Transition of Anticoncentration in Gaussian Boson Sampling

Adam Ehrenberg,[1,2] Joseph T. Iosue,[1,2] Abhinav Deshpande,[3] Dominik Hangleiter,[1,4] and Alexey V. Gorshkov[1,2]
[1]Joint Center for Quantum Information and Computer Science, NIST/University of Maryland, College Park, Maryland 20742, USA
[2]Joint Quantum Institute, NIST/University of Maryland, College Park, Maryland 20742, USA
[3]IBM Quantum, Almaden Research Center, San Jose, California 95120, USA
[4]Simons Institute for the Theory of Computing, University of California at Berkeley, Berkeley, California 94720, USA

(Received 4 April 2024; revised 28 November 2024; accepted 3 February 2025; published 8 April 2025)

Gaussian boson sampling is a promising method for experimental demonstrations of quantum advantage because it is easier to implement than other comparable schemes. While most of the properties of Gaussian boson sampling are understood to the same degree as for these other schemes, we understand relatively little about the statistical properties of its output distribution. The most relevant statistical property, from the perspective of demonstrating quantum advantage, is the "anticoncentration" of the output distribution as measured by its second moment. The degree of anticoncentration features in arguments for the complexity-theoretic hardness of Gaussian boson sampling. In this Letter, we develop a graph-theoretic framework for analyzing the moments of the Gaussian boson sampling distribution. Using this framework, we show that Gaussian boson sampling undergoes a transition in anticoncentration as a function of the number of modes that are initially squeezed compared to the number of photons measured at the end of the circuit. When the number of initially squeezed modes scales sufficiently slowly with the number of photons, there is a lack of anticoncentration. However, if the number of initially squeezed modes scales quickly enough, the output probabilities anticoncentrate weakly.

DOI: 10.1103/PhysRevLett.134.140601

Quantum sampling problems have attracted a lot of interest given the strong theoretical evidence for an exponential speedup of quantum algorithms over the best possible classical algorithms [1]. Aaronson and Arkhipov introduced one of the most deeply studied sampling frameworks in their seminal work on boson sampling [2]. The boson sampling task is to approximately sample from the outcome distribution of measuring n single photons in m optical modes transformed by a Haar-random linear-optical unitary, which can be implemented as a random network of beam splitters and phase shifters [3]. Aaronson and Arkhipov [2] focused on single-photon input states, but these can be challenging to produce experimentally [4] because existing single-photon sources are not sufficiently reliable to avoid an exponential amount of postselection [5]. Therefore, there has been an interest in generalizing the original boson sampling setup to other input states.

The currently most feasible generalization is Gaussian boson sampling (GBS) [6–9], which uses Gaussian input states. These states are significantly easier to prepare reliably than single-photon states. At the same time, similar statements can be made about the hardness of sampling from the corresponding output distribution [9–12], and several large-scale GBS experiments have been performed recently [13–16].

Broadly speaking, the hardness of boson sampling is based on the connection between output probabilities and the permanent, which is, classically, #P-hard to compute exactly [17]. Similarly, the hardness of GBS arises from the fact that output probabilities are controlled by a generalization of the permanent called the hafnian, while the permanent counts the number of perfect matchings in a weighted bipartite graph, the hafnian counts the number of perfect matchings in an arbitrary weighted graph [18]. Because the hafnian generalizes the permanent, it is also difficult to compute classically.

However, the complexity of classically computing an individual output probability defined in terms of the permanent or the hafnian is not itself sufficient to prove hardness of sampling from the overall probability distributions. The standard hardness argument based on Stockmeyer's algorithm [1,19] requires that outcome probabilities of *random* boson sampling instances be hard to *approximate*. Jointly with provable hardness of nearly exactly computing output probabilities [10], so-called "anticoncentration" of the outcome probabilities serves as evidence for this. Intuitively, if most outcome probabilities are similarly large, then a good classical sampling algorithm needs a very precise estimate of each probability's relative magnitude because all of them are important. Anticoncentration quantifies this idea as, most concisely, the second moment of the outcome probabilities of the GBS distribution (i.e., the probability of getting the same outcome from two independent samples) averaged over the choice of linear-optical unitary and normalized by

the square of the first moment [[1], Sec. IV.D]. While a weak form of anticoncentration holds in boson sampling [2], under what conditions and to which degree anticoncentration holds in GBS is an open question.

In this Letter, we analyze the moments of GBS in the photon-collision-free limit. In this limit, the output distribution is dominated by outcomes with at most a single photon in each mode, and the moments of GBS approximately reduce to moments of squared hafnians of Gaussian random matrices. We show that evaluating those moments reduces to counting the connected components of certain graphs. Using this perspective, we find a closed-form expression for the first moment and derive analytical properties of the second moment. We then identify a transition in anticoncentration in GBS: when the number of initially squeezed modes is large enough compared to the measured number of photons n, a weak version of anticoncentration holds where the normalized average second moment scales as $\sqrt{n}$; when too few modes are initially squeezed, there is a lack of anticoncentration, as this normalized moment scales exponentially in n.

The rest of this Letter proceeds as follows. We first provide background information and set up the system and problem of interest. We then derive the graph-theoretic formalism for computing the first moment of the output probabilities. We proceed to discuss how to apply the formalism to calculate certain properties of the second moment. These results let us finally prove the transition in anticoncentration.

Setup—We consider a photonic system with m modes that is transformed by a Haar-random linear-optical unitary $U \in \mathrm{U}(m)$ acting on the modes of the system; see Fig. 1. In the paradigmatic version of GBS [8,9], the first k of the m modes are prepared in single-mode squeezed vacuum states with equal squeezing parameter r, while the remaining $m-k$ modes are prepared in the vacuum state. After applying U, all m modes are measured in the Fock basis.

