Evidence for the conjecture that sampling generalized cat states with linear optics is hard

Peter P. Rohde,[1,*] Keith R. Motes,[1] Paul A. Knott,[2,3] Joseph Fitzsimons,[4,5] William J. Munro,[3] and Jonathan P. Dowling[6]

[1]*Australian Research Council Centre of Excellence for Engineered Quantum Systems, Macquarie University, Sydney NSW 2113, Australia*

[2]*School of Physics and Astronomy, University of Leeds, Leeds LS2 9JT, United Kingdom*

[3]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[4]*Singapore University of Technology and Design, 20 Dover Drive, Singapore*

[5]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore*

[6]*Hearne Institute for Theoretical Physics and Department of Physics & Astronomy, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

(Received 2 October 2013; revised manuscript received 13 December 2014; published 30 January 2015)

Boson sampling has been presented as a simplified model for linear optical quantum computing. In the boson-sampling model, Fock states are passed through a linear optics network and sampled via number-resolved photodetection. It has been shown that this sampling problem likely cannot be efficiently classically simulated. This raises the question as to whether there are other quantum states of light for which the equivalent sampling problem is also computationally hard. We present evidence, without using a full complexity proof, that a very broad class of quantum states of light—arbitrary superpositions of two or more coherent states—when evolved via passive linear optics and sampled with number-resolved photodetection, likely implements a classically hard sampling problem.

DOI: 10.1103/PhysRevA.91.012342 PACS number(s): 03.67.Ac, 03.67.Lx, 42.50.−p, 89.70.Eg

I. INTRODUCTION

Linear optical quantum computing (LOQC) [1,2] has become a leading candidate for the implementation of large-scale universal quantum computation [3]. While LOQC is possible in principle, the technological requirements are daunting, requiring technologies that are not readily available today, such as fast feed-forward and optical quantum memory. Thus, the search for simplified, more technologically realistic models for LOQC is a priority.

One recent proposal, by Aaronson and Arkhipov (AA) [4], known as boson sampling, significantly simplifies the requirements for LOQC, allowing a type of nonuniversal quantum device that implements a classically hard algorithm using technologies that are, for the mostpart, available today. In the boson-sampling model, we simply input n copies of the single-photon Fock state into a passive linear optics network, comprised of beam splitters and phase shifters, and perform photodetection at the output. This yields a sampling problem, which is believed to be classically hard to simulate [4]. Thus, the full model requires only single-photon Fock state preparation, passive linear optics, and photodetection, technologies that are all available today on a small scale. For a review on various photon sources and photodetectors see Ref. [5]. Note that number-resolving photodetectors are not required in the limit of large n as there is likely only zero or one photon per output mode [6]. Several elementary experimental demonstrations have recently been performed [7–11].

In boson sampling, the classical hardness of the sampling problem relates to the computational complexity of calculating the amplitudes in the output superposition. In the case of Fock state inputs, the output amplitudes are related to matrix permanents, the computation of which are known to be complete for the complexity class #P and hence are not believed to be efficiently computable by classical means.

The classical hardness of this Fock-state sampling raises the question as to whether there are other quantum states of light, which also yield classically hard sampling problems. It was shown recently by Seshadreesan *et al.* [12] that photon-added coherent states (PACSs) and by Olson *et al.* [13] that photon-added or photon-subtracted squeezed vacuum (PASSV) states are an example of such states. Additionally, it was shown by Lund *et al.* [14] that a certain class of Gaussian state inputs yields a computationally hard sampling problem. It is known that passive linear optics may be efficiently simulated with Gaussian inputs and nonadaptive Gaussian measurements [15,16]. However, the more general question as to which quantum states of light may be efficiently simulated with number-resolved measurements is an open question.

Given the result of AA for single photons, the natural question is whether this generalizes to other quantum states. Here we consider a more generalized boson-sampling device where the input states are not Fock states, but rather superpositions of coherent states. This is a very broad class of continuous-variable optical states.

We will structure this paper as follows. We first give a review of AA's boson-sampling formalism in terms of Fock and vacuum states and show the typical expression obtained at the output. Then, we analyze cat sampling in three separate limits:

(i) First we analyze even and odd cat states and show that their Taylor expansions reduce to the vacuum and single-photon Fock state respectively as $\alpha \to 0$. Thus, in the zero amplitude limit, cat sampling exactly reduces to boson sampling and therefore yields a computationally hard problem.

(ii) Second, we analyze small, but nonzero, amplitude odd cat states. This is equivalent to Fock-state sampling with some residual components that are treated as an error. This error is related to the AA proof for approximate boson sampling,

*dr.rohde@gmail.com; http://www.peterrohde.org

where it is required that the error rate satisfies a $1/\mathrm{poly}(n)$ bound. Thus small, but nonzero, amplitude odd cat states are also computationally hard.

(iii) Third, we analyze general cat states, which are arbitrary superpositions of two or more coherent states. We demonstrate that the output state is a highly entangled superposition of an exponential number of multimode coherent states [17–21], where the amplitude of each term is related to a permanentlike combinatoric problem, which would require exponential resources to compute via a brute-force approach. This provides strong evidence that such generalized optical sampling problems might in general be implementing classically hard problems. Determining a complete characterization of the computational complexity of such problems is a notoriously difficult open problem, but based on the evidence we present here, it likely resides in a classically hard class comparable to ideal boson sampling.

Next, to further support our evidence we present a complexity theoretic argument for the hardness of cat-state sampling. We show that unless the polynomial hierarchy collapses to the third level there must not exist an efficient randomized classical algorithm, which can produce an output distribution approximating that of an arbitrary interferometer with multiplicative error of $\sqrt{2}$ or less.

While such states may be more challenging to prepare than Fock states, addressing this question sheds light on what makes a quantum optical system classically hard to simulate, and may provide motivation for developing technologies for preparing quantum states of light beyond Fock states. We end this paper by discussing the prospects for experimentally preparing general cat states.

II. REVIEW OF BOSON SAMPLING

We begin by reviewing the boson-sampling model using single photons as illustrated in Fig. 1. For an elementary introduction to boson sampling, see Ref. [22]. First we prepare an m-mode state, where the first n modes are prepared with the single photon Fock state, and the remainder with the vacuum state,

$$\begin{aligned}|\psi_{\mathrm{in}}\rangle &= |1_1,\ldots,1_n,0_{n+1},\ldots,0_m\rangle \\ &= a_1^\dagger \ldots a_n^\dagger |0_1,\ldots,0_m\rangle,\end{aligned} \tag{1}$$

where $a_i^\dagger$ is the photon creation operator on the ith mode, and $m = O(n^2)$. Note that when n photons are randomly input into the m modes the sampling problem remains classically difficult [14]. This has become colloquially known as scattershot boson sampling.

