Detailed study of Gaussian boson sampling

Regina Kruse,[1] Craig S. Hamilton,[2,*] Linda Sansoni,[1] Sonja Barkhofen,[1] Christine Silberhorn,[1] and Igor Jex[2]
[1]*Integrated Quantum Optics, Universität Paderborn, Warburger Strasse 100, 33098 Paderborn, Germany*
[2]*FNSPE, Czech Technical University in Prague, Brêhová 7, 119 15, Praha 1, Czech Republic*

(Received 23 January 2018; published 18 September 2019)

Since the development of boson sampling, there has been a quest to construct more efficient and experimentally feasible protocols to test the computational complexity of sampling from photonic states. In this paper, we interpret and extend the results presented previously [Phys. Rev. Lett. **119**, 170501 (2017)]. We derive an expression that relates the probability to measure a specific photon output pattern from a Gaussian state to the *Hafnian* matrix function and use it to design a Gaussian boson sampling protocol. Then, we discuss the advantages that this protocol has relative to other photonic protocols and the experimental requirements for Gaussian boson sampling. Finally, we relate it to the previously most general protocol, scattershot boson sampling [Phys. Rev. Lett. **113**, 100502 (2014)].

DOI: 10.1103/PhysRevA.100.032326

I. INTRODUCTION

Boson sampling, introduced by Aaronson and Arkhipov (AABS) [1,2] is a nonuniversal model of quantum computation that may demonstrate the advantage of quantum-computational schemes over classical algorithms. From a computational point of view, this is especially interesting, as it may provide evidence against the extended Church-Turing thesis, and experimentally it is attractive as it requires a straightforward implementation: N single-photon Fock states are launched in an N^2-dimensional linear interferometer and the output pattern of photons is measured. This experimental feasibility has inspired many groups to implement proof-of-principle experiments to demonstrate the viability of this protocol [3–6]. However, because of a lack of deterministic single-photon sources, these implementations had to use probabilistic, postselected photon-pair sources (postselected Fock boson sampling [PFBS]). The use of probabilistic sources means that the probability of generating high photon numbers in these schemes decreases exponentially with photon number. Since a boson sampling experiment that may provide evidence against the extended Church-Turing thesis requires $N = 50$–100 photons [1,7,8], a probabilistic approach to photon generation is not likely to reach this benchmark.

To improve the performance of boson sampling machines, some groups have concentrated on the development of on-demand single-photon sources to overcome the probabilistic nature of photon generation [9–11]. Alternatively, theoretical work by Tamma and Laibacher [12,13] has shown that arbitrary, distinguishable multimode single photons can be used if special care is taken at the detection stage. Other theoretical proposals have been sought to overcome photon-generation problems by multiplexing the photon sources, either spatially [14] or in time [15]. The latter, scattershot boson sampling (SBS), proposed by Lund *et al.* [14], is a way to avoid the exponential scaling of probabilistic sources. This protocol makes use of N^2 parallel two-mode squeezed states to generate N photon pairs, where one photon of each pair acts as a herald for the other photon, which enters the input of the interferometer. These latter photons are the ones that are sampled in the AABS protocol. This increase in the number of resources improves the generation probability to a polynomial scaling for large photon numbers. An alternative method utilizing more sources was shown in Ref. [15], where sources were used in series, in between interferometers, yielded further improvements in the generation probability of photons.

Although SBS and PFBS use weakly squeezed Gaussian states (mean number of photons $\langle n\rangle \ll 1$) as the photon-generation resource, these approaches reduce the protocol to sampling from single-photon Fock states and do not exploit the full Gaussian nature of their initial states. This poses the question, from both theoretical and experimental perspectives, of whether a hybrid approach considering the full Gaussian nature of the input states and photon-counting measurement schemes can improve existing sampling protocols. Such an approach benefits from the methods and concepts developed in the framework of both continuous- and discrete-variable quantum information, as Gaussian states are the basis of continuous-variable quantum information and have been demonstrated to be a powerful resource for highly scalable systems, for example, in the context of cluster-state generation [16]. The special case of sampling from thermal states was studied in Refs. [17,18] and shown to be in $\mathsf{BPP}^{\mathsf{NP}}$, whereas measuring photons from coherent states is well known and is in the simplest complexity class, P.

In a recent paper [19], we introduced Gaussian boson sampling (GBS) that answers questions about the complexity of sampling from a general squeezed state. In that paper, we derived an expression that connects the probability to measure a specific output pattern of photons from a general Gaussian state to the Hafnian matrix function. This was then used to develop a regime of boson sampling from squeezed states, which

*hamilcra@fjfi.cvut.cz

 ©2019 American Physical Society

has specific advantages when compared to previous regimes, i.e., SBS. In this paper, we extend our formula to account for displaced squeezed states (the addition of coherent light) and the presence of higher order photon number contributions in a single output mode. Next, we detail the construction of our GBS protocol with single-mode squeezed states, discuss why the computation of the Hafnian is in the #P complexity class, and provide arguments, similar to those of Aaronson and Arkhipov (AA) [1], that approximate GBS is still in #P. From this discussion, we derive several requirements on the experimental parameters and finally relate our GBS protocol to the most efficiently known boson sampling protocol, SBS. We then show that SBS is a special subclass of GBS protocols and demonstrate that GBS provides significant experimental advantages over current experimental realisations.

Our paper is structured as follows. In Sec. II, we review the main points of the AABS protocol. In Sec. III, we derive the closed-formula expression that connects the probability to measure a specific photon output pattern from a general Gaussian state. Next, in Sec. IV, we comment on the complexity of the Hafnian and go into detail on the construction of our GBS protocol with single-mode squeezed states. Section V summarizes our arguments for the hardness of approximate GBS, and we derive several requirements for an experiment in Sec. VI. In Sec. VII, we introduce a regime of GBS where we allow for possibly different squeezed states, which allows us to sample from any symmetric matrix. Additionally, in Sec. VIII, we show that the most widely known protocol, SBS, is a specialized subclass of GBS problems and compare the experimental feasibility of our GBS protocol with existing experimental approaches in Sec. IX. Finally, we give some conclusions in Sec. X.

II. REVIEW: AABS

In this section, we briefly review the original proposal by Aaronson and Arkhipov (AABS) [1,2]. Specifically, we are interested in an outline of their hardness proof, as we base our arguments for approximate GBS (Sec. V) on this. For the AABS scheme, shown in Fig. 1(a), N pure, single photons are inserted into the first N modes of an $M = O(N^2)$-dimensional Haar random interferometer $\mathbf{T}$. At the output, we measure the number of photons in each mode, generating the photon pattern $\bar{n} = n_1 n_2 \ldots n_M$, where n_j is the number of photons in the jth mode, thereby sampling the output distribution of the device. It is assumed that all the photons leave in different modes, giving $\binom{M}{N}$ different output patterns. The probability to measure a specific photon pattern $\bar{n}$ is given by the permanent of the sampled submatrix of $\mathbf{T}$, which we call $\mathbf{T}_S$

$$\Pr(\bar{n}) = |\mathrm{Perm}(T_S)|^2 = \left| \sum_{\sigma \in P_N} \prod_{i=1}^{N} T_{S_{i,\sigma(i)}} \right|^2 . \tag{1}$$

Here, P_N are all permutations of size N. The process for constructing the submatrix $\mathbf{T}_S$ is illustrated for three photons in Fig. 1(b). We select the columns of $\mathbf{T}$ corresponding to the position of the input photons and the rows of $\mathbf{T}$ corresponding to the output positions [20]. It is the intersection of these rows and columns that selects the entries of the matrix $\mathbf{T}_S$.

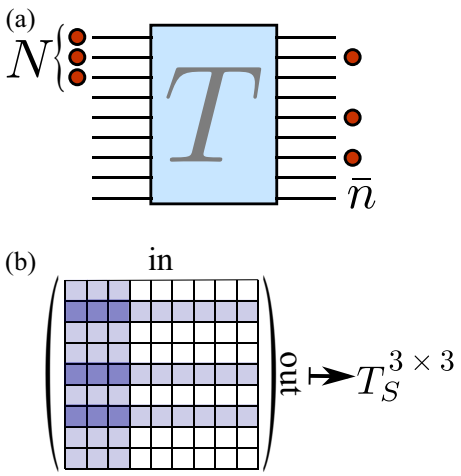

FIG. 1. (a) AABS scheme: N photons are injected in the first N input modes of an interferometer $\mathbf{T}$ and the output patterns $\bar{n}$ are sampled. The corresponding probability for a particular pattern $\bar{n}$ depends on the permanent of the sampled submatrix $\mathbf{T}_S$. (b) A typical construction of the sampled submatrix $\mathbf{T}_S$ for three photons where the first three columns are preset by the input modes and the rows are selected by the output pattern $\bar{n}$. The matrix elements given by their intersections define the submatrix $\mathbf{T}_S$.

The key point of AABS is that the permanent is, in computational complexity theory, a #P-complete problem, which means that it cannot be efficiently computed on a classical machine. Therefore, the calculation of all output pattern probabilities should also fall into the #P complexity class, and thus the output of the device cannot be efficiently sampled by a classical machine. To prove this claim, AA prove two main theorems, one for the exact sampling from such a distribution (i.e., from the exact probability distribution $\mathcal{D}_A$) and one for approximate sampling (from an approximation of $\mathcal{D}_A$, i.e., $\mathcal{D}'_A$). In Sec. V, we recall the main arguments of their complexity proof for the second theorem, i.e., the approximate sampling, and introduce arguments for approximate GBS, one of which is based upon the AA proof and another that is unique to GBS.

III. PHOTO COUNTS FROM A GAUSSIAN STATE

In this section, we derive the probability to measure photons from a general Gaussian state and derive the closed-formula expression for the probability to measure a specific photon output pattern $\bar{n}$. We showed in Ref. [19] that this probability is related to the Hafnian [21,22] of a submatrix $\mathbf{A}_S$, which is dependent upon the covariance matrix of the measured state. This result is the equivalent to the result for Fock states (e.g., Ref. [20]), which provides the foundation for boson sampling schemes with single photons.

The probability of a photon pattern is found by calculating the overlap of our Gaussian state $\hat{\rho}$ with the number state operator $\hat{\bar{n}} = \otimes_{j=1}^{M} \hat{n}_j$, where $\hat{n}_j = |n_j\rangle \langle n_j|$ measures n_j photons in output mode j,

$$\Pr(\bar{n}) = \mathrm{Tr}[\hat{\rho}\, \hat{\bar{n}}]. \tag{2}$$

In the following analysis, we will use the phase-space representation of quantum mechanics [23–25], similar to the approach used in Refs. [18,26]. Equation (2) is now written as the overlap integral of the Q and P functions of the state and measurement operator respectively,

$$\Pr(\bar{n}) = \pi^M \int d\boldsymbol{\alpha} Q_{\hat{\rho}}(\boldsymbol{\alpha}) P_{\bar{n}}(\boldsymbol{\alpha}), \tag{3}$$

where $d\boldsymbol{\alpha} = \prod_{j=1}^{M} d\alpha_j d\alpha_j^*$, $Q_{\hat{\rho}}(\boldsymbol{\alpha})$ is the Q function representation of the Gaussian state [27], and $P_{\bar{n}}(\boldsymbol{\alpha})$ is the P representation [28,29] of the number state operator.