Reference [8] proves that, given a unitary U, the probability of obtaining an outcome count vector $\mathbf{n} = (n_1, n_2, \ldots, n_m) \in \mathbb{N}_0^m$ with total photon count $2n = \sum_{i=1}^m n_i$ is given by

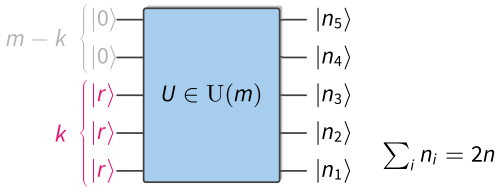

FIG. 1. In GBS, k out of m modes are prepared in single-mode squeezed vacuum states with squeezing parameter r, while the remaining modes are prepared in the vacuum state $|0\rangle$. The modes are then transformed by a Haar-random linear-optical unitary U and measured in the Fock basis with outcome counts n_i summing to $2n$.

$$P_U(\mathbf{n}) = \frac{\tanh^{2n} r}{\cosh^k r} \left|\mathrm{Haf}\left(U^\top_{1_k,\mathbf{n}} U_{1_k,\mathbf{n}}\right)\right|^2, \tag{1}$$

where $U_{1_k,\mathbf{n}}$ denotes the $k \times 2n$ submatrix of U given by its first k rows and the columns selected according to the nonzero entries of $\mathbf{n}$ each copied n_i times [20]. Moreover,

$$\mathrm{Haf}(A) = \frac{1}{2^n n!} \sum_{\sigma \in S_{2n}} \prod_{j=1}^{n} A_{\sigma(2j-1),\sigma(2j)} \tag{2}$$

denotes the hafnian of a $2n \times 2n$ symmetric matrix A.

We work in the regime in which the output states are, with high probability, photon-collision-free, meaning that the output states have at most one photon in each mode, i.e., that $n_i \in \{0, 1\}$ for all i. A sufficient condition for this to be the case is that the expected number of photons $\mathbb{E}[2n] = k\sinh^2(r) = o(\sqrt{m})$ [21]. Reference [10] provides evidence that, in this regime, for any observed photon number $n = o(\sqrt{m})$, the distribution over submatrices is well-captured by a generalization of the circular orthogonal ensemble (COE) [22].

Conjecture 1 (Hiding [10])—For any k such that $1 \leq k \leq m$ and $2n = o(\sqrt{m})$, the distribution of the symmetric product $U^\top_{1_k,\mathbf{n}} U_{1_k,\mathbf{n}}$ of submatrices of a Haar-random $U \in \mathrm{U}(m)$ closely approximates in total variation distance the distribution of the symmetric product $X^\top X$ of a complex Gaussian matrix $X \sim \mathcal{N}(0, 1/m)_c^{k \times 2n}$ with mean 0 and variance $1/m$.

We proceed, assuming that Conjecture 1 is true. Anticoncentration can then be quantified by the inverse of the second moment of the output probabilities normalized by the squared first moment, for an arbitrary outcome $\mathbf{n}$ in the photon-collision-free subspace [23],

$$p_2(k, n) \coloneqq \mathop{\mathbb{E}}_{U \sim U(m)} [P_U(\mathbf{n})]^2 \Big/ \mathop{\mathbb{E}}_{U \sim U(m)} [P_U(\mathbf{n})^2]. \tag{3}$$

We choose this normalization to ensure that the uniform (maximally anticoncentrated) distribution returns a value of 1, but a distribution peaked on a single value (minimally anticoncentrated) returns the inverse of the size of photon-collision-free outcome space. $p_2(k, n)$ lower-bounds the fraction of the outcomes with probability larger than that of the uniform distribution, i.e., those most relevant to the sampling task. For anticoncentrated distributions, this fractional support is constant and thus sufficiently large to reduce the conjectured average-case hardness of relative-error approximation of GBS probabilities to approximate sampling hardness. Conversely, if the fractional support is exponentially small, this reduction breaks because an approximate sampler can assume that nearly all probabilities are zero; see (Ref. [1], Sec. IV.D.2) for details.

This is why we consider different degrees of anticoncentration: we speak of strong anticoncentration if $p_2(k, n) \geq \mathrm{const}$; we speak of weak anticoncentration if

$p_2(k,n) \geq 1/\mathrm{poly}(n)$. If $p_2(k,n) = O(1/n^a)$ for any constant $a > 0$, however, there is a lack of anticoncentration. Together, these definitions capture the relevant regimes with respect to the hardness reduction: a strong version, a weak version, and no version of the reduction work; see Ref. [24] for details.

Conjecture 1 and Eq. (1) allow us to reduce the evaluation of anticoncentration in GBS to a combinatorial problem regarding moments of generalized COE matrices. Let

$$M_t(k,n) \coloneqq \mathop{\mathbb{E}}_{X\sim\mathcal{G}^{k\times 2n}}[|\mathrm{Haf}(X^\top X)|^{2t}] \tag{4}$$

be the tth moment of the squared hafnian as a function of the parameters k and n, where we have abbreviated $\mathcal{N}(0,1)_c^{k\times 2n}$ as $\mathcal{G}^{k\times 2n}$ [25]. Then the inverse normalized second moment of the COE Hafnians

$$m_2(k,n) \coloneqq M_1(k,n)^2/M_2(k,n) \approx p_2(k,n) \tag{5}$$

captures anticoncentration. This equivalence, as well as the details of the above approximations and the relation to different definitions of anticoncentration, are discussed in a companion work to this Letter [24].

