical unitary transformation using a product of beamsplitters and phaseshifters. Here we show that any *single* beamsplitter that nontrivially mixes two modes, also densely generates the set of $m \times m$ unitary transformations (or orthogonal transformations, in the real case) on $m \geq 3$ modes. (We prove the same result for any 2-mode real optical gate, and for any 2-mode optical gate combined with a generic phaseshifter.) Experimentally, this means that one does not need tunable beamsplitters or phaseshifters for universality: any nontrivial beamsplitter is universal. Theoretically, it means that one cannot produce "intermediate" models of quantum-optical computation (analogous to the Clifford group for qubits) by restricting the allowed beamsplitters and phaseshifters: there is a dichotomy; one either gets a trivial set or else a universal set. No similar classification theorem for gates acting on qubits is currently known. We leave open the problem of classifying optical gates that act on 3 or more modes.

1 Introduction

Universal quantum computers have proved difficult to build. As one response, researchers have proposed limited models of quantum computation, which might be easier to realize. Three examples are the one clean qubit model of Knill and Laflamme [13], the commuting Hamiltonians model of Bremner, Jozsa, and Shepherd [3], and the BosonSampling model of Aaronson and Arkhipov [1]. None of these models are known or believed to be capable of universal quantum computation (or, depending on modeling details, even universal *classical* computation). But all of them can perform certain estimation or sampling tasks for which no polynomial-time classical algorithm is known.

One obvious way to define a limited model of quantum computation is to restrict the set of allowed gates. However, almost every gate set is universal [15], and so are most "natural" gate sets. For example, Controlled-NOT together with any real 1-qubit gate that does not square to the identity is universal [18]. As a result, very few nontrivial examples of non-universal gate sets are known. All known non-universal gate sets on $O(1)$ qubits, such as the Clifford group [8], are efficiently classically simulable, if the input and measurement outcomes both belong to an appropriately chosen qubit basis[1]. As a result, it is tempting to conjecture that there does not *exist* such an intermediate gate set: or more precisely, that any gate set on $O(1)$ qubits is either efficiently classical simulable (with appropriate input and output states), or else universal for quantum computing. Strikingly, this dichotomy conjecture remains open even for the special case of 1- and 2-qubit gates! We regard proving or disproving the conjecture as an important open problem for quantum computing theory.

---

*MIT. email: adam@csail.mit.edu.

†MIT. email: aaronson@csail.mit.edu.

[1]But not necessarily otherwise! For instance, suppose that a nonuniversal gate set G is efficiently simulable if inputs and outputs are in the computational basis. Now conjugate G by a change of qubit basis to obtain a gate set G'. Clearly G' is efficiently classically simulable in the new qubit basis. However, it is unclear how to simulate the gates G' if inputs and outputs are in the computational basis. Along these lines, there is evidence that Clifford gates [12], permutation gates [11], and even diagonal gates [3] can be hard to simulate in arbitrary bases.

ISSN 1433-8092

In this paper, we prove a related conjecture in the quantum linear optics model. In quantum optics, the Hilbert space is not built up as a tensor product of qubits; instead it's built up as a direct *sum* of optical modes. An optical *gate* is then just a unitary transformation that acts nontrivially on $O(1)$ of the modes, and as the identity on the rest. Whenever we have a k-mode gate, we assume that we can apply it to any subset of k modes (in any order), as often as desired. The most common optical gates considered are *beamsplitters*, which act on 2 modes and correspond to a 2×2 unitary matrix with determinant -1;[2] and *phaseshifters*, which act on 1 mode and simply apply a phase $e^{i\theta}$. Note that any unitary transformation acting on the 1-photon Hilbert space automatically gets "lifted," by homomorphism, to a unitary transformation acting on the Hilbert space of n photons, and every n-photon linear-optical transformation arises in this way (see [1, Section 3] for details). For this reason, when proving gate universality results, we can restrict our attention to the case of 1 photon.

We call a set of optical gates *universal* on m modes if it generates a dense subset of either $SU(m)$ (in the complex case) or $SO(m)$ (in the real case). Previously, Reck et al. [17] showed that the set of *all* phaseshifters and all beamsplitters is universal, on any number of modes. Therefore it is natural to ask: is there *any* set of beamsplitters and phaseshifters that gives rise to a nontrivial set of unitary transformations, yet still falls short of universality?

We answer this question in the negative. In particular, we show that any beamsplitter that acts nontrivially on 2 modes is universal on 3 or more modes. Our proof uses standard representation theory and the classification of closed subgroups of $SU(3)$ [7][9]. From an experimental perspective, this shows that any nontrivial beamsplitter suffices to create any desired optical network. From a computational complexity perspective, this result implies a dichotomy theorem for optical gate sets: any set of beamsplitters or phaseshifters generates a set of operations that is either trivially classically simulable, or else universal for quantum optics. Note that our result holds only for beamsplitters, i.e., optical gates that act on 2 modes and have determinant -1. We leave as an open problem whether our result can be extended to arbitrary 2-mode gates, or to gates that act on 3 or more modes.

Our work is the first that we know of to explore limiting the power of quantum optics by limiting the gate set. Previous work has considered varying the available input states and measurements. For example, Knill, Laflamme, and Milburn [14] famously showed that linear optics with single photon input states and adaptive measurements is universal for quantum computation. Restricting to nonadaptive measurements seems to reduce the computational power of linear optics, but Aaronson and Arkhipov [1] gave evidence that the resulting model is still impossible to simulate efficiently using a classical computer. If Gaussian states are used as inputs, and measurements are taken in the Gaussian basis only, then the model is efficiently classically simulable [2], but the case of Gaussian inputs and photon-number measurements is not yet understood. For a summary of what's currently known, see Aaronson and Arkhipov ([1, Section 1.4]).

We hope that this work will serve as a first step toward proving the dichotomy conjecture for *qubit*-based quantum circuits (i.e., the conjecture that every set of gates is either universal for quantum computation or else efficiently classically simulable). The tensor product structure of qubits gives rise to a much more complicated problem than the direct sum structure of linear optics. For that reason, one might expect the linear-optical "model case" to be easier to tackle first, and the present work confirms that expectation.

