Generation of Universal Quantum Linear Optics by Any Beamsplitter

Adam Bouland

Based on joint work with Scott Aaronson

Two-level Unitaries

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Two-level Unitaries

Reck et al: By composing 2-level unitaries, can create any matrix in U(m)

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' & 0 & 0 \\ c' & d' & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \ldots$$

Two-level Unitaries

What if you can't perform any two-level unitary, but only those from some finite set S?

(Assume you can apply any element in S as many times as you want, to whatever indices you want.)

Two-level Unitaries

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

(Assume you can apply any element in S as many times as you want, to whatever indices you want.)

$$\begin{pmatrix} \alpha & \beta^* & 0 \\ \beta & -\alpha^* & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -\alpha^* & 0 & \beta \\ 0 & 1 & 0 \\ \beta^* & 0 & \alpha \end{pmatrix} \cdots$$

Two-level Unitaries

- Obviously don't generate SU(m)

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & e^{i\phi} \\ e^{i\omega} & 0 \end{bmatrix}$$

- Not obvious:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \qquad \begin{bmatrix} 0.786 + 0.123i & -0.203 \\ 0.203 & 0.786 - 0.123i \end{bmatrix}$$

Our results

Q: Are there any interesting sets S which don't generate SU(m), SO(m), or merely permutations for large m?

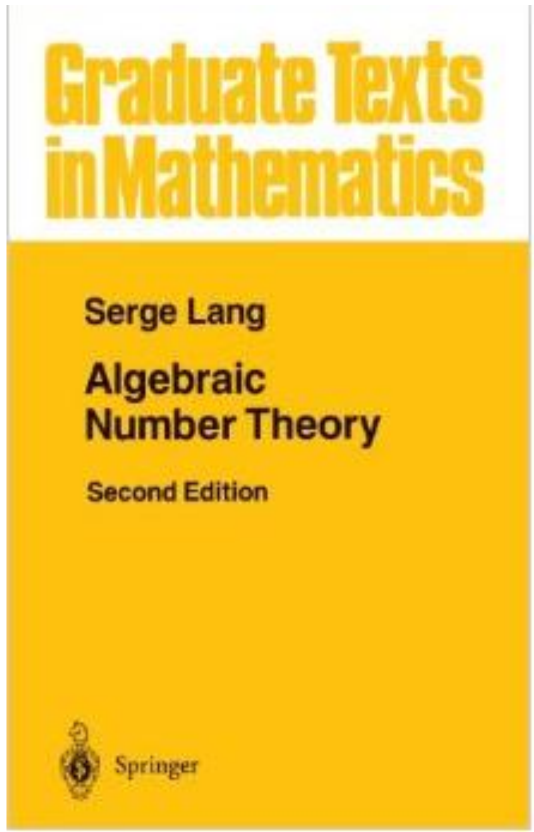
NO

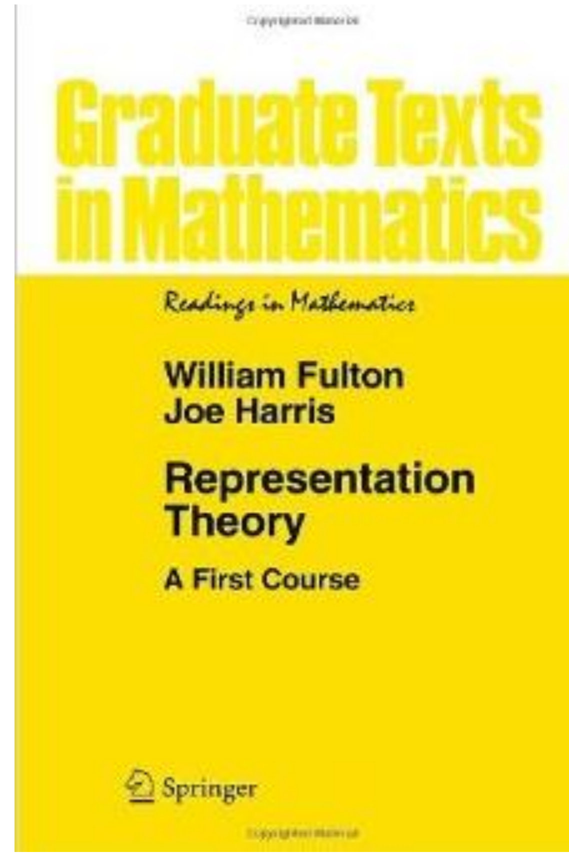
Our results

- **Thm**: [B. Aaronson ’14] Any two level-unitary of determinant -1 with all non-zero entries densely generates SU(m) or SO(m) for m>=3.
  - Real -> generates SO(m)
  - Complex -> generates SU(m)