An M-mode Gaussian state can be fully characterized by its $2M \times 2M$ covariance matrix σ and a displacement vector d [23,30]

$$\sigma_{ij} = \tfrac{1}{2}\langle\{\hat{\xi}_i, \hat{\xi}_j^\dagger\}\rangle - d_i d_j^*, \quad d_i = \langle\hat{a}_i\rangle, \tag{4}$$

where $\hat{\xi}_i$ runs over all creation and annihilation operators $\hat{a}_j$, $\hat{a}_j^\dagger$ and we assume $d_i = 0$ for this derivation (we discuss the case $d_i \neq 0$ in Sec. III B). Note that σ here corresponds to the measured modes of the system (i.e., at the output of an interferometer). If we do not measure a mode, then the corresponding rows and columns of that mode are removed from the covariance matrix and the state that remains is also a Gaussian state. From the covariance matrix σ, we can construct the Q function of the state by convolving the corresponding Wigner function with another Gaussian function [24],

$$Q_{\hat{\rho}}(\alpha) = \frac{1}{\sqrt{|\pi\sigma_Q|}} \exp\left[-\frac{1}{2}\alpha_\nu^\dagger \sigma_Q^{-1} \alpha_\nu\right], \tag{5}$$

where $\sigma_Q = \sigma + \mathbb{I}_{2M}/2$ with $\mathbb{I}_{2M}$ is the $2M \times 2M$ identity matrix and $\alpha_\nu = [\alpha_1, \alpha_2 \ldots \alpha_M, \alpha_1^*, \alpha_2^* \ldots \alpha_M^*]^t$. The P function of the n-photon number state $|n\rangle\langle n|$ is [31]

$$P_n(\alpha) = \frac{e^{|\alpha|^2}}{n!}\left(\frac{\partial^2}{\partial\alpha\partial\alpha^*}\right)^n \delta(\alpha)\delta(\alpha^*), \tag{6}$$

where $\delta(\alpha)$ is the two-dimensional Dirac δ function $\delta(\alpha) = \delta(\mathrm{Re}(\alpha))\delta(\mathrm{Im}(\alpha))$. When we insert these into Eq. (3) and perform integration by parts, we arrive at

$$\Pr(\bar{n}) = \frac{1}{\bar{n}!\sqrt{|\sigma_Q|}} \prod_{j=1}^{M}\left(\frac{\partial^2}{\partial\alpha_j\partial\alpha_j^*}\right)^{n_j} \exp\left[\frac{1}{2}\alpha_\nu^t \mathbf{A}\alpha_\nu\right]\Bigg|_{\alpha_\nu=0}, \tag{7}$$

where we have defined

$$\mathbf{A} = \begin{pmatrix} 0 & \mathbb{I}_M \\ \mathbb{I}_M & 0 \end{pmatrix}\left[\mathbb{I}_{2M} - \sigma_Q^{-1}\right]. \tag{8}$$

We have switched from $\alpha_\nu^\dagger$ in (5) to α_ν^t in (7) ($\alpha_\nu^t = \alpha_\nu^\dagger P$, with P as a permutation matrix). We introduce P only to reorder the vector $\alpha^\dagger$ and thus simplify the final expression.

In order to evaluate the expression in Eq. (7), we expand the derivatives using Faà di Bruno's formula, a higher order chain rule [32]. For now, to stay in the typical boson sampling framework, we restrict ourselves to measure either $n_j = \{0, 1\}$ photons at each output mode (we will discuss higher photon numbers in a single output mode in Sec. III A). For N measured photons, in total we have $2N$ derivatives ($\partial\alpha_j$, $\partial\alpha_j^*$ per photon) in Eq. (7), each having an index j (for α_j) and $j + M$ (for α_j^*). The expansion of the derivatives yields [33]

$$\frac{\partial^{2N} e^{\frac{1}{2}\alpha_\nu^t \mathbf{A}\alpha_\nu}}{\prod_i^N \partial\alpha_i\partial\alpha_i^*} = e^{\frac{1}{2}\alpha_\nu^t \mathbf{A}\alpha_\nu} \sum_{\substack{j=1 \\ \pi_j \in \{2N\}}}^{|\pi|} \left(\prod_{\substack{k=1 \\ B_k \in \pi_j}}^{|\pi_j|} \frac{\partial^{|B_k|}\alpha_\nu^t \mathbf{A}\alpha_\nu}{\prod_{\substack{l=1 \\ l \in B_k}}^{|B_k|} \partial\alpha_l^{(*)}} \right), \tag{9}$$

where the first sum runs over all partitions π_j (where $|\pi|$ represents the number of partitions) of the set $\{\alpha_i^{(*)} = \alpha_i, \alpha_i^*\}$ (size $2N$) and the first product over B_k is over all k blocks of the partition π_j (the number of blocks of π_j is $|\pi_j|$). The partial derivative is formed from the size of the block $|B_k|$ (the number of indices contained within B_k), which gives the order of the derivative and is differentiated with respect to the elements of that block, the α_l or α_l^*.

The expansion of the derivatives can therefore be related to the different partitions of the set of photon indices. To illustrate this point, we consider the case when a single photon is detected in both modes 1 and 2, and thus we have to find all partitions of the set of indices $\{\alpha_1, \alpha_1^*, \alpha_2, \alpha_2^*\}$. One such partition, $\{\alpha_1\}, \{\alpha_1^*, \alpha_2, \alpha_2^*\}$, corresponds to the term in the derivative expansion

$$\frac{\partial\alpha_\nu^t \mathbf{A}\alpha_\nu}{\partial\alpha_1} \frac{\partial^3\alpha_\nu^t \mathbf{A}\alpha_\nu}{\partial\alpha_1^*\partial\alpha_2\partial\alpha_2^*}. \tag{10}$$

When calculating the derivatives of $\alpha_\nu^t \mathbf{A}\alpha_\nu$ in Eq. (7), we find that, as it is a quadratic function of α_ν, all derivatives of third order or higher vanish. In addition, since we evaluate the derivatives at $\alpha_\nu = 0$, all derivatives of first order also vanish. Therefore, the only partitions that contribute to the overall probability are ones where the $2N$ elements are sorted into N sets, each of size 2. This means that, in the above formalism, for $2N$ variables, $|\pi_j| = N\,\forall j$, $|B_k| = 2\,\forall k$ and the number of partitions is $|\pi| = (2N-1)!!$, where $(.)!!$ denotes the double factorial,[1] the product over all odd numbers less than or equal to $2N-1$.

These partitions π_j (of $2N$ numbers into N blocks of size 2) can be interpreted as permutations of the $2N$ photon indices, which can be stored in a vector μ_j. For each partition, the blocks are ordered with respect to their smallest element (lowest to highest) and the numbers within a block are also ordered in increasing size. In terms of the permutation vector μ_j, these conditions can be written as

$$\mu_j(2k-1) < \mu_j(2k),$$
$$\mu_j(2k-1) < \mu_j(2k+1),$$

for $k = 1, \ldots, N$. The set of permutations that satisfy these conditions are known as the perfect matching permutations (PMP) [34] and there are $(2N-1)!!$ such permutations (or partitions).[2]

[1] In the case, where the argument of the double factorial is even, $(2N)!!$, the product runs over all even numbers less than or equal to $2N$.

[2] E.g., for $N = 2$ photons detected in modes 3 and 4 of a $M = 4$ mode unitary, we have to consider the set of indices $\{3, 4, 7, 8\}$. The number of PMP is $(2N-1)!! = 3$. The partitions (and permutations)

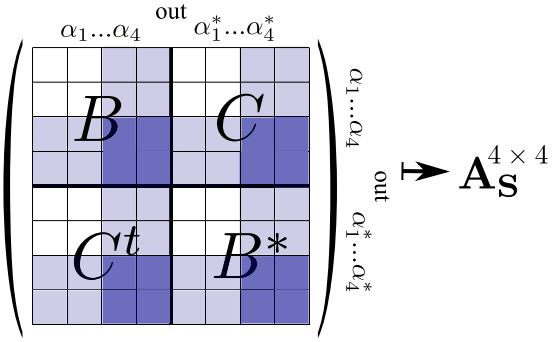

FIG. 2. Construction of the submatrix $\mathbf{A}_S$ from the state matrix $\mathbf{A}$ for two photons measured in last two output modes 3 and 4 of an $M = 4$ mode interferometer. Contrary to the Fock boson sampling schemes, the selection of the matrix entries in $\mathbf{A}_S$ is independent of the input state and only depends upon the output photon pattern, $\bar{n}$. For details, see text.

With this definition, we are now able to write down the final result for Eq. (7),

$$\Pr(\bar{n}) = \frac{1}{\bar{n}!\sqrt{|\sigma_Q|}} \sum_{\mu_j \in \{PMP\}}^{(2N-1)!!} \prod_{k=1}^{N} \mathbf{A}_{\mu_j(2k-1),\mu_j(2k)} \,. \tag{11}$$

The indices of the measured photons' position, stored in μ, define $\mathbf{A}_S$, a submatrix of $\mathbf{A}$. The sum in (11), over all PMP of $\mathbf{A}_S$, is exactly the Hafnian of that matrix, as defined by Caianiello [21,22]. As such, we are able to write down a closed-form expression that connects the probability to measure a specific output pattern $\bar{n}$ from any Gaussian state with the Hafnian matrix function [19]

$$\Pr(\bar{n}) = \frac{1}{\bar{n}!\sqrt{|\sigma_Q|}} \mathrm{Haf}(\mathbf{A}_S) \,. \tag{12}$$

This formula, due to the nature of the Hafnian function, constitutes the basis for a truly GBS protocol, which we discuss in the next section.

As $\mathbf{A}$ is a symmetric matrix of dimension $2M \times 2M$ (due to the structure of the initial covariance matrix), it can be divided into four blocks of dimension $M \times M$, as indicated in Fig. 2. The structure of $\mathbf{A}$ is a combination of the squeezed and thermal contributions present in the state. However, if we only have squeezed light present in the state, then $\mathbf{C} = 0$ and $\mathbf{B} \neq 0$, and if we only have thermal light, then the opposite is true, $\mathbf{B} = 0$, $\mathbf{C} \neq 0$. For the latter case, our formalism reproduces the results for thermal states derived in Ref. [18] by using a matrix identity for the Hafnian [35] [cf. Eq. (24)]. The construction of the submatrix $\mathbf{A}_S$ depends only on the measured output pattern [compare Figs. 1(a) and 2], in contrast to standard boson sampling schemes. Any detected N-photon event then selects a $2N \times 2N$ submatrix, where a detected photon in mode j selects the columns j and $j + M$ of $\mathbf{A}$ and the rows with the same indices. This is illustrated for a two-photon example[3] by the blue bars in Fig. 2.

A. Multiple photons in the same mode

In the above derivation, we restricted ourselves to the case where we only detect $n_j = \{0, 1\}$ photons per output mode; however, the formalism of Eq. (12) is not limited to this case. To consider the case of having more than one photon per output mode, we have to adapt the submatrix that we sample from. Consider the simplest example, a single-mode system. The system matrix $\mathbf{A}$ is given by

$$\mathbf{A} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}. \tag{13}$$

If we now consider a two-photon detection event in this mode, then Eq. (7) is given by

$$\Pr(n_1 = 2) = \frac{1}{\sqrt{|\sigma_Q|}} \frac{1}{2!} \frac{\partial^2}{\partial \alpha_1^2} \frac{\partial^2}{\partial \alpha_1^{*2}} e^{\frac{1}{2}\alpha_v^t \mathbf{A} \alpha_v} \Big|_{\alpha_v = 0} . \tag{14}$$

Terms like this are not covered directly by the calculation of the Hafnian. We can circumvent this problem by artificially "moving" this photon to another "psuedomode" and forming a new matrix $\mathbf{A}'$ by repeating the corresponding rows and columns of $\mathbf{A}$; i.e., we write

$$\Pr(n_1 = 1, n_2 = 1) = \frac{1}{2!\sqrt{|\sigma_Q|}} \frac{\partial}{\partial \alpha_1} \frac{\partial}{\partial \alpha_1^*} \frac{\partial}{\partial \alpha_2} \frac{\partial}{\partial \alpha_2^*} e^{\frac{1}{2}\alpha_v^t \mathbf{A}' \alpha_v} \Big|_{\alpha = 0} , \tag{15}$$

where we have defined $\mathbf{A}'$ as a new matrix constructed as

$$\mathbf{A}' = \begin{pmatrix} A_{11} & A_{12} & A_{11} & A_{12} \\ A_{21} & A_{22} & A_{21} & A_{22} \\ A_{11} & A_{12} & A_{11} & A_{12} \\ A_{21} & A_{22} & A_{21} & A_{22} \end{pmatrix}. \tag{16}$$

This can be repeated for each extra photon in that mode, such that there is always one mode per photon and $\mathbf{A}'$ is $2N \times 2N$ matrix. Note that $\mathbf{A}'$ is not a proper quantum covariance matrix. We only define it as a way to use the Hafnian expression for higher order photon-detection events.