First moment and graph-theoretic formalism—We begin by analyzing the (rescaled) first moment M_1 of the output probabilities. In order to derive our graph-theoretic formalism, we use Eq. (2) to expand the hafnian in Eq. (4) as a sum over permutations of a product of matrix elements. From there, the key is to use the fact that the matrix elements are independent complex Gaussian, meaning that $\mathbb{E}_{X\sim\mathcal{G}^k}[X_i X_j^*] = \delta_{ij}$ and $\mathbb{E}_{X\sim\mathcal{G}^k}[X_i X_j] = 0 = \mathbb{E}_{X\sim\mathcal{G}^k}[X_i^* X_j^*]$. This yields

$$M_1(k,n) = \frac{(2n)!}{(2^n n!)^2} \sum_{\tau\in S_{2n}} \sum_{\{o_i\}_{i=1}^n}^{k} \prod_{j=1}^{n} \delta_{o_{\lceil\frac{\tau(2j-1)}{2}\rceil} o_{\lceil\frac{\tau(2j)}{2}\rceil}}. \tag{6}$$

Let us briefly discuss Eq. (6); see Appendix A for details. The sum over $\tau\in S_{2n}$ and the product over index j come from Eq. (2); the sum over the indices $o_i \in [k] \coloneqq \{1,2,\ldots,k\}$ is due to an expansion of $X^\top X$ as a matrix product. Note that, when $\tau(2j-1)$ and $\tau(2j)$ form a tuple $(2\ell-1, 2\ell)$, then the Kronecker δ always equals 1 for index o_ℓ, such that summing over o_ℓ yields a factor of k. When $\tau(2j-1)$ and $\tau(2j)$ do not form such a tuple, we get a nontrivial relationship between indices that decreases the number of independent degrees of freedom, thus decreasing the number of factors of k in τ's contribution. Therefore, to evaluate Eq. (6), one must determine the number of "free indices" of all permutations in S_{2n}. We accomplish this with our graph-theoretic approach.

Specifically, define a graph G_τ as follows [see Fig. 2(a)]. Let G_τ have $2n$ vertices labeled O_1 through O_{2n}. These uppercase vertices are not directly equivalent to the lowercase indices in Eq. (6). Instead, each index o_j splits into two vertices O_ℓ and $O_{\ell'}$ such that $\lceil\tau(\ell)/2\rceil = j = \lceil\tau(\ell')/2\rceil$ (in other words, $o_{\lceil\tau(\ell)/2\rceil}$ maps to a vertex O_ℓ). Let G_τ have a black edge between O_{2j-1} and O_{2j} for all $j\in[n]$, and a red edge between O_ℓ and $O_{\ell'}$ if $\lceil\tau(\ell)/2\rceil = \lceil\tau(\ell')/2\rceil$. These two kinds of edges mimic two types of ways that dependencies in Eq. (6) can be induced through an index j. Red edges identify the ℓ and ℓ' that map to the same value via τ and the ceiling function. Hence, red edges identify which vertices came from the same o index. Black edges identify that Eq. (6) has a Kronecker δ between $o_{\lceil\tau(2j-1)/2\rceil}$ and $o_{\lceil\tau(2j)/2\rceil}$.

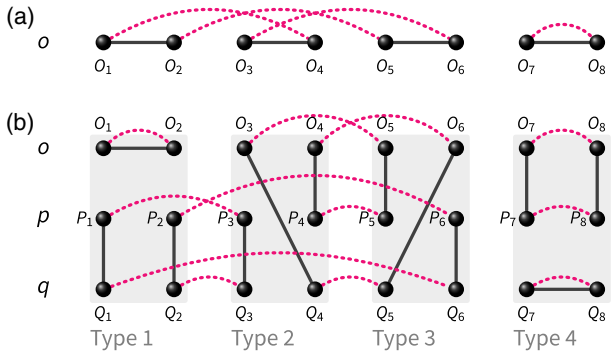

FIG. 2. Examples of graphs used to calculate the (a) first and (b) second moments of GBS outcome probabilities. (a) $G\in\mathbb{G}_4^1$. There are eight vertices O_1 to O_8 representing the index o (labeled in the left column). The black (solid) edges connect only adjacent pairs, whereas the red (dashed) edges form an arbitrary perfect matching. This graph has two connected components, meaning it contributes k^2 to the first moment. (b) $G\in\mathbb{G}_4^2$. The black (solid) edges are, from left to right, Type 1, Type 2, Type 3, and Type 4, as denoted by the gray background. $z = 1+0\times 4^3 + 1\times 4^2 + 2\times 4^1 + 3\times 4^0 = 28$ (this is calculated by converting 0123 from base 4 to base 10 and adding 1 such that the final result is in $[4^4]$). Note that black (solid) edges stay within two adjacent columns. Red (dashed) edges stay within each row and form a perfect matching on each row, thus also forming a perfect matching on the entire graph. This graph contributes k^5 to the second moment, as there are five connected components.

We see, then, that the number of connected components of G_τ, $C(G_\tau)$ is equivalent to the number of free indices in the sum in Eq. (6). Therefore,

$$M_1(k,n) = \frac{(2n)!}{(2^n n!)^2} \sum_{\tau\in S_{2n}} k^{C(G_\tau)}. \tag{7}$$

There is a degeneracy where many permutations induce the same final graph. Each graph has the same fixed set of black edges and then one of $(2n-1)!!$ possible sets of red edges (this is the number of ways of pairing $2n$ elements when order does not matter). For each graph G corresponding to some assignment of the red edges, there are $2^n n!$ permutations τ such that $G_\tau = G$. Therefore, instead of studying G_τ as instantiated by permutations τ, we study the underlying graphs G. Define $\mathbb{G}_n^1$ to be the set of graphs on

$2n$ vertices with one perfect matching defined by the fixed set of black edges and one perfect matching defined by the arbitrary red edges. We can thus rewrite $M_1 = (2n-1)!! \sum_{G \in \mathbb{G}_n^1} k^{C(G)}$ and state our first result.

