6.845 Final Project: Classifying Beamsplitters

Adam Bouland[*]

December 20, 2012

1 Introduction

Quantum linear optics provides a promising candidate for the realization of quantum computation. The computational power of quantum optics varies with what input states, gate sets, and measurements are present in the model. Quantum linear optics with single photon input states and adaptive measurements is universal for quantum computation [6]. Using non-adaptive measurements reduces the computational power of linear optics, but there is evidence that this model is still impossible to efficiently simulate using a classical computer [1]. If Gaussian states are used as inputs, and measurements are taken in the Gaussian basis only, then the model is efficiently classically simulable [2].

The above authors have considered what happens to the power of quantum optics when the available input states or measurements are restricted. In this work, we consider what happens when we restrict the gate set used in the computation. In the circuit model of quantum computation, there are restricted gate sets such as the Clifford group which generate classically simulable quantum circuits [4]. A priori, it seems there could be an analogous subset of linear optical elements, a “linear optical Clifford group”, that is efficiently classically simulable for a certain set of measurements.

In order to create a linear optical Clifford group, we would need to find a gate set which is not universal for linear optical state evolution. Reck et al. [7] showed that the collection of all phase shifters and all beam splitters is universal for linear quantum optics. Therefore it is natural to ask: is there *any* set of beamsplitters and phase shifters which gives rise to a nontrivial set of unitary transformations, yet still falls short of universality?

We provide evidence that there is no such set. In particular, we show that any single beam splitter which mixes modes generates a continuous group on 3 or more modes. This shows that it is not possible to create a set of nontrivial beamsplitters which generate a discrete subgroup of the unitaries; any set which mixes modes will always generate a continuous subgroup.

We further conjecture that any beam splitter which mixes modes generates $SU(m)$ or $SO(m)$ on $m \geq 3$ modes, i.e. that any beamsplitter is universal for quantum linear optics. This conjecture would strengthen our result to imply that any set of beamsplitters is either universal or obviously not universal. In separate work, we have shown this conjecture holds in the case of real beamsplitters. We believe this holds in the complex case as well, and we are actively working to prove this result.

[*] Based on joint work with Scott Aaronson

2 Formal statement of theorem

A two-mode lossless beamsplitter is a two-by-two unitary matrix. We will assume it does not apply a phase to the modes it acts upon, i.e. it has determinant 1. Suppose also that we can permute modes in our system. Permuting two modes is equivalent to applying the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ to the modes, so combining this with the beamsplitter we can assume WLOG the beamsplitter has determinant -1. Therefore any beam splitter (plus a mode swap) has the form $\left(\begin{smallmatrix} \alpha & \beta \\ \beta^* & -\alpha^* \end{smallmatrix}\right)$ where $|\alpha|^2 + |\beta|^2 = 1$. A beamsplitter is called *non-trivial* if $|\alpha| \neq 0$ and $|\beta| \neq 0$.

Consider three distinct modes 1,2 and 3 of our optical system. We can apply our beamsplitter to any two of these modes i, j. Let b_{ij} denote the matrix action of applying the beamsplitter to modes i and j. For example for the beamsplitter $\left(\begin{smallmatrix} \alpha & \beta \\ \beta^* & -\alpha^* \end{smallmatrix}\right)$ we have that

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

If a beam splitter is trivial, then on m modes the matrices b_{ij} generates a subgroup of P_m, the set of m by m unitary matrices with all entries having norm zero or one. This is an obviously non-universal model of linear optics. Our main result is that any non-trivial beam splitter densely generates a continuous subgroup of the unitary group on 3 or more modes.

Theorem 2.1. *Consider any non-trivial beam splitter. Then the set $\{b_{12}, b_{13}, b_{23}\}$ obtained by applying the above beamsplitter to 2 out of 3 total photon modes densely generates a continuous subgroup of $SU(3)$.*

We further conjecture that this set is actually universal, that is it generates $SU(m)$ or $SO(m)$ on m modes so long as $m \geq 3$. However the current proof falls short of showing this. We now proceed to a proof of our main theorem.

