

Linear Cross-Entropy Certification of Quantum Computational Advantage in Gaussian Boson Sampling

Javier Martínez-Cifuentes^{1,*}, Hubert de Guise², and Nicolás Quesada¹

¹Department of Engineering Physics, *École Polytechnique de Montréal*, Montréal, Quebec H3T 1J4, Canada

²Department of Physics, *Lakehead University*, Thunder Bay, Ontario P7B 5E1, Canada



(Received 18 April 2024; revised 15 August 2024; accepted 16 September 2024; published 24 October 2024)

Validation of quantum advantage claims in the context of Gaussian boson sampling (GBS) currently relies on providing evidence that the experimental samples genuinely follow their corresponding ground truth, i.e., the theoretical model of the experiment that includes all the possible losses that the experimenters can account for. This approach to verification has an important drawback: it is necessary to assume that the ground truth distributions are computationally hard to sample, that is, that they are sufficiently close to the distribution of the ideal, lossless experiment, for which there is evidence that sampling, either exactly or approximately, is a computationally hard task. This assumption, which cannot be easily confirmed, opens the door to classical algorithms that exploit the noise in the ground truth to efficiently simulate the experiments, thus undermining any quantum advantage claim. In this work, we argue that one can avoid this issue by validating GBS implementations using their corresponding ideal distributions directly. We explain how to use a modified version of the linear cross-entropy, a quantity that we call the LXE score, to find reference values that help us assess how close a given GBS implementation is to its corresponding ideal model. Finally, we analytically compute the score that would be obtained by a lossless GBS implementation.

DOI: [10.1103/PRXQuantum.5.040312](https://doi.org/10.1103/PRXQuantum.5.040312)

I. INTRODUCTION

Gaussian boson sampling (GBS) [1,2] is a model of quantum computation with the possibility to demonstrate quantum computational advantage [3], i.e., to show that quantum devices are capable of significantly outperforming classical computers at specified computational tasks. Broadly speaking, an ideal GBS experiment consists of sending single-mode squeezed states into a Haar-random lossless interferometer, i.e., a random network of beam splitters and wave plates. The photon-number distribution of the output light is then measured using photon-number-resolving or threshold detectors [4]. It has been shown that, under some reasonable conjectures [1,2,5], it is computationally hard to sample exactly or approximately from the probability distribution of the resulting experimental outcomes (i.e., the distribution of the strings of non-negative integers resulting from the measurement). Here, approximate sampling is understood as sampling from a

probability distribution that is close in total variation distance to the ideal GBS distribution [6]. The hardness of the task of sampling is what gives this model of computation the possibility of demonstrating quantum advantage.

Real-world implementations of GBS, such as those reported in Refs. [7–10], suffer from losses and imperfections in preparation, transmission, and detection of light. It is therefore expected that the theoretical probability distributions associated with these experiments, commonly referred to as *ground truth distributions*, will differ from the *ideal distribution* (which does not include any type of losses in its definition). However, it is *assumed* that the ground truth distributions are close in total variation distance to the ideal distribution, sufficiently close as to be able to invoke the hardness of approximate sampling in order to claim that it is computationally hard to classically reproduce the outcomes of the experiment. This assumption allows the experimenters to claim that their implementations achieve a quantum advantage.

Presuming that the ground truth distributions are hard to sample, a given GBS implementation must be followed by a validation of its outcomes [3], i.e., a verification that the experiment is operating correctly. This validation amounts to providing evidence that the experimental samples closely follow the ground truth distribution. Since the direct estimation of the total variation distance between

*Contact author: jmartcifun@gmail.com

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

the real distribution of the samples and the ground truth requires exponentially many runs of the experiment [3,11], the validation of GBS implementations usually relies on other *sample-efficient* statistical measures (i.e., measures requiring polynomially many samples [3]) that assess how correlated are the experimental outcomes to the ground truth distribution.