Our results

Proof:

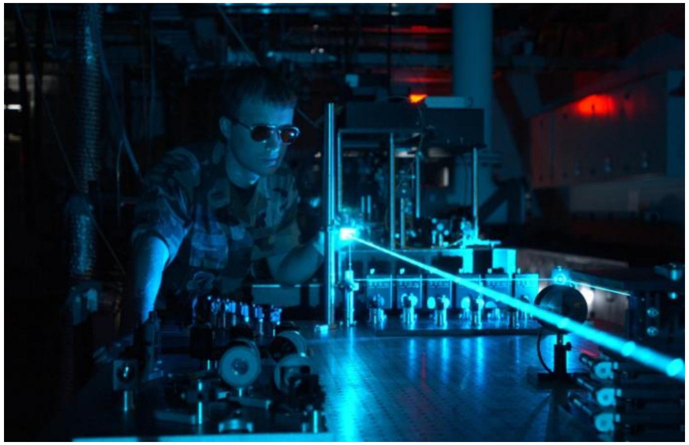




$\mathbb{R}$ $\mathbb{C}$

Quantum Optics

1 photon, m modes



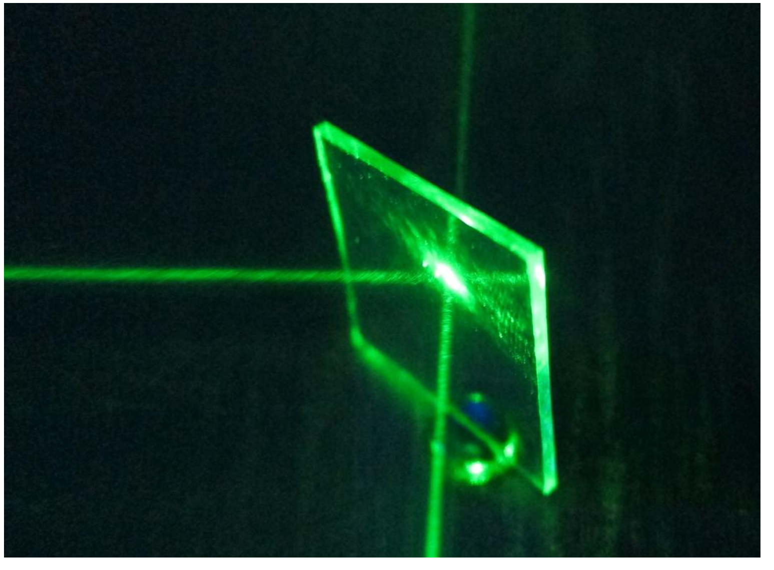
$$|100\rangle$$

$$|010\rangle$$

$$|001\rangle$$

Beamsplitter

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



Beamsplitter

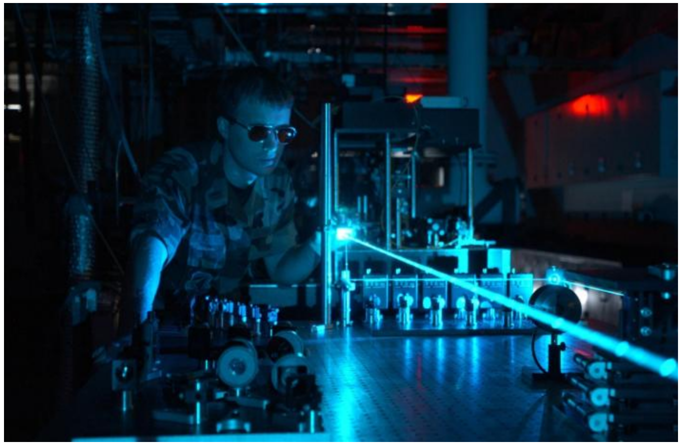
$$b = \begin{pmatrix} \alpha & \beta^* \\ \beta & -\alpha^* \end{pmatrix} \qquad b_{12} = \begin{pmatrix} \alpha & \beta^* & 0 \\ \beta & -\alpha^* & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Beamsplitter = a two-level unitary of determinant -1.