Next we propagate this state through a passive linear optics network, which can be expressed by a unitary map on the creation operators,

$$\hat{U}:\ \hat{a}_i^\dagger \to \sum_{j=1}^{m} U_{i,j}\hat{a}_j^\dagger. \tag{2}$$

With this map, the output state can be expressed as

$$|\psi_{\mathrm{out}}\rangle = \sum_S \gamma_S |s_1,\ldots,s_m\rangle, \tag{3}$$

where S are the different photon number configurations, s_i is the number of photons in mode i associated with configuration S, and $\gamma_S \in \mathbb{C}$ are the respective amplitudes. The number of configurations scales exponentially with n, $|S| = \binom{n+m-1}{n}$. The total photon number is conserved, thus $\sum_i s_i = n$ for all S. Performing number-resolved photodetection, which are described by projection operators $\hat{\Pi}(n) = |n\rangle\langle n|$, we sample from the distribution $P_S = |\gamma_S|^2$, each time obtaining an m-fold coincidence measurement outcome of a total of n photons.

As shown by AA the sampling amplitudes are related to matrix permanents,

$$\begin{aligned}\gamma_S &= \frac{\mathrm{Per}(U_S)}{\sqrt{\prod_{i=1}^m s_i! \prod_{j=1}^m t_j!}} \\ &= \frac{\sum_{\sigma\in S_n}\prod_{j=1}^n U_{j,\sigma_i}}{\sqrt{\prod_{i=1}^m s_i! \prod_{j=1}^m t_j!}},\end{aligned} \tag{4}$$

where U_S is an $n \times n$ submatrix of U as a function of the respective configuration S, S_n is the group of permutations, and s_i (t_j) is the number of photons in the input (output) mode associated with mode i (j). The best known classical algorithm for calculating matrix permanents is by Ryser [23], requiring $O(2^n n^2)$ time steps. Because this requires exponential time to evaluate, sampling from the distribution P_S is believed to be a classically hard problem. Importantly, boson sampling does not allow us to calculate matrix permanents as this would require an exponential number of measurements.

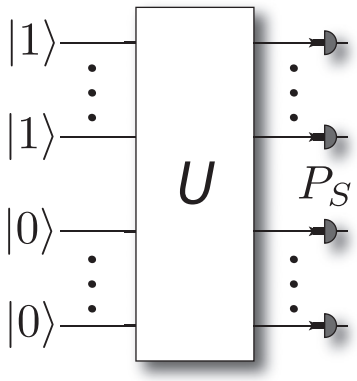

FIG. 1. The boson-sampling model for quantum computation. A series of single-photon and vacuum states are prepared, $|1,\ldots,1,0,\ldots,0\rangle$, and passed through a linear optics network, $\hat{U}$. The experiment is repeated many times and each time the output distribution is measured via coincidence number-resolved photodetection, sampling from the distribution P_S.

III. ZERO AMPLITUDE CAT ANALYSIS

Cat state is a generic term for an arbitrary superposition of macroscopic states and may be used for quantum information processing [24]. In quantum optics, this is generally understood to mean a superposition of two coherent states, potentially with large amplitudes. This is the definition we will use in this work. Two illustrative examples are the even

(+) and odd (−) cat states, so called because they contain only even or odd photon-number terms, respectively,

$$|\mathrm{cat}_{\pm}\rangle = \frac{(|\alpha\rangle \pm |-\alpha\rangle)}{\sqrt{2\left(1 \pm e^{-2|\alpha|^2}\right)}}. \tag{5}$$

The odd cat state has the property that all of the even photon-number terms vanish. In the limit of $\alpha \to 0$ its amplitude identically approaches the single-photon state as shown here,

$$\begin{aligned}\lim_{\alpha\to 0}|\mathrm{cat}_-\rangle &= \lim_{\alpha\to 0}\frac{\sqrt{2}e^{\frac{-|\alpha|^2}{2}}}{\sqrt{1-e^{-2|\alpha|^2}}}\left(\alpha|1\rangle + \frac{\alpha^3|3\rangle}{\sqrt{3!}} + \cdots\right)\\ &\approx |1\rangle + O(\alpha^2)|3\rangle\\ &\to |1\rangle. \end{aligned}\tag{6}$$

In the limit as $\alpha \to 0$ we ignore all higher-order α terms.

Furthermore, the vacuum state [we require $O(n^2)$ vacuum states to be consistent with the boson-sampling model] is given by a trivial cat state containing only a single term in the superposition ($t = 1$) with the respective amplitude $\alpha = 0$. Alternately, the vacuum state can be regarded as the zero amplitude limit of the even cat state,

$$\begin{aligned}\lim_{\alpha\to 0}|\mathrm{cat}_+\rangle &= \lim_{\alpha\to 0}\frac{\sqrt{2}e^{\frac{-|\alpha|^2}{2}}}{\sqrt{1+e^{-2|\alpha|^2}}}\left(\alpha|0\rangle + \frac{\alpha^2|2\rangle}{\sqrt{2!}} + \cdots\right)\\ &\approx |0\rangle + O(\alpha^2)|2\rangle\\ &\to |0\rangle. \end{aligned}\tag{7}$$

Thus, it is immediately clear that in the $\alpha \to 0$ amplitude limit, cat-state sampling reduces to ideal boson sampling, using an appropriate configuration of odd and even cat states, which is a provably hard problem. We use the term provably hard to mean computationally hard, assuming that ideal and approximate boson sampling are computationally hard. Specifically, to implement exact boson sampling with cat states, we choose our input state to be

$$\begin{aligned}|\psi_{\mathrm{in}}\rangle &= \lim_{\alpha\to 0}(|\mathrm{cat}_-\rangle_1 \ldots |\mathrm{cat}_-\rangle_n |\mathrm{cat}_+\rangle_{n+1} \ldots |\mathrm{cat}_+\rangle_m)\\ &= |1_1, \ldots, 1_n, 0_{n+1}, \ldots, 0_m\rangle, \end{aligned}\tag{8}$$

which is exactly the form of Eq. (1). This example is trivial but the point is to show a simple example of cat states leading to a computationally hard problem in a particular limit, which raises the question as to whether it remains hard as we transition out of that limit. In Appendix B we present an example of this reduction in the case of Hong-Ou-Mandel interference to explicitly demonstrate that small amplitude cats behave as single photons. This demonstrates that in certain regimes, cat-state sampling reproduces single-photon statistics.

IV. SMALL AMPLITUDE CAT ANALYSIS

Having established that cat sampling reduces to boson sampling in the zero amplitude limit, the obvious next question is what if the amplitude is small but nonzero? It was shown by AA that boson sampling, when corrupted by erroneous samples, remains computationally hard provided that the error rate scales as $1/\mathrm{poly}(n)$. If we consider a small, but nonzero, amplitude odd cat state, we can treat the non-single-photon terms, which scale as a function of α, as erroneous terms. The error that these erroneous terms induce must be kept below the $1/\mathrm{poly}(n)$ bound. Specifically,

$$|\mathrm{cat}_-\rangle = \underbrace{\gamma_1(\alpha)|1\rangle}_{\text{single photon}} + \underbrace{\gamma_3(\alpha)|3\rangle + \ldots}_{\text{error terms}}, \tag{9}$$

where $\gamma_i(\alpha)$ defines the odd photon-number distribution and follows from Eq. (23). The two underbraced components represent the desired single-photon term and the remaining photon-number terms, which are treated as errors.