B. Nonzero displacement

Finally, we analyze the situation where we consider a nonzero displacement in our state; i.e., we allow for $d_j \neq 0$ in Eq. (4). In this case, the Q function for a displaced, multimode Gaussian state (squeezed and thermal contributions) is

are then

$$\pi_1 = \{34\}\{78\},\ \pi_2 = \{37\}\{48\},\ \pi_3 = \{38\}\{47\},$$
$$\mu_1 = 3, 4, 7, 8\ \ \mu_2 = 3, 7, 4, 8\ \ \mu_3 = 3, 8, 4, 7.$$

[3] In this case, where photons detected in modes 3 and 4 from $M = 4$ overall modes, select the 4×4 submatrix

$$\mathbf{A}_S^{4\times 4} = \begin{pmatrix} A_{33} & A_{34} & A_{37} & A_{38} \\ A_{43} & A_{44} & A_{47} & A_{48} \\ A_{73} & A_{74} & A_{77} & A_{78} \\ A_{83} & A_{84} & A_{87} & A_{88} \end{pmatrix}.$$

given by

$$Q(\alpha,\alpha^*)=\frac{1}{\sqrt{|\sigma_Q|}}\exp\left[-\frac{1}{2}(\alpha_\nu-d_\nu)^\dagger\sigma_Q^{-1}(\alpha_\nu-d_\nu)\right]. \tag{17}$$

Expanding the exponent yields

$$\begin{aligned}&-\tfrac{1}{2}(\alpha_\nu-d_\nu)^\dagger\sigma_Q^{-1}(\alpha_\nu-d_\nu)\\&\quad=-\tfrac{1}{2}d_\nu^\dagger\sigma_Q^{-1}d_\nu-\tfrac{1}{2}\alpha_\nu^\dagger\sigma_Q^{-1}\alpha_\nu+F\alpha_\nu\,,\end{aligned} \tag{18}$$

where we defined $F=d_\nu^\dagger\sigma_Q^{-1}$. Inserting this into Eq. (3) [or (7)], we arrive at

$$\begin{aligned}\Pr(\bar n)=&\frac{\exp\left[-\frac{1}{2}d_\nu^\dagger\sigma_Q^{-1}d_\nu\right]}{\bar n!\sqrt{|\sigma_Q|}}\\&\times\prod_{j=1}^{M}\left(\frac{\partial^2}{\partial\alpha_j\partial\alpha_j^*}\right)^{n_j}\exp\left[\frac{1}{2}\alpha_\nu^t\mathbf{A}\alpha_\nu+F\alpha_\nu\right]\Bigg|_{\alpha_\nu=0}.\end{aligned} \tag{19}$$

As $F\alpha_\nu$ is a linear function of α_ν we have extra, first-order terms that are nonzero in the expansion of the derivatives (9), when compared to the squeezing-only case (10). For example, it is now possible that partitions of the form $\{\alpha_1\},\{\alpha_1^*\},\{\alpha_2\},\{\alpha_2^*\}$ or $\{\alpha_1\},\{\alpha_1^*\},\{\alpha_2,\alpha_2^*\}$ will contribute to the overall probability. These partitions, respectively, lead to terms in the expansion of the derivatives

$$\frac{\partial F\alpha_\nu}{\partial\alpha_1}\frac{\partial F\alpha_\nu}{\partial\alpha_1^*}\frac{\partial F\alpha_\nu}{\partial\alpha_2}\frac{\partial F\alpha_\nu}{\partial\alpha_2^*}=F_1F_{1+M}F_2F_{2+M}\qquad\text{and}$$

$$\frac{\partial F\alpha_\nu}{\partial\alpha_1}\frac{\partial F\alpha_\nu}{\partial\alpha_1^*}\frac{\partial^2\alpha_\nu^\dagger A\alpha_\nu}{\partial\alpha_2\partial\alpha_2^*}=F_1F_{1+M}A_{2,2+M}$$

(and we have ignored contributions that evaluate to zero at $\alpha_\nu=0$). Re-examining Eq. (9), we now have a total number of partitions

$$|\pi|=\sum_{k=0}^{N}\binom{2N}{2k}[2(N-k)-1]!! \tag{20}$$

instead of $(2N-1)!!$. The individual partitions are formed by first taking $2k$ of the $2N$ variables, to give $2k$ single-index partitions and then $N-k$ double-index partitions. This subset gives us a product of the first-order terms F_j, corresponding to those indices within the subset. The remaining $2N-2k$ indices give us a submatrix of A, and we calculate the Hafnian of this submatrix. We can write each partition of the $2N$ numbers as

$$\pi_j=\bigcup_{l=1}^{2k}B_l^1\bigcup_{l'=1}^{2N-2k}B_{l'}^2, \tag{21}$$

where B^1 are the single-index blocks of π_j and B^2 are the blocks of size 2 (as we had before). This leads to a modified expression for the probability of a photon pattern, akin to Eq. (12),

$$\begin{aligned}\Pr(\bar n)=&\frac{e^{-\frac{1}{2}d_\nu^\dagger\sigma_Q^{-1}d_\nu}}{\bar n!\sqrt{|\sigma_Q|}}\sum_{\substack{j=1\\ \pi_j\in\{2N\}}}^{|\pi|}\left[\left(\prod_{\substack{k=1\\ B_j^1\in\pi_j}}^{|B_j^1|}F_k\right)\mathrm{Haf}\left(A_{B_j^2}\right)\right]\\=&\frac{e^{-\frac{1}{2}d_\nu^\dagger\sigma_Q^{-1}d_\nu}}{\bar n!\sqrt{|\sigma_Q|}}\left[\mathrm{Haf}(A_S)+\sum_{j_1,j_2,j_1\neq j_2}F_{j_1}F_{j_2}\mathrm{Haf}\left(A_{S-\{j_1,j_2\}}\right)\right.\\&\left.+\cdots+\prod_{j}^{2N}F_j\right],\end{aligned} \tag{22}$$

where the first sum is over all partitions of the set of $2N$ indices, the product is over all indices in the blocks B_j^1, and the remaining indices in blocks B_j^2 form $A_{B_j^2}$, a submatrix of A, which we then take the Hafnian of.

We can give an interpretation to the terms in Eq. (22). The first term in the sum can be identified as the contribution where all the photons come from the covariance matrix (squeezed and thermal light) and none from displacement operator. The last term only contains the contributions from the displacement operators, i.e., when all the photons come from the coherent state. The intermediate terms mix photons from the squeezed, thermal, and coherent contributions of the state.

In the case where we only have coherent light ($\sigma_Q=\mathbb{I}$), Eq. (22) reduces to

$$\Pr(\bar n)=\frac{e^{-\frac{1}{2}d_\nu^\dagger\sigma_Q^{-1}d_\nu}}{\bar n!\sqrt{|\sigma_Q|}}\prod_{j=1}^{2N}F_j=\frac{e^{-\sum_j|d_j|^2}}{\bar n!}\prod_{j=1}^{N}|d_j|^{2n_j}\,, \tag{23}$$

as expected [24]. Depending on the squeezing and displacement levels in our state, the weights of the respective contributions vary; i.e., for an almost purely squeezed state, the first term will dominate the other terms, and for a large displacement, the last term will dominate the photon counting probability.

IV. CONSTRUCTION OF GBS WITH SQUEEZED STATES

In this section we develop the protocol boson sampling from a Gaussian state. We start by describing the main requirements for a Gaussian boson sampling protocol, and in subsequent sections we comment on the details of such a protocol, including approximate GBS.

The main requirement for Fock boson sampling protocols is the computational complexity of the underlying matrix function, the permanent, which is in the #P complexity class. The Hafnian, also in the #P class [36], is a more general function than the permanent, as the Hafnian counts the number of perfect matchings in a general, undirected graph whereas the permanent is restricted to a bipartite graph. This is encapsulated in the formula

$$\mathrm{Perm}(G)=\mathrm{Haf}\left[\begin{pmatrix}0&G\\G^t&0\end{pmatrix}\right], \tag{24}$$

where we can express the permanent of a matrix G in terms of the Hafnian [35].

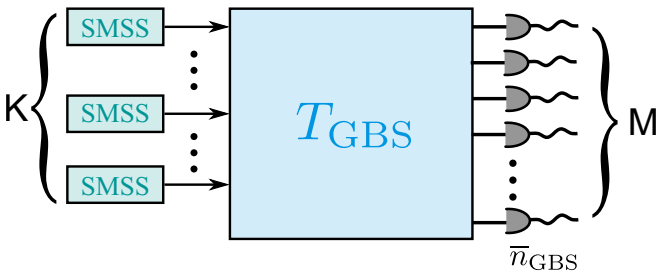

FIG. 3. Schematic of the GBS protocol. We send K single-mode squeezed states into a Haar random interferometer T_{GBS} of size M and sample the output photon distribution $\bar{n}_{\mathrm{GBS}}$ at the end.

Having discussed this necessary requirement for a boson sampling problem, we proceed to construct the GBS protocol based on squeezed states. We use squeezed states, as it is known that thermal states can be approximated in $\mathsf{BPP}^{\mathrm{NP}}$ [18,37], a complexity class easier than #P.

We depict the physical setup of the protocol in Fig. 3, where K single-mode squeezed states enter a linear interferometer $\mathbf{T}_{\mathrm{GBS}}$ and at the output we measure all M modes of the system and record all photo counts. This choice of squeezing and linear transformation leads to $\mathbf{B} \neq 0$ and $\mathbf{C} = 0$ in the overall system matrix $\mathbf{A}$ (see Fig. 2). For this scheme, the matrix $\mathbf{A}$ is defined by the input state and the interferometer $\mathbf{T}_{\mathrm{GBS}}$. The single-mode squeezed states in our system are described by the matrix

$$S = \begin{pmatrix} \bigoplus_{j=1}^{M} \cosh r_j & \bigoplus_{j=1}^{M} \sinh r_j \\ \bigoplus_{j=1}^{M} \sinh r_j & \bigoplus_{j=1}^{M} \cosh r_j \end{pmatrix}, \tag{25}$$

where r_j is the squeezing parameter of the single-mode squeezed states in the jth mode and $\bigoplus_{j=1}^{M} x_j = \mathrm{diag}(x_1, x_2, \ldots, x_M)$, a direct sum of numbers, yielding a diagonal matrix. Note that for $M - K$ entries $r_j = 0$, corresponding to a vacuum state input. Then, the covariance matrix at the output of the interferometer is given by

$$\sigma = \frac{1}{2} \begin{pmatrix} T_{\mathrm{GBS}} & 0 \\ 0 & T^{*}_{\mathrm{GBS}} \end{pmatrix} SS^{\dagger} \begin{pmatrix} T^{\dagger}_{\mathrm{GBS}} & 0 \\ 0 & T^{t}_{\mathrm{GBS}} \end{pmatrix} \tag{26}$$

and $\mathbf{A}$ in Eq. (8) is calculated to be $\mathbf{A} = \mathbf{B} \oplus \mathbf{B}^{*}$, with

$$B = T_{\mathrm{GBS}} \left(\bigoplus_{j=1}^{M} \tanh r_j \right) T^{t}_{\mathrm{GBS}} \,. \tag{27}$$

It is easy to show that the Hafnian of a direct sum, as in $\mathbf{A}$, can be written as the product of the Hafnians of the two submatrices. Thus, we can simplify Eq. (12) to

$$\Pr(\bar{n}) = \frac{1}{\sqrt{|\sigma_Q|}} |\mathrm{Haf}(B_S)|^2, \tag{28}$$

where we have restricted ourselves to the measurement outcome of $n_j = \{0, 1\}$ per mode. As $\mathbf{B}_S$ is a submatrix of $\mathbf{B}$, its construction is obtained by keeping the intersection of the rows and columns where a photon was measured, a single index per photon. $\mathbf{B}_S$ will be an even-sized matrix, as physically this corresponds to measuring an even number of photons from the multimode squeezed state. The probability to measure an odd number of photons from such a state is always zero. Note that in the case of odd N, Eq. (12) still applies but the identity (28) is invalid.

