Boson Sampling from a Gaussian State

A. P. Lund,[1] A. Laing,[2] S. Rahimi-Keshari,[1] T. Rudolph,[3] J. L. O'Brien,[2] and T. C. Ralph[1]
[1]Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia
[2]Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom
[3]Optics Section, Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom
(Received 26 November 2013; revised manuscript received 21 March 2014; published 5 September 2014)

We pose a randomized boson-sampling problem. Strong evidence exists that such a problem becomes intractable on a classical computer as a function of the number of bosons. We describe a quantum optical processor that can solve this problem efficiently based on a Gaussian input state, a linear optical network, and nonadaptive photon counting measurements. All the elements required to build such a processor currently exist. The demonstration of such a device would provide empirical evidence that quantum computers can, indeed, outperform classical computers and could lead to applications.

DOI: 10.1103/PhysRevLett.113.100502 PACS numbers: 03.67.Lx, 03.67.Ac, 42.50.-p

Introduction.—Quantum computers are expected to be able to outperform their classical counterparts for a number of different calculations [1]. However, there is a large disparity between the number of quantum bits (qubits) that can currently be coherently controlled (≈ 10) and the number required for a calculation such as prime factoring on a scale that would challenge classical computers ($\approx 10^6$). As a result there is considerable interest in nonuniversal quantum computers that can solve specific problems that are intractable to classical computation but require significantly less overhead. Such devices could experimentally demonstrate the power of quantum computing over classical computers and might lead to technologically significant applications.

An example of a computational problem that can be solved efficiently by a particularly simple quantum processor, but which is, nonetheless, believed to be hard for classical computation, is boson sampling [2]. Consider a passive, linear unitary transformation that takes n individual bosons and scatters them into $m \gg n$ output modes. Given a particular arrangement of bosons at the input, $\mathbf{S}$, and a particular unitary U which describes how the field amplitudes evolve through the scattering process, the problem is to produce a fair sample of the output probability distribution, $P(\mathbf{R}|\mathbf{S}, U)$, where $\mathbf{R}$ is the arrangement of bosons at the output. Aaronson and Arkipov (AA) [2] prove that, if a classical algorithm existed to efficiently sample this distribution for a randomly chosen U, then modulo a number of technical points and conjectures, a collapse would occur within the polynomial hierarchy of complexity classes [3]. This conflicts with the widespread belief that such collapses do not occur and, hence, provides strong evidence that an efficient classical algorithm does not exist.

The boson-sampling problem maps directly onto that of sampling the output photon counting distribution when single photon states are injected into a large linear-optical network. If such a device was constructed, then the observed output would be samples of the required probability distribution—it would effectively be a quantum processor that could efficiently solve the boson-sampling problem. We refer to such a device as a boson sampler. This observation has led to a number of proof of principle experiments where three to four photons have been injected into five to six mode optical networks [4–7]. While the potential for scaling up the network size for such experiments is optimistic [8], the potential for scaling to much larger input photon numbers is more pessimistic, at least in the short term. This is because current single photon sources are spontaneous, so the probability for producing an n photon input state drops exponentially with n. While deterministic single photon sources are in development, they are only likely to provide a solution to this problem in the medium to long term. In contrast, deterministic sources of squeezed states, nonclassical Gaussian states of high purity, are currently available [9].

It is known that squeezed states in combination with linear optics, highly elaborate feed-forward adaption, and single photon counting can, in principle, lead to universal quantum computation [10]. On the other hand, it is also known that the output statistics from squeezed states (or, indeed, any Gaussian states) evolved through linear optics and measured via quadrature measurements are classically simulatable [11]. This leaves open the intriguing possibility that a Gaussian state evolved through nonadaptive linear optics and measured via photon counting may not be efficiently classically simulatable.

In this Letter, we show that a nonadaptive linear optical network which takes a particular Gaussian state as its input, and takes photon number counting statistics as its output, can efficiently sample distributions that are believed to be

computationally hard to sample with a classical computer. We will refer to such a device as a Gaussian boson sampler. Specifically, we show that a randomized boson-sampling problem, in which the task is to sample from the output of a boson sampler whose input is randomly chosen, shot by shot, from all possible n photon inputs, can be efficiently solved by this particular type of Gaussian boson sampler. If a classical computer could efficiently sample from the same distribution as a Gaussian boson sampler, then it would, as a subset of its samples, produce samples from the standard boson sampler. As the latter is believed to be impossible, we will show it follows that the randomized exact boson sampling problem is also hard for a classical computer. A more subtle and physically relevant question is whether approximate boson sampling remains hard in the randomized case. We present strong evidence that this is, indeed, the case.