In Appendix C we show that the bound on the amplitude of the cat states for a provably hard sampling problem to take place is

$$\alpha^{2n}\mathrm{csch}^n(\alpha^2) > 1/\mathrm{poly}(n), \tag{10}$$

where we input odd cat states in every mode requiring a $|1\rangle$ and vacuum in the remaining modes. Although this function is exponential in n the probability of successfully sampling from the correct distribution will satisfy this bound for sufficiently small values of n and α. The value of n may still be large enough however to implement a postclassical boson-sampling device. Thus, it follows that for nonzero, but sufficiently small α, cat sampling remains computationally hard.

We have established that cat state boson sampling is a provably computationally hard problem in two regimes: (i) in the $\alpha \to 0$ amplitude limit, in which case we reproduce ideal boson sampling, and (ii) for nonzero but sufficiently small amplitudes, in which case the non-single-photon-number terms may be regarded as errors, which remains a computationally hard problem, subject to the bound given in Eq. (10). Having established this, the remainder of this paper is dedicated to the completely general case, whereby the terms in the cat states may have arbitrary amplitude, potentially at a macroscopic scale.

V. ARBITRARY AMPLITUDE CAT ANALYSIS

In this section we will consider arbitrary superpositions of an arbitrary number of coherent states, in which case a general cat is of the form,

$$|\mathrm{cat}\rangle = \sum_{j=1}^{t}\lambda_j|\alpha_j\rangle. \tag{11}$$

Let the input state to our generalized boson-sampling model comprise m arbitrary superpositions of t coherent states, which we will refer to as generalized cat states,

$$|\psi_{\mathrm{in}}\rangle = \bigotimes_{i=1}^{m}\sum_{j=1}^{t}\lambda_j^{(i)}|\alpha_j^{(i)}\rangle, \tag{12}$$

where $|\alpha_j^{(i)}\rangle$ is the coherent state of amplitude $\alpha \in \mathbb{C}$ of the jth term in the ith mode, and $\lambda_j^{(i)} \in \mathbb{C}$ is the amplitude of the jth term of the superposition in the ith mode.[1] It should be

[1]Continuous superpositions are a simple generalization of our formalism, and with this generalization arbitrary states could be expressed as continuous superpositions of coherent states.

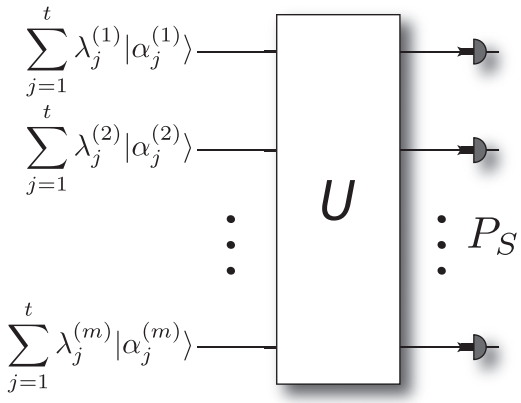

FIG. 2. The model for generalized boson sampling with superpositions of coherent states—cat states. The input state to each mode is an arbitrary superposition of coherent states, some of which are set to the vacuum. Following the application of a linear optics network, the distribution is sampled via number-resolved photodetection.

noted here that, in line with traditional boson sampling, we can choose a number of the modes to be the vacuum. This is achieved by setting $\lambda_1^{(i)} = 1$ and $\alpha_1^{(i)} = 0$.

Expanding this expression yields a superposition of multimode coherent states of the form,

$$|\psi_{\text{in}}\rangle = \sum_{\vec{t}=1}^{t} \lambda_{t_1}^{(1)} \dots \lambda_{t_m}^{(m)} |\alpha_{t_1}^{(1)}, \dots, \alpha_{t_m}^{(m)}\rangle, \tag{13}$$

where $\vec{t}$ is shorthand for $\{t_1,...,t_m\}$. We propagate this state through the passive linear optics network $\hat{U}$ illustrated in Fig. 2. Such a unitary network has the property that a multimode coherent state is mapped to another multimode coherent state,

$$\hat{U}|\alpha^{(1)}, \dots, \alpha^{(m)}\rangle \to |\beta^{(1)}, \dots, \beta^{(m)}\rangle, \tag{14}$$

where the relationship between the input and output amplitudes is given by (see Appendix A),

$$\beta^{(j)} = \sum_{k=1}^{m} U_{j,k} \alpha^{(k)}. \tag{15}$$

$\hat{U}$ acts on each term in the superposition of Eq. (13) independently. Thus, the output state will be of the form,

$$\begin{aligned} |\psi_{\text{out}}\rangle &= \hat{U}|\psi_{\text{in}}\rangle \\ &= \sum_{\vec{t}=1}^{t} \lambda_{t_1}^{(1)} \dots \lambda_{t_m}^{(m)} |\beta_{\vec{t}}^{(1)}, \dots, \beta_{\vec{t}}^{(m)}\rangle. \end{aligned} \tag{16}$$

The number of terms in the output superposition is t^m, scaling exponentially with the number of modes, provided $t > 1$.

Our goal is to sample this distribution using number-resolved photodetectors, which are described by the measurement projectors,

$$\hat{\Pi}_i(n) = |n\rangle_i \langle n|_i, \tag{17}$$

where n is the photon-number measurement outcome on the ith mode. Multimode measurements are described by the projectors,

$$\hat{\Pi}(S) = \hat{\Pi}_1(S_1) \otimes \dots \otimes \hat{\Pi}_m(S_m), \tag{18}$$

where $S = \{S_1, \dots, S_m\}$ is the multimode measurement signature, with S_i photons measured in the ith mode. The sample probabilities are given by

$$P_S = \langle \psi_{\text{out}}|\hat{\Pi}(S)|\psi_{\text{out}}\rangle. \tag{19}$$

In the case of continuous-variable states, the number of measurement signatures, $|S|$, is unbounded as the photon number is undefined, unlike Fock states where the total photon-number is conserved.

Without presenting a rigorous complexity argument, we argue that this sampling problem is likely to be classically hard if three intuitive criteria are satisfied:

(i) There must be an exponential number of terms in the output distribution. This rules out brute-force simulation by explicitly calculating the state vector.

(ii) The terms in the superposition must be entangled, such that the distribution cannot be trivially sampled by independently sampling each mode.

(iii) Each of the amplitudes in the output distribution must be related to a computationally hard problem. This ensures that classical simulation of the individual amplitudes is not efficient.

We have chosen these criteria as they are general properties that classically hard problems are known to exhibit, but we do not prove that these criteria are sufficient to establish whether a problem is likely to be classically hard. For example, ideal boson sampling is known to be computationally hard, satisfying all three criteria. However, fermionic sampling is known to be classically efficient, and violates criteria (iii), as it relates to matrix determinants rather than permanents, which reside in P.