Theorem 1—The sum over graphs in $\mathbb{G}_n^1$ satisfies

$$\sum_{G \in \mathbb{G}_n^1} k^{C(G)} = k(k+2)\ldots(k+2n-2), \tag{8}$$

and hence $M_1(k,n) = (2n-1)!!(k+2n-2)!!/(k-2)!!$.

The proof proceeds by induction over n, where the inductive step reduces a graph in $\mathbb{G}_n^1$ to one in $\mathbb{G}_{n-1}^1$ through an analysis of the red edge connected to O_1. There are two options for this red edge: either it connects to O_2, the vertex with which O_1 shares a black edge, or it attaches to some $O_{x>2}$. The former creates a connected component of size two; the latter reduces to a graph in $\mathbb{G}_{n-1}^1$ by merging vertices O_1, O_2, and O_x (which does not change the number of connected components). Full details can be found in Appendix A.

Second moment—We now sketch the application of our graph-theoretic formalism to the (rescaled) second moment M_2, deferring the details to the companion piece [24]. We expand $|\mathrm{Haf}(X^\top X)|^4$ using Eq. (2), which becomes a sum of products of matrix elements that are indexed by four permutations in S_{2n}. The independence of matrix elements again enforces that we have an equal number of copies of X_{ij} and X_{ij}^* for the expectation value not to vanish. However, because there are more copies of X and X^*, there are more ways of matching the indices. Accounting for these possibilities leads to an expression analogous to Eq. (6), but with three key differences: (1) instead of summing over a single permutation, we now sum over three permutations, labeled τ, α, β (as in the first moment, one of the original four permutations eventually becomes redundant); (2) instead of summing over n indices $\{o_i\}_{i=1}^n$, we now sum over $3n$ indices $\{o_i, q_i, p_i\}_{i=1}^n$; (3) each factor is now a sum of four possible Kronecker δ terms.

As before, we define a useful set of graphs; see Fig. 2(b) for an example. We expand each index in $\{o_i, q_i, p_i\}_{i=1}^n$ to two graph vertices $\{O_i, Q_i, P_i\}_{i=1}^{2n}$, and we organize them into $2n$ columns and three rows assigned to O, P, and Q vertices, respectively. We then use the Kronecker δs to define black and red edges between these vertices. Fixing permutations τ, α, β, there is a red edge between O_ℓ and $O_{\ell'}$ if $\lceil \tau(\ell)/2 \rceil = \lceil \tau(\ell')/2 \rceil$, and similarly for the P and Q vertices using permutations α and β, respectively. This means that the red edges are constrained to lie within rows in the graph. Furthermore, these red edges again identify the vertices originating from the same index. Because each factor has four Kronecker δ terms, each factor contributes one of four patterns of black edges, which we refer to as Type 1, Type 2, Type 3, and Type 4. The black edges are constrained to lie within pairs of adjacent columns, and they also admit a symmetry between O and Q vertices (arising from the fact that o and q indices stem from X^* terms, whereas p indices stem from X terms [26]). Each graph then has one of 4^n possible sets of black edges indexed by an integer z. We thus call these graphs $G_{\tau,\alpha,\beta}(z)$.

As in the first moment, the number of connected components $C[G_{\tau,\alpha,\beta}(z)]$ of the graph $G_{\tau,\alpha,\beta}(z)$ gives the number of free indices of its corresponding term in the expansion of the hafnian, meaning that graph contributes $k^{C[G_{\tau,\alpha,\beta}(z)]}$ to the sum. The second moment then becomes

$$M_2(k,n) = \frac{(2n)!}{(2^n n!)^4} \sum_{\tau,\alpha,\beta \in S_{2n}} \sum_{z \in [4^n]} k^{C[G_{\tau,\alpha,\beta}(z)]}. \tag{9}$$

We also again use the fact that many permutations induce the same final graph. We thus define $\mathbb{G}_n^2(z)$ to be the set of graphs for the zth set of black edges and $\mathbb{G}_n^2 := \cup_{z \in [4^n]} \mathbb{G}_n^2(z)$. Because there are now three permutations associated to each graph, we obtain a degeneracy factor of $(2^n n!)^3$ and find

$$M_2(k,n) = (2n-1)!! \sum_{G \in \mathbb{G}_n^2} k^{C(G)}. \tag{10}$$

We can now state our second result.

Theorem 2—The second moment $M_2(k,n)$ is a degree-$2n$ polynomial in k and can be written as $M_2(k,n) = (2n-1)!! \sum_{i=1}^{2n} c_i k^i$, where c_i is the number of graphs $G \in \mathbb{G}_n^2$ that have i connected components.

Theorem 2 follows from Eq. (10) and verifying the limits of summation, which we do in the companion piece [24].

Transition in anticoncentration—We now use Theorems 1 and 2 in order to show that anticoncentration in GBS undergoes a transition as a function of k; when $k = 1$, GBS lacks anticoncentration, and when $k \to \infty$ (which, of course, requires $m \to \infty$ as well) it anticoncentrates weakly.

In order to do so, we analyze the polynomial coefficients c_i, observing that for $k = 1$, $M_2(k,n) = (2n-1)!! \sum_{i=1}^{2n} c_i$, and for $k \to \infty$ [27], $M_2(k,n) \approx (2n-1)!! c_{2n} k^{2n}$. The following lemma states our results for these regimes.

Lemma 1—We have that (i) $M_2(1,n) = ((2n-1)!!)^4 4^n$ and (ii) $c_{2n} = (2n)!!$.