3 Proof of main theorem:

Throughout this section, we will say that a matrix $A \in U(n)$ approximates matrix $B \in U(n)$ within a factor of $\epsilon > 0$ if and only if $\max\limits_{u \in \mathbb{C}^n : |u|=1} |(A - B)u| \leq \epsilon$ where $|u|$ denotes the L2 norm of u.

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:

$$R_1 = b_{12}b_{13} = \begin{pmatrix} \alpha^2 & \beta^* & \alpha\beta^* \\ \alpha\beta & -\alpha^* & |\beta|^2 \\ \beta & 0 & -\alpha^* \end{pmatrix} \quad R_2 = b_{23}b_{13} = \begin{pmatrix} \alpha & 0 & \beta^* \\ |\beta|^2 & \alpha & -\alpha^*\beta^* \\ -\alpha^*\beta & \beta & \alpha^{*2} \end{pmatrix} \quad R_3 = b_{12}b_{23} = \begin{pmatrix} \alpha & \alpha\beta^* & \beta^{*2} \\ \beta & -|\alpha|^2 & -\alpha^*\beta^* \\ 0 & \beta & -\alpha^* \end{pmatrix}$$

Since $\{R_1, R_2, R_3\}$ are products of matrices of determinant -1, they are all elements of $SU(3)$. Let G be the subgroup of $SU(3)$ generated by taking finite products from the set $\{R_1, R_2, R_3\}$, and then taking the closure of this set under the operator norm. First we will show that these matrices generate an irreducible representation (denoted irrep) of G.

Claim 3.1. *The set $\{R_1, R_2, R_3\}$ densely 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. We will show that U is a constant multiple of the identity, i.e. $A = E = I$ and $D = G = H = B = C = F = 0$. This suffices to show that our representation is irreducible. Indeed, suppose our representation is reducible. Then by a change of basis, our representation can be made block diagonal. In this 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 R_1, R_2 and R_3. Written in our original basis, this matrix will not be a constant multiple of the identity. Hence if only constant multiples of the identity commute with R_1, R_2, and R_3, the representation must be irreducible. This is the converse of Schur's first lemma.

First, suppose U commutes with R_1, i.e. that

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

This imposes a series of 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, in that order.

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

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 that $I = E$.

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

Next suppose that U commutes with R_2, i.e. that

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

This imposes another series of nine equations. We have kept only the equations from the (1,1), (2,1) and (2,2) entries of the above matrices, respectively. Here we have simplified using $I = E$, $G\beta = B\beta^*$ and

$C\beta^* = D\beta$.

$$D\beta = D\beta\beta^* - G\alpha^*\beta \tag{8}$$
$$E\beta\beta^* - H\alpha^*\beta = A\beta\beta^* - C\alpha^*\beta^* \tag{9}$$
$$H\beta = D\beta\beta^* - F\alpha^*\beta^* \tag{10}$$

Note that (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 (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 $C\beta^* = D\beta$.

We now break into two cases. If $B = 0$, we have from above that $B = F = G = 0$. By (8) we also have that $D\beta = D\beta\beta^* \Rightarrow D = 0$ since $0 < |\beta| < 1$. Hence we have $C = 0$ as well by the fact that $C\beta^* = D\beta$. Therefore our matrix U is diagonal and constant, as desired.

Now it suffices to show that any other case ($B \neq 0$) cannot happen by drawing a contradiction.

In this case, we furthermore have that U commutes with R_3. Using our currently established facts, this means

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

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

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

Since we are in the case $B \neq 0$, equation (11) give that $\alpha = -\alpha^*$, i.e. α is pure imaginary.

Furthermore since $G\beta = B\beta^*$, $G \neq 0$ as well.

Using this new knowledge, we now write out equations (2) and (3)

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

Summing these equations, we see that $G = D$. Plugging this back into (13) we see that

$$\beta = 1 - \alpha$$

Since α is pure imaginary this contradicts $|\alpha|^2 + |\beta|^2 = 1$.

Hence if U commutes with all elements of G, then it is a constant matrix. Hence these matrices generate an irreducible representation of G of dimension 3. □

If G is finite, then these matrices precisely generate an irreducible representation of G. We can use this fact to rule out the possibility that G is finite using the classification of all irreducible representations of finite subgroups of $SU(3)$.