Boson sampling.—A quantum optical processor which can solve the boson-sampling problem consists of n single photon states which are injected into n of the modes of a m-mode linear-optical network. Following AA, we consider the case where $m = n^2$ (see note [12]). The initial state is

$$|\mathbf{S}\rangle = \prod_{h=1}^{n^2} (\hat{a}_h^\dagger)^{s_h} |0\rangle, \tag{1}$$

where $\mathbf{S} = (s_1, \ldots, s_m)$ is a particular tuple of n^2 numbers, n of which take the value 1 and the other $n^2 - n$ take the value zero, $\hat{a}_h^\dagger$ is the photon creation operator for the hth mode and $|0\rangle$ is the global vacuum state of all n^2 modes. After the unitary, we have $\hat{\mathcal{U}}|\mathbf{S}\rangle$ where $\hat{\mathcal{U}}$ is the unitary transformation in the Fock basis generating the unitary describing the scattering process U, $\hat{\mathcal{U}}\hat{a}_h^\dagger\hat{\mathcal{U}}^\dagger = \sum_{k=1}^m U_{hk}\hat{a}_k^\dagger$. AA show strong evidence that a classical sampling algorithm C which takes as inputs U and $\mathbf{S}$ and outputs samples from the output number distribution $P(\mathbf{R}|\mathbf{S}, U) = |\langle\mathbf{R}|\hat{\mathcal{U}}|\mathbf{S}\rangle|^2$, $\mathbf{R} = (r_1, \ldots, r_m)$, cannot be done efficiently. The probability of each particular configuration in the output is proportional to the norm squared of the permanent of a submatrix within U [13]. Further, AA showed that even computing samples from a distribution close to the exact case (where the precision is an additional input parameter) is likely to be hard for a classical computer. Using results about the computational complexity of estimating matrix permanents shows that, if one assumes the sampling can be done efficiently with only classical resources, then the polynomial hierarchy collapses. The polynomial hierarchy is a hierarchy of computational complexity classes with levels corresponding to problems with greater computational power. A collapse within the hierarchy means that problems at a particular level and above actually have the same complexity (see [14] for more discussion). Physically, a boson sampler could be built provided one can accurately prepare the linear interactions to arbitrary precision. Such a device would efficiently produce samples from the distribution. The results of AA suggest that such a device has powers which are outside the classical polynomial hierarchy.

Two-mode Squeezing.—Spontaneous parametric down-conversion involves coherently down-converting photons from a strong pump beam into two modes. The output state of these two modes is a two-mode squeezed vacuum of the form

$$\sqrt{1-\chi^2}\sum_{p=0}^{\infty}\chi^p|p\rangle_1|p\rangle_2, \tag{2}$$

where $|p\rangle_i = \hat{a}_i^{\dagger p}/\sqrt{p!}|0\rangle$ is a p photon number state of the ith mode and $0 \le \chi < 1$ is a parameter determining the strength of the squeezing. This state is a Gaussian state and is regularly produced, to a good approximation, in many labs around the world.

Given a linear optical unitary on n^2 modes, it is possible to construct an instance of the n photon boson-sampling problem using two-mode squeezed vacuum states, $2n^2$ optical modes and photon counting. The configuration is shown schematically in Fig. 1. For each input mode in the given unitary, one half of a two mode squeezed state is input into it. This, therefore, requires n^2 two mode squeezing operations. The other half of each state is sent directly to a photon counter. The total state prior to detection is

$$|\phi\rangle_{1,2} = (1-\chi^2)^{\frac{n^2}{2}}\hat{\mathcal{U}}^{(2)}\prod_{h=1}^{n^2}\left(\sum_{p=0}^{\infty}\chi^p|p\rangle_{h1}|p\rangle_{h2}\right), \tag{3}$$

where the state subscript $h1$ ($h2$) refers to the set of modes that do not (do) pass through the unitary $\hat{\mathcal{U}}^{(2)}$; we have