Among the current, most widely used techniques we can find Bayesian hypothesis testing [12], which consists in demonstrating how likely is the ground truth to explain the experimental samples relative to an adversarial classical model. Another strategy is to use the heavy output generation test and other cross-entropy measures [3,7], which intend to verify if classically generated samples are able to produce “heavier outputs” in the ground truth distribution, i.e., events with higher ground truth probability, than the experimental samples. A further technique is to compare the correlations between modes present in the photon-number-resolving or threshold detection samples with those predicted by the ground truth model, and by adversarial models or samplers [8,13,14]. A fourth validation method is based on binning the detectors in groups of certain sizes, and then analytically computing the corresponding grouped probability distribution [15,16]. This procedure is done for the ground truth and for adversarial models. These analytical distributions are then compared with those obtained using the experimental samples.

All of the previously mentioned techniques have their own limitations. For instance, some rely on the computation of probabilities of individual samples, a task whose cost grows exponentially with the number of photons or clicks detected in different output modes of the interferometer, thus making the techniques *computationally inefficient* validation strategies. Moreover, one can find situations in which these techniques reach contradicting conclusions about the validity of a set of experimental samples [17]. In addition, when verifying the experimental outcomes against adversarial samplers that do not have a well-defined probability distribution associated with them, it is not even possible to perform some of these tests (e.g., Bayesian testing) [18]. These issues suggest that the current widely used GBS validation methods are not sufficient to readily tell if the experimental samples unambiguously follow from the ground truth distribution and, consequently, they cannot readily validate a quantum advantage claim. This also opens the door to classical algorithms that generate samples that outperform the experimental outcomes at these validation tasks [17,18], or classical strategies that “spoof” some of these validation techniques [19].

Perhaps more importantly, the degree of confidence in these methods for verifying quantum advantage claims is strongly tied to the confidence in the hardness of the task of sampling from the ground truth distribution. However, at this time, there is not a reliable statistical measure

that allows us to determine whether any ground truth distribution is sufficiently close to the ideal model of its corresponding experiment. This fact may allow classical algorithms to exploit the losses in the experiments in order to generate samples that, by using the same techniques for verifying GBS implementations, are found to follow the corresponding ground truth distributions more closely [20].

The current state of affairs of GBS validation differs significantly from that of the field of random circuit sampling (RCS) verification. It has been identified that the linear cross-entropy benchmark (XEB) [3,21,22], a quantity constructed from the linear cross-entropy between the outcomes of a random circuit and its corresponding ideal distribution, serves as a witness of quantum advantage in RCS implementations. The reason behind the success of this metric, despite having its own limitations [23], is that random circuits are extremely sensitive to noise; the presence of errors in experimental implementations leads to samples whose real distributions are uncorrelated with the ideal distribution [3,22,24], and, moreover, exponentially close to the uniform distribution in the sample space. The XEB for samples following the uniform distribution identically vanish. When the experimental samples follow directly from the ideal distribution, the XEB is equal to 1. Furthermore, obtaining an XEB different enough from zero is considered to be a computationally hard task [3]. Quantum advantage is thus verified when this benchmark is sufficiently different from zero.

GBS experiments are not as sensitive to loss as RCS implementations are to gate errors, and this hinders the definition of a validation metric as decisive as the XEB for the verification of GBS quantum advantage claims. Nevertheless, there are two important features of RCS validation that could be used to overcome several of the difficulties surrounding the verification of GBS experiments. The first of them is validating the experimental outcomes directly against their corresponding ideal model. This relieves the verification process from the assumption that it is computationally hard to sample from the ground truth distribution. The second one is the determination of *reference values* (of a given statistical measure) associated with the ideal distribution, as well as to other probability distributions that may differ from that of an ideal implementation. These reference values can be used to assess how far the experimental samples are from the ideal distribution.

In this work, we take the XEB as a blueprint for defining a figure of merit for GBS validation having the first of the two previously mentioned features. We construct this quantity, which we call the *linear cross-entropy score* (LXE score), from a normalized version of the linear cross-entropy between the ideal GBS distribution and a test probability distribution (corresponding to the actual distribution of the experimental outcomes, or the distributions of adversarial models or samplers), averaged over the

Haar measure of the unitary group, and evaluated at the limit of a large number of modes. We include the average over Haar-random unitaries in the definition of the score in order to study the behavior of the normalized linear cross-entropy for a typical implementation of GBS. On the other hand, we focus on setups with a large number of modes because this is the regime in which the hardness of the task of sampling is more manifest.