2 Background and Our Results

In a linear optical system with m modes, the state of a photon is described by a vector $|\psi\rangle$ in an m-dimensional Hilbert space. The basis states of the system are represented by strings $|s_1, s_2 \ldots s_m\rangle$ where $s_i \in \{0, 1\}$ denotes the number of photons in the i^{th} mode, and $\Sigma_{j=1}^{m} s_j$ is the total number of photons (in this case, 1). For example a 1-photon, 3-mode system has basis states $|100\rangle$, $|010\rangle$ and $|001\rangle$.

[2] Some references use a different convention and assume that beamsplitters have determinant $+1$ [16]. Note that these two conventions are equivalent if one assumes that one can permute modes, i.e. apply the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ which has determinant -1.

A k-local gate g is a $k \times k$ unitary matrix which acts on k modes at a time while acting in direct sum with the identity on the remaining $m - k$ modes. A *beamsplitter* b is a 2-local gate with determinant -1. Therefore any beamsplitter has the form $b = \begin{pmatrix} \alpha & \beta^* \\ \beta & -\alpha^* \end{pmatrix}$ where $|\alpha|^2 + |\beta|^2 = 1$. Let b_{ij} denote the matrix action of applying the beamsplitter to modes i and j of a one-photon system. For example, if $m = 3$, we have that

$$b_{12} = \begin{pmatrix} \alpha & \beta^* & 0 \\ \beta & -\alpha^* & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad b_{31} = \begin{pmatrix} -\alpha^* & 0 & \beta \\ 0 & 1 & 0 \\ \beta^* & 0 & \alpha \end{pmatrix}$$

when written in the computational basis. A beamsplitter is called *nontrivial* if $|\alpha| \neq 0$ and $|\beta| \neq 0$, i.e. if the beamsplitter mixes modes.

We say that a set S of optical gates *densely generates* a continuous group G of unitary transformations, if the group H generated by S is a dense subgroup of G (that is, if $H \leq G$ and H contains arbitrarily close approximations to every element of G). Then we call S *universal on m modes* if it densely generates $SU(m)$ or $SO(m)$ when acting on m modes. (Due to the irrelevance of global phases, this is physically equivalent to generating $U(m)$ or $O(m)$ respectively.) In this definition we are assuming that whenever we have a k-mode gate in S, we can apply it to any subset of k modes (in any order), as often as desired. Note that we consider real $SO(m)$ evolutions to be universal as well; this is because the distinction between real and complex optical networks is mostly irrelevant to computational applications of linear optics, such as the KLM protocol [14] and BosonSampling [1].

A basic result in quantum optics, proved by Reck et al. [17], says that the collection of all beamsplitters and phaseshifters is universal. Specifically, given any target unitary U on m modes, there exists a sequence of $O(m^2)$ beamsplitters and phaseshifters whose product is exactly U. Reck et al.'s proof also shows an analogous result for real beamsplitters - namely, that any orthogonal matrix O can be written as the product of $O(m^2)$ real beamsplitters. It can easily be shown that there exist two beamsplitters b, b' whose products densely generate $O(2)$. Therefore b and b' can be used to simulate any real beamsplitter, and hence by Reck et al. [17], the set $\{b, b'\}$ is universal for linear optics.

In this paper, we consider the universality of a *single* beamsplitter b. If b is trivial, then on m modes the matrices b_{ij} generates a subgroup of P_m, the set of $m \times m$ unitary matrices with all entries having norm zero or one. This is obviously non-universal, and the state evolutions on any number of photons are trivial to simulate classically. Our main result is that any nontrivial beamsplitter densely generates either all orthogonal transformations on 3 modes (in the real case), or all unitary transformations on 3 modes (in the complex case). From this, it follows easily from Reck et al. [17] that such a beamsplitter is also universal on m modes for any $m \geq 3$.

Theorem 2.1. *Let b be any nontrivial beamsplitter. Then the set $S = \{b_{12}, b_{13}, b_{23}\}$, obtained by applying b to all possible pairs among 3 photon modes,*[3] *densely generates either $SO(3)$ (if all entries of b are real) or $SU(3)$ (if any entry of b is non-real).*

Corollary 2.2. *Any nontrivial beamsplitter is universal on $m \geq 3$ modes.*

Proof. By Theorem 2.1, the set $S = \{b_{12}, b_{13}, b_{23}\}$ densely generates all orthogonal matrices with determinant 1. But since b has determinant -1, we know that S must generate all orthogonal matrices with determinant -1 as well.[4] Therefore, S densely generates the action of any real beamsplitter b' acting on 2 out of 3 modes. So by Reck et al [17], S also densely generates all orthogonal matrices on m modes for $m \geq 3$. □

[3] Technically, we could also consider the unitaries b_{21}, b_{31}, b_{32}, obtained by applying b to the same pairs of modes but reversing their order. However, this turns out not to give us any advantage.

[4] Indeed any orthogonal O with determinant -1 can be written as $O = b_{12}^{-1}O' = b_{12}O'$ for some O' of determinant 1.

Note that, although our proof of universality on 3 modes is nonconstructive, by the Solovay-Kitaev Theorem [6], there is an efficient algorithm that, given any target unitary U, finds a sequence of b's approximating U up to error ϵ in $O(\log(\frac{1}{\epsilon}))$ time. Thus, our universality result also implies an efficient algorithm to construct any target unitary using beamsplitters in the same manner as Reck et al.

We now proceed to a proof of Theorem 2.1.

3 Proof of Main Theorem

We first consider applying our fixed beamsplitter

$$b = \begin{pmatrix} \alpha & \beta^* \\ \beta & -\alpha^* \end{pmatrix},$$

where α and β are complex and $|\alpha|^2 + |\beta|^2 = 1$, to 2 modes of a 3-mode optical system. We take pairwise products of these beamsplitter actions to generate 3 special unitary matrices. These 3 unitaries densely generate some group of matrices $G \leq SU(3)$. We then use the representation theory of subgroups of $SU(3)$ described in the work of Fairbairn, Fulton and Klink [7] and Hanany and He [9][10] to show that the beamsplitter must generate either all $SO(3)$ matrices (if the beamsplitter is real) or all $SU(3)$ matrices (if the beamsplitter has a complex entry).