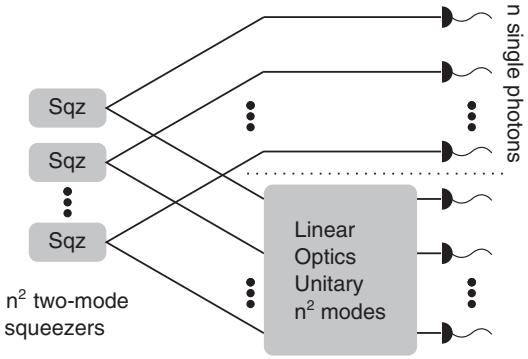

FIG. 1. Schematic of the boson-sampling device with squeezed state inputs and postselection. If only a particular detection arrangement of n photons of the upper mode are retained then this device can sample the probability distribution $P(\mathbf{R}|\mathbf{S}, U)$, but not efficiently. However, if *all* n photon arrangements are retained then the probability distribution $P(\mathbf{R}, \mathbf{S}|U)$ can be sampled efficiently.

written the unitary in this form to emphasize that it only acts on the second set of modes. Consider cases when the particular arrangement of n single photons (and zero photons in all other modes) described by the tuple $\mathbf{S} = (s_1, \ldots, s_m)$ is counted in the set of modes $h1$. The reduced state for measuring $|\mathbf{S}\rangle_1$ is then $\hat{\mathcal{U}}^{(2)}|\mathbf{S}\rangle_2$, which is equivalent to an instance of the boson-sampling problem. However, as the probability of detecting the particular arrangement $\mathbf{S}$ is

$$P_1(\mathbf{S}) = \chi^{2n}(1-\chi^2)^{n^2}, \tag{4}$$

this adds an exponential overhead to the boson-sampling algorithm.

For the case of exact sampling, this does not change the arguments of AA. The exact sampling theorem uses Stockmeyer's approximate counting algorithm [15] to estimate within a multiplicative factor the probability of detecting a particular configuration of bosons at the output. Specifically, if an efficient classical algorithm for boson sampling exists, then Stockmeyer's algorithm implies the unlikely result that estimating this probability is a problem in the third level of the polynomial hierarchy. Stockmeyer's algorithm allows for prefactors to the probability of order $2^{-\mathrm{poly}(n)}$ without changing the level of the polynomial hierarchy that this algorithm is contained in (see [14] for more details). Hence, if the probability of an outcome $\mathbf{R}_0$ from a boson sampler was $P(\mathbf{R}_0|\mathbf{S}, U)$, then the probability of the same outcome from our Gaussian boson sampler is $P_1(\mathbf{S})P(\mathbf{R}_0|\mathbf{S}, U)$, thus, the prefactor is of the form permitted and the hardness argument for exact sampling still holds [16].

Approximate boson sampling.—We now allow C to sample from a probability distribution, $\mathbf{Q_R}$ which is constrained in variation distance to the exact probability distribution, $\mathbf{P_R}$ as

$$\sum_{\mathbf{R}\in\mathcal{R}} |\mathbf{P_R} - \mathbf{Q_R}| \leq \beta, \tag{5}$$

where β is an input parameter to the approximate sampling algorithm and $\mathcal{R}$ represents the set of all configurations of Fock state detections.

Approximate sampling does not necessarily allow for exponentially small scaling of the probabilities without changing its complexity properties, and so, a more detailed analysis is required to show this. The reason is because C could adversarially choose to corrupt the probability of the configuration in which we are interested (i.e., the matrix permanent of a particular submatrix from the unitary matrix) yet still be a good sampler over the rest of the distribution and satisfy the approximate sampling requirement of Eq. (5). This is possible because the single probability that is of interest could be exponentially small compared with the sum of all other probabilities.

The key concept presented in AA is that, if the submatrix of which we wish to estimate the permanent is randomly embedded in a large random unitary matrix, then C cannot know *a priori* which particular configuration, $\mathbf{R}'$, is of interest. Therefore, provided Eq. (5) holds and C correctly approximates most of the $\mathbf{P_R}$, including the randomly chosen $\mathbf{P_{R'}}$, with a high probability, then being able to efficiently compute the approximate boson-sampling problem enables Gaussian permanent estimation (i.e., the estimation of the permanent of a complex matrix with entries whose real and imaginary parts are Gaussian random variables) with an algorithm within the polynomial hierarchy, and hence, the polynomial hierarchy collapses. This requires two conjectures to be true and AA provide evidence for these conjectures. They are the Permanent of Gaussians Conjecture which says that it is #P hard to approximate the permanent of a Gaussian random matrix and the Permanent Anticoncentration Conjecture, which says that the permanents of Gaussian random matrices are not concentrated around zero. Given that these two conjectures are true, the hardness argument for exact sampling carries over to approximate sampling. However, using the two mode squeezing sources results in an exponentially small probability of injecting photons into only the first n modes. This means the physical device, the Gaussian boson sampler, does not produce samples equivalent to the original boson-sampling problem efficiently. We propose two solutions to this problem in the following.