In addition, we propose a validation strategy that exploits the second of the aforementioned features. The technique consists of computing the LXE scores for the most commonly used classical adversarial samplers or models, as well as for the ideal GBS distribution, and using them as reference values. We would then compare these reference values to the estimated score of the experimental outcomes. In this way, we can assess how close a given GBS implementation is to its corresponding ideal model, and to its most challenging adversaries.

After discussing the details of the definition of the LXE score, we set off to determine the first two reference values to be used in the validation strategy. To do this, we focus on implementations using photon-number-resolving detectors. The first of these reference values corresponds to a model that leads to a uniform probability distribution for each sector of the total number of detected photons, N , in the experimental samples. This value follows directly from the normalization of the linear cross-entropy and is equal to 1. The second reference value, the *ideal score*, corresponds to a GBS implementation using single-mode squeezed states as input of the first R modes of a lossless interferometer, with the remaining $M - R$ modes receiving the vacuum state. We consider two versions of this GBS setup: the first uses input squeezed states with the same squeezing parameter, while the second uses squeezed states with different squeezing parameters.

By expressing the linear cross-entropy between two GBS distributions as an integral over several real parameters (a technique that makes its computation independent from the use of measurement outputs), and by using the Weingarten calculus [25] in order to compute the average over Haar-random unitaries, we were able to find an analytical expression for the ideal score as a function of N and R . To the extent of our knowledge, this approach to the analysis of cross-entropy measures in the context of GBS has not been employed before.

We find that part of the dependence of the ideal score on parameter R can be expressed as a polynomial of degree $2N$, whose coefficients can be computed by counting the number of undirected graphs with a certain number of connected components. For setups that use input states with different squeezing parameters, the coefficients also depend on the lengths of the connected components of the graph. This result is akin to the conclusions found by Ehrenberg *et al.* [26,27] in their recent study on anticoncentration in GBS. In their work, they computed the first

and second moments of the output GBS distribution in the photon-collision-free limit, in which nearly all detection patterns have at most one photon in each mode. In this regime, the output distribution can be approximated by the modulus squared of hafnians of Gaussian random matrices [5,28,29]. The authors developed a graph-theoretical method for computing the moments of this approximate distribution, and found that the second moment can be expressed as a polynomial of degree $2N$ in R , whose coefficients are determined by counting the number of graphs with a given number of connected components. Moreover, they related the first and second moments to the LXE score of an ideal model that uses input squeezed states with the same squeezing parameter [27]. Even though their expression for the ideal score is very similar to our findings, the definition and origin of the graphs involved in the computation of our results differ from those used in Refs. [26,27]. At this time, it is necessary to make a more thorough analysis of the computation of the coefficients in both cases in order to find a clear relation between these two results.

Focusing on the case $R = M$, we find that the ideal score has a particularly simple expression in terms of N , and it is the same whether we use input squeezed states with the same squeezing parameter or not. We compare this analytical expression with numerical estimations of the ideal score for setups that are not in the limit of $M \rightarrow \infty$. This comparison allows us to investigate how good our results approximate the estimated ideal score of real-world GBS implementations. Additionally, we also make numerical estimations of the score for a simple GBS model with transmission losses, which allows us to study the behavior of the LXE score in the presence of noise.

It is worth mentioning that determining probability amplitudes for pure Gaussian states requires the computation of hafnians of matrices half the size of those used in the computation of probabilities of mixed states. This implies that the estimation of the LXE score can be done for a range of detected photons approximately twice as large as that used in the validation of recent GBS experiments [7–10], thus representing a significant improvement in the validation of these implementations.

We consider that the LXE score will be of significant importance and utility to the field of GBS verification. Moreover, our computation of the ideal score sets the stage for an alternative approach to the validation of GBS implementations, one where we assert that verifying GBS should require the evaluation of probabilities corresponding to unitary models, not to mixed-state ground truths.