Consider applying our beamsplitter to a 3-mode system. Let R_1, R_2, R_3 be defined as the pairwise products of the beamsplitter actions below:

$$R_1 = b_{12}b_{13} = \begin{pmatrix} \alpha^2 & \beta^* & \alpha\beta^* \\ \alpha\beta & -\alpha^* & |\beta|^2 \\ \beta & 0 & -\alpha^* \end{pmatrix} \quad R_2 = b_{23}b_{13} = \begin{pmatrix} \alpha & 0 & \beta^* \\ |\beta|^2 & \alpha & -\alpha^*\beta^* \\ -\alpha^*\beta & \beta & \alpha^{*2} \end{pmatrix}$$

$$R_3 = b_{12}b_{23} = \begin{pmatrix} \alpha & \alpha\beta^* & \beta^{*2} \\ \beta & -|\alpha|^2 & -\alpha^*\beta^* \\ 0 & \beta & -\alpha^* \end{pmatrix}$$

Since R_1, R_2, R_3 are even products of matrices of determinant -1, they are all elements of $SU(3)$. Let $G \leq SU(3)$ be the subgroup densely generated by the set $\{R_1, R_2, R_3\}$. Let G_M be the set of matrices representing G under this construction. First we will show that these matrices G_M form an irreducible representation of G.

Claim 3.1. *The set $\{R_1, R_2, R_3\}$ generates an irreducible 3-dimensional representation of G.*

Proof. Suppose that some matrix

$$U = \begin{pmatrix} A & D & G \\ B & E & H \\ C & F & I \end{pmatrix}$$

commutes with R_1, R_2, and R_3. Then we claim that U is a constant multiple of the identity, i.e. $A = E = I$ and $D = G = H = B = C = F = 0$.

From the claim, it follows easily that the representation is irreducible. Indeed, suppose the representation is reducible. Then by a change of basis, it can be made block diagonal. In the new basis, the matrix consisting of 1's on the diagonal in the first block, and 2's in the diagonal of the second block, commutes with all elements of G, and in particular with R_1, R_2, R_3. But that matrix is not a multiple of the identity. Hence if only multiples of the identity commute with R_1, R_2, R_3, the representation must be irreducible.

We now prove the claim. First, since U commutes with R_1,

$$\begin{pmatrix} A & D & G \\ B & E & H \\ C & F & I \end{pmatrix} \begin{pmatrix} \alpha^2 & \beta^* & \alpha\beta^* \\ \alpha\beta & -\alpha^* & |\beta|^2 \\ \beta & 0 & -\alpha^* \end{pmatrix} = \begin{pmatrix} \alpha^2 & \beta^* & \alpha\beta^* \\ \alpha\beta & -\alpha^* & |\beta|^2 \\ \beta & 0 & -\alpha^* \end{pmatrix} \begin{pmatrix} A & D & G \\ B & E & H \\ C & F & I \end{pmatrix}$$

This imposes 9 equations. Below we give the equations coming from the (1,1), (1,2), (2,2), (2,3), and (3,2) entries of the above matrices respectively.

$$
\begin{aligned}
(D\alpha + G)\beta &= (C\alpha + B)\beta^* && (1)\\
(A - E - F\alpha)\beta^* &= D(\alpha^2 + \alpha^*) && (2)\\
B\beta^* &= D\alpha\beta + F\beta\beta^* && (3)\\
B\alpha\beta^* + E\beta\beta^* - H\alpha^* &= G\alpha\beta - H\alpha^* + I\beta\beta^* && (4)\\
C\beta^* &= D\beta && (5)
\end{aligned}
$$

Note that equations (5) and (1) imply that

$$G\beta = B\beta^* \tag{6}$$

So by equation (4) we have

$$E\beta\beta^* = I\beta\beta^* \tag{7}$$

So since $0 < |\beta| < 1$, we have $I = E$.

In total so far we have $I = E$, $G\beta = B\beta^*$ and $C\beta^* = D\beta$.

Next, since U commutes with R_2,

$$\begin{pmatrix} A & D & G \\ B & E & H \\ C & F & E \end{pmatrix} \begin{pmatrix} \alpha & 0 & \beta^* \\ |\beta|^2 & \alpha & -\alpha^*\beta^* \\ -\alpha^*\beta & \beta & \alpha^{*2} \end{pmatrix} = \begin{pmatrix} \alpha & 0 & \beta^* \\ |\beta|^2 & \alpha & -\alpha^*\beta^* \\ -\alpha^*\beta & \beta & \alpha^{*2} \end{pmatrix} \begin{pmatrix} A & D & G \\ B & E & H \\ C & F & E \end{pmatrix}$$

This imposes another 9 equations. Here are the equations from the (1,1), (2,1) and (2,2) entries respectively, which we have simplified using $I = E$, $G\beta = B\beta^*$ and $C\beta^* = D\beta$:

$$
\begin{aligned}
D\beta &= D\beta\beta^* - G\alpha^*\beta && (8)\\
E\beta\beta^* - H\alpha^*\beta &= A\beta\beta^* - C\alpha^*\beta^* && (9)\\
H\beta &= D\beta\beta^* - F\alpha^*\beta^* && (10)
\end{aligned}
$$

Note that equations (8) and (10), combined with the fact that $G\beta = B\beta^*$, imply that $D\beta = H\beta$, and hence $D = H$.

Plugging this in to equation (9), we see that $E\beta\beta^* - D\alpha^*\beta = A\beta\beta^* - C\alpha^*\beta^*$. Using $C\beta^* = D\beta$ these last two terms cancel, so $E\beta\beta^* = A\beta\beta^*$, and hence $E = A$. So overall we have established that $A = E = I$, $D = H$, $B = F$, $G\beta = B\beta^*$ and $C\beta^* = D\beta$.