Part (i) follows from a simple, direct computation using the expansion of the second moment in terms of Kronecker δs. Part (ii) follows by reducing the graph counting problem to a special instance of the first moment with $k = 2$; this reduction happens because the types of edges that are allowed in order to get $2n$ connected components are quite restrictive.

Theorem 2 and Lemma 1 imply that, when $k = n^0 = 1$, the inverse normalized second moment is negligible,

$$m_2(1,n) = \frac{[(2n-1)!!^2]^2}{(2n-1)!! 4^n} = 4^{-n}. \tag{11}$$

Now, let k be arbitrarily large (in the companion work, we provide evidence for the conjecture that k need only be polynomially large in n, and, even further, that superquadratic scaling is sufficient [24]). Note also that, in order to satisfy the constraint in Conjecture 1, as k increases, the average squeezing per mode r must decrease accordingly. In this limit, $M_2(k,n)$ is dominated by the behavior of its leading order in k, which is $(2n-1)!!(2n)!!k^{2n}$. Additionally, $M_1(k,n) = (2n-1)!!(k+2n-2)!!/(k-2)!! \sim (2n-1)!!k^n$ and, hence, the k dependence of $m_2(k,n)$ vanishes. Using Stirling's approximation on the remaining n dependence yields

$$m_2(k,n) \sim \frac{[(2n-1)!!]^2}{(2n)!} = \frac{(2n)!}{4^n(n!)^2} \sim \frac{1}{\sqrt{\pi n}}. \quad (12)$$

This proves the central claim of our work. In Ref. [24], we also show how anticoncentration of the approximate GBS distribution relates to anticoncentration of the true distribution.

Discussion and conclusion—In this Letter, we have shown a transition in anticoncentration in the output probabilities of GBS as a function of the number of initially squeezed modes. The presence of anticoncentration is additional evidence for the hardness of GBS, and our results thus yield clear advice for experiments in the photon-collision-free regime: given a desired average photon number, distribute the required squeezing for this number across all modes.

Our results give rise to an interesting state of affairs when considered in conjunction with the hiding property: in both GBS and standard boson sampling, the hiding property is known to fail outside of the highly dilute photon-collision-free regime, which is characterized by $m = O(n^2)$ [28,29], while it is conjectured to hold for any $m = \omega(n^2)$ [2,10]. Standard boson sampling anticoncentrates weakly with inverse normalized second moment $1/n$ in the same regime [[2], Lemma 8.8]. The only relevant scale is thus the relative size of the number of modes to the number of photons. In GBS, we now find an additional relevant scale, the number of squeezed modes in the input state. This scale does not seem to be relevant to the hiding property in GBS, which holds for $m = \omega(n^2)$ and *any* k under Conjecture 1, but we find that it is very relevant to the anticoncentration property.

For a potential explanation of the relevance of this scale, we refer to scattershot boson sampling, which is "intermediate" between standard boson sampling and GBS. In scattershot boson sampling, n single photons are distributed randomly across the input modes using postselection on two-mode squeezed states. In order to satisfy photon-collision-freeness in the input state with high probability, the total squeezing in the input needs to be distributed across $\omega(n^2)$ initial squeezed states [6]; see Appendix B for details.

Our results also connect to the classical simulability of GBS. The hafnian of A can be computed in time exponential in the rank of A [30]. The absence of anticoncentration for small $k \ll n$ overlaps with this regime of efficient classical simulability, as the rank of $X^\top X$ is upper-bounded by k.

But does it also extend beyond this regime? While we have proved the existence of this transition, our above work is not sufficient to pin down its precise location. However, we conjecture that weak anticoncentration holds for $k = \omega(n^2)$, but there is a lack of anticoncentration for $k = O(n^2)$. In a companion work [24], we give evidence for this conjecture by fully analyzing the coefficients c_i of $M_2(k,n)$.

Note added—After our paper was posted to the arXiv, Ref. [31] was posted to the arXiv, where the authors also study second moments of Gaussian Boson Sampling.

Acknowledgments—We are grateful to Changhun Oh for sharing his independent calculation of the first moment. We also thank Changhun Oh, Bill Fefferman, Marcel Hinsche, Max Alekseyev, and Benjamin Banavige for helpful discussions, and we thank Marcel Hinsche for comments on an earlier version of the manuscript. This material is based upon work supported by the U.S. Department of Energy, Office of Science, Accelerated Research in Quantum Computing, Fundamental Algorithmic Research toward Quantum Utility (FAR-Qu). Additional support is acknowledged from DARPA SAVaNT ADVENT, AFOSR MURI, DoE ASCR Quantum Testbed Pathfinder program (Award No. DE-SC0019040 and No. DE-SC0024220), NSF QLCI (Award No. OMA-2120757), NSF STAQ program, AFOSR, and NQVL: QSTD:Pilot:FTL. Support is also acknowledged from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. J. T. I thanks the Joint Quantum Institute at the University of Maryland for support through a JQI fellowship. D. H. acknowledges funding from the U.S. Department of Defense through a QuICS Hartree fellowship and from the Simons Institute for the Theory of Computing, supported by DOE QSA.

[1] D. Hangleiter and J. Eisert, Rev. Mod. Phys. **95**, 035001 (2023).
[2] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).
[3] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[4] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, Z. Wang, L. You, J. J. Renema, S. Hoefling, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **123**, 250503 (2019).
[5] D. J. Brod, E. F. Galvão, A. Crespi, R. Osellame, N. Spagnolo, and F. Sciarrino, Adv. Opt. Photonics **1**, 034001 (2019).
[6] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Phys. Rev. Lett. **113**, 100502 (2014).
[7] S. Rahimi-Keshari, A. P. Lund, and T. C. Ralph, Phys. Rev. Lett. **114**, 060501 (2015).