Criteria (i) is achieved by virtue of our choice of input state—there are t^m terms in the output distribution.

It is easily seen that criteria (ii) holds in general. As a simple example, consider the input state,

$$|\psi_{\text{in}}\rangle = \mathcal{N}^2(|\alpha\rangle + |-\alpha\rangle) \otimes (|\alpha\rangle + |-\alpha\rangle) = |\text{cat}_+, \text{cat}_+\rangle, \tag{20}$$

a tensor product of two even cat states. Passing this separable two-mode state through a 50/50 beam splitter gives rise to the output state,

$$|\psi_{\text{out}}\rangle = \hat{H}|\psi_{\text{in}}\rangle = |\text{cat}', 0\rangle + |0, \text{cat}'\rangle, \tag{21}$$

where $|\text{cat}'\rangle = \mathcal{N}_+^2(|\sqrt{2}\alpha\rangle + |-\sqrt{2}\alpha\rangle)$ is a cat state. This is a path-entangled superposition of a cat state across two modes. Thus, while Eq. (14) demonstrates that a unitary network maps a tensor product of coherent states to a tensor product of coherent states, such a network will in general generate path entanglement when the input state is a tensor product of superpositions of coherent states. Note the structural similarity between cat state interference and two-photon Hong-Ou-Mandel-type (HOM) [25] interference. In the case of HOM interference we have $\hat{H}|1,1\rangle = (|2,0\rangle + |0,2\rangle)/\sqrt{2}$, whereas for cat states we have $\hat{H}|\text{cat}, \text{cat}\rangle = |\text{cat}', 0\rangle + |0, \text{cat}'\rangle$.

It was recently and independently reported by Jiang *et al.* [26] that linear optics networks fed with nonclassical pure

states of light almost always generate modal entanglement, consistent with our observation here. This ensures that the output state to our generalized boson-sampling device is highly entangled, thus satisfying criteria (ii). However, Jiang *et al.* present no discussion about our hardness criteria (iii); they do not connect their states to a computationally hard problem. Thus their work provides a necessary but not sufficient proof of computational hardness. It is important, as in our work here, to examine such nonclassical input states individually and make the case for the importance of criteria (iii). For example, it is well known from the Gottesman-Knill theorem that some systems with exponentially large Hilbert spaces that satisfy our criteria (i) and (ii) can nevertheless be efficiently simulated. An example is the circuit model for quantum computation that deploys only gates from the Clifford algebra.

Finally let us consider criteria (iii). Let the expansion for a coherent state be

$$|\alpha\rangle = \sum_{n=0}^{\infty} f_n(\alpha)|n\rangle, \tag{22}$$

in the photon-number basis, where,

$$f_n(\alpha) = e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}}, \tag{23}$$

is the amplitude of the n-photon term. Then,

$$\langle n|\alpha\rangle = f_n(\alpha). \tag{24}$$

Thus, acting the measurement projector for configuration S, Eq. (18), on the output state, Eq. (16), we obtain

$$\hat{\Pi}(S)|\psi_{\text{out}}\rangle = \gamma_S|S_1, S_2, \ldots, S_m\rangle, \tag{25}$$

where,

$$\gamma_S = \sum_{\vec{t}=1}^{t} \left(\prod_{j=1}^{m} \lambda_{t_j}^{(j)} f_{S_j} \left(\sum_{k=1}^{m} U_{j,k} \alpha_{t_j}^{(k)} \right) \right), \tag{26}$$

and the sampling probability takes the form $P_S = |\gamma_S|^2$. We can group the terms under the product and label them $A_{j,\vec{t}}^{(S)}$. Then the amplitudes are given by

$$\gamma_S = \sum_{\vec{t}=1}^{t} \prod_{j=1}^{m} A_{j,\vec{t}}^{(S)}, \tag{27}$$

which has the same analytic structure as the permanent when $t = m$ but sums over additional terms that are not present in the permanent. Evaluating this combinatoric problem requires exponential resources using brute force. Via brute force, evaluating this expression requires summing t^m terms. Given that Eq. (27) has the same analytic form as the matrix permanent, which is known to be classically hard, this implies a striking similarity between cat-state sampling and Fock-state sampling, with the constraint that A is of a form whose permanent is not trivial. In fact, in the $\alpha \to 0$ limit, evaluating this combinatoric expression must be as hard as calculating an $n \times n$ matrix permanent, since we know that in this limit the problem reduces to ideal boson sampling. In the original proof by Aaronson and Arkhipov, it is required that U is Haar random. It is an open question as to whether A can be made Haar random in the presented generalized boson-sampling model.

In the trivial case of $t = 1$ this expression simplifies to

$$\gamma_S = \prod_{j=1}^{m} f_{S_j} \left(\sum_{k=1}^{m} U_{j,k} \alpha_1^{(k)} \right), \tag{28}$$

which evaluates in polynomial time. In this case the input state is simply a tensor product of coherent states, and the runtime is consistent with the known result that simulating coherent states is trivial as the tensor product structure allows sampling to proceed by independently sampling each mode, each of which is an efficient sampling problem. However, when $t > 1$ the complexity of directly arithmetically evaluating Eq. (26) grows exponentially.

VI. A COMPUTATIONAL COMPLEXITY ARGUMENT

We now provide a complexity theoretic argument for the hardness of cat-state sampling. We will consider the problem of weakly simulating such a system with a randomized classical algorithm, and show that the existence of any such algorithm, which can approximate the output to within a constant multiplicative factor of $\sqrt{2}$, would imply a collapse of certain classical computational complexity classes, which are believed to be distinct. The polynomial hierarchy, denoted as PH, is composed of an infinite number of levels k, which are composed of the complexity classes $\Sigma_k\text{P} = \text{NP}^{\Sigma_{k-1}\text{P}}$, $\Delta_k\text{P} = \text{P}^{\Sigma_{k-1}\text{P}}$, and $\Pi_k\text{P} = \text{coNP}^{\Sigma_{k-1}\text{P}}$, where $\Sigma_0\text{P} = \Delta_0\text{P} = \Pi_0\text{P} = \text{P}$. We show that if the measurement results in a cat-state interferometry experiment are specified by a string x, and each x occurs with probability $p(x)$, then if there exists an efficient (polynomial time) randomized algorithm which, for all such cat-state interferometry experiments, produces output x with probability $p'(x)$ such that $\frac{1}{\sqrt{2}}p(x) \leqslant p'(x) \leqslant \sqrt{2}p(x)$ for all x, then the polynomial hierarchy collapses to the third level (i.e., $\text{PH} = \Delta_3\text{P}$). While such a result would not be quite as strong as $\text{P} = \text{NP}$, it has a well established connection to this problem, and it is widely believed that the polynomial hierarchy has an infinite number of inequivalent levels.

