Generation of Universal Linear Optics by Any Beamsplitter

Technical version: arXiv:1310.6718

Adam Bouland* Scott Aaronson†

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 [15], the commuting Hamiltonians model of Bremner, Jozsa, and Shepherd [3], and the boson sampling 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 [17], and so are most "natural" gate sets. For example, Controlled-NOT together with any real one-qubit gate that does not square to the identity is universal [21]. 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.

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 two modes and correspond to a 2×2 unitary matrix with determinant -1;[2] and *phaseshifters*, which act on one mode and simply apply a phase $e^{i\theta}$. Note that any unitary transformation acting on the one-photon Hilbert space automatically gets "lifted," by homomorphism, to a unitary transformation acting on the Hilbert space of n photons. Furthermore, every element of the *n-photon linear-optical group*—that is, every n-photon unitary transformation achievable using linear optics—arises in this way (see [1], Sec. III for details). Of course, if $n \geq 2$, then there are also n-photon unitaries that cannot be achieved linear-optically: that is, the n-photon linear-optical group is a proper subgroup of the full unitary group on the n-photon Hilbert space.

*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 [14], permutation gates [13], and even diagonal gates [3] can be hard to simulate in arbitrary bases.

[2] Some references use a different convention and assume that beamsplitters have determinant $+1$ [19]. 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.

We call a set of optical gates S *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). To clarify, if S is universal, this does *not* mean that linear optics with S is universal for quantum computing! It only means that S densely generates the one-photon linear-optical group—or equivalently, the n-photon linear-optical group for any value of n. The latter kind of universality is certainly *relevant* for quantum computation: first, it already suffices for the boson sampling proposal of Aaronson and Arkhipov [1]; and second, if the single resource of adaptive measurements is added, then universal linear optics becomes enough for universal quantum computation, by the famous result of Knill, Laflamme, and Milburn (KLM) [16]. On the other hand, if we wanted to map a k-qubit Hilbert space *directly* onto an m-mode linear-optical Hilbert space, then as observed by Cerf, Adami and Kwiat [5], we would need $m \geq 2^k$ just for dimension-counting reasons.

Previously, Reck *et al.* [20] showed that the set of *all* phaseshifters and all beamsplitters is universal for linear optics, on any number of modes. Therefore it is natural to ask: is there *any* S set of beamsplitters and phaseshifters that generates a nontrivial set of linear-optical transformations, yet that still falls short of generating *all* of them? Here by "nontrivial," we simply mean that S does *something* more than permuting the modes around or adding phases to them.

If such a set S existed, we could then ask the *further* question of whether the n-photon subgroup generated by S was

(a) efficiently simulable using a classical computer, despite being nontrivial (much like the Clifford group for qubits),

(b) already sufficient for applications such as boson sampling and KLM, despite not being the full n-photon linear-optical group, or

(c) of "intermediate" status, neither sufficient for boson sampling and KLM nor efficiently simulable classically.

The implications for our dichotomy conjecture would of course depend on the answer to that further question.

In this paper, however, we show that the further question never even arises, since *no such set S exists*. Indeed, any beamsplitter that acts nontrivially on two modes is universal on three or more modes. More formally, we show

Theorem 1. *Let b be any nontrivial beamsplitter. Then when acting on pairs of photons on three modes, b densely generates either all $SO(3)$ matrices (if all entries of b are real) or all $SU(3)$ matrices (if any entry of b is non-real).*

Together with the Solovay-Kitaev theorem [6], this implies we can use any nontrivial beamsplitter b to efficiently simulate any other beamsplitter b'. So by Reck *et al.* [20] we have the following corollary:

Corollary 2. *Any nontrivial beamsplitter is universal on $m \geq 3$ modes.*

What makes this result surprising is that universality holds *even if the beamsplitter angles are all rational multiples of π*. A priori, one might guess that by restricting the beamsplitter angles to (say) $\pi/4$, one could produce a linear-optical analogue of the Clifford group; but our result shows that one cannot.

Our proof uses makes heavy use of representation theory. More specifically, suppose we have a beamsplitter b which acts nontrivially on two modes. We consider the set of three-by-three matrices M densely generated by applying b to pairs of modes in a 3-mode system. We first show using standard representation theory that the matrices M form an irreducible representation of a subgroup of $SU(3)$. We then use the classification of finite subgroups of $SU(3)$ and their representations [7, 11, 9] to show that the set M cannot represent any finite group. Interestingly the classification of $SU(3)$ subgroups from 1964 [7] contains errors [18], and proving that S is infinite requires use of the corrected classification which was only completed in 2014 [9, 10]. Once we establish that S is infinite, we use the representation theory of Lie subgroups of $SU(3)$ to complete the proof of universality [4]. We refer the interested reader to our full version (arXiv:1310.6718) for details.

From an experimental perspective, our result shows that any complex nontrivial beamsplitter suffices to create any desired optical network. From a computational complexity perspective, it 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 (even on n-photon input states), or else universal for quantum linear optics. In particular, any nontrivial beamsplitter can be used to perform boson sampling; there is no way to define an "intermediate" model of boson sampling[3] by restricting the allowed beamsplitters and phaseshifters.

Note that our result holds only for beamsplitters, i.e., optical gates that act on two modes and have determinant -1. We leave as an open problem whether our result can be extended to arbitrary two-mode gates, or to gates that act on $k \geq 3$ modes. 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 exceptional finite subgroups of $SU(4)$ are known [12]. 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.

Our work is the first that we know of to explore limiting the power of quantum linear optics by limiting the gate set. Previous work has considered varying the available input states and measurements. For example, as mentioned earlier, Knill, Laflamme, and Milburn [16] showed that linear optics with 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 simulable classically [2]; but with Gaussian-state inputs and *photon-number* measurements, there is recent evidence for computational hardness.[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.

Acknowledgements

We thank Bela Bauer for pointing out Ref. [18] and Patrick Otto Ludl for helpful correspondence. 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, by a TIBCO Chair, and by 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] Here by "intermediate," we mean computationally intermediate between classical computation and universal boson sampling.

[4] See http://www.scottaaronson.com/blog/?p=1579

[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] N. J. Cerf, C. Adami, and P. G. Kwiat. Optical simulation of quantum logic. *Phys. Rev. A*, 57:R1477–R1480, 1998.

[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 SU(3) 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] W. Grimus and P. O. Ludl. Finite flavour groups of fermions. *J. Phys. A: Math. Theor.* 45:233001, 2012.

[10] W. Grimus and P. O. Ludl. On the characterization of the SU(3)-subgroups of type C and D. *J. Phys. A: Math. Theor.* 45:233001, 2012.

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

[12] 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.

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

[14] R. Jozsa and M. Nest. Classical simulation complexity of extended Clifford circuits. *Quantum Information and Computation*, 14(7):633-648, 2014.

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

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

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

[18] P. O. Ludl. Comments on the classification of the finite subgroups of SU(3). *J. Phys. A: Math. Theor.* 44:255204, 2011.

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

[20] 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.

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