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

[9] R. Kruse, C. S. Hamilton, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Phys. Rev. A **100**, 032326 (2019).

[10] A. Deshpande, A. Mehta, T. Vincent, N. Quesada, M. Hinsche, M. Ioannou, L. Madsen, J. Lavoie, H. Qi, J. Eisert, D. Hangleiter, B. Fefferman, and I. Dhand, Sci. Adv. **8**, eabi7894 (2022).

[11] D. Grier, D. J. Brod, J. M. Arrazola, M. B. d. A. Alonso, and N. Quesada, Quantum **6**, 863 (2022).

[12] U. Chabaud and M. Walschaers, Phys. Rev. Lett. **130**, 090602 (2023).

[13] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Science **370**, 1460 (2020).

[14] H.-S. Zhong *et al.*, Phys. Rev. Lett. **127**, 180502 (2021).

[15] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada, and J. Lavoie, Nature (London) **606**, 75 (2022).

[16] Y.-H. Deng *et al.*, Phys. Rev. Lett. **151**, 150601 (2023).

[17] L. Valiant, Theory Comput. Sci. **8**, 189 (1979).

[18] A. Barvinok, *Combinatorics and Complexity of Partition Functions*, Algorithms and Combinatorics Vol. 30 (Springer International Publishing, Cham, 2016).

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

[20] Note that squeezed states are supported only on even Fock states, so the total photon count $2n$ must always be even.

[21] A. Arkhipov and G. Kuperberg, Geom. Topol. Monogr. **18**, 1 (2012).

[22] Note that, strictly speaking, the conjecture is only formulated for the regime $n \leq k$ in Ref. [10]. However, the evidence provided there for the case $k = n$—Ref. [2] proves that $n \times n$ submatrices of Haar-random unitaries are approximately Gaussian—clearly also holds for the case $k \leq n$.

[23] Note that, as defined, $p_2(k, n)$ depends on some particular outcome $\mathbf{n}$. However, under Conjecture 1, the specific choice of $\mathbf{n}$ does not actually matter.

[24] A. Ehrenberg, J. T. Iosue, A. Deshpande, D. Hangleiter, and A. V. Gorshkov, companion article, Second moment of Hafnians in Gaussian boson sampling, Phys. Rev. A **111**, 042412 (2025).

[25] Note that we consider unit variance because rescaling X by $1/\sqrt{m}$ just leads to an overall prefactor that, like the prefactor in Eq. (1), is irrelevant to the normalized second moment (5).

[26] There is no inherent difference between X and X^*: The symmetry between them is broken when choosing a specific index to use as a reference point in the calculation.

[27] For any n, there exists some sufficiently large k for which the leading order term dominates. The exact required scaling of k with n is investigated more thoroughly in a companion piece (Ref. [24]).

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

[29] T. Jiang, Ann. Probab. **34**, 1497 (2006).

[30] A. Björklund, B. Gupt, and N. Quesada, ACMJ. Exp. Algor. **24**, 1.11:1 (2019).

[31] J. Martínez-Cifuentes, H. de Guise, and N. Quesada, , PRX Quantum **5**, 040312 (2024).

[32] J. M. Arrazola, T. R. Bromley, and P. Rebentrost, Phys. Rev. A **98**, 012322 (2018).

[33] P. Feijão, F. V. Martinez, and A. Thévenin, BMC Bioinf. **16**, S1 (2015).

End Matter

Appendix A: Details of the first moment—Here, we derive Eq. (6) and prove Theorem 1, beginning with the former:

$$\mathop{\mathbb{E}}_{X\sim\mathcal{G}^{k\times 2n}}\left[|\mathrm{Haf}(X^\top X)|^2\right] = \left(\frac{1}{2^n n!}\right)^2 \sum_{\sigma,\tau\in S_{2n}} \mathop{\mathbb{E}}_{X\sim\mathcal{G}^{k\times 2n}} \left[\prod_{j=1}^{n}\left(\sum_{\ell_j=1}^{k} X_{\ell_j\sigma(2j-1)}X_{\ell_j\sigma(2j)}\right)\left(\sum_{o_j=1}^{k} X^*_{o_j\tau(2j-1)}X^*_{o_j\tau(2j)}\right)\right] \tag{A1}$$

$$= \left(\frac{1}{2^n n!}\right)^2 \sum_{\sigma,\tau\in S_{2n}} \mathop{\mathbb{E}}_{X\sim\mathcal{G}^{k\times 2n}} \left[\sum_{\{\ell_i,o_i\}_{i=1}^n=1}^{k}\left(\prod_{j=1}^{n} X_{\ell_j\sigma(2j-1)}X_{\ell_j\sigma(2j)}X^*_{o_j\tau(2j-1)}X^*_{o_j\tau(2j)}\right)\right] \tag{A2}$$

$$= \left(\frac{1}{2^n n!}\right)^2 \sum_{\sigma,\tau\in S_{2n}} \sum_{\{\ell_i,o_i\}_{i=1}^n=1}^{k} \mathop{\mathbb{E}}_{X\sim\mathcal{G}^{k\times 2n}} \left[\left(\prod_{j=1}^{n} X_{\ell_j\sigma(2j-1)}X_{\ell_j\sigma(2j)}X^*_{o_j\tau(2j-1)}X^*_{o_j\tau(2j)}\right)\right] \tag{A3}$$

$$= \left(\frac{1}{2^n n!}\right)^2 \sum_{\sigma,\tau\in S_{2n}} \sum_{\{\ell_i,o_i\}_{i=1}^n=1}^{k} \left(\prod_{j=1}^{n} \delta_{\ell_j o_{j'}}\delta_{\ell_j o_{j''}}\right), \tag{A4}$$