Our approach follows the method developed by Bremner, Jozsa, and Shepherd [27], which they used to show the intractability of classical simulation of certain circuits composed of commuting gates. The technique has since been extended to other settings, including the one clean qubit (DQC1) model [28,29]. This approach makes use of the notion of postselection, in which the computational cost of performing a certain computation is counted only if that computation results in a particular value of a chosen postselection register.

We provide informal definitions of two computational complexity classes based on post-selection, based on those used in Ref. [28], which will be used extensively in our proof. More formal definitions of these classes can be found in Ref. [27]. These classes are defined in terms of circuits composed of either classical or quantum gates with identified output and postselection registers O_x and P_x respectively. A language L is in the class PostBPP if and only if there exists

a uniform family of classical circuits and a $0 < \delta < 1/2$ such that:

(i) if $x \in L$ then $\text{Prob}(O_x = 1|P_x = 0\ldots0) \geqslant \frac{1}{2} + \delta$,

(ii) if $x \notin L$ then $\text{Prob}(O_x = 1|P_x = 0\ldots0) \leqslant \frac{1}{2} - \delta$.

Similarly, a language L is in the class PostBQP if there exists a uniform family of quantum circuits satisfying the above criteria.[2] We also define a third complexity class PostCAT to capture the notion of postselection applied to the interferometry experiments we are concerned with. We will say that a language L is in PostCAT if there exists a uniform family of n-port linear interferometers acting on cat-state inputs satisfying the preceding criteria.

The complexity of the first two classes has previously been studied, and it is known that PostBPP exactly corresponds to another complexity class known as BPP_{path}, which is contained within $\Delta_3\text{P}$ [30]. On the other hand, it was shown by Aaronson that PostBQP = PP [31]. This is rather surprising, since $\text{PH} \subseteq \text{P}^{\text{PP}}$, which implies a difference between the power of postselected classical and quantum computation unless $\text{P}^{\text{PP}} = \text{PH} = \Delta_3\text{P}$. Following from the definitions of PostBPP and PostBQP given above, this further implies that an efficient classical randomized algorithm cannot mimic the output of an arbitrary quantum circuit, since such a situation would yield PostBQP = PostBPP and so collapse the polynomial hierarchy. In fact, this last statement can be made stronger: The existence of a polynomial time randomized classical algorithm, which approximates the output distribution to an arbitrary quantum circuit to within multiplicative error of $\sqrt{2}$, would yield $\text{PH} = \Delta_3\text{P}$ [27,28].

All that must be done, then, in order to prove our claim is to show that PostBQP $\subseteq$ PostCAT, from which it would follow that the existence of an efficient randomized classical algorithm, which can approximate the output distribution of an arbitrary linear interferometer applied to cat-state inputs to within a multiplicative error of $\sqrt{2}$ would imply that PostCAT $\subseteq$ PostBPP and hence $\text{PH} = \Delta_3\text{P}$. However, that PostBQP $\subseteq$ PostCAT follows directly from the work of Ralph *et al.* [32], who showed that arbitrary quantum circuits could be implemented exactly, albeit probabilistically, on qubits encoded as a superposition of even and odd parity cat states. Although the set of gates they introduce is probabilistic, there is always some probability of obtaining a measurement result, which correctly implements the desired gate with unit fidelity. Hence by postselecting on such an outcome, the system can be made to deterministically implement an arbitrary quantum circuit. Since postselection could also be applied to output qubits from the circuit while remaining in PostCAT, it follows that any computation in PostBQP is also in PostCAT. Thus we must conclude that unless $\text{PH} = \Delta_3\text{P}$, there must not exist an efficient randomized classical algorithm, which can produce an output distribution approximating that of an arbitrary interferometer with multiplicative error of $\sqrt{2}$ or less.

[2]Here the gate set is assumed to be some standard universal set, such as the Hadamard and Toffoli gates. More exotic gate sets can potentially lead to more powerful models, but this class provides a lower bound on the power of postselected quantum computation, which is sufficient for our purposes.

VII. PREPARING CAT STATES

Finally, we will discuss the prospects for experimentally preparing cat states of the form used in our derivation. There exists a significant number of schemes for generating a finite number of superpositions of coherent states all of which are extremely difficult to scale to higher-order cat states. For example, superpositions of coherent states with equal amplitudes but different phases can be produced with quantum nondemolition (QND) measurements [33] via the interaction of a strong Kerr nonlinearity [34,35]. Another approach is to use strong Kerr nonlinearities together with coupled Mach-Zehnder interferometers [35] but this is impractical as outside the cavity a strong Kerr would require a coherent electromagnetically induced transparency [36,37] effect in an atomic gas cloud and even there in practice the nonlinearities are too weak for our purposes.

In a similar way that measurements of photon number can produce discrete coherent state superpositions in phase; measurements of the phase can produce discrete coherent state superpositions in amplitude. This can be understood via the number-phase uncertainty relation. Any improved knowledge of the phase of a state induces kicks in the number and vice versa. In this way, by combining such different measurements, one can produce discrete superpositions in both phase and amplitude; approaching the arbitrary superpositions of coherent states we require here. Exactly such a scheme was proposed by Jeong *et al.* [38,39]. By combining both types of detection schemes, even with detectors of nonunit efficiency, they show that a large number of propagating superpositions of coherent states may be thus produced. These states then could be used in proof-of-principle experiments for our protocol outlined here.

VIII. CONCLUSION

We have presented evidence that a linear optics network, fed with arbitrary superpositions of coherent states, and sampled via number-resolved photodetection, is likely to be a classically hard problem. We have shown that sampling within multiplicative errors is hard and we have also presented evidence that it has similar complexity to boson sampling, a model for which sampling with even additive error is known to be hard. Our argument is based on three realistic criteria for computational hardness of the sampling problem. In the case of input states comprising superpositions of coherent states, these three criteria are satisfied. In the case of criteria (iii), we find that the amplitudes are related to a permanentlike function of a matrix, strikingly similar to ideal boson sampling. In fact, if this permanentlike function is shown to be in the Haar random class of matrices, then our result is provably hard following Aaronson and Arkhipov's proof.

Furthermore, we show two examples of how sampling with normal cat states reduces to a computationally hard problem,

(i) In the limit of $\alpha \to 0$ amplitude cat states, cat sampling reduces to ideal boson sampling.

(ii) When the amplitude is increased slightly away from zero, odd cat-state sampling is hard for sufficiently small amplitudes following the bound of Eq. (10). We show this by treating the non-single-photon-number terms as an error model.

Furthermore, given that (i) is known to be computationally hard, as it reduces to ideal boson sampling, it follows that our combinatoric expression for evaluating the amplitudes in the output superposition, Eq. (27), is equivalent to evaluating a permanent in this limit. For arbitrary α, the combinatoric expression maintains the same analytic form. This presents strong evidence that arbitrarily large cat states yield a hard sampling problem akin to standard boson sampling. With all of these results combined, these observations present strong evidence that such a generalized sampling problem is likely classically hard to simulate and is indeed hard within multiplicative errors.