Now suppose $B = 0$. Then we have from above that $B = F = G = 0$. By equation (8) we also have $D\beta = D\beta\beta^* \Rightarrow D = 0$ since $0 < |\beta| < 1$. Hence we have $C = 0$ as well by the fact that $C\beta^* = D\beta$. Therefore U is a multiple of the identity, as desired.

So it suffices to prove that $B = 0$. Suppose $B \neq 0$; then we will derive a contradiction.

Since U commutes with R_3,

$$\begin{pmatrix} A & D & G \\ B & A & D \\ C & B & A \end{pmatrix} \begin{pmatrix} \alpha & \alpha\beta^* & \beta^{*2} \\ \beta & -|\alpha|^2 & -\alpha^*\beta^* \\ 0 & \beta & -\alpha^* \end{pmatrix} = \begin{pmatrix} \alpha & \alpha\beta^* & \beta^{*2} \\ \beta & -|\alpha|^2 & -\alpha^*\beta^* \\ 0 & \beta & -\alpha^* \end{pmatrix} \begin{pmatrix} A & D & G \\ B & A & D \\ C & B & A \end{pmatrix}$$

This imposes yet another 9 equations, but we will only need the one coming from the (2,2) entry of the above matrices to complete the proof:

$$B\alpha\beta^* = -B\alpha^*\beta^* \tag{11}$$

Since $B \neq 0$, equation (11) implies that $\alpha = -\alpha^*$, i.e. α is pure imaginary. Furthermore, since $G\beta = B\beta^*$, we have $G \neq 0$ as well. Using this, we can write out equations (2) and (3) as follows:

$$(-B\alpha)\beta^* = D(\alpha^2 - \alpha) \quad \Rightarrow \quad G\beta = D(1-\alpha) \tag{12}$$
$$B\beta^* = D\alpha\beta + F\beta\beta^* \quad \Rightarrow \quad G = D\alpha + G\beta \tag{13}$$

Summing these equations, we see that $G = D$. Plugging back into equation (13), we see that $\beta = 1-\alpha$. Since α is pure imaginary this contradicts $|\alpha|^2 + |\beta|^2 = 1$.

To summarize, if U commutes with all elements of G, then U is a multiple of the identity. This proves the claim and hence the theorem. □

We have learned that the set G_M forms a 3-dimensional irreducible representation of G. We now leverage this fact, along with the classification of finite subgroups of $SU(3)$, to show that G is not finite.

Claim 3.2. *G is infinite.*

Proof. By Claim 3.1, if G is finite then $\{R_1, R_2, R_3\}$ generates an irreducible representation of G. The finite subgroups of $SU(3)$ consist of the finite subgroups of $SU(2)$, eleven exceptional finite subgroups, and two infinite families of "dihedral-like" groups, whose irreducible representations are classified in [7] [9][10]. Our proof proceeds by simply enumerating the possible finite groups that G could be, and showing that $\{R_1, R_2, R_3\}$ cannot generate an irreducible representation of any of them.

First we eliminate the possibility that G is an exceptional finite subgroup of $SU(3)$. Of the eleven exceptional subgroups, only six of them have 3-dimensional irreps: they are labeled $\Sigma(60)$, $\Sigma(168)$, $\Sigma(216)$, $\Sigma(36 \times 3)$, $\Sigma(216 \times 3)$, and $\Sigma(360 \times 3)$. So by Claim 3.1, if G is finite and exceptional, then it is one of these six groups.

The character tables of these groups are provided in [7] and [9]. Recall that the character of an element of a representation is the trace of its representative matrix. The traces of the matrices R_1, R_2, R_3, denoted T_1, T_2, T_3, are given by

$$T_1 = \alpha^2 - 2\alpha^* \tag{14}$$
$$T_2 = (\alpha^*)^2 + 2\alpha \tag{15}$$
$$T_3 = -|\alpha|^2 + \alpha - \alpha^* = -|\alpha|^2 + 2\mathrm{Im}(\alpha) \tag{16}$$

We will show that these cannot be the characters of the elements of a 3-dimensional irrep of $\Sigma(60)$, $\Sigma(168)$, $\Sigma(216)$, $\Sigma(36 \times 3)$,$\Sigma(216 \times 3)$ or $\Sigma(360 \times 3)$.

There are two 3-dimensional irreps of $\Sigma(60)$ up to conjugation [7]. The characters of their elements all lie in the set $\left\{0, -1, 3, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$. Note that $0 < |\alpha|^2 < 1$, which means that T_3 cannot be in this set unless $T_3 = \frac{1-\sqrt{5}}{2}$ and $\mathrm{Im}(\alpha) = 0$. But then this implies $\alpha = \pm\sqrt{\frac{\sqrt{5}-1}{2}}$. Plugging this into T_1 and T_2, we see they are not in the set of allowed values. Hence G is not $\Sigma(60)$.

There are two 3-dimensional irreps of $\Sigma(168)$ up to conjugation [7]. The characters of their elements all lie in the set $S = \left\{0, \pm 1, 3, \frac{1}{2}(-1 \pm i\sqrt{7})\right\}$. Since $0 < |\alpha|^2 < 1$, if T_3 is in this set it must have value $\frac{1}{2}(-1 \pm i\sqrt{7})$. Therefore we must have $\alpha = \pm\frac{3}{4} \pm \frac{\sqrt{7}}{4}i$. This implies that $\alpha^2 = \frac{2}{16} \pm \frac{3\sqrt{7}}{16}i$ and $2\alpha^* = \pm\frac{3}{4} \pm \frac{\sqrt{7}}{4}i$. Regardless of the signs chosen, this means that T_1 is not in the set S of allowed values. Hence G is not $\Sigma(168)$.

There is one 3-dimensional irrep of $\Sigma(216)$ up to conjugation [7]. The characters of its elements all lie in the set $\{0, -1, 3\}$. Since T_3 cannot be in this set, G is not $\Sigma(216)$.