Because of the intrinsic complexity of the Hafnian, the complexity of GBS in the exact case is ensured. However, this does not guarantee the complexity for an approximate Gaussian boson sampling protocol, which we discuss next.

A. Complexity of multiple photons in the same mode and displacement contributions

In this section, we comment on the complexity of the two other instances of the GBS expression, that of multiple photons in the same mode and that of the contribution of displaced light.

As shown in the previous section, we can incorporate the measurement result of multiple photons in the same mode by modifying the matrix $\mathbf{A}$. The extra photons can be included by repeating the rows and columns of the original matrix to generate an extended matrix. These extra rows and columns do not increase the rank of the matrix $\mathbf{A}$ and thus do not increase the complexity of calculating the output pattern in the way that detecting a photon in another mode would. While this method allows us to write the expression using the Hafnian, a more computationally efficient method to incorporate multiphoton events was described by Kan [38].

The complexity of measuring photons from a displaced state is in the P complexity class, as the output state can be written as a vector of displacement amplitudes and the probability of photon numbers in each mode is independent of each other. This is in contrast to squeezed or thermal states, where the complexity arises from the correlations between modes. From Eq. (22), the complexity of the combination of squeezed and displaced light still comes from the squeezed light (the Hafnian terms) and therefore displaced light does not increase the complexity of the problem, as expected.

V. APPROXIMATE GBS

In this section, we present the ideas of approximate GBS. First, we briefly recall the main arguments of AA [1] that approximate AABS is a #P-hard problem, as we use a key result of theirs, which is to hide the matrix we wish to sample within a larger unitary transformation. The approximate AABS problem $|\mathrm{GPE}|^2_{\pm}$ states that given a matrix $\mathbf{X} \in \mathbb{C}^{N \times N}$ of independent and identically distributed (i.i.d.) complex normal entries and error bounds ϵ, δ, the estimation of the permanent $|\mathrm{Perm}(X)|^2$ up to an additive error $\pm \epsilon N!$ with a success probability of $1 - \delta$ for any possible $\mathbf{X}$ takes a time polynomial in $(N, 1/\epsilon, 1/\delta)$. The main requirement that the boson sampling computer has to fulfill in this instance is that it is "robust," meaning that if a small fraction ϵ of all events are "badly wrong," the remaining $1 - \epsilon$ results are still valid to encode the boson sampling scheme.

If we suppose that an approximate boson sampling computer works this way, we can use the robust encoding to prevent a classical adversary from corrupting our sampling. The procedure to show that approximate AABS up to an

additive error is hard uses the fact that we hide the interesting probability (i.e., the sampling of a specific $\mathbf{T}_S$) among all the other random outputs of our boson sampling scheme. The solution that AA propose is to choose the $(M \times M)$-dimensional interferometer matrix $\mathbf{T}$ according to the Haar measure. Then, any sufficiently small submatrix is, in variation distance, close to a matrix whose entries are independent and identically drawn from the complex normal distribution. This means that the adversary will not know which instance we are interested in and therefore cannot corrupt the result, on average.

The sampling from such a device is random in the sense that we cannot predict the output pattern of N photons, even if the same input state is used. This choice fulfils the robustness criterion and the need to hide the interesting sampling probability in a multitude of other possible output patterns. Then, using Stockmeyer's counting algorithm [39], AA show that $|\mathrm{GPE}|^2_{\pm}$ is in $\mathsf{BPP}^{\mathsf{NP}^{\mathcal{O}}}$, where $\mathcal{O}$ is an oracle for approximate AABS. If there is an efficient classical algorithm to simulate $\mathcal{O}$, then the polynomial hierarchy will collapse, having severe consequences for the computational complexity theory.

While $\mathsf{BPP}^{\mathsf{NP}}$ is enough to claim that boson sampling is not classically "simple," it remains an open question of whether approximate AABS is indeed in #P. Nevertheless, AA provide evidence in the form of two conjectures, the *permanents-of-Gaussians* conjecture, which says that estimating the permanent up to multiplicative error $\mathrm{GPE}_{\times}$ is in #P. The second *permanent-anticoncentration* conjecture implies a polynomial-time equivalence of the sampling up to additive error $|\mathrm{GPE}|^2_{\pm}$ and the sampling up to multiplicative error $\mathrm{GPE}_{\times}$. If these conjectures hold, this would mean that $\mathsf{P}^{\#\mathsf{P}} = \mathsf{BPP}^{\mathsf{NP}}$, unless approximate AABS is in #P.

A. Approximate GBS

In this section, we discuss approximate GBS. The device we are considering here is a Haar-random interferometer with N^2 modes where we pump N modes with identical squeezed states. With these settings, we consider only those measurement events with N photons in N different output modes. We start by defining our problem:

Problem 1. $|\mathrm{GHE}|^2_{\pm}$. Given as input a matrix $\mathbf{X} \sim \mathbb{CN}(0,1)^{N\times N}$, whose entries are i.i.d. complex Gaussians, together with error bounds $\epsilon, \delta \geqslant 0$, estimate $|\mathrm{Haf}(XX^t)|^2$ to within additive error $\pm\epsilon N!/(cM)^N$ with probability at least $1-\delta$ over $\mathbf{X}$, in $\mathrm{poly}(N, 1/\epsilon, 1/\delta)$ time and $0 < c < 1$ is a parameter dependent upon the number of photons (described in Appendix A).

We can immediately use the result from AA to "hide" $\mathbf{X}$ in $\mathbf{T}_{\mathrm{GBS}}$ that fails with a probability smaller than $\delta/4$. We define O as an oracle for $|\mathrm{GHE}|^2_{\pm}$ if it reproduces the desired distribution, D_A, with an approximate distribution, D'_A, such that the error between the two is given by

$$||D_A - D'_A|| \leqslant \beta \propto \delta\epsilon. \tag{29}$$

Theorem 1. Let $\mathcal{O}$ be an approximate oracle for $|\mathrm{GHE}|^2_{\pm}$. Then, $|\mathrm{GHE}|^2_{\pm} \in \mathsf{FBPP}^{\mathsf{NP}^{\mathcal{O}}}$.

We can prove this theorem by following the same steps as Aaronson and Arkhipov used to prove their Theorem 1.3 (Sec. 5.2 in Ref. [2]) and also the steps shown in the supplemental information of Ref. [12]. This proof is given in Appendix A. As in AABS, if an efficient, classical algorithm exists for $|\mathrm{GHE}|^2_{\pm}$, then $\mathsf{BPP}^{\mathsf{NP}} = \mathsf{P}^{\#\mathsf{P}}$ and the polynomial hierarchy collapses, as in other versions of the boson sampling problem. The extra factor c^N in the definition of this problem represents the nature of GBS and is related to the probability to generate N photons from the squeezed sources and the fact that the unitary matrix appears twice in Eqs. (27) and (28). This increases the size of the error bound, but the expected value of $|\mathrm{Haf}(XX^t)|^2$ scales faster to compensate for this.[4] As in Ref. [2], we must conjecture that approximate GBS is #P hard.

One difference between GBS and other boson sampling protocols is that in the former the number of photons is not fixed (see Secs. VI C and VI D) because of the nature of Gaussian states. We can restrict our device to a fixed photon number at a cost polynomial in that number. This means we can focus on the same class of output states in AABS.

We briefly comment on the regime where identical squeezed states enter every interferometric mode ($M = N^2$). The matrix that is sampled in this case is $\mathbf{B} \propto \mathbf{T}_{\mathrm{GBS}}\mathbf{T}^t_{\mathrm{GBS}}$, which is known as a circular orthogonal matrix [40]. A sufficiently small submatrix of this class has been shown to be close to a matrix of random complex entries, as required for approximate boson sampling. It only remains to show that we can "hide" a certain matrix within the larger matrix $\mathbf{B}$ to prove approximate GBS in this case.

VI. FURTHER REQUIREMENTS

In the previous section, we outlined our arguments that the approximate GBS problem is also in the #P complexity class. However, there are several aspects unique to GBS that must be satisfied to guarantee that the sampling is complex. We now comment on those, as well as on optimal experimental parameters.

A. Number of single-mode squeezed states

For permanents and Hafnians it is known that the matrix rank determines the complexity of the computation [38,41]. The rank of the matrix that we sample in GBS, Eq. (27), is determined by the number of independent single-mode squeezed states (see Appendix B for this proof). This means that if we want to sample N photons, then we have to pump at least $K = N$ input modes with single-mode squeezed states to saturate the complexity. Therefore, we require $K \geqslant N$ single-mode squeezed states at the input of the interferometer.

B. Dilute sampling

In Secs. III and IV, we required that we measure only $n_j = \{0, 1\}$ in each output mode to avoid the repetition of rows and columns in the $\mathbf{B}_S$ matrix. The reason is that these repeated photons do not increase the rank of the sampled matrix and thus the complexity of the boson sampling problem [38]. Therefore, we have to show that the probability to

[4] $E(|\mathrm{Haf}(XX^t)|^2) \propto 2^n n^{3.8n}$ (from numerical simulations).

measure more than one photon in an output mode can be made sufficiently small.

Consider N single-mode squeezed states at the input, each with a mean number of 1 photon ($\sinh^2 r = 1$). Then, if we have an interferometer of size $M = N^2$ that is balanced (all entries are of similar size), we have at the output a mean number of $\frac{1}{N}$ photons per mode. This is due to the interferometer distributing all photons equally on average among the output modes, which a Haar random unitary can provide due to the intrinsic randomness of the Haar measure. If we now examine a single output mode of such a system, tracing over all other modes, we obtain approximately a thermal state with a mean photon number $\langle n \rangle \approx \frac{1}{N}$. As a rule-of-thumb guide to the concentration of photons within the setup, we calculate the ratio between the probability of two or more photo counts versus the probability of one photo count for a single-mode thermal state,

$$\frac{\sum_{n_j \geqslant 2}^{\infty} \Pr(n_j)}{\Pr(n_j = 1)} = \frac{1}{N} \approx \langle n \rangle. \tag{30}$$

The mathematical details of these arguments are given in Appendix C. As the higher order coincidences have a very low probability of occurring, a low-photon-number resolving capability is enough to faithfully exclude higher order events in a single channel. This is the same requirement that SBS has in the heralding part of the scheme.

C. Valid GBS events

In Fock boson sampling experiments, such as AABS, a fixed number of photons enter and exit the linear interferometer **T**. That means that these experiments sample from the family of photon patterns with N photons $\{P_N\}$

$$\left\{p_1, p_2, \ldots, p_{C_N}\right\}_N = \{P_N\}, \tag{31}$$

where p_j is the probability of a particular pattern and $C_N = \binom{M}{N}$ is the number of possible patterns of N single photons in M modes. We discard configurations with more than one photon in any output mode and thus $\sum_j p_j < 1$.

As we use Gaussian states, the number of photons N within the setup is not fixed but is a distribution of even photon numbers, in the range $[0, \infty)$ (in the case of squeezed states with no loss). The mean photon number is finite and in a following section we will discuss how to optimize experimental parameters to maximize a given photon number. Therefore, in GBS we sample from photon pattern families with different total number of photons N,

$$\begin{aligned} &\{\{p_0 = |\sigma_Q|\}_0, \{p_1, p_2, \ldots, p_{C_2}\}_2, \\ &\qquad \ldots, \{p_1, p_2, \ldots, p_{C_{2N}}\}_{2N}, \ldots\} \\ &= \{\{P_0\}, \{P_2\}, \ldots, \{P_{2N}\}, \ldots\} \end{aligned} \tag{32}$$

with $\sum_{N=0}^{\infty}\{P_{2N}\} = 1$.

As with AABS, we must discard events with more than one photon per mode. In addition to this, we also discard events with more photons than are allowed by the size of the interferometer and the regime we are operating in (see Secs. V A and VII). This means that $N < O(\sqrt{M})$ for GBS.