Because coherent states form an overcomplete basis, any pure optical state can be expressed in terms of coherent states, suggesting that most quantum states of light may yield hard sampling problems. This observation further motivates interest in developing sources for quantum states of light other than Fock states.

ACKNOWLEDGMENTS

We would like to thank Mark Wilde for helpful discussions. This research was conducted by the Australian Research Council Centre of Excellence for Engineered Quantum Systems (Project No. CE110001013). J.P.D. would like to acknowledge the Air Force Office of Scientific Research, the Army Research Office, and the National Science Foundation. This work was partly supported by DSTL (Contract No. DSTLX1000063869). This material is based in part on research supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01.

APPENDIX A: PROPAGATING MULTIMODE COHERENT STATES THROUGH PASSIVE LINEAR OPTICS NETWORKS

The unitary map describing a passive linear optics network is given by

$$\hat{U}:\ \hat{a}_i^\dagger \rightarrow \sum_{j=1}^{m} U_{i,j}\hat{a}_j^\dagger, \tag{A1}$$

and taking the Hermitian conjugate yields,

$$\hat{U}:\ \hat{a}_i \rightarrow \sum_{j=1}^{m} U_{i,j}^*\hat{a}_j. \tag{A2}$$

A coherent state can be expressed in terms of a displacement operator acting on the vacuum state,

$$|\alpha^{(i)}\rangle_i = \hat{D}_i(\alpha^{(i)})|0\rangle_i, \tag{A3}$$

where the displacement operator may be expressed in terms of creation and annihilation operators as

$$\hat{D}_i(\alpha^{(i)}) = \exp(\alpha^{(i)}\hat{a}_i^\dagger - \alpha^{(i)*}\hat{a}_i). \tag{A4}$$

Applying the unitary map Eqs. (A1) and (A2), we obtain

$$\hat{U}\,\hat{D}_i(\alpha_i) = \exp\left(\alpha^{(i)}\sum_{j=1}^{m} U_{i,j}\hat{a}_j^\dagger - \alpha^{(i)*}\sum_{j=1}^{m} U_{i,j}^*\hat{a}_j\right). \tag{A5}$$

Let,

$$\hat{U}|\alpha^{(1)},\ldots,\alpha^{(m)}\rangle = |\beta^{(1)},\ldots,\beta^{(m)}\rangle. \tag{A6}$$

Then,

$$\hat{U}|\alpha^{(1)},\ldots,\alpha^{(m)}\rangle = \hat{U}\,\hat{D}_1(\alpha^{(1)})\ldots\hat{D}_m(\alpha^{(m)})|0_1,\ldots,0_m\rangle. \tag{A7}$$

For each term,

$$\begin{aligned}\hat{U}\,\hat{D}_i(\alpha^{(i)}) &= \prod_{j=1}^{m}\exp(\alpha^{(i)}U_{i,j}\hat{a}_j^\dagger - \alpha^{(i)*}U_{i,j}^*\hat{a}_j)\\ &= \prod_{j=1}^{m}\hat{D}_j(U_{i,j}\alpha^{(i)}).\end{aligned} \tag{A8}$$

Thus,

$$\begin{aligned}\hat{U}\prod_{i=1}^{m}|\alpha^{(i)}\rangle_i &= \hat{U}\prod_{i=1}^{m}\hat{D}(\alpha^{(i)})|0\rangle_i\\ &= \prod_{i=1}^{m}\prod_{j=1}^{m}\hat{D}_j(U_{i,j}\alpha^{(i)})|0\rangle\\ &= \bigotimes_{j=1}^{m}\left|\sum_{i=1}^{m}U_{i,j}\alpha^{(i)}\right\rangle_j\\ &= \bigotimes_{j=1}^{m}|\beta^{(j)}\rangle_j.\end{aligned} \tag{A9}$$

And

$$\beta^{(j)} = \sum_{i=1}^{m} U_{i,j}\alpha^{(i)}, \tag{A10}$$

as per Eq. (15).

APPENDIX B: REPRODUCING HONG-OU-MANDEL INTERFERENCE USING SMALL AMPLITUDE ODD CAT STATES

We begin with our generalized cat-state result from Eq. (26).

$$\gamma_s = \sum_{\vec{t}=1}^{t}\left(\prod_{j=1}^{m}\lambda_{t_j}^{(j)} f_{S_j}\left(\beta_{\vec{t}}^{(j)}\right)\right), \tag{B1}$$

and input the odd cat state, which has the form

$$|\text{cat}_-\rangle = \frac{|\alpha\rangle - |-\alpha\rangle}{\sqrt{2(1-\exp[-2\alpha^2])}}. \tag{B2}$$

When considering the specific example of $|\text{cat}_-\rangle$ the $\lambda_{t_j}^{(j)}$ of Eq. (B1) goes to $(-1)^{t_j}$. Eq. (B1) then becomes

$$\gamma_s = \sum_{\vec{t}=1}^{t}\left(\prod_{j=1}^{m}(-1)^{t_j}\frac{f_{S_j}\left(\beta_{\vec{t}}^{(j)}\right)}{\sqrt{2(1-\exp[-2\alpha^2])}}\right). \tag{B3}$$

Since the $\beta_{\vec{t}}^{(j)}$'s in Eq. (B3) depend on α, we substitute the argument of f_{S_j} using Eq. (23),

$$\gamma_s = \frac{1}{(\sqrt{2(1-\exp[-2\alpha^2])})^m} \tag{B4}$$

$$\times \sum_{\vec{t}=1}^{t} \left(\prod_{j=1}^{m} (-1)^{t_j} \exp\left[-\frac{|\beta_{\vec{t}}^{(j)}|^2}{2} \right] \frac{(\beta_{\vec{t}}^{(j)})^{S_j}}{\sqrt{S_j!}} \right). \tag{B5}$$

Next we take a first-order approximation. Since α is small, the exponential in the numerator goes to one while the exponential in the denominator goes to $\exp(x) \approx 1 + x$ because otherwise this would diverge. This yields

$$\begin{aligned}
\gamma_s &\approx \frac{1}{(\sqrt{2(1-(1-2\alpha^2))})^m} \sum_{\vec{t}=1}^{t} \left(\prod_{j=1}^{m} (-1)^{t_j} (1) \frac{(\beta_{\vec{t}}^{(j)})^{S_j}}{\sqrt{S_j!}} \right) \\
&= \frac{1}{(2\alpha)^m \sqrt{S_1!S_2!\ldots S_m!}} \sum_{\vec{t}=1}^{t} \left(\prod_{j=1}^{m} (-1)^{t_j} (\beta_{\vec{t}}^{(j)})^{S_j} \right) \\
&= \frac{1}{(2\alpha)^m \sqrt{S_1!S_2!\ldots S_m!}} \sum_{\vec{t}=1}^{t} (-1)^{\sigma(\vec{t})} \prod_{j=1}^{m} (\beta_{\vec{t}}^{(j)})^{S_j}.
\end{aligned} \tag{B6}$$

In the limit of small α we know that the odd cat state reduces to a single photon Fock state. Here we consider the case of a cat state being input into the first two modes and let the unitary be the Hadamard gate. In small α this corresponds to inputting a single-photon Fock state into the first two modes and interfering them in a single 50/50 beam splitter. Therefore, the corresponding bunching in the output modes would to be expected. In this section we show that our expression of Eq. (B6) does show the expected bunching.