There are eight 3-dimensional irreps of $\Sigma(36 \times 3)$ up to conjugation [9]. The characters of their elements all lie in the set $S = \{0, \pm 1, \pm e_3, \pm e_3^2, \pm e_4, \pm e_{12}^7, \pm e_{12}^{11} \pm 3, \pm 3e_3, \pm 3e_3^2\}$ where $e_n = e^{\frac{2\pi i}{n}}$. Since $\mathrm{Re}(T_3) = -|\alpha|^2$ and $0 < |\alpha|^2 < 1$, if $T_3 \in S$ then we must have $T_3 \in \{\pm e_3, \pm e_3^2, \pm e_{12}^7, \pm e_{12}^{11}\}$.

Solving for α gives us $\alpha \in \left\{ \frac{\pm\sqrt{5}\pm\sqrt{3}i}{4}, \frac{\pm\sqrt{8\sqrt{3}-1}\pm i}{4} \right\}$. A straightforward evaluation of possible values of T_1 shows $T_1 \notin S$. So T_1 and T_3 cannot be characters of these irreps, and hence G is not $\Sigma(36 \times 3)$.

There are seven 3-dimensional irreps of $\Sigma(216 \times 3)$ up to conjugation [9]. The characters of their elements all lie in the set

$$S = \{0, \pm 1, 3, \pm e_3, \pm e_3^2, -e_9^2, -e_9^4, -e_9^5, -e_9^7, \pm e_9^2 + e_9^5, 2e_9^2 + e_9^5, -e_9^2 - 2e_9^5, e_9^4 + e_9^7, e_9^4 + 2e_9^7, -2e_9^4 - e_9^7\}.$$

If $T_3 \in S$, then for each case we can solve for α and hence T_1. As above, a straightforward calculation shows that for no $T_3 \in S$ do we have $T_1 \in S$. Hence G is not $\Sigma(216 \times 3)$.

There are four 3-dimensional irreps of $\Sigma(360 \times 3)$ up to conjugation [9]. The characters of their elements all lie in the set

$$S = \{0, \pm 1, \pm e_3, \pm e_3^2, 3e_3, 3e_3^2, -e_5 - e_5^4, -e_5^2 - e_5^3, -e_{15} - e_{15}^4, -e_{15}^7 - e_{15}^{13}, -e_{15}^{11} - e_{15}^{14}, -e_{15}^2 - e_{15}^8\}.$$

Again a straightforward calculation shows that for no $T_3 \in S$ do we have $T_1 \in S$. Hence G is not $\Sigma(360 \times 3)$.

We have therefore shown that G_M is not an irrep of an exceptional finite subgroup of $SU(3)$.

Next we will show that G_M is not in one of the two infinite families of "dihedral-like" finite subgroups of $SU(3)$, which are called $\Delta(3n^2)$ and $\Delta(6n^2)$ and are indexed by $n \in \mathbb{N}$. The 3-dimensional irreps of $\Delta(3n^2)$ are labeled by integers $m_1, m_2 \in \{0, \ldots, n-1\}$, and have conjugacy classes labeled by letters A, C, E and numbers $p, q \in \{0, \ldots, n-1\}$. The respective characters are either 0 for conjugacy classes $C(p,q)$ and $E(p,q)$ or

$$e^{\frac{2\pi i}{n}(m_1 p + m_2 q)} + e^{\frac{2\pi i}{n}(m_1 q - m_2(p+q))} + e^{\frac{2\pi i}{n}(-m_1(p+q) + m_2 p)} \tag{17}$$

for conjugacy class $A(p,q)$.

Assume that G_M is an irrep of $\Delta(3n^2)$ for some n—we will derive a contradiction shortly. Then the trace of each R_i must be zero (if R_i is a representative of conjugacy class C or E) or of the form of equation (17) (if R_i is a representative of conjugacy class A). However, we can show that none of the traces T_i can be 0 because our beamsplitter is nontrivial. Indeed T_3 cannot be zero as $0 < |\alpha|^2 < 1$. We know that in order for T_1 to be zero, we need $\alpha^2 = 2\alpha^*$, which implies $|\alpha| = 2$ which is not possible, and likewise with T_2. Hence each T_i must have the form of equation (17), which implies each R_i is in conjugacy class $A(p_i, q_i)$ for some choice of p_i, q_i. However, looking at the multiplication table for this group provided in [7, Table VIII], we have that $A(p,q)A(p',q') = A\left(p + q \mod n, p' + q' \mod n\right)$. Hence the T_i's cannot possibly generate all of $\Delta(3n^2)$ for any n, since they cannot generate elements in the conjugacy classes $C(p,q)$ or $E(p,q)$. This contradicts our assumption that the R_i's generate an irrep of $\Delta(3n^2)$. Therefore G_M is not an irrep of $\Delta(3n^2)$ for any n.

Next we turn our attention to the second family of dihedral-like finite subgroups of $SU(3)$, labeled $\Delta(6n^2)$. The group $\Delta(6n^2)$ contains 6 families of conjugacy classes, labeled by A, B, C, D, E, F and by integers p, q as above. The 3-dimensional irreps of $\Sigma(6n^2)$ are again labeled by (m_1, m_2), which now take values in $(m, 0), (0, m)$ or (m, m), as well as $t \in \{0, 1\}$. The character of each element is

$$\mathrm{Tr}(A(p,q)) = e^{\frac{2\pi i}{n}(m_1 p + m_2 q)} + e^{\frac{2\pi i}{n}(m_1 q - m_2(p+q))} + e^{\frac{2\pi i}{n}(-m_1(p+q) + m_2 p)} \tag{18}$$

$$\mathrm{Tr}(B(p,q)) = (-1)^t e^{\frac{2\pi i}{n}(m_1 p + m_2 q)} \tag{19}$$

$$\mathrm{Tr}(D(p,q)) = (-1)^t e^{\frac{2\pi i}{n}\left(m_1(\frac{n}{2} - p - q) + m_2 p\right)} \tag{20}$$

$$\mathrm{Tr}(F(p,q)) = (-1)^t e^{\frac{2\pi i}{n}\left(m_1 q + m_2(\frac{n}{2} - p - q)\right)} \tag{21}$$

$$\mathrm{Tr}(C(p,q)) = \mathrm{Tr}(E(p,q)) = 0 \tag{22}$$

We now eliminate the possibility that G_M is an irrep of $\Delta(6n^2)$ for any n. Again assume by way of contradiction that G_M is an irrep of $\Delta(6n^2)$ for some n. Then each R_i must be in one of the families of conjugacy classes A, B, C, D, E, F, and each trace T_i must have the corresponding character from equations (18)-(22). As noted previously each T_i cannot be 0, so in fact each R_i must be in classes A, B, D or F. Furthemore, we will show the following Lemma:

Lemma 3.3. *If G_M is an irrep of $\Delta(6n^2)$, then at least two of the R_i are in conjugacy class family A.*

By Lemma 3.3, at most one of the R_i's is in class B, D or F while the remaining R_i's are in class A. However, by examining the multiplication table for this group provided in [7, Table VIII], one can see that any number of elements from conjugacy class A plus one element from class B, D, or F cannot generate the entire group. This contradicts our assumption that the R_i's generate an irrep of $\Delta(6n^2)$. Hence G_M is not an irrep of $\Delta(6n^2)$ so G cannot be $\Delta(6n^2)$ by Claim 3.1.

We now prove Lemma 3.3 before continuing the proof of Claim 3.2.

Proof of Lemma 3.3 . Assume that G_M is an irrep of $\Delta(6n^2)$. We will show that at most one of the matrices R_1, R_2, R_3 can be of class B, D or F. Hence at least two of $\{R_1, R_2, R_3\}$ must be representatives of conjugacy class A. We proceed by enumerating all pairs R_i, R_j for $i \neq j$ and show that it's not possible for both R_i and R_j to be of class B, D or F.

Let $\alpha = a + bi$ where a and b are real. If R_i is of conjugacy class B, D or F, then T_i has norm 1, which imposes the following equations on a and b:

$$|T_1|^2 = 1 \Rightarrow (a^2+b^2)^2 + 4[a^2(1-a) + b^2(3+a)] = 1 \tag{23}$$

$$|T_2|^2 = 1 \Rightarrow (a^2+b^2)^2 + 4[a^2(1+a) + b^2(1-3a)] = 1 \tag{24}$$

$$|T_3|^2 = 1 \Rightarrow (a^2+b^2)^2 + 4b^2 = 1 \tag{25}$$

First suppose that R_1 and R_2 are both members of conjugacy classes B, D, or F. Then $|T_1| = |T_2| = 1$. The only solutions to equations (23) and (24) in which $0 < |\alpha|^2 = a^2 + b^2 < 1$ are $\left(a = 0, b = \pm\sqrt{\sqrt{5}-2}\right)$ and $\left(a = \pm\frac{1}{2}\sqrt{3(\sqrt{5}-2)}, b = \pm\frac{1}{2}\sqrt{\sqrt{5}-2}\right)$. Note also that the product R_1R_2 must be in conjugacy class C or E according to the group multiplication table in [7, Table VIII]. Hence the trace of R_1R_2 must be 0 if G_M is an irrep of $\Delta(6n^2)$. This implies that

$$\mathrm{Tr}(R_1R_2) = \alpha^3 - \alpha^{*3} + |\beta|^2\left(1 + \beta + \beta^* - |\alpha|^2\right) - |\alpha|^2 = 0 \tag{26}$$

Since we have $\alpha = a + bi$ where the values of a and b are one of the six possibilities above, one can see that there is no β which satisfies equation (26). Indeed, note that $\alpha^3 - \alpha^{*3}$ is nonzero and pure imaginary, while the rest of the expression is real, so the terms in equation (26) cannot sum to zero. This provides the desired contradiction. We conclude that R_1 and R_2 cannot both be of conjugacy class B, D, or F.

Next suppose that R_1 and R_3 are both of conjugacy class B, D or F. Then $|T_1| = |T_3| = 1$. If $\alpha = a + bi$ as before, the equations (23) and (25), combined with the fact that $0 < |\alpha|^2 = a^2 + b^2 < 1$, imply that $a = 0$ and $b = \pm\sqrt{\sqrt{5}-2}$. Again, using the group multiplication table in [7, Table VIII] we must have that R_1R_3 is of class C or E so

$$\mathrm{Tr}(R_1R_3) = \alpha^3 + \alpha^*|\alpha|^2 + \alpha^{*2} + |\beta|^2(1 + \beta + \beta^* + \alpha^2) = 0 \tag{27}$$

Since $\alpha = \pm i\sqrt{\sqrt{5}-2}$, this is a contradiction—for the terms $\alpha^3 + \alpha^*|\alpha|^2$ of equation (27) are nonzero and pure imaginary while the remaining terms are real. Hence R_1 and R_3 cannot both be of conjugacy class B, D, or F.

Finally suppose that R_2 and R_3 are both of conjugacy class B, D, or F. Then $|T_2| = |T_3| = 1$. If $\alpha = a + bi$ then the only solutions to equations (24) and (25) in which $0 < |\alpha|^2 = a^2 + b^2 < 1$ are $\left(a = 0, b = \pm\sqrt{\sqrt{5}-2}\right)$ and $(a \approx 0.437668, b \approx \pm 0.457975)$. Furthermore using the group multiplication table in [7, Table VIII] we must have that R_2R_3 is of class C or E so

$$\mathrm{Tr}(R_2R_3) = \alpha^2 - \alpha^{*3} - \alpha|\alpha|^2 + |\beta|^2(\alpha\beta^* - \alpha^*\beta^* - 2\alpha^*) = 0 \tag{28}$$

With slightly more work, one can again check that equation (28) cannot be satisfied with the above values of α, under the additional constraint that $|\alpha|^2 + |\beta|^2 = 1$, providing the desired contradiction. Hence R_2 and R_3 cannot both be of conjugacy class B, D, or F, which completes the proof of Lemma 3.3.

□

We have therefore eliminated the possiblity that G_M is an irrep of $\Delta(6n^2)$ for any n, and so $G \neq \Delta(6n^2)$ by Claim 3.1.