D. Photon number distribution

Given that squeezed states (and Gaussian states in general) produce a distribution of photon numbers and not a definitive number, we now describe that distribution and explain how to maximize the probability of the desired number of photons by adjusting the strength of the single-mode squeezers, given the number of squeezed states. The probability to generate 2ν photons from a single-mode squeezed state [24] can be identified as a negative binomial distribution [42]. The probability distribution to generate 2ν photons from K single-mode squeezed states is then a convolution of the individual distributions and can be calculated using the Fourier transformation of the negative binomial distribution's characteristic function. This probability is then given by

$$\begin{aligned} P_K(2\nu) &= \binom{\nu + K/2 - 1}{\nu} \operatorname{sech}^K(r) \tanh^{2\nu}(r) \\ &= \frac{\Gamma(\nu + K/2)}{\Gamma(K/2)\nu!} \operatorname{sech}^K(r) \tanh^{2\nu}(r), \end{aligned} \tag{33}$$

where $\Gamma(x)$ is the Γ function. The mean number of photons is $K \sinh^2 r$ and the modal number of photons (most common number) is $n_{\text{modal}} = 2\lfloor (K/2 - 1)\sinh^2(r) \rfloor$. An example of this distribution is shown in Fig. 4 for $K = 15$ single-mode squeezed states with equal squeezing parameters, $r_j = r = 0.8814$. With this choice of parameter, the mean photon number per squeezer is $\langle n_{\text{GBS}} \rangle = 1$ and the modal number, highlighted in red, is six photon pair events (or 12 photons).

When designing an experiment, it will be necessary to optimize the squeezing parameter to generate the desired number of photons. This photon number is dependent on the size of the interferometer, M, and the number of input single-mode squeezed states, K, which will be determined by experimental resources. In principle, GBS experiments can operate when the number of single-mode squeezed states is in the range $N \leqslant K \leqslant M = N^2$. Given these parameters, the squeezing parameters of all the single-mode squeezed states (which are assumed to be identical) can be adjusted such that the model number of the distribution (see Fig. 4) is 2ν. To

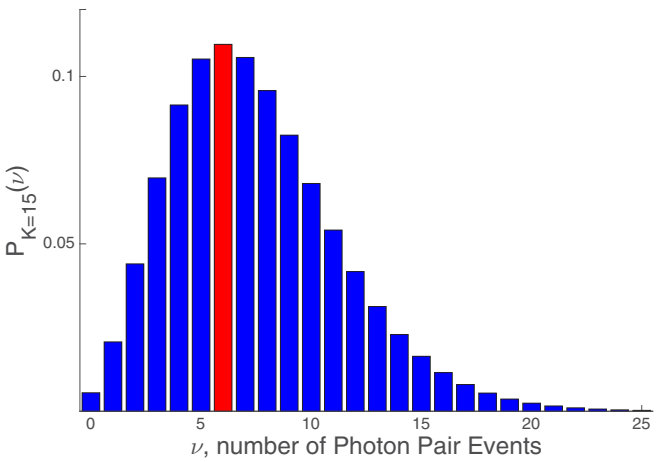

FIG. 4. Probabilities to generate ν photon pair events from $K = 15$ single-mode squeezed states with a squeezing parameter of $r = 0.8814$. The modal number of this distribution is colored red.

do this optimization, we assume that we are only interested in a specific number of photons, 2ν, and we set the squeezing parameters of all the single-mode squeezed states (which are identical) so that this is the modal number of the distribution (meaning that 2ν is the most probable number of photons to be created).

We calculate the scaling of the modal probability with increasing ν for two explicit examples (the details of this calculation are in Appendix D). For $K = 2\nu$ single-mode squeezed states (the minimum number of squeezers that we can have), the modal probability scales as $1/\sqrt{\pi\nu}$. When we pump every mode, $K = M = 4\nu^2$, the modal probability scales as $1/\sqrt{2\pi\nu}$. In both cases, the modal probability decreases as $1/\sqrt{\nu}$, which is only a polynomial cost of photon generation. Note that this is the same scaling as found for SBS [14].

E. Computation time of Hafnian relative to permanent

The main aim of boson sampling protocols is to generate a state that a classical computer cannot simulate in reasonable time; therefore, the relative computational time of the permanent and the Hafnian is important. The permanent of an $N \times N$ matrix can be calculated in $O(N2^N)$ steps, whereas the Hafnian can be calculated in $O(2^{N/2})$ steps [43]. This means that in order to achieve a comparable runtime, GBS has to sample twice the number of photons as other boson sampling schemes. This is comparable to SBS, however, as we have no need for heralding in GBS. This requirement also has implications for the size of the interferometer necessary, which in the worst-case scenario is $4N^2$, a constant increase compared to SBS (where a network of size N^2 is considered).

VII. ALTERNATIVE REGIME FOR GBS

We now describe another mode of operation, unique to GBS. This is motivated by the fact that we have additional control over our system, namely that we can alter the initial input state by the squeezing parameters of the individual single-mode squeezed states, a property which is not present in either AABS or SBS.

In GBS, the matrix that we sample from is given by Eq. (27). This construction, if we can control both $\mathbf{T}_{\mathrm{GBS}}$ and each r_j, means that we can generate *any* symmetric matrix, up to an overall factor, by use of the Autonne-Takagi decomposition [44]. This is a type of singular-value decomposition that factorizes a complex, symmetric matrix into a unitary matrix and a diagonal matrix of positive numbers (in the range $[0, \infty]$.) This means we can adjust our Hafnian problem (from the previous section) to estimate $|\mathrm{Haf}(\Upsilon)|^2_{\pm}$, the Hafnian of a symmetric matrix $\boldsymbol{\Upsilon}$ of random numbers from complex normal distribution (rather than $\mathbf{X}\mathbf{X}^t$ as in the previous section). If we require $\boldsymbol{\Upsilon}$ to be a matrix of complex normal numbers, we can hide this in the larger matrix $\mathbf{B}$, also of complex normal numbers, and not a unitary matrix as before. Therefore, there is no need for a "hiding" lemma, as the whole matrix $\mathbf{B}$ is a user-defined matrix of random numbers and clearly the desired submatrix can be hidden within. We can calculate this larger matrix using the Autonne-Takagi decomposition, which can be done exactly with no approximations needed. Therefore, if we want to sample from a particular matrix $\mathbf{B}$, we find the decomposition $\mathbf{B} = \mathbf{U}\mathbf{D}\mathbf{U}^t$ and then rescale it by $\sqrt{2}\lambda_{\max}$, where $\lambda_{\max}$ is the maximum singular value of $\mathbf{B}$. This is because the $\tanh r_j$ that appear in the diagonal matrix of Eq. (27) can only take values between [0,1] ($r \in [0, \infty]$). The rescaled matrix $\mathbf{D}/(\sqrt{2}\lambda_{\max})$ corresponds to the set $\{\tanh r_j\}$, the squeezing parameters of the initial input states, and $U = T_{\mathrm{GBS}}$, the interferometer that this state enters. We note that any random submatrix of $\mathbf{B}$ will be full-rank for the same reasons as laid out in Appendix B. We now briefly discuss the photon generation probability when we have input states of different squeezing parameters. The convolution of these distributions was studied in Ref. [45], which found an analytical recurrence relation for the probability of $2N$ photons. This distribution is termed a "mixture negative binomial distribution," which is a negative binomial where one of the parameters (in this case, the number of squeezed states) is itself a random parameter. Numerical simulations of this distribution for 20 squeezers with arbitrary squeezing parameters demonstrate that this distribution is shaped like a negative binomial distribution, with a clear peak. Thus, by rescaling the squeezing parameters by an arbitrary constant, the photon number distribution can be shifted to better reach the desired modal number of photons. The scaling of this modal probability with total photon number, necessary to show that a higher number of photons can be created efficiently, remains an open problem.

How large does the matrix $\mathbf{T}_{\mathrm{GBS}}$ need to be to hide a $N \times N$ submatrix within it? Here, we will conjecture that it needs to be only a *linear* factor of N, $M = O(N) = \kappa N$, and not a quadratic relationship as in AABS (and our first argument for approximate GBS in Sec. V A). A significant reason for the quadratic relationship is to ensure that the submatrix that is sampled is close to a random matrix of complex Gaussian numbers, which is now a redundant requirement in this regime, as explained above.

However, a smaller matrix will may complicate two issues: the distributed error for approximate sampling and the occurrence of photon bunching. For the first issue, the size of the set of good outcomes, $G_{M,N}$ (see Appendix A for definitions) still scales exponentially with the number of photons if $M = O(N)$. This means that the error that the adversary adds to the device will be spread across these outcomes, as in AABS.

The second issue is the problem of photon bunching at the output of the device. Photon bunching leads to repeated rows and columns in the matrix argument of both the permanent and Hafnian for boson sampling, as explained in Sec. III A. It has been shown that the computational runtime to calculate the permanent of a matrix with repeated rows and columns is reduced but still has exponential form [46,47]. A similar result for Hafnians has also been shown [38]. This would suggest that the boson sampling is still a #P hard problem for modest levels of photon bunching, in that the complexity depends upon the number of distinct channels occupied, although the tolerable level of photon bunching remains an open question. Thus, the main problem with photon bunching it that it inefficiently uses photon resources. This is less of a problem for GBS due to the nature of photon generation (discussed in a following section below). The full solution for the hardness of approximate GBS in this regime, that takes into account bunching and photon generation, is an open problem.

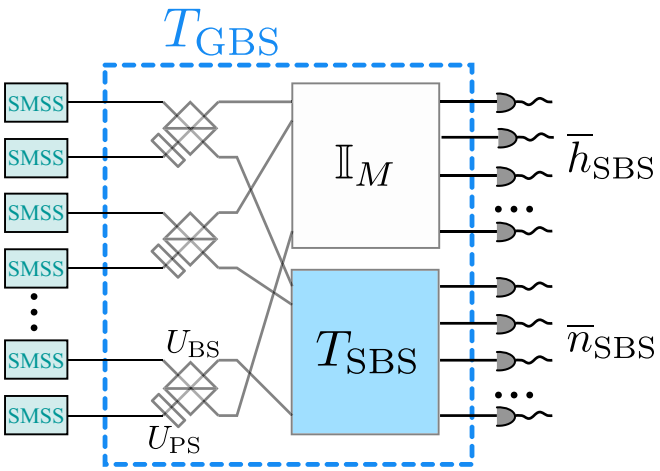

FIG. 5. SBS is a special case of GBS. $2M$ single-mode squeezed states (SMSS) enter an array of phase shifters U_{PS} and beam splitters U_{BS} to transform them to two-mode squeezed states, which are required in SBS. Then, one half of the photons is directly routed to a detection unit to generate the heralding pattern $\bar{h}_{\mathrm{SBS}}$, while the other half enters the interferometer T_{SBS} and generates the sampling pattern $\bar{n}_{\mathrm{SBS}}$. The dashed blue box frames the corresponding GBS interferometer.

VIII. RELATIONSHIP TO SBS

In this section, we now demonstrate the relationship between SBS and GBS, by describing the SBS setup in terms of GBS and can formally show the connection between the two protocols by using the relationship between the permanent and the Hafnian.

Figure 5 shows a typical SBS setup. On the left of the figure, we have $2M$ (identical) single-mode squeezed states, which are then combined, pairwise, at an array of phase shifters, $\mathbf{U}_{\mathrm{PS}}$, and beam splitters, $\mathbf{U}_{\mathrm{BS}}$, that are described by the two unitary transformations

$$U_{\mathrm{PS}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad U_{\mathrm{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{34}$$

This transformation creates the initial M two-mode squeezed states necessary for SBS. One mode of each two-mode squeezed state is sent directly to a set of detectors (i.e., transformed by the identity $\mathbb{1}_M$), where the detection of a photon heralds the presence of the other photon from the photon pair. This latter photon then enters the corresponding input mode of a Haar random interferometer $\mathbf{T}_{\mathrm{SBS}}$, with dimension M, and at the output we measure all modes to detect the position of the photons. This yields two photon patterns at the output, $\bar{n}$ for the sampled photons and $\bar{h}$ for the herald photons.