Adding adaption.—If we consider the case where n single photons are found in the n^2 conditioning detectors and zero everywhere else, irrespective of the exact location of those counts, then the overall probability is increased due to the number of ways these counts could be achieved to

$$\binom{n^2}{n}\chi^{2n}(1-\chi^2)^{n^2}. \tag{6}$$

As shown in the Supplemental Material [14], this probability has a maximum when

$$\chi_{\max} = \frac{1}{\sqrt{n+1}}, \tag{7}$$

and, using the Stirling approximation, it is possible to show that the asymptotic behavior of the probability is

$$P(n|\chi_{\max}) \sim \frac{1}{e\sqrt{2\pi}}\frac{1}{\sqrt{n}}. \tag{8}$$

The location of the n single photon detections is correlated with the location of preparing a single photon state. Hence, if the input modes to the unitary can be adapted via feed forward so that the n modes containing the single photons are switched such that they are described by the tuple $\mathbf{S}$, then the boson-sampling algorithm can be efficiently

performed with only an $O(\sqrt{n})$ overhead in running time. This is similar to, but less complex than, building Migdall *et al*. type photon sources [17]. This is now an efficient method for solving the boson-sampling problem, but this has come at the price of requiring a technically challenging adaption strategy, though clearly much less challenging than full universal quantum computation [10].

Randomized boson sampling.—We now present our main result. We consider the case in which there is no adaption, but we still retain all events where n single photons are found in the n^2 conditioning detectors and zero everywhere else. We show that, if there is a classical algorithm within the polynomial hierarchy for approximate sampling from this nonadaptive configuration, then the Gaussian permanent estimation problem lies within the polynomial hierarchy. As discussed previously, this implies a collapse of the polynomial hierarchy and so represents strong evidence that no such algorithm exists.

Consider the case of measuring n single photons in the heralding modes as mentioned above in the adaptive case. The probability of this event scales as $1/\sqrt{n}$ [see Eq. (8)] and the exact location of the photons is i.i.d. In the output modes is a photon number distribution of n photons which, conditional on a particular result, is an instance of the boson-sampling problem. Therefore, this configuration randomly samples from $\binom{n^2}{n}$ instances of the boson-sampling problem, where both the input and output are known. We have already shown that the hardness argument for approximate sampling still holds for particular detection configurations at the heralding detectors. The problem, then, is to show that the extra level of randomness introduced by sampling over many input configurations does not change the complexity of the sampling problem.

As discussed previously, the proof of the hardness of approximate sampling requires that the submatrix of interest is randomly embedded in a large random unitary matrix in such a way that that there is no way for an adversary to know *a priori* which configuration is of interest. To achieve this, the random unitary matrix should be picked according to the Haar measure. Specifically, it can be proved that, for boson sampling, there exists an algorithm within the polynomial hierarchy which outputs $m \times n$ Haar random unitary matrices that have the $n \times n$ matrix X, whose matrix permanent is to be estimated, as a submatrix located in a uniformly random location [2]. As the number of columns in the output is equal to the columns in the input, the random location here is only determined by which rows make up the submatrix corresponding to the different possible output configurations. For randomized boson sampling, the random unitary matrix can be generated in a similar way but is square, and both the rows and columns of the unitary which encode the matrix permanent of the original problem are randomly chosen and uniformly distributed corresponding to the different possible output and input configurations. This, then, ensures that there is no set of events within the subset of output events that could be used to corrupt the probability in which we are interested while maintaining the conditions for approximate sampling. The random matrix will still be a Haar random unitary, as needed, because the buildup of the rectangular matrix to a square matrix occurs through the addition of extra random columns that are orthogonal to the columns that encode the problem. The use of Stockmeyer's approximate counting algorithm [15] to estimate the probabilities for the output configurations would also proceed as before. The probability that is to be estimated would be multiplied by the exponential prefactor from Eq. (4). However, the prefactor is bounded below by 2^{-n^2} which, as explained before, is permitted for Stockmeyer's approximate counting algorithm. These arguments show that estimating the permanent of Gaussianly distributed random matrices is a problem within the polynomial hierarchy if an efficient classical algorithm exists for the randomized boson-sampling problem, and hence, the polynomial hierarchy collapses. This completes our proof. Recall that the subset of interest (i.e., those events where n photons are detected on both sides of all down-converters) is postselected with a probability that depends only polynomially on the number of photons, provided we choose χ as per Eq. (7). Thus, the Gaussian boson sampler efficiently samples the distribution. See the Supplemental Material [14] for additional discussion.