Finally we will show that G is not a finite subgroup of $SU(2)$. Since $SU(2)$ is a double cover of $SO(3)$, if G is a finite subgroup of $SU(2)$, then G must be either a finite subgroup of $SO(3)$ or else the double cover of such a subgroup. We first eliminate the finite subgroups of $SO(3)$. The dihedral and cyclic subgroups have no 3-dimensional irreps; hence G cannot be one of these by Claim 3.1. The icosahedral subgroup is isomorphic to $\Sigma(60)$ so has already been eliminated. The octahedral and tetrahedral subgroups do have 3-dimensional irreps. However, the characters of their elements all lie in the set $\{0, \pm 1, \pm 3\}$, so these can be eliminated just as the exceptional groups of $SU(3)$ were eliminated.

Now all that remains are double covers of the finite subgroups of $SO(3)$. The binary dihedral groups, also known as the dicyclic groups, have no 3-dimensional irreps, so G cannot be a binary dihedral group by Claim 3.1. The binary tetrahedral group has one 3-dimensional irrep, with character values in the set $\{0, \pm 1, \pm 3\}$. So T_3 cannot be in this set as noted above.

The binary octahedral group has two 3-dimensional irreps, with character values also in $\{0, \pm 1, \pm 3\}$, so is likewise eliminated. The binary icosahedral group has two 3-dimensional irreps, with all characters in the set $\{0, -1, 3, \frac{\sqrt{5}\pm 1}{2}\}$. As discussed in the case of $\Sigma(60)$, our traces cannot take these values.

In summary, by enumeration of the finite subgroups of $SU(3)$, we have shown that G cannot be finite.

□

Corollary 3.4. *G is a continuous (Lie) subgroup of $SU(3)$.*

Proof. G is infinite by Claim 3.2. Furthermore G is closed because it is the set of matrices *densely* generated by $\{R_1, R_2, R_3\}$. It is well-known that a closed, infinite subgroup of a Lie group is also a Lie group (this is Cartan's theorem [5]). The corollary follows. □

Next we show that G must be either $SO(3)$, $SU(2)$ or $SU(3)$. Furthermore, the set of matrices G_M densely generated by $\{R_1, R_2, R_3\}$ consists of either all $SO(3)$ matrices or all $SU(3)$ matrices.

Claim 3.5. *G is either $SO(3)$, $SU(2)$, or $SU(3)$. Furthermore, G_M consists of either all 3×3 special unitary matrices (if the beamsplitter b has a non-real entry), or all 3×3 special orthogonal matrices (if b is real).*

Proof. Since R_1, R_2, and R_3 do not commute, G is nonabelian. By Corollary 3.4, we know G is a Lie group, and furthermore G is closed. The nonabelian closed connected Lie subgroups of $SU(3)$ are well-known [4]: they are $SU(3)$, $SU(2) \times U(1)$, $SU(2)$, and $SO(3)$. Meanwhile, the closed disconnected Lie subgroups of $SU(3)$ are $\Delta(3\infty)$ and $\Delta(6\infty)$, as described in [7].

Note that $\Delta(3\infty)$ and $\Delta(6\infty)$ are the analogues of $\Delta(3n^2)$ and $\Delta(6n^2)$ as $n \to \infty$. Our above arguments showing that $G \neq \Delta(3n^2)$ and $G \neq \Delta(6n^2)$ carry over in this limit, because at no point did we use the fact that n or m were finite. Therefore G cannot be either of these continuous groups.

By Claim 3.1, G has a 3-dimensional irrep. Of the remaining groups, only $SU(2)$, $SO(3)$, and $SU(3)$ have 3-dimensional irreps. Furthermore, it is well known that the only 3-dimensional irrep of $SU(2)$ is as $SO(3)$. This is because $SU(2)$ has exactly one irrep in each finite dimension (See [4, Section II.5] or [19] for details), and $SU(2)$ has an obvious representation as $SO(3)$ via the fact that $SU(2)$ is a double cover of $SO(3)$. Since we are only concerned with the set of matrices G_M generated, without loss of generality we can assume G is either $SO(3)$ or $SU(3)$.

It is well-known that the only 3-dimensional irrep of $SU(3)$ is the natural one, as the group of all 3×3 special unitary matrices ([4, Section VI.5]). Likewise, the only 3-dimensional irrep of $SO(3)$ is the natural one, up to conjugation by a unitary [4]. Hence G_M consists of either all 3×3 special unitary matrices (case A), or all 3×3 special orthogonal matrices conjugated by some unitary U (case B).

We now show that if the beamsplitter b is real, then we are in case B and without loss of generality the conjugating unitary U is real. Hence G_M is the set of all 3×3 orthogonal matrices. Otherwise, if b has a complex entry, we will show we are in case A and G_M is the set of all 3×3 special unitary matrices.

First, suppose b is real. Then all matrices in our generating set are orthogonal, so all matrices in G_M are orthogonal. Hence we are in case B, and since all matrices in G_M are real, without loss of generality U is a real matrix as well.

Now suppose that b has a complex entry. Then either α or β are not real. First, suppose α is not real. Then $\mathrm{Tr}(R_1) = \alpha^2 - 2\alpha^*$ is not real because $0 < |\alpha| < 1$. But since conjugating a matrix by a unitary preserves its trace, and we are in case B, the traces of all matrices in G_M must be real. In particular $\mathrm{Tr}(R_1)$ must be real, which is a contradiction. Therefore if α is not real then we must be in case A.

Next, suppose β is not real. Then we can obtain a similar contradiction. Let $\beta = p + qi$ where p and q are real. By direct calculation one can show that $\mathrm{Im}\left(\mathrm{Tr}(R_1 R_2 R_3 R_1)\right) = |\beta|^4 \left(\beta^{*2} + 2\beta\right)$. Since our beamsplitter is nontrivial, $|\beta|^4 \neq 0$, so this quantity is 0 if and only if $\beta^{*2} + 2\beta = 0 \Leftrightarrow 2q(1-p) = 0$. But this cannot occur, since $q \neq 0$ (because β is not real), and $1 - p \neq 0$ (because the beamsplitter is nontrivial). Hence in this case $\mathrm{Tr}(R_1 R_2 R_3 R_1)$ is imaginary, which contradicts the fact we are in case B. Therefore if β is not real then we must be in case A, which completes the proof. □

Theorem 2.1 follows from Claim 3.5. Having proved our main result, we can now easily show two alternative versions of the theorem as well.