As the input state is dependent upon the herald pattern, the probability to measure a specific pattern from an SBS experiment is actually a conditional probability, $\Pr(\bar{n}|\bar{h})$. We can relate this to a joint probability using Bayes' theorem. This joint probability, to measure the combined pattern $\bar{n} \cap \bar{h}$, is exactly the probability which we obtain when we consider this specific setup as a GBS experiment,

$$\Pr_{\mathrm{SBS}}(\bar{n}) = \Pr(\bar{n}|\bar{h}) = \frac{\Pr_{\mathrm{GBS}}(\bar{n} \cap \bar{h})}{\Pr(\bar{h})}. \tag{35}$$

The denominator in Eq. (35) is the probability of generating the heralding pattern, which, due to the identity transformation in the herald arm, is simply the probability to generate the total number of photons that $\bar{h}$ represents. We can therefore interpret SBS as a specialized GBS experiment that samples from an interferometer of a very specific shape,

$$T_{\mathrm{GBS}} = \mathbb{I}_M \oplus T_{\mathrm{SBS}} \times \bigoplus_{j=1}^{M} U_{\mathrm{BS}_j} U_{\mathrm{PS}_j}. \tag{36}$$

A more formal proof of this connection between SBS and GBS can be given by using the relationship between the permanent and the Hafnian. We begin with the SBS experiment, where, for simplicity, all M two-mode squeezed states have equal squeezing parameter r and the generated photons then enter the interferometer $\mathbb{I}_M \oplus \mathbf{T}_{\mathrm{SBS}}$. The probability to measure the sampling pattern $\bar{n}$ given a herald pattern $\bar{h}$ is

$$\Pr_{\mathrm{SBS}}(\bar{n}|\bar{h}) = \frac{|\mathrm{Perm}(T_S)|^2}{\bar{n}!\,\bar{h}!} = \frac{\mathrm{Perm}(T_S)\mathrm{Perm}(T_S^*)}{\bar{n}!\,\bar{h}!}, \tag{37}$$

where $\mathbf{T}_S$ is the submatrix that is constructed from the input and output positions of the photons. Note that the input position of the photons is given by the pattern, $\bar{h}$. To map this probability to our GBS experiments, we have to express the SBS protocol in terms of covariance matrices. The Gaussian output state after the SBS interferometer has the covariance matrix

$$\sigma = \tfrac{1}{2}(\mathbb{I} \oplus T_{\mathrm{SBS}} \oplus \mathbb{I} \oplus T_{\mathrm{SBS}}^*) S_{\mathrm{TM}} S_{\mathrm{TM}}^\dagger (\mathbb{I} \oplus T_{\mathrm{SBS}} \oplus \mathbb{I} \oplus T_{\mathrm{SBS}}^*)^\dagger, \tag{38}$$

where

$$S_{\mathrm{TM}} = \left(\begin{array}{cc|cc} \cosh(r)\,\mathbb{I}_{2M} & & 0_M & \sinh(r)\,\mathbb{I}_M \\ & & \sinh(r)\,\mathbb{I}_M & 0_M \\ \hline 0_M & \sinh(r)\,\mathbb{I}_M & & \\ \sinh(r)\,\mathbb{I}_M & 0_M & & \cosh(r)\,\mathbb{I}_{2M} \end{array}\right), \tag{39}$$

which encodes the operation of the two mode squeezers (the black bars are for better clarity of the four blocks). The order of the modes is

$$[\hat{a}_1, \ldots, \hat{a}_M, \hat{b}_1, \ldots, \hat{b}_M, \hat{a}_1^\dagger, \ldots, \hat{a}_M^\dagger, \hat{b}_1^\dagger, \ldots, \hat{b}_M^\dagger], \tag{40}$$

where $\hat{a}_j$ denotes the M herald modes and $\hat{b}_j$ are the M sampling modes. The probability for a valid GBS event in this interpretation is given by

$$\Pr_{\mathrm{GBS}}(\bar{n} \cap \bar{h}) = \frac{\mathrm{Haf}(\mathbf{A}_S)}{\bar{n}!\,\bar{h}!\sqrt{|\sigma_Q|}}, \tag{41}$$

with $\sqrt{|\sigma_Q|} = \cosh^{2M}(r)$ for M two-mode squeezed states. The matrix $\mathbf{A}_S$ has a simple form and is given by

$$\mathbf{A}_S = -\tanh(r) \begin{pmatrix} 0 & T_S^\dagger & 0 & 0 \\ T_S^* & 0 & 0 & 0 \\ 0 & 0 & 0 & T_S^t \\ 0 & 0 & T_S & 0 \end{pmatrix} = B_S \oplus B_S^*. \tag{42}$$

We can use Eq. (24) to express the Hafnian in terms of the permanent

$$\begin{aligned}\mathrm{Haf}(\mathbf{A}_S) &= \mathrm{Haf}(B_S)\mathrm{Haf}(B_S^*)\\ &= \tanh^{2N}(r)\mathrm{Perm}(T_S)\mathrm{Perm}(T_S^*)\\ &= \tanh^{2N}(r)|\mathrm{Perm}(T_S)|^2\,. \end{aligned} \tag{43}$$

We finally arrive at

$$\mathrm{Pr}_{\mathrm{GBS}}(\overline{n}\cap\overline{h}) = \frac{\mathrm{sech}^{2M}(r)\tanh^{2N}(r)|\mathrm{Perm}(T_S)|^2}{\overline{n}!\,\overline{h}!} \tag{44}$$

and

$$\mathrm{Pr}(\overline{h}) = \mathrm{sech}^{2M}(r)\tanh^{2N}(r). \tag{45}$$

Combining Eqs. (44) and (45) and comparing them to Eq. (37), we can see that

$$\frac{\mathrm{Pr}_{\mathrm{GBS}}(\overline{n}\cap\overline{h})}{\mathrm{Pr}(\overline{h})} = \frac{|\mathrm{Perm}(T_S)|^2}{\overline{n}!\,\overline{h}!} = \mathrm{Pr}_{\mathrm{SBS}}(\overline{n}|\overline{h})\,, \tag{46}$$

as expected. This demonstrates how SBS can be considered as a subset of all possible GBS experiments.

This viewpoint also illustrates why we are allowed to retain multiple photons from the same squeezer. In GBS, we use a coherent superposition[5] over all (even) photon number states. Our ignorance of the input state in the Fock basis allows us to use "paths" where all the photons come from the same squeezer, without being able to distinguish these events from the ones where the photons come from different squeezers. In contrast, in SBS, the herald detectors collapse our input state to a specific one, giving us exact knowledge of this state in the Fock basis.

IX. RATE OF PHOTON GENERATION

In this section, we describe one of the main advantages that GBS has in an experimental implementation, the rate of photon generation. We then compare the GBS scheme to existing Boson sampling implementations.

A. Resource efficiency compared to single-photon schemes

In Sec. VI D, we discussed the probability to generate ν photon pair events from the $K \geqslant 2\nu$ single-mode squeezed states to saturate the complexity of the GBS scheme [Eq. (33)]. In this section, we compare how this probability scales in comparison to existing boson sampling schemes with probabilistic single-photon inputs.

PFBS protocols generate their single-photon input states with a limited number of K two-mode squeezers, where SBS as a special case with N^2 two-mode squeezers. The probability to generate ν photon pair events from K two-mode squeezed states and equal squeezing parameter r is given by the binomial distribution [14]

$$\mathrm{Pr}_{K,\mathrm{PFBS}}(\nu) = \binom{K}{\nu}\mathrm{sech}^{2K}(r)\tanh^{2\nu}(r)\,. \tag{47}$$

The ratio of Eqs. (47) and (33) to generate ν photon pairs from K two-mode squeezed states for PFBS and $2K$ single-mode squeezed states for GBS (as a fair comparison) is (for identical squeezing parameter r)

$$\begin{aligned}\frac{\mathrm{Pr}_{\mathrm{PFBS}}(\nu)}{\mathrm{Pr}_{\mathrm{GBS}}(\nu)} &= \binom{K}{\nu}\left[\binom{K+\nu-1}{\nu}\right]^{-1}\\ &= \frac{K!(K-1)!}{(K-\nu)!(K+\nu-1)!}\\ \Rightarrow \lim_{N\to\infty,K>\nu}\frac{\mathrm{Pr}_{\mathrm{PFBS}}(\nu)}{\mathrm{Pr}_{\mathrm{GBS}}(\nu)} &\approx \left(\frac{K-\nu}{K-1}\right)^{\nu}. \end{aligned} \tag{48}$$

This ratio scales exponentially in favor of GBS, with an improvement of roughly ν^ν. We can explain this behavior by all the possible ways to generate ν photon pairs in total in each protocol. While PFBS is restricted to a single photon pair event per squeezer, GBS is not hindered by this restriction and can use multiple photon pairs from the same squeezers, signified by the extra term $(\nu-1)$ in the binomial factor. In the special case of SBS with $K = N^2$ squeezers, this number converges to Euler's number e.

We also note that in GBS we do not have to implement ν^2 squeezers at the input to saturate the complexity of the sampling problem, but only 2ν. Therefore, compared to SBS, we can save a quadratic factor in the number of squeezers.

B. Comparison to current sources

To compare the GBS approach with existing protocols, we plot the probabilities of obtaining N photons from different types of sources in Fig. 6. We first compare the single-photon efficiency $p = p_{\mathrm{gen}}p_{\mathrm{extr}}$, which we define as the product of the generation probability, p_{gen}, and the extraction probability, p_{extr}, of state-of-the-art solid-state sources from He *et al.* [10] (dashed blue line, $p = 0.247$), Loredo *et al.* [11] (blue dash-dotted line, $p = 0.14$), and Wang *et al.* [9] (densely dashed blue line, $p = 0.284$), where for the latter we use the efficiency of the demultiplexer implemented to inject photons in different inputs of the boson sampler ($p_{\mathrm{gen}} = 0.845$) as an additional factor for the single photon efficiency $p = 0.337p_{\mathrm{gen}}$. All of these approaches converge exponentially to zero for high N and only differ in their single-photon success probability. The green dash-dotted line shows the theoretical SBS scaling to higher photon numbers (proportional to $\frac{1}{\sqrt{N}}$).[6]

Finally, we plot the theoretical scaling of our GBS protocol for $K = N^2$ sources with the green, solid line. We observe the e-fold improvement toward the SBS schemes and the expected $\frac{1}{\sqrt{N}}$ scaling. For comparison, we also show the scaling behavior of an almost perfect single-photon source with

[5]Note that there is no phase relation between single photons, while GBS, in contrast to AABS and SBS, relies on coherent superpositions of photon numbers and thus phase control of the input states is required.

[6]The experimental implementation of Ref. [48] does not use as many photon pair sources as the number of modes (9- and 13-mode unitaries with $K = 6$ photon pair sources); for this reason, we do not report a scaling of their approach.

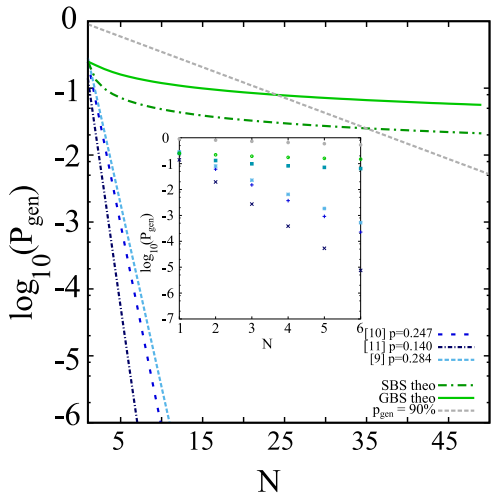

FIG. 6. Comparison of single-photon efficiency for different boson sampling approaches. The first three lines represent the current state of the art with solid-state sources [9–11]. In comparison, we plot the scaling performance of SBS [14] and GBS and an almost optimal deterministic source with 90% efficiency. Even for this high value, GBS ($K = N^2$) is advantageous for more than ≈25 photons and SBS for more than ≈35 photons.