Our result: Any beamsplitter which mixes modes generates SO(m) and SU(m) on single photon with m>=3 modes

Quantum Optics

n photons, m modes



$$\binom{n+m-1}{n}$$

$$|200\rangle|011\rangle$$

$$|110\rangle|101\rangle$$

$$|020\rangle|002\rangle$$

Quantum Optics

- Unitary on larger space “lifted” by homomorphism from single photon space.

$$\phi(U) : U(m) \rightarrow U\left(\binom{n+m-1}{n}\right)$$

“The linear optical group”

Quantum Optics

Despite not being able to perform all unitaries, optics are difficult to simulate classically:

- Non-adaptive: BosonSampling

- Adaptive: BQP (KLM protocol)

Quantum Optics

- Def: A set of beamsplitters is **universal for quantum optics on m modes** if it densely generates SU(m) or SO(m) when acting on a single photon over m modes.

Solovay-Kitaev: Any set of universal optical elements is computationally equivalent.

Our results

Theorem [B. Aaronson '14]: Any beamsplitter which mixes modes is universal for quantum optics on 3 or more modes

Our results

Theorem [B. Aaronson '14]: For any beamsplitter b, quantum optics with b is either efficiently classically simulable or else universal for quantum optics

A priori: could get a model

- Nontrivially [illegible] like Clifford group
- Still capable o[illegible]ersal optics via an encoding, lik[illegible]tes
- Computationally intermediate

Our results

Theorem [B. Aaronson '14]: For any beamsplitter b, quantum optics with b is either efficiently classically simulable or else universal for quantum optics

Samp-BPP ⟷ Universal Boson Sampling/ KLM

Our results

Theorem [B. Aaronson '14]: For any beamsplitter b, quantum optics with b is either efficiently classically simulable or else universal for quantum optics

Proof Sketch

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

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

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

Proof Sketch

Let $G_M=\overline{\langle R_1,R_2,R_3\rangle}$

G_M represents $G < SU(3)$

Fact 1: G_M is a 3-dimensional irreducible representation (irrep) of G

Fact 2: G is closed

We know all irreps of closed subgroups of SU(3)

Proof Sketch

Closed Subgroups of SU(3) (1917/1963/**2013**):

- Subgroups of SU(2)
- 12 exceptional groups
- Two sets of infinite families:
- 2 disconnected Lie groups
- 4 connected Lie groups

Proof Sketch

Closed Subgroups of SU(3) (1917/1963/**2013**):

- ~~Subgroups of SU(2)~~
- ~~12 exceptional groups~~
- ~~Two sets of infinite families:~~
- ~~2 disconnected Lie groups~~
- ~~4 connected Lie groups~~

G=SU(3) or SO(3)

Proof Sketch

TABLE II. Character table for the group $\Sigma(60)$.

Permutation type	1^5	$1^2\,3$	12^2	5	5
Element type	E	(C_3, C_3^2)	C_2	(C_5, C_5^4)	(C_5^2, C_5^3)
Order of class	1	20	15	12	12
Number of commuting elements	60	3	4	5	5
Σ_1	1	1	1	1	1
Σ_3	3	0	-1	$\frac{1}{2}(1+5^{\frac{1}{2}})$	$\frac{1}{2}(1-5^{\frac{1}{2}})$
Σ'_3	3	0	-1	$\frac{1}{2}(1-5^{\frac{1}{2}})$	$\frac{1}{2}(1+5^{\frac{1}{2}})$
Σ_4	4	1	0	-1	-1
Σ_5	5	-1	1	0	0

Proof Sketch

TABLE II. Character table for the group $\Sigma(60)$.