Corollary 3.6. *Any nontrivial* 2*-mode optical gate* $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *(not necessarily of determinant* -1*), plus the set of all phaseshifters densely generates* $SU(m)$ *on* $m \geq 3$ *modes.*

Proof. Since g is unitary we have $\det(g) = e^{i\theta}$ for some θ. By composing g with a phase of $e^{i\frac{\pi-\theta}{2}}$, we obtain a nontrivial beamsplitter g' of determinant -1. The gate g' is universal by Theorem 2.1, hence this gate set is universal as well. □

Corollary 3.7. *Any nontrivial* 2*-mode real optical gate* g *is universal for quantum linear optics.*

Proof. Since g is real, g must have determinant ± 1. The case of $\det(g) = -1$ is handled by Theorem 2.1, so we now prove the $\det(g) = +1$ case. In this case g is a rotation by an angle θ. The fact that g is nontrivial means θ is not a multiple of $\pi/2$. The beamsplitter actions b_{12}, b_{23}, b_{13} can be viewed as 3-dimensional rotations by angle θ about the x, y and z axes. So the question reduces to "For which angles θ (other than multiples of $\pi/2$) do rotations by θ about the x, y and z axes fail to densely generate all possible rotations?"

This question is easily answered using the well-known classification of closed subgroups of $SO(3)$. The finite subgroups of $SO(3)$ are the cyclic, dihedral, tetrahedral, octahedral, and icosahedral groups. One can easily check that our gate g cannot generate a representation of one of these groups, and hence densely generates some infinite group G. By the same reasoning as in Corollary 3.4, we conclude that G is a Lie subgroup of $SO(3)$.

The Lie subgroups of $SO(3)$ are $SO(3)$, $U(1)$ (all rotations about one axis) and $U(1) \times \mathbb{Z}_2$ (all rotations about one axis, plus a rotation by π perpendicular to the axis). Again one can easily eliminate the possibility that G is $U(1)$ or $U(1) \times \mathbb{Z}_2$, and hence G must be all of $SO(3)$.

We have proven universality on 3 modes for real nontrivial g with determinant $+1$. Universality on $m \geq 3$ modes follows by a real analog of Reck et al. [17], namely that any rotation matrix in $SO(m)$ can be expressed as the product of $O(m^2)$ real 2×2 optical gates of determinant 1. □

4 Open Questions

At the moment our dichotomy theorem only holds for beamsplitters, which act on 2 modes at a time and have determinant -1. As we said before, we leave open whether the dichotomy can be extended to 2-mode gates with determinant other than -1. Although the phases of gates are irrelevant in the qubit model, the phases unfortunately *are* relevant in linear optics—and that is the source of the difficulty. Note that the previous universality result of Reck et al. [17] simply assumed that arbitrary phaseshifters were available for free, so this issue did not arise.

Another open problem is whether our dichotomy can be extended to k-mode optical gates for all constants k. Such a result would complete the linear-optical analogue of the dichotomy conjecture for standard quantum circuits. The case $k = 3$ seems doable because the representations of all finite subgroups of $SU(4)$ are known [10]. But already the case $k = 4$ seems more difficult, because the representations of all finite subgroups of $SU(5)$ have not yet been classified. Thus, a proof for arbitrary k would probably require more advanced techniques in representation theory.

5 Acknowledgements

A.B. was supported by the National Science Foundation Graduate Research Fellowship under Grant No. 1122374 and by the Center for Science of Information (CSoI), an NSF Science and Technology Center, under grant agreement CCF-0939370. S.A. was supported by the National Science Foundation under Grant No. 0844626 and by an NSF STC grant, a TIBCO Chair, a Sloan Fellowship, and an Alan T. Waterman Award.

References

[1] S. Aaronson and A. Arkhipov. The Computational Complexity of Linear Optics. *Theory of Computing*, 9(4):143–252, 2013.

[2] S. D. Bartlett and B. C. Sanders. Requirement for quantum computation. *Journal of Modern Optics*, 50:2331–2340, 2003.

[3] M. Bremner, R. Jozsa, and D. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proc. Roy. Soc. London*, A467(2126):459–472, 2010.

[4] T. Bröcker and T. tom Dieck. *Representations of Compact Lie Groups*. Springer, 2003.

[5] E. Cartan. La théorie des groupes finis et continus et l'analysis situs. *Mémorial des Sciences Mathématiques*, 42:1–61, 1930.

[6] C. Dawson and M. Nielsen. The Solovay-Kitaev Algorithm. *Quantum Information and Computation*, 6(1):81–95, 2006.

[7] W. M. Fairbairn, T. Fulton, and W. H. Klink. Finite and Disconnected Subgroups of SU3 and their Application to the Elementary-Particle Spectrum. *Journal of Mathematical Physics*, 5(8):1038, 1964.

[8] D. Gottesman. The Heisenberg representation of quantum computers. In S. P. Corney, R. Delbourgo and P. D. Jarvis, editors, *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, volume 1, pages 32–43, Cambridge, MA, 1999. International Press.

[9] A. Hanany and Y. He. Non-abelian finite gauge theories. *Journal of High Energy Physics*, 1999(02):013, 1999.

[10] A. Hanany and Y.-H. He. A monograph on the classification of the discrete subgroups of SU(4). *Journal of High Energy Physics*, 2001(02):027, 2001.

[11] S. P. Jordan. Permutational quantum computing. *Quantum Information and Computation*, 10(5):470–497, 2010.

[12] R. Jozsa and M. Nest. Classical simulation complexity of extended Clifford circuits. *arXiv:1305.6190*, 2013.

[13] E. Knill and R. Laflamme. Power of One Bit of Quantum Information. *Physical Review Letters*, 81(25):5672–5675, 1998.

[14] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[15] S. Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters*, 75(2):346–349, 1995.

[16] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[17] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58–61, 1994.

[18] Y. Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computation. *Quantum Information and Computation*, 3(1):84–92, 2003.

[19] Q. Yuan. http://qchu.wordpress.com/2011/06/26/the-representation-theory-of-su2/, 2011.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de