Claim 3.2. *G is not finite*

Proof. The finite subgroups of $SU(3)$ consist of the finite subgroups of $SU(2)$, six exceptional finite subgroups, and two infinite families of "dihedral-like" groups [3].

First we eliminate the possibility that G is an exceptional finite subgroup of $SU(3)$. These are labelled $\Sigma(60)$, $\Sigma(168)$, $\Sigma(360)$, $\Sigma(36)$, $\Sigma(72)$ and $\Sigma(216)$. Of these only three of them have three-dimensional irreducible representations: $\Sigma(60)$, $\Sigma(168)$ and $\Sigma(216)$. Therefore by Claim 3.1 we know G is not $\Sigma(360)$, $\Sigma(36)$, or $\Sigma(72)$.

The character tables of these groups is provided in [3]. 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 elements of a 3-dimensional irrep of $\Sigma(60)$, $\Sigma(168)$ and $\Sigma(216)$.

There are two irreps of $\Sigma(60)$ up to conjugation [3]. The characters of the elements in the representation all lie in the set $\left\{0, -1, 3, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$. Note that since $0 < |\alpha|^2 < 1$, T_3 cannot be in this set unless $T_3 = \frac{1-\sqrt{5}}{2}$, which implies $\mathrm{Im}(\alpha) = 0$. 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. The characters of this representation are 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 $2\alpha^* = \pm\frac{3}{4} \pm \frac{\sqrt{7}}{4}i$. Irregardless 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. The characters of this represenation are in the set $\{0, -1, 3\}$. Since T_3 cannot be in this set, G is not $\Sigma(216)$. We have therefore shownt that G is not an irrep of an exceptional finite subgroup of $SU(3)$.

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

$$e^{\frac{2\pi i}{n}(m_1p+m_2q)} + e^{\frac{2\pi i}{n}(m_1q-m_2(p+q))} + e^{\frac{2\pi i}{n}(-m_1(p+q)+m_2p)} \tag{17}$$

First we show that none of the traces T_i can be zero. Obviously 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 for G to be an irrep of $\Delta(3n^2)$ for some n, we would need each T_i to have the form of equation 17. However looking at the group table for this group, this conjugacy class does not generate all of $\Delta(3n^2)$ for any n. Therefore G is not $\Delta(3n^2)$ for any n.

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

$$\mathrm{Tr}(A(p,q)) = e^{\frac{2\pi i}{n}(m_1p+m_2q)} + e^{\frac{2\pi i}{n}(m_1q-m_2(p+q))} + e^{\frac{2\pi i}{n}(-m_1(p+q)+m_2p)} \tag{18}$$

$$\mathrm{Tr}(B(p,q)) = (-1)^t e^{\frac{2\pi i}{n}(m_1p+m_2q)} \tag{19}$$

$$\mathrm{Tr}(D(p,q)) = (-1)^t e^{\frac{2\pi i}{n}\left(m_1(\frac{n}{2}-p-q)+m_2p\right)} \tag{20}$$

$$\mathrm{Tr}(F(p,q)) = (-1)^t e^{\frac{2\pi i}{n}\left(m_1q+m_2(\frac{n}{2}-p-q)\right)} \tag{21}$$

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

As noted previously each T_i cannot be zero. Note that the traces of the elements in conjugacy classes B, D and F have norm 1, and are equal to $e^{i\theta}$ where θ is a rational multiple of 2π.

Next we show that at most one of the T_i's can have norm 1. This implies that at least two of the matrices R_1, R_2, R_3 must be of conjugacy class A, and at most one can be in conjugacy classes B, D, or F. But by examining the multiplication table for this group provided in [3], one can see that elements from conjugacy class A plus an element from either class B, D, or F does not generate the entire group. Therefore this will suffice to show that G is not $\Delta(6n^2)$.

Let $\alpha = a + bi$. If T_i has norm one, this imposes the following equations on a and b:

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

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

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

If $|T_1| = |T_2| = 1$, then the only solutions to this pair of equations in which $0 < |\alpha|^2 = a^2 + b^2 < 1$ is are $a = 0$ and $b = \pm\sqrt{\sqrt{5}-2}$ and $a = \pm\frac{1}{2}\sqrt{3(\sqrt{5}-2)}$ and $b = \pm\frac{1}{2}\sqrt{\sqrt{5}-2}$.