90% generation probability (gray dashed line). Even in this case, the polynomial scaling of the Gaussian protocols allows for better generation probabilities in the high-photon-number regime; the break-even point for GBS is around 25 photons, while the one for SBS is higher with 35 photons. As the "interesting" regime for boson sampling experiments begins around $N = 50$–100 photons [1,7,8], Gaussian protocols are more likely to reach the required photon numbers with reasonable generation rates. Indeed, this break-even point can already be reached with existing sources of parametric down-conversion [49,50].

X. CONCLUSIONS

In this paper, we have demonstrated how to use the full nature of squeezed states to construct a boson sampling protocol and extended our results and analysis from Ref. [19]. First, we derived an expression for the probability to measure a specific photon sampling pattern from a general Gaussian state, which depends upon the Hafnian, a matrix function more general than the permanent. Our work in this paper extends this formula to include displacement contributions, so that all Gaussian states are covered, and we also discussed how to include higher order detection events into our formalism. Following this, we discuss a boson sampling protocol, using squeezed states entering a linear interferometer, which is based on the fact that to calculate the Hafnian is a #P problem. We then propose arguments for why approximate sampling from Gaussian states is also a #P problem and explained the various requirements for the complexity in GBS to be satisfied. Furthermore, we related our protocol to the most general protocol up to date SBS and showed that it is a subset of our GBS scheme. Finally, we compared the theoretical generation probability of GBS with the actual generation rates of current experiments, showing the promise of sampling squeezed states instead of single photons.

Within experimental quantum optics, starting with a squeezed state, using linear optical transformations and post-selecting measurement outcomes is a very common method to create different families of photonic states and is universal for quantum computation. We can model this situation with GBS if we "move" all the measurements to the end of the computation, after the linear optical elements. This means that the GBS protocol includes other photonic boson sampling protocols as special cases, which we have demonstrated here with SBS, but also those problems involving Schrödinger cat states and photon added and subtracted states [51–53]. We also note that due to the time-reversal symmetry of quantum mechanics, GBS also includes the situation of Fock boson sampling with Gaussian measurements [54–56].

Another important aspect in boson sampling schemes is the verification of the correct operation of the device in an efficient manner [57–61]. As the size of the output state space with single photons is exponentially large, full state tomography would be a practically impossible task. In recent works [62,63], statistical averages that can be calculated were used to verify the device operation. As Gaussian states are completely characterized by their covariance matrix, which is of size M^2 and can be efficiently measured [64], then an interesting question is if this information can be used, in combination with the methods developed in the continuous-variable field, to help verify the correct operation of the device.

While boson sampling is demanding and makes use of experiments at their full capabilities, we show here, through GBS, a new regime with advantages that will bring the protocol within the reach of current technology.

ACKNOWLEDGMENTS

This work has received funding from the European Union's Horizon 2020 Research and Innovation Program under the QUCHIP Project Grant No. 641039. C.S.H. and I.J. received support from the Grant Agency of the Czech Republic under Grant No. GACR 17-00844S, Ministry of Education RVO 68407700 and "Centre for Advanced Applied Sciences", Registry No. CZ.02.1.01/0.0/0.0/16_019/0000778, supported by the Operational Programme Research, Development and Education, co-financed by the European Structural and Investment Funds and the state budget of the Czech Republic. The authors thank an anonymous referee for useful suggestions to improve this paper. We also thank A. Arkhipov, T. C. Ralph, A. Björklund, S. Rahimi-Keshari, J. Hilgert, and T. Weich for useful discussions.

APPENDIX A: PROOF THAT $|\mathrm{GHE}|^2_{\pm} \in \mathsf{FBPP}^{\mathsf{NP}^{\mathcal{O}}}$

We can prove this statement by using the same techniques as in Ref. [1]. We wish to estimate the probability of a particular outcome $\bar{n}$ from the distribution D of all outcomes from the matrix $\mathbf{B}$ [Eq. (28) from the main text]

$$B \propto T_{\mathrm{GBS}} \mathbb{I}_N \oplus 0_{M-N} T^t_{\mathrm{GBS}} \Rightarrow B_{\bar{n}} \propto X_{\bar{n}} X^t_{\bar{n}}/M, \tag{A1}$$

where we have used a result from Ref. [1] that a submatrix of the unitary $\mathbf{T}_{\mathrm{GBS}}$ is close to a matrix whose individual

entries are random numbers drawn from the complex normal distribution, rescaled by the size of $\mathbf{T}_{\rm GBS}$, in this case $\mathbf{X}_{\bar{n}}/\sqrt{M}$. The probability of our specific event is then (recall that we have $K = N$ squeezers with identical squeezing parameter r)

$$\Pr_D[\bar{n}] = p_{\bar{n}} = \frac{1}{\sqrt{|\sigma_Q|}}|\mathrm{Haf}(B_{\bar{n}})|^2 = \frac{\tanh^N(r)}{\cosh^N(r)}\left|\mathrm{Haf}\left(\frac{X_{\bar{n}}X_{\bar{n}}^t}{M}\right)\right|^2 = c^N\left|\mathrm{Haf}\left(X_{\bar{n}}X_{\bar{n}}^t\right)\right|^2, \quad \text{(A2)}$$

where we have simplified the factors in front of the Hafnian as c^N $(0 < c < 1)$.

If we assume we have access to an oracle, O, that approximates the distribution D with D',

$$q_{\bar{n}} = \Pr_{D'}[\bar{n}] = \Pr[O(B, 0^{1/\beta}, r) = \bar{n}], \quad \text{(A3)}$$

where the oracle takes a particular submatrix $\mathbf{B}$, error bound β, and bit string r, a source of randomness, which corresponds to which outcome the oracle generates. The distance between the two distributions is defined as

$$\Delta_{\bar{n}} = |p_{\bar{n}} - q_{\bar{n}}|, \quad ||D - D'|| = 1/2\sum_{\bar{n}}\Delta_{\bar{n}} < \beta, \quad \text{(A4)}$$

where $\Delta_{\bar{n}}$ is the error between the actual probability and the approximated probability for a particular outcome $\bar{n}$ and the total error (over all possible outcomes) is upper bounded by β. As in Ref. [1], we show that we can approximate $p_{\bar{n}}$ by using a combination of the oracle and Stockmeyer's counting algorithm. We are only interested in the subset of collision-free states, where all the photons leave in different modes. The size of this subset is $|G_{M,N}| = \binom{M}{N}$, where M is the number of modes and N is number of photons. We now need to show that $p_{\bar{n}}$ and $q_{\bar{n}}$ are close with high probability. The expected size of an individual error is

$$E[\Delta_{\bar{n}}] = \frac{\sum_{\bar{n}}\Delta_{\bar{n}}}{|G_{M,N}|} < \frac{2\beta}{|G_{M,N}|} < 3\beta\frac{N!}{M^N}, \quad \text{(A5)}$$

where the last step is obtained by using Stirling's formula. Then, by using Markov's inequality,

$$\Pr\left[\Delta_{\bar{n}} > 3k\beta\frac{N!}{M^N}\right] < \frac{1}{k} \quad \text{for} \quad k > 1. \quad \text{(A6)}$$

In a GBS protocol, we are interested in calculating the probability of a particular outcome, $\bar{n}^*$, which an adversary may corrupt beyond an acceptable level of noise. The nature of the protocol provides two protections against such an adversary. First, as the matrix we sample is one of a random numbers, an adversary will not learn any information from looking at $\mathbf{T}_{\rm GBS}$, where all submatrices look identical. Next, as the size of $|G_{M,N}|$ is exponentially large, an adversary cannot know, on average, which particular outcome is of interest and therefore cannot corrupt the corresponding $q_{\bar{n}^*}$ to make it sufficiently different from $p_{\bar{n}^*}$, given the bounded level of noise. For these two reasons, we can assume that the expected error for a particular $\Delta_{\bar{n}^*}$ is the same as the average error, $\Delta_{\bar{n}}$. Thus, the above statements about the expected error also hold for a specific outcome $\bar{n}^*$.

The next step in the proof is to use Stockmeyer's counting algorithm to approximate the probability $q_{\bar{n}}$ (with $q'_{\bar{n}}$), which can be done in $\mathsf{FBPP}^{\mathsf{NP}^{\mathcal{O}}}$ with probability

$$\Pr[|q'_{\bar{n}} - q_{\bar{n}}| > \alpha\, q_{\bar{n}}] < \frac{1}{2^M} \quad \text{(A7)}$$

in a time polynomial in M and $1/\alpha$. For that, we need the expected value of $q_{\bar{n}}$,

$$\mathrm{E}[q_{\bar{n}}] = \frac{\Pr(N)}{|G_{M,N}|} < 2\frac{N!}{\sqrt{N}\,M^N}. \quad \text{(A8)}$$

This probability is a product of the probability to be in the "good" space of N photons, $G_{M,N}$ (which scales as $1/\sqrt{N}$; see Appendix D) divided by the size of this space, $|G_{M,N}|$. The probabilities $q_{\bar{n}}$ are lower bounded by $2^{-\mathrm{poly(N)}}$ and therefore can be approximated by Stockmeyer's counting algorithm in poly(M, δ, ϵ). Using Markov's inequality again,

$$\Pr\left[q_{\bar{n}} > 2k\frac{N!}{\sqrt{N}M^N}\right] < \frac{1}{k}, \quad \text{(A9)}$$

and again we can assume that this results also holds for $q_{\bar{n}^*}$ for the same reasons above.

Finally, setting $k = 4/\delta$ and $\epsilon = 6\beta k$, and combining all these steps, it can be shown that

$$\begin{aligned}
&\Pr\left[|q'_{\bar{n}^*} - p_{\bar{n}^*}| > \epsilon\frac{N!}{M^N}\right] \\
&\leqslant \Pr\left[|q'_{\bar{n}^*} - q_{\bar{n}^*}| > \frac{\epsilon}{2}\frac{N!}{M^N}\right] + \Pr\left[|q_{\bar{n}^*} - p_{\bar{n}^*}| > \frac{\epsilon}{2}\frac{N!}{M^N}\right] \\
&\leqslant \Pr\left[q_{\bar{n}^*} > 2k\frac{N!}{\sqrt{N}M^N}\right] + \Pr\left[|q'_{\bar{n}^*} - q_{\bar{n}^*}| > \frac{3\beta}{2}\sqrt{N}q_{\bar{n}^*}\right] \\
&\quad + \Pr\left[\Delta_{\bar{n}^*} > 3k\beta\frac{N!}{M^N}\right] \\
&\leqslant \frac{1}{k} + \frac{1}{2^M} + \frac{1}{k} = \frac{\delta}{2} + \frac{1}{2^M}, \quad \text{(A10)}
\end{aligned}$$

where we have used a result, Eq. (D6), from the supplemental information of Ref. [12],[7] in moving from the first line to the second. In going from the second to third line, we have used Eqs. (A9), (A7), and (A6) respectively. Adding in the probability of failure for the hiding lemma $\delta/4$, we see that the total probability of failure remains less than δ (for large M). This completes the proof. ■

APPENDIX B: PROOF THAT A SUBMATRIX OF $B = U\Gamma U^t$ IS RANK K

$\mathbf{U}$ is a $N^2 \times N^2$ unitary matrix randomly drawn from the Haar measure and $\mathbf{\Gamma}$ is a matrix that has the $K \times K$ identity matrix $(K \geqslant N)$ in the upper left block and zeros elsewhere, with $\mathbf{\Gamma}^2 = \mathbf{\Gamma}$. The (random) position of the measured photons selects a submatrix of $\mathbf{B}$, which can be modeled with a projective matrix $\mathbf{P}$ with either 1 or 0 in each diagonal position, dependent upon whether a row or column is selected. Thus,

[7] The result from Ref. [12] is

$$\Pr[|x - y| > z] \leqslant \Pr[y > z/c] + \Pr[|x - y| > c\,y], \quad (z, c > 0). \quad \text{(A11)}$$

we define

$$X = PU\Gamma, \tag{B1}$$

where we can use the results from AA that the $N \times N$ $\mathbf{X}$ is close to a matrix of i.i.d. complex normal numbers. Then, it can be shown, with probability 1, that $\mathbf{X}\mathbf{X}^t$ is a matrix of full rank [65] as singular matrices exist in a lower dimensional space [due to the constraint $\det(X) = 0$], which, when integrated over, along with the continuous density of the original Haar matrices, will yield zero probability of singular matrices.