Permutation type	1^5	$1^2\,3$	12^2	5	5
Element type	E	(C_3, C_3^2)	C_2	(C_5, C_5^4)	(C_5^2, C_5^3)
Order of class	1	20	15	12	12
Number of commuting elements	60	3	4	5	5
Σ_1	1	1	1	1	1
Σ_3	3	0	-1	$\frac{1}{2}(1+5^{\frac{1}{2}})$	$\frac{1}{2}(1-5^{\frac{1}{2}})$
Σ'_3	3	0	-1	$\frac{1}{2}(1-5^{\frac{1}{2}})$	$\frac{1}{2}(1+5^{\frac{1}{2}})$
Σ_4	4	1	0	-1	-1
Σ_5	5	-1	1	0	0

Proof Sketch

$$T_1 = \alpha^2 - 2\alpha^*$$

$$T_2 = (\alpha^*)^2 + 2\alpha$$

$$T_3 = -|\alpha|^2 + \alpha - \alpha^*$$

TABLE II. Character table for the group $\Sigma(60)$.

Permutation type	1^5	$1^2\,3$	12^2	5	5
Element type	E	(C_3, C_3^2)	C_2	(C_5, C_5^4)	(C_5^2, C_5^3)
Order of class	1	20	15	12	12
Number of commuting elements	60	3	4	5	5
Σ_1	1	1	1	1	1
Σ_3	3	0	-1	$\frac{1}{2}(1+5^{\frac{1}{2}})$	$\frac{1}{2}(1-5^{\frac{1}{2}})$
Σ'_3	3	0	-1	$\frac{1}{2}(1-5^{\frac{1}{2}})$	$\frac{1}{2}(1+5^{\frac{1}{2}})$
Σ_4	4	1	0	-1	-1
Σ_5	5	-1	1	0	0

Proof Sketch

$$T_1 = \alpha^2 - 2\alpha^*$$

$$T_2 = (\alpha^*)^2 + 2\alpha$$

$$T_3 = -|\alpha|^2 + \alpha - \alpha^*$$

TABLE II. Character table for the group $\Sigma(60)$.

Permutation type	1^5	$1^2\,3$	12^2	5	5
Element type	E	(C_3, C_3^2)	C_2	(C_5, C_5^4)	(C_5^2, C_5^3)
Order of class	1	20	15	12	12
Number of commuting elements	60	3	4	5	5
Σ_1	1	1	1	1	1
Σ_3	3	0	-1	$\frac{1}{2}(1+5^{\frac{1}{2}})$	$\frac{1}{2}(1-5^{\frac{1}{2}})$
Σ'_3	3	0	-1	$\frac{1}{2}(1-5^{\frac{1}{2}})$	$\frac{1}{2}(1+5^{\frac{1}{2}})$
Σ_4	4	1	0	-1	-1
Σ_5	5	-1	1	0	0

Proof Sketch

$$T_1 = \alpha^2 - 2\alpha^*$$

$$T_2 = (\alpha^*)^2 + 2\alpha$$

$$T_3 = -|\alpha|^2 + \alpha - \alpha^*$$

$$\alpha = \pm\sqrt{\frac{\sqrt{5}-1}{2}}.$$

Table II. Character table for the group $\Sigma(60)$.

Permutation type	1^5	$1^2\,3$	12^2	5	5
Element type	E	(C_3, C_3^2)	C_2	(C_5, C_5^4)	(C_5^2, C_5^3)
Order of class	1	20	15	12	12
Number of commuting elements	60	3	4	5	5
Σ_1	1	1	1	1	1
Σ_3	3	0	-1	$\frac{1}{2}(1+5^{\frac{1}{2}})$	$\frac{1}{2}(1-5^{\frac{1}{2}})$
Σ_3'	3	0	-1	$\frac{1}{2}(1-5^{\frac{1}{2}})$	$\frac{1}{2}(1+5^{\frac{1}{2}})$
Σ_4	4	1	0	-1	-1
Σ_5	5	-1	1	0	0

Conclusion

- **Thm**: [B. Aaronson '14] Any beamsplitter $\begin{pmatrix} \alpha & \beta^* \\ \beta & -\alpha^* \end{pmatrix}$ which mixes modes is universal on ≥3 modes.

Open questions

- Can we extend to multi-mode beamsplitters?
- Can we extend this to two-level unitaries with other determinants?
- Can we account for realistic errors?
- Is there a qubit version of this theorem?

Questions

?