where we have defined j' to be the index such that $\sigma(2j-1) = \tau(2j'-1)$ or $\tau(2j')$ and, similarly, j'' to be the index such that $\sigma(2j) = \tau(2j''-1)$ or $\tau(2j'')$ (note: $j' = j''$ if $\{\sigma(2j-1), \sigma(2j)\} = \{\tau(2j-1), \tau(2j)\}$, which is an equality

of *sets*, meaning order does not matter). The first equation uses Eq. (2), while the second follows from exchanging product and sum, and the penultimate comes from the linearity of expectation. To derive the final equation, recall that the X_{ij} are independent identically distributed complex Gaussian random variables with mean 0 and variance 1. Thus, the expectation of a product of entries vanishes unless there are an equal number of unconjugated and conjugated copies of all entries. By the definition of j', we ensure that the entry $X_{\ell_j \sigma(2j-1)}$ is matched to one of the X^* entries as long as ℓ_j and $o_{j'}$ match, hence the first Kronecker δ. The second Kronecker δ arises similarly.

We can exactly calculate j' by noting $\sigma(2j-1) \in \{\tau(2j'-1), \tau(2j')\} \Leftrightarrow \{\tau^{-1}[\sigma(2j-1)]\}/2 \in \{j'-\frac{1}{2}, j'\}$. Thus, $j' = \lceil \{\tau^{-1}[\sigma(2j-1)]\}/2 \rceil$. Similarly, $j'' = \lceil \{\tau^{-1}[\sigma(2j)]\}/2 \rceil$. Therefore,

$$\mathop{\mathbb{E}}_{X\sim\mathcal{G}^{k\times 2n}}\left[|\mathrm{Haf}(X^\top X)|^2\right] = \left(\frac{1}{2^n n!}\right)^2 \sum_{\sigma,\tau\in S_{2n}} \sum_{\{\ell_i,o_i\}_{i=1}^n=1}^{k} \left(\prod_{j=1}^{n} \delta_{\ell_j o_{\lceil \frac{\tau^{-1}(\sigma(2j-1))}{2} \rceil}} \delta_{\ell_j o_{\lceil \frac{\tau^{-1}[\sigma(2j)]}{2} \rceil}}\right) \tag{A5}$$

$$= \frac{(2n)!}{(2^n n!)^2} \sum_{\tau\in S_{2n}} \left[\sum_{\{\ell_i,o_i\}_{i=1}^n=1}^{k} \left(\prod_{j=1}^{n} \delta_{\ell_j o_{\lceil \frac{\tau^{-1}(2j-1)}{2} \rceil}} \delta_{\ell_j o_{\lceil \frac{\tau^{-1}(2j)}{2} \rceil}}\right)\right] \tag{A6}$$

$$= \frac{(2n)!}{(2^n n!)^2} \sum_{\tau\in S_{2n}} \left[\sum_{\{o_i\}_{i=1}^n=1}^{k} \left(\prod_{j=1}^{n} \delta_{o_{\lceil \frac{\tau(2j-1)}{2} \rceil}, o_{\lceil \frac{\tau(2j)}{2} \rceil}}\right)\right]. \tag{A7}$$

In the first equality, we use the definitions of j', j''. In the second, we notice that τ and σ occur only together as $\tau^{-1}\circ\sigma$, meaning we can perform a change of variables to reduce to a single sum over a redefined $\tau^{-1} \in S_{2n}$ while gaining a factor $(2n)!$. The third equality comes from summing over the ℓ_j indices and redefining $\tau^{-1} \to \tau$. This is Eq. (6).

We now prove Theorem 1 by induction on n. Let $f(k,n)$ be the lhs of Eq. (8). For the base case $n = 1$, there is only a single possible graph G that has a single connected component. Thus $f(k,1) = k$. For the inductive step, which is visualized in Fig. 3, consider two subsets of $\mathbb{G}_n^1$. The first set has graphs that possess a red edge between O_1 and O_2, which means that these two vertices form their own connected component (as O_1 and O_2 are always connected with a black edge). Summing $k^{C(G)}$ over all graphs of this type then yields a contribution of $kf(k,n-1)$. The other subset of $\mathbb{G}_n^1$ contains graphs that possess a red edge between O_1 and a vertex $O_x \neq O_2$. In these graphs, the number of connected components in the graph does not change if one collapses the three vertices O_1, O_2, and O_x into a single vertex (because they are all connected but do not form a full connected component). Therefore, because there are $2n-2$ choices for the vertex O_x linked to O_1 by a red edge, we get an overall contribution of $(2n-2)f(k,n-1)$ when summing $k^{C(G)}$ over these graphs.

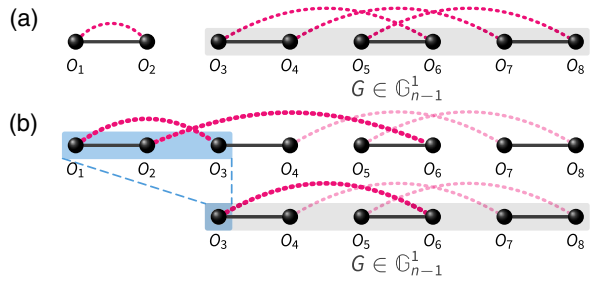

FIG. 3. Visualization of the inductive step in the proof of the first moment, which proceeds in two cases determined by the red edge touching O_1. In (a), the O_1 and O_2, which are linked by a black (solid) edge, are also linked by a red (dashed) edge, meaning they comprise a single connected component. This contributes a factor of k times the contribution from a graph in $\mathbb{G}_{n-1}^1$, which comes from the remaining $2n-2$ vertices and their edges. In (b), O_1 is linked via a red edge to one of $2n-2$ $O_x \neq O_2$ (here, $x = 3$). The number of connected components does not change after identifying and combining O_1, O_2, O_x (visualized by the blue background) into a redefined O_x, meaning we again reduce down to a graph in $\mathbb{G}_{n-1}^1$, but this time without the multiplicative factor of k.