Experimental considerations.—Challenges in building a Gaussian boson sampler as described above would be: (i) constructing a large number (n^2) of identical two mode squeezers (note again [12]), (ii) injecting them into a large, highly connected, highly coherent, and low loss optical network, and (iii) counting photons with high efficiency. All of these requirements will test current technology. One solution is to construct a large scale integrated optics circuit, ideally with the squeezed sources and photon counters built in to minimize loss [18]. Alternatively, time multiplexed squeezed sources might offer a compact solution (see for example [19]).

A major consideration for experiments will be errors, in particular loss. It is not known if active error correction is possible for boson samplers. Passive error correction against loss is possible for the boson sampler by simply postselecting for the desired photon number n [20]. A similar strategy will work for the Gaussian boson sampler provided the losses on the directly detected modes are much smaller than those undergoing the unitary transformation. Error correction via postselection does not scale efficiently with the problem, going as η^n, where η is the average efficiency of each optical path. The question is, then, whether it is possible to reach problems of an interesting size before the efficiency requirements become too severe. We estimate that, for $n = 20$ and average path transmissions of $\eta_1 = 0.99$ and $\eta_2 = 0.9$, the postselection efficiency would be $\approx 8\%$. Combined with the optimal

probability of success from Eq. (7), we conclude that ≈ 0.0025 of experimental runs would produce a sample point. Given MHz repetition rates, this would still lead to thousands of samples per second.

Conclusion.—We have shown that a Gaussian boson sampler comprised of two mode squeezed state inputs, a nonadaptive linear optical network, and photon counting can solve a randomized boson-sampling problem efficiently, specifically with an $O(\sqrt{n})$ overhead in run time compared to solving the same problem with single photon sources. We have presented strong evidence that the randomized boson-sampling problem is computationally hard for a classical computer. We believe this device may represent the best short term possibility for experimentally demonstrating a quantum processor that can perform calculations that would challenge the abilities of the best classical processors.

We acknowledge correspondence with Scott Aaronson. This research was conducted in part by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE110001027). A. L., T. R., and J. L. O. B acknowledge support from the Army Research Office (ARO) Grant No. W911NF-14-1-0133. A. L. and J. L. O. B acknowledge support from the Engineering and Physical Sciences Research Council (EPSRC), the European Research Council (ERC), the Centre for Nanoscience and Quantum Information (NSQI), the U.S. Air Force Office of Scientific Research (AFOSR) and the U.S. Army Research Laboratory (ARL). J. L. O. B. acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies.

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).
[3] L. J. Stockmeyer, Theor. Comput. Sci. **3**, 1 (1976).
[4] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Science **339**, 794 (2013).
[5] J. B. Spring *et al.*, Science **339**, 798 (2013).
[6] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Nat. Photonics **7**, 540 (2013).
[7] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Nat. Photonics **7**, 545 (2013).
[8] A. Peruzzo *et al.*, Science **329**, 1500 (2010).
[9] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics* 2nd Ed. (Wiley-VCH, Weinheim, 2004).
[10] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[11] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).
[12] Strictly speaking, AA only prove that the $n \times n$ matrix which encodes the Gaussian permanent estimation problem can be embedded into a random $n \times m$ unitary, if $m > n^6$. AA state that they believe that the complexity arguments will still hold when $m = n^2$, which we follow here. The arguments concerning the complexity of the randomized boson-sampling problem follow equally well if the n^6 scaling is insisted upon.
[13] L. G. Valiant, Theor. Comput. Sci. **8**, 189 (1979).
[14] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.100502, which includes Ref. [3].
[15] L. J. Stockmeyer, in *Conference Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing, Boston, Mass., 1983* (Association for Computing Machinery, New York, 1983) pp. 118–126.
[16] AA indicate they are aware of this exact sampling result for squeezed states but do not discuss it further.
[17] A. L. Migdall, D. Branning, and S. Casteletto, Phys. Rev. A **66**, 053805 (2002).
[18] J. Silverstone *et al.*, Nat. Photonics **8**, 104 (2013).
[19] N. C. Menicucci, X. Ma, and T. C. Ralph, Phys. Rev. Lett. **104**, 250503 (2010).
[20] P. P. Rohde and T. C. Ralph, Phys. Rev. A **85**, 022332 (2012).