We begin by putting an odd cat state $|\text{cat}_-\rangle$ with $t = 2$ terms into the first $m = 2$ modes. Then Eq. (B6) becomes

$$\begin{aligned}
\gamma_s &\approx \frac{1}{(2\alpha)^2 \sqrt{S_1!S_2!}} \sum_{t_1,t_2=1}^{2} (-1)^{\sigma(\vec{t})} \prod_{j=1}^{2} (\beta_{t_1,t_2}^{(j)})^{S_j} \\
&= \frac{1}{(2\alpha)^2 \sqrt{S_1!S_2!}} \sum_{t_1,t_2=1}^{2} (-1)^{\sigma(t_1+t_2)} (\beta_{t_1,t_2}^{(1)})^{S_1} (\beta_{t_1,t_2}^{(2)})^{S_2} \\
&= \frac{1}{(2\alpha)^2 \sqrt{S_1!S_2!}} [(\beta_{1,1}^{(1)})^{S_1} (\beta_{1,1}^{(2)})^{S_2} - (\beta_{1,2}^{(1)})^{S_1} (\beta_{1,2}^{(2)})^{S_2} \\
&\quad - (\beta_{2,1}^{(1)})^{S_1} (\beta_{2,1}^{(2)})^{S_2} + (\beta_{2,2}^{(1)})^{S_1} (\beta_{2,2}^{(2)})^{S_2}].
\end{aligned} \tag{B7}$$

Now to calculate the $\beta_{\vec{t}}^{(j)}$'s for this case we first take the tensor product between the first two modes. Ignoring the normalization factor this yields

$$\begin{aligned}
|\text{cat}_-\rangle &= (|\alpha\rangle - |-\alpha\rangle) \otimes (|\alpha\rangle - |-\alpha\rangle) \\
&= |\alpha,\alpha\rangle - |\alpha,-\alpha\rangle - |-\alpha,\alpha\rangle + |-\alpha,-\alpha\rangle.
\end{aligned} \tag{B8}$$

Next we pass them through a 50/50 beam splitter,

$$U|\text{cat}_-\rangle = |\sqrt{2}\alpha,0\rangle - |0,\sqrt{2}\alpha\rangle - |0,-\sqrt{2}\alpha\rangle + |-\sqrt{2}\alpha,0\rangle. \tag{B9}$$

Now we read off the $\beta_{\vec{t}}^{(j)}$'s to be

$$\begin{aligned}
\beta_{1,1}^{(1)} &= \beta_{1,2}^{(2)} = \sqrt{2}\alpha \\
\beta_{2,2}^{(1)} &= \beta_{2,1}^{(2)} = -\sqrt{2}\alpha \\
\beta_{1,2}^{(1)} &= \beta_{2,1}^{(1)} = \beta_{1,1}^{(2)} = \beta_{2,2}^{(2)} = 0.
\end{aligned} \tag{B10}$$

Now Eq. (B7) becomes

$$\begin{aligned}
\gamma_s = \frac{1}{(2\alpha)^2 \sqrt{S_1!S_2!}} &[(\sqrt{2\alpha})^{S_1} (0)^{S_2} - (0)^{S_1} (\sqrt{2}\alpha)^{S_2} \\
&- (0)^{S_1} (-\sqrt{2}\alpha)^{S_2} + (-\sqrt{2}\alpha)^{S_1} (0)^{S_2}].
\end{aligned} \tag{B11}$$

Because we are dealing in the limit of small α, a nonzero number arbitrarily close to zero raised to a zero power is one, so the terms $0^{S_j} = \delta_{S_j,0}$. Now Eq. (B11) becomes

$$\begin{aligned}
\gamma_s = \frac{1}{(2\alpha)^2 \sqrt{S_1!S_2!}} &[(\sqrt{2\alpha})^{S_1} \delta_{S_2,0} - (\sqrt{2}\alpha)^{S_2} \delta_{S_1,0} \\
&- (-\sqrt{2}\alpha)^{S_2} \delta_{S_1,0} + (-\sqrt{2}\alpha)^{S_1} \delta_{S_2,0}].
\end{aligned} \tag{B12}$$

For this example we know that there are three possible signature outcomes. We expect that the configuration $S_1 = S_2 = 1$ is not possible due to HOM photon bunching and thus in this case $\gamma_s = 0$. For configurations $S_1 = 0$ and $S_2 = 2$ or $S_1 = 2$ and $S_2 = 0$ we would expect a nonzero configuration amplitude of $\gamma_s = 1/2$ in each case. Next, we will show that this is indeed the case.

1. Configuration $S_1 = S_2 = 1$

With configuration $S_1 = S_2 = 1$ Eq. (B12) becomes

$$\begin{aligned}
\gamma_s &\approx \frac{1}{4\alpha^2} [(\sqrt{2}\alpha)\delta_{1,0} - (\sqrt{2}\alpha)\delta_{1,0} \\
&\quad - (-\sqrt{2}\alpha)\delta_{1,0} + (-\sqrt{2}\alpha)\delta_{1,0}] \\
&= 0,
\end{aligned} \tag{B13}$$

which vanishes as expected.

2. Configuration $S_1 = 0$ and $S_2 = 2$

With configuration $S_1 = 0$ and $S_2 = 2$ Eq. (B12) becomes

$$\begin{aligned}
\gamma_s &= \frac{1}{(2\alpha)^2 \sqrt{0!2!}} [(\sqrt{2\alpha})^0 \delta_{2,0} - (\sqrt{2}\alpha)^2 \delta_{0,0} \\
&\quad - (-\sqrt{2}\alpha)^2 \delta_{0,0} + (-\sqrt{2}\alpha)^0 \delta_{2,0}] \\
&= \frac{1}{4\alpha^2\sqrt{2}} [-2\alpha^2 - 2\alpha^2] \\
&= -\frac{1}{\sqrt{2}},
\end{aligned} \tag{B14}$$

and the corresponding classical probability is $1/2$ as expected.

3. Configuration $S_1 = 2$ and $S_2 = 0$

With configuration $S_1 = 2$ and $S_2 = 0$ Eq. (B12) becomes

$$\begin{aligned}
\gamma_s = \frac{1}{(2\alpha)^2 \sqrt{2!0!}} &[(\sqrt{2\alpha})^2 \delta_{0,0} - (\sqrt{2}\alpha)^0 \delta_{2,0} \\
&- (-\sqrt{2}\alpha)^0 \delta_{2,0} + (-\sqrt{2}\alpha)^2 \delta_{0,0}]
\end{aligned}$$

$$= \frac{1}{4\alpha^2\sqrt{2}}[2\alpha^2 + 2\alpha^2]$$
$$= \frac{1}{\sqrt{2}}, \tag{B15}$$

again with classical probability $1/2$ as expected.