Overall then, we find that

$$f(k,n) = kf(k,n-1) + (2n-2)f(k,n-1) \tag{A8}$$

$$= (k+2n-2)f(k,n-1) \tag{A9}$$

$$= (k+2n-2)(k+2n-4)\ldots(k+2)k, \tag{A10}$$

where the final line uses the inductive hypothesis to complete the proof.

The structure of this proof is similar to the calculation of $\mathbb{E}_{X\sim\mathcal{G}^{n\times n}}[|\mathrm{Haf}X|^4]$ in Ref. [32] (the similarity arises because there are four copies of X in both calculations).

Additionally, similar graphs, and a similar calculation involving enumerating the number of graphs with a given number of connected components, show up in the bioinformatic study of breakpoint graphs used in comparative genomics [33].

Appendix B: Scattershot boson sampling explanation of the transition—In scattershot boson sampling (SBS) [6], $m = \omega(n^2)$ two-mode squeezed vacuum (TMSV) states with squeezing parameter r are prepared. The photon number distribution of a TMSV state is supported on Fock states of the form $|n\rangle|n\rangle$ for $n \in \mathbb{N}_0$. One half of each TMSV is then measured in the Fock basis, yielding, with high probability, an outcome $n_i \in \{0, 1\}$ (assuming r is small enough). Collecting outcomes in the vector $\mathbf{n} = (n_1, \ldots, n_m)$, the other half of the input modes is now in the postselected state $|\mathbf{n}\rangle = \otimes_{i=1}^{m} |n_i\rangle$. This postselected state $|\mathbf{n}\rangle$ is then passed through the linear-optical unitary U and measured in the Fock basis, yielding outcome $\mathbf{o} = (o_1, \ldots, o_m)$ with probability $P_U(\mathbf{n}, \mathbf{o}) = |\mathrm{Per}(U_{\mathbf{n},\mathbf{o}})|^2$, where the rows and columns of the submatrix $U_{\mathbf{n},\mathbf{o}}$ correspond to the indices with nonzero entries in $\mathbf{n}$ and $\mathbf{o}$. But, conditioned on $|\mathbf{n}\rangle$ and $|\mathbf{o}\rangle$ being photon-collision-free and the hiding property, the distribution of matrices $U_{\mathbf{n},\mathbf{o}}$ equals that of the boson sampling submatrices $U_{\mathbf{1}_n,\mathbf{o}}$, where the photons in the input state are, by convention, in the first n modes. The properties of SBS postselected on photon-collision-free outcomes in a fixed photon number sector are therefore equal to the properties of standard boson sampling.

We now argue that this equivalency hinges essentially on the fact that $\omega(n^2)$ of the input modes are squeezed. To this end, consider a modification of SBS in which only k out of the m modes are prepared in one half of a TMSV state, while the remaining $m - k$ modes are prepared in the vacuum state, which resembles the GBS setting. Let us also consider a squeezing parameter r of every TMSV state chosen such that $\sinh^2(r) = n/k$, yielding a mean photon number of n after postselection.

Recall that a TMSV state with squeezing parameter r and phase ϕ has a Fock expansion given by

$$|\mathrm{TMSV}\rangle = \frac{1}{\cosh(r)} \sum_{\ell=0}^{\infty} (-e^{i\phi} \tanh r)^n |n\rangle|n\rangle, \qquad \text{(B1)}$$

thus leading to a probability of $\tanh^{2\ell} r / \cosh^2 r$ to measure ℓ photons in one mode. Therefore, if the input consists of k TMSV states, then the probability that measuring one half of each state produces a photon collision is

$$\begin{aligned}
\Pr[\text{photon collision}] &= 1 - \left(\frac{1}{\cosh^2 r} + \frac{\tanh^2 r}{\cosh^2 r}\right)^k \\
&= 1 - \left(\frac{1}{1 + n/k} + \frac{n/k}{(1 + n/k)^2}\right)^k \\
&= 1 - \left[1 - \left(\frac{n/k}{1 + n/k}\right)^2\right]^k \\
&= 1 - \exp\left(-\frac{n^2}{k} + kO(n/k)^3\right), \qquad \text{(B2)}
\end{aligned}$$

assuming $k = \omega(n)$. This photon collision probability remains lower-bounded by a constant for $k = O(n^2)$, but vanishes for any $k = \omega(n^2)$. Thus, the probability of a photon collision in the input state of SBS remains high until $k = \Theta(n^2)$ and decays then. But because in SBS the roles of the (postselected) input state and the output state are symmetric, a photon collision implies a failure of hiding and, therefore, a failure of anticoncentration in the regime $k = O(n^2)$. Conversely, for $k = \omega(n^2)$ we believe that hiding holds [2,29], and hence Lemma 8.8 of Aaronson and Arkhipov [2] shows weak anticoncentration for SBS with an inverse normalized second moment of $1/n$ in this regime.

This shows that generalized SBS with a variable number of input squeezed states undergoes a transition in anticoncentration similar to the one we find here for GBS. It is not at all clear that the transition in SBS implies a transition in GBS, however, as GBS does not involve postselection. Indeed, in SBS, the anticoncentration coincides with—or rather is—a transition in the hiding property. In GBS, in contrast, we see the transition in anticoncentration, but hiding is conjectured to hold for all k. Further, the situation in GBS is not immediately comparable to that in this modified SBS scenario because the input single-mode squeezed states are supported on even numbers of photons, and therefore any nonzero photon number input states are photon-collision-full. Therefore, the connections outlined here deserve future consideration.