In the first case, we see that $T_2 = -(\sqrt{5}-2) \pm 2i\sqrt{\sqrt{5}-2}$. Therefore if $T_2 = e^{i\theta}$ we have $\cos(\theta) = -(\sqrt{5}-2)$. We now show that θ is an irrational multiple of π, which eliminates the possiblity that T_2 and T_3 are simultaneously traces of elements of classes B,D or E. Indeed, it can be easily shown that if θ is a rational multiple of π, then $2\cos\theta$ is an algebraic integer, and furthermore all conjugates of $2\cos(\theta)$ are of norm less than two [5]. The minimal polynomial for $2\sqrt{5}-4$ is $x^4 + 8x - 4$, which has another root of norm greater than 2. Therefore θ is not a rational multiple of π, which eliminates this possibility.

In the second case, if $T_1 = e^{i\theta}$ we see that $\cos(\theta) = -1 + \frac{\sqrt{5}}{2} \pm \sqrt{3(\sqrt{5}-2)}$. The minimal polynomial for $2\cos(\theta)$ is $x^4 + 8x^3 + 62x^2 - 56x - 191$, which has roots of norm greater than two. Hence by the same arguments as above θ is an irrational multiple of π, which eliminates this possibility.

If $|T_2| = |T_3| = 1$, then the only solution to this pair of equations in which $0 < |\alpha|^2 = a^2 + b^2 < 1$ is $a = 0$ and $b = \pm\sqrt{\sqrt{5}-2}$, or two other solutions with closed form. The first possibility was previously eliminated since it implies $T_2 = e^{i\theta}$ where θ is an irrational multiple of π. The second two solutions can be eliminated using the same techniques as above. In this case if $T_3 = e^{i\theta}$ the minimal polynomial for $2\sin(\theta) = 2\cos(\theta - \frac{\pi}{2})$ is $x^6 + 10x^4 + 41x^2 - 288$, which has roots of norm more than two.

If $|T_1| = |T_3| = 1$, then the only solution to this pair of equations in which $0 < |\alpha|^2 = a^2 + b^2 < 1$ is $a = 0$ and $b = \pm\sqrt{\sqrt{5}-2}$. In this case if $T_1 = e^{i\theta}$, then $\cos(\theta) = 2 - \sqrt{5}$. This possibility was previously eliminated in the case $|T_1| = |T_2| = 1$.

Hence at most one of these traces can have norm 1, which eliminates subgroup $\Delta(6n^2)$ as described above.

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

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

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

Therefore, by enumeration of the finite subgroups of $SU(3)$, we have shown that G is not finite. □

Corollary 3.3. *G is a continuous subgroup of $SU(3)$*

4 Conclusion

At the moment our proof requires that the beamsplitters are have phase ±1. An open question is whether or not this theorem can be extended to cover beam splitters which apply a phase, or if it can be extended to multi-mode beam splitters. A positive answer to either of these questions would provide stronger evidence against the existence of a "linear optical Clifford group".

More broadly, we hope that this research will help to address the question of whether or not it is possible to construct a complexity class intermediate between BPP and BQP by restricting gates in the circuit model. We conjecture that this is not possible: that any quantum gate set on a finite number of qubits is either BQP-complete or efficiently classically simulable in some appropriately chosen basis. A proof of this conjecture would require more sophisticated techniques than those employed in this work, since the tensor product structure of quantum circuits is more complex than the direct sum structure of linear optics. We hope that our work will serve as a stepping stone for proving this more general conjecture.

References

[1] Scott Aaronson and Alex Arkhipov. The Computational Complexity of Linear Optics. *Proceedings of ACM STOC 2011*.

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

[3] W.M. Fairbairn, T. Fulton, and W.H. Klink. Finite and Disconnected Subgroups of $SU(3)$ and their Application to the Elementary Particle Spectrum. *J. Math. Phys 5, 1038*, 1964.

[4] Daniel 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.

[5] Jörg Jahnel. When is the (Co)Sine of a Rational Angle Equal to a Rational Number? *Arxiv preprint arXiv:1006.2938v1*, pages 1–6, 2010.

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

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