Thus, our result generalizes to the expected results for passing a single-photon Fock state input in modes one and two through a Hadamard gate. This shows that our cat-state generalization works for the odd cat state in the limit of small α, which is equivalent to Aaronson and Arkhipov's boson sampling.

APPENDIX C: NONZERO AMPLITUDE ODD CAT STATES AS AN ERROR MODEL

According to the error bound derived by Aaronson and Arkhipov, the probability of sampling from the correct distribution must not exceed the bound of $1/\text{poly}(n)$ in order for it to implement classically hard boson sampling. The correct input distribution is $|1,\ldots,1,0,\ldots,0\rangle$ and the probability of successfully sampling from it depends on the odd cat states since we input odd cat states in every mode requiring a $|1\rangle$ and vacuum in the remaining modes. Thus, the single-photon component of the odd cat state must be successfully sampled n times.

Consider the odd cat state from Eq. (B2). The amplitude of the single-photon term of an odd cat state is given by,

$$\gamma_1 = \frac{f_1(\alpha) - f_1(-\alpha)}{\sqrt{2\left(1 - e^{-2|\alpha|^2}\right)}}, \tag{C1}$$

where $f_n(\alpha)$ is defined in Eq. (23). In order to get the classical probability we calculate γ_1^2. The amplitude of the $n = 1$ coherent state photon term is then

$$f_1(\alpha) = \alpha e^{-\frac{|\alpha|^2}{2}}, \tag{C2}$$

thus, the probability of having sampled from the correct term is

$$\begin{aligned} P &= {\gamma_1}^{2n} \\ &= \left(\frac{\alpha e^{\frac{-|\alpha|^2}{2}} - (-\alpha)e^{\frac{-|\alpha|^2}{2}}}{\sqrt{2(1 - e^{-2|\alpha|^2})}}\right)^{2n} \\ &= \left(\frac{2\alpha e^{\frac{-|\alpha|^2}{2}}}{\sqrt{2(1 - e^{-2|\alpha|^2})}}\right)^{2n} \\ &= \left(\frac{4\alpha^2 e^{-|\alpha|^2}}{2(1 - e^{-2|\alpha|^2})}\right)^{n} \\ &= \left(\frac{2\alpha^2}{e^{|\alpha|^2}(1 - e^{-2|\alpha|^2})}\right)^{n} \\ &= \left(\frac{2\alpha^2}{e^{|\alpha|^2} - e^{-|\alpha|^2}}\right)^{n} \\ &= (\alpha^2 \text{csch}(|\alpha|^2))^n \\ &= \alpha^{2n}\text{csch}^n(|\alpha|^2), \end{aligned} \tag{C3}$$

where the hyperbolic trigonometric identity $\text{csch}(x) = 2/(e^x - e^{-x})$ was used. Following AA's given bound this requires that

$$\alpha^{2n}\text{csch}^n(|\alpha|^2) > 1/\text{poly}(n), \tag{C4}$$

in order for the sampling problem to be in a regime, which is provably computationally hard.

[1] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).

[2] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. Milburn, Rev. Mod. Phys. **79**, 135 (2007).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[4] S. Aaronson and A. Arkhipov, in *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC'11)* (ACM, New York, 2011), pp. 333–342.

[5] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Rev. Sci. Instrum. **82**, 071101 (2011).

[6] A. Arkhipov and G. Kuperberg, Geometry & Topology Monographs **18**, 1 (2012).

[7] B. J. Metcalf, N. Thomas-Peter, J. B. Spring, D. Kundys, M. A. Broome, P. C. Humphreys, X.-M. Jin, M. Barbieri, W. S. Kolthammer, J. C. Gates *et al.*, Nat. Commun. **4**, 1356 (2012).

[8] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Science **339**, 794 (2013).

[9] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys *et al.*, Science **339**, 798 (2013).

[10] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Nat. Photon. **7**, 545 (2013).

[11] M. Tillmann, B. Daki, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Nat. Photon. **7**, 540 (2013).

[12] K. P. Seshadreesan, J. P. Olson, K. R. Motes, P. P. Rohde, and J. P. Dowling, arXiv:1402.0531.

[13] J. P. Olson, K. P. Seshadreesan, K. R. Motes, P. P. Rohde, and J. P. Dowling, arXiv:1406.7821.

[14] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Phys. Rev. Lett. **113**, 100502 (2014).

[15] S. D. Bartlett and B. C. Sanders, Phys. Rev. Lett. **89**, 207903 (2002).

[16] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).

[17] B. C. Sanders, Phys. Rev. A **46**, 2966 (1992).

[18] C. C. Gerry, Phys. Rev. A **55**, 2478 (1997).

[19] C. C. Gerry, A. Benmoussa, and R. A. Campos, Phys. Rev. A **66**, 013804 (2002).

[20] C. C. Gerry and R. Grobe, Phys. Rev. A **75**, 034303 (2007).

[21] C. C. Gerry, J. Mimih, and A. Benmoussa, Phys. Rev. A **80**, 022111 (2009).

[22] B. T. Gard, K. R. Motes, J. P. Olson, P. P. Rohde, and J. P. Dowling, arXiv:1406.6767.
[23] H. J. Ryser, Comb. Math., Carus Math. Mono. No. 14 (1963).
[24] A. Gilchrist, K. Nemoto, W. J. Munro, T. Ralph, S. Glancy, S. L. Braunstein, and G. Milburn, J. Opt. B: Quantum Semiclassical Opt. **6**, S828 (2004).
[25] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[26] Z. Jiang, M. D. Lang, and C. M. Caves, Phys. Rev. A **88**, 044301 (2013).
[27] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. London, Ser. A **467**, 459 (2011).
[28] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. **112**, 130502 (2014).
[29] T. Morimae, H. Nishimura, K. Fujii, and S. Tamate, arXiv:1409.6777.
[30] Y. Han, L. A. Hemaspaandra, and T. Thierauf, SIAM J. Comput. **26**, 59 (1997).
[31] S. Aaronson, Proc. R. Soc. London, Ser. A **461**, 3473 (2005).
[32] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, Phys. Rev. A **68**, 042319 (2003).
[33] P. Alsing, G. J. Milburn, and D. F. Walls, Phys. Rev. A **37**, 2970 (1988).
[34] S. Haroche, *Exploring the Quantum: Atoms, Cavities and Photons* (Oxford University Press, Oxford, UK, 2006).
[35] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, UK, 2005).
[36] S. E. Harris, Phys. Today **50**, 36 (2008).
[37] S. E. Harris, J. E. Field, and A. Imamoğlu, Phys. Rev. Lett. **64**, 1107 (1990).
[38] A. P. Lund, H. Jeong, T. C. Ralph, and M. S. Kim, Phys. Rev. A **70**, 020101(R) (2004).
[39] H. Jeong, A. P. Lund, and T. C. Ralph, Phys. Rev. A **72**, 013801 (2005).