This paper is organized as follows. In Sec. II we describe the GBS setup that we consider throughout the article, and we introduce the concept of the *model* of a GBS implementation. In Sec. III we discuss how to use the LXE score to validate GBS experiments. Section IV is devoted to the detailed computation of the ideal LXE score for setups that use input squeezed states with the same squeezing

parameter, while Sec. V shows how to compute the score for models that use different squeezing parameters. In Sec. VI we bring attention to some interesting features of the ideal score when $R = M$. Here, we also present the numerical estimations of the score for GBS setups that are not in the limit of $M \rightarrow \infty$, and for some simple models that include transmission losses. Finally, we conclude in Sec. VII.

II. GBS SETUP

Consider a GBS setup (see Fig. 1) where M modes are prepared in single-mode, nondisplaced Gaussian states. The nature of these states need not be specified at this point; they could be squeezed, thermal, squashed, etc. The initial M -mode state is sent through an arbitrary linear, lossless interferometer, which is mathematically described by an $M \times M$, *Haar-random* unitary matrix $\mathbf{U}$. The output light of the interferometer is then measured using photon-number-resolving detectors, which can determine the number of output photons in each mode; i.e., they measure the output state of the system in the Fock basis.

The output state of the interferometer, $\hat{\rho}$, which is also an M -mode nondisplaced Gaussian state, is completely described by a $2M \times 2M$, complex Husimi covariance matrix Σ [2,30], whose entries are computed as $\Sigma_{j,k} = \frac{1}{2} \langle \{\hat{\xi}_j, \hat{\xi}_k^\dagger\} \rangle + \frac{1}{2} \delta_{j,k}$. The $\{\hat{\xi}_k\}$ are the components of the operator vector $\hat{\xi} = (\hat{a}_1, \dots, \hat{a}_M, \hat{a}_1^\dagger, \dots, \hat{a}_M^\dagger)$, where $\hat{a}_k^\dagger$ and $\hat{a}_k$ are the bosonic creation and annihilation operators of the output modes, which satisfy the canonical commutation relations $[\hat{a}_j, \hat{a}_k] = [\hat{a}_j^\dagger, \hat{a}_k^\dagger] = 0$ and $[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{j,k}$. Here $\{\hat{a}, \hat{b}\} := \hat{a}\hat{b} + \hat{b}\hat{a}$ stands for the anticommutator of

operators $\hat{a}$ and $\hat{b}$, $\langle \hat{a} \rangle = \text{Tr}(\hat{a}\hat{\rho})$, and $\delta_{j,k}$ is the Kronecker delta.

The result of the photon-number-resolving measurement, i.e., the detection pattern, is an M string of non-negative integers $\mathbf{n} = (n_1, \dots, n_M)$, where each n_k represents the number of photons detected at mode k ($n_k = 0$ means that no light has been detected). By defining the matrix

$$\mathbf{A} = \mathbf{X}(\mathbb{I}_{2M} - \Sigma^{-1}), \quad \mathbf{X} = \begin{pmatrix} \mathbf{0} & \mathbb{I}_M \\ \mathbb{I}_M & \mathbf{0} \end{pmatrix}, \quad (1)$$

where $\mathbb{I}_M$ is the identity matrix of size $M \times M$, we can compute the probability of detecting outcome $\mathbf{n}$ as [1,2]

$$\text{Pr}(\mathbf{n}|\mathbf{A}) = \frac{\text{Pr}(\mathbf{0}|\mathbf{A})}{\mathbf{n}!} \text{haf}[\mathbf{A}_{\mathbf{n}}], \quad (2)$$

where $\text{Pr}(\mathbf{0}|\mathbf{A}) = \sqrt{\det(\mathbb{I}_{2M} - \mathbf{X}\mathbf{A})}$ is the vacuum probability, $\mathbf{n}! = \prod_{k=1}^M n_k!$, and

$$\text{haf}[\mathbf{O}] = \frac{1}{2^m m!} \sum_{\sigma \in S_{2m}} \prod_{j=1}^m O_{\sigma(2j-1), \sigma(2j)} \quad (3)$$

is the *hafnian* of the symmetric $2m \times 2m$ matrix $\mathbf{O}$ [31]. Here, S_m stands for the symmetric group of degree m , i.e., the group of all permutations of m objects.