APPENDIX C: DERIVATION OF THE BUNCHING PROBABILITY

In this Appendix, we show that the probability of two or more photons in the same output mode is low for the case where we have $M = N^2$ modes. The photon number distribution of a single-mode thermal state is [24]

$$\Pr(n) = \frac{\langle n\rangle^n}{(1+\langle n\rangle)^{n+1}}, \tag{C1}$$

where $\langle n\rangle$ is the mean number of photons of that state and the ratio of collision events to collision-free events is then

$$\frac{\sum_{n\geqslant 2}\Pr(n)}{\Pr(1)} = \langle n\rangle. \tag{C2}$$

We have a mean total number of photons exiting the interferometer $\sum_j \langle n\rangle_j = N$, regardless of the number of squeezers. Thus, the mean photon number per mode is $\langle n\rangle = 1/N$, automatically ensuring a dilute regime of photons at the output (for large N).

APPENDIX D: DERIVATION OF THE MODAL PROBABILITY

The modal number of photons from K single-mode squeezed states, described by the negative binomial distribution (33), is given by

$$n_{\text{modal}} = 2\lfloor (K/2-1)\sinh^2(r)\rfloor. \tag{D1}$$

If we set $n_{\text{modal}} = 2\nu$ photons, then we can rearrange the above equation to

$$\sinh^2(r) \approx \frac{2\nu}{K-2}, \tag{D2}$$

which determines the squeezing strength r of each individual squeezer. Below, we will calculate how the probability of this modal number scales for large photon numbers for two different number of squeezers, $K = 2\nu$ and $K = (2\nu)^2$, i.e., the minimal number and the maximal number of squeezers. Throughout this section, we assume that ν (and thus N) are sufficiently large to make useful approximations in the binomial coefficients.

1. $K = 2\nu$

To ensure the complexity requirements are satisfied when we measure 2ν photons, we must set $K = 2\nu$, and thus $\sinh^2(r) \approx 1$ for large N(or K) from (D1). When we insert this into Eq. (33) and evaluate at 2ν photons, we have

$$P_{2\nu}(2\nu) \approx \binom{2\nu}{\nu}\operatorname{sech}^{2\nu}(r)\tanh^{2\nu}(r) \tag{D3}$$

and using $\binom{2\nu}{\nu} \approx 4^\nu/\sqrt{\pi\nu}$, $\operatorname{sech}^2(r) = 1/2$ and $\tanh^2(r) = 1/2$ yields

$$P_{2\nu}(2\nu) = \frac{4^\nu}{\sqrt{\pi\nu}}\frac{1}{2^\nu}\frac{1}{2^\nu} = \frac{1}{\sqrt{\pi\nu}}. \tag{D4}$$

Thus, the modal probability decreases as $1/\sqrt{\nu}$.

2. $K = 4\nu^2$

We can also calculate the case when we have $K = 4\nu^2$ squeezers (i.e., one in every mode). Then, we have

$$\sinh^2(r) \approx \frac{1}{2\nu}. \tag{D5}$$

Then,

$$P_{4\nu^2}(2\nu) \approx \binom{2\nu^2+\nu}{\nu}\operatorname{sech}^{4\nu^2}(r)\tanh^{2\nu}(r), \tag{D6}$$

and using $\binom{2\nu^2+\nu}{\nu} \approx (2\nu+1)^\nu e^\nu/\sqrt{2\pi\nu}$, $\operatorname{sech}^2(r) = 1+(2\nu)^{-1}$, and $\tanh^2(r) = (2\nu+1)^{-1}$ yields

$$\begin{aligned} P_{4\nu^2}(2\nu) &\approx \frac{(2\nu+1)^\nu e^\nu}{\sqrt{2\pi\nu}}\left(1+\frac{1}{2\nu}\right)^{-2\nu^2}\left(\frac{1}{2\nu+1}\right)^\nu \\ &\approx \frac{1}{\sqrt{2\pi\nu}}. \end{aligned} \tag{D7}$$

Again, the modal probability decreases as $1/\sqrt{\nu}$.

[1] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, 2011), pp. 333–342.

[2] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).

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

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

[5] 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).

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

[7] A. Neville, C. Sparrow, R. Clifford, E. Johnston, P. M. Birchall, A. Montanaro, and A. Laing, Nat. Phys. **13**, 1153 (2017).

[8] P. Clifford and R. Clifford, The classical complexity of boson sampling, in *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms* (Society for Industrial and Applied Mathematics Philadelphia, PA, 2018), pp. 146–155.

[9] H. Wang, Y. He, Y.-H. Li, Z.-E. Su, B. Li, H.-L. Huang, X. Ding, M.-C. Chen, C. Liu, J. Qin *et al.*, Nat. Photon. **11**, 361 (2017).

[10] Y. He, X. Ding, Z.-E. Su, H.-L. Huang, J. Qin, C. Wang, S. Unsleber, C. Chen, H. Wang, Y.-M. He *et al.*, Phys. Rev. Lett. **118**, 190501 (2017).

[11] J. C. Loredo, M. A. Broome, P. Hilaire, O. Gazzano, I. Sagnes, A. Lemaitre, M. P. Almeida, P. Senellart, and A. G. White, Phys. Rev. Lett. **118**, 130503 (2017).

[12] S. Laibacher and V. Tamma, Phys. Rev. Lett. **115**, 243605 (2015).

[13] S. Laibacher and V. Tamma, arXiv:1801.03832 [quant-ph].

[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. Barkhofen, T. J. Bartley, L. Sansoni, R. Kruse, C. S. Hamilton, I. Jex, and C. Silberhorn, Phys. Rev. Lett. **118**, 020502 (2017).

[16] J.-i. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa, APL Photon. **1**, 060801 (2016).

[17] V. Tamma and S. Laibacher, Phys. Rev. A **90**, 063836 (2014).

[18] S. Rahimi-Keshari, A. P. Lund, and T. C. Ralph, Phys. Rev. Lett. **114**, 060501 (2015).

[19] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Phys. Rev. Lett. **119**, 170501 (2017).

[20] S. Scheel, arXiv:quant-ph/0406127.

[21] E. R. Caianiello, Nuovo Cimento **11**, 492 (1954).

[22] E. R. Caianiello, *Combinatorics and Renormalization in Quantum Field Theory* (W. A. Benjamin, New York, 1973).

[23] A. Ferraro, S. Olivares, and M. G. Paris, arXiv:quant-ph/0503237.

[24] S. M. Barnett and P. Radmore, *Methods in Theoretical Quantum Optics* (Oxford University Press, Oxford, UK, 1996).

[25] W. P. Schleich, *Quantum Optics in Phase Space* (John Wiley & Sons, New York, 2011).

[26] V. V. Dodonov, O. V. Man'ko, and V. I. Man'ko, Phys. Rev. A **49**, 2993 (1994).

[27] K. Husimi, Proc. Physico-Math. Society of Japan. 3rd Series **22**, 264 (1940).

[28] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).

[29] E. C. G. Sudarshan, Phys. Rev. Lett. **10**, 277 (1963).

[30] R. Simon, N. Mukunda, and B. Dutta, Phys. Rev. A **49**, 1567 (1994).

[31] C. Gardiner and P. Zoller, *Quantum Noise: A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics*, Vol. 56 (Springer Science & Business Media, Berlin, 2004).

[32] L. Comtet, *Advanced Combinatorics* (D. Reidel, Dordrecht, Netherlands, 1974).

[33] M. Hardy, Electron. J. Combin **13**, 13 (2006).

[34] D. Callan, arXiv:0906.1317.

[35] H. Minc, *Permanents* (Addison-Wesley, New York, 1978).

[36] L. Valiant, Theor. Comput. Sci. **8**, 189 (1979).

[37] L. Chakhmakhchyan, N. J. Cerf, and R. Garcia-Patron, Phys. Rev. A **96**, 022329 (2017).

[38] R. Kan, J. Multivariate Anal. **99**, 542 (2008).

[39] L. Stockmeyer, in *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1983), pp. 118–126.

[40] T. Jiang, J. Math. Phys. **50**, 063302 (2009).

[41] A. I. Barvinok, Math. Op. Res. **21**, 65 (1996).

[42] J. M. Hilbe, *Negative Binomial Regression* (Cambridge University Press, Cambridge, UK, 2011).

[43] A. Björklund, in *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, Philadelphia, PA, 2012), pp. 914–921.

[44] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. (Cambridge University Press, Cambridge, UK, 2013).

[45] E. Furman, Stat. Prob. Lett. **77**, 169 (2007).

[46] S. Aaronson and T. Hance, arXiv:1212.0025 [quant-ph].

[47] S. Chin and J. Huh, Sci. Rep. **8**, 6101 (2018).

[48] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi *et al.*, Sci. Adv. **1**, e1400255 (2015).

[49] G. Harder, V. Ansari, B. Brecht, T. Dirmeier, C. Marquardt, and C. Silberhorn, Opt. Express **21**, 13975 (2013).

[50] G. Harder, T. J. Bartley, A. E. Lita, S. W. Nam, T. Gerrits, and C. Silberhorn, Phys. Rev. Lett. **116**, 143601 (2016).

[51] P. P. Rohde, K. R. Motes, P. A. Knott, J. Fitzsimons, W. J. Munro, and J. P. Dowling, Phys. Rev. A **91**, 012342 (2015).

[52] J. P. Olson, K. P. Seshadreesan, K. R. Motes, P. P. Rohde, and J. P. Dowling, Phys. Rev. A **91**, 022317 (2015).

[53] K. P. Seshadreesan, J. P. Olson, K. R. Motes, P. P. Rohde, and J. P. Dowling, Phys. Rev. A **91**, 022334 (2015).

[54] L. Chakhmakhchyan and N. J. Cerf, Phys. Rev. A **96**, 032326 (2017).

[55] A. P. Lund, S. Rahimi-Keshari, and T. C. Ralph, Phys. Rev. A **96**, 022301 (2017).

[56] U. Chabaud, T. Douce, D. Markham, P. van Loock, E. Kashefi, and G. Ferrini, Phys. Rev. A **96**, 062307 (2017).

[57] C. Gogolin, M. Kliesch, L. Aolita, and J. Eisert, arXiv:1306.3995.

[58] S. Aaronson and A. Arkhipov, arXiv:1309.7460.

[59] J. Carolan, J. D. A. Meinecke, P. J. Shadbolt, N. J. Russell, N. Ismail, K. Wörhoff, T. Rudolph, M. G. Thompson, J. L. O'Brien, J. C. F. Matthews, and A. Laing, Nat. Photon. **8**, 621 (2014).

[60] N. Spagnolo, C. Vitelli, M. Bentivegna, D. J. Brod, A. Crespi, F. Flamini, S. Giacomini, G. Milani, R. Ramponi, P. Mataloni *et al.*, Nat. Photon. **8**, 615 (2014).

[61] M. Bentivegna, N. Spagnolo, C. Vitelli, D. J. Brod, A. Crespi, F. Flamini, R. Ramponi, P. Mataloni, R. Osellame, E. F. Galvão *et al.*, Int. J. Quantum Inform. **12**, 1560028 (2014).

[62] M. C. Tichy, K. Mayer, A. Buchleitner, and K. Mølmer, Phys. Rev. Lett. **113**, 020502 (2014).

[63] M. Walschaers, J. Kuipers, J.-D. Urbina, K. Mayer, M. C. Tichy, K. Richter, and A. Buchleitner, New J. Phys. **18**, 032001 (2016).

[64] J. Řeháček, S. Olivares, D. Mogilevtsev, Z. Hradil, M. G. A. Paris, S. Fornaro, V. D'Auria, A. Porzio, and S. Solimeno, Phys. Rev. A **79**, 032111 (2009).

[65] R. Israel, https://mathoverflow.net/q/110474.