Matrix $\mathbf{A}_{\mathbf{n}}$ is constructed by taking the k th and $(k+M)$ th rows and columns of $\mathbf{A}$ and repeating them n_k times. If $n_k = 0$, the corresponding rows and columns are removed. Note that the size of this matrix is $2N \times 2N$, where $N = \sum_{k=1}^M n_k$ is the *total number of detected photons* in outcome $\mathbf{n}$.

Equation (2) will also hold for descriptions of the GBS setup that include Gaussian noise and losses (transmission loss is a good example of this type of operation). In these cases, the output state of the interferometer will remain Gaussian [30], and we can readily define a matrix Σ or $\mathbf{A}$ that completely describes the output state. On the other hand, non-Gaussian noise will lead to output states that cannot be completely defined by an $\mathbf{A}$ matrix.

Focusing on setups whose descriptions include only Gaussian processes, we can consider matrix $\mathbf{A}$ to contain all the relevant information about the theoretical description of a GBS experiment using photon-number-resolving detectors. We therefore refer to $\mathbf{A}$ as the *model* of the GBS setup, and we interpret $\text{Pr}(\mathbf{n}|\mathbf{A})$ as the probability of obtaining outcome $\mathbf{n}$ given model $\mathbf{A}$.

As mentioned before, for a GBS setup that uses input single-mode squeezed states and a lossless interferometer, it has been shown that, assuming that certain conjectures hold, sampling from the distribution in Eq. (2), either exactly or approximately, is a computationally hard task whose cost increases exponentially with the size and rank

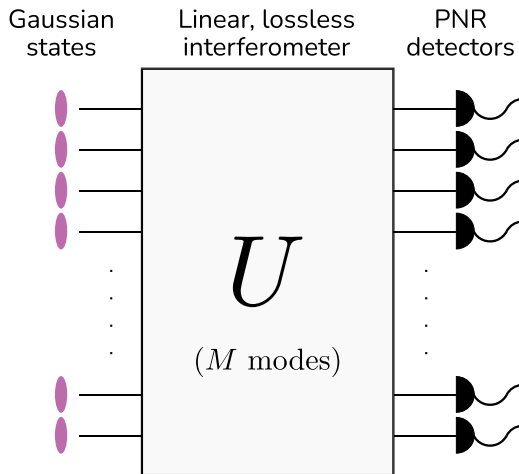


FIG. 1. Description of a general, ideal GBS setup. A set of input single-mode, nondisplaced Gaussian states are sent into a linear, lossless interferometer described by an $M \times M$, *Haar-random* unitary matrix $\mathbf{U}$. The output of the interferometer is measured using photon-number-resolving (PNR) detectors.

of $\mathbf{A}_n$ [1,2,5]. We refer to the theoretical description of this setup as the *ideal squeezed state model*, and we denote it $\mathbf{A}_{\text{sqz}}$.

Any real-world implementation of GBS using squeezed states will suffer from inevitable losses, and their presence makes the experiment differ from the ideal model. Nevertheless, GBS experiments are designed to minimize noise as much as possible, so the probability distribution of the experimental samples is close enough to the ideal model and, by invoking the hardness of approximate sampling, it remains computationally hard to generate samples from this distribution. Theoretical models of GBS experiments using squeezed states that also include all the losses that the experimenters can account for are called *ground truth models*.

Verification of quantum advantage claims in the recent implementations of GBS experiments has relied on demonstrating that the *real distribution* of the samples genuinely follows from the ground truth of the experiments [7–10]. The main strategy to do this is to use a number of statistical measures to rule out *adversarial models* or *adversarial samplers*. An adversarial model is a theoretical description of a GBS setup that leads to a probability distribution that can be sampled efficiently. These classical models can be obtained, for instance, by using classical Gaussian states (such as thermal, distinguishable squeezed, or squashed states [9,10,17]) as input of the interferometers, an approach that intends to represent the effect of losses on the input squeezed states. On the other hand, an adversarial sampler is any efficient algorithm (not necessarily motivated by a physical model) that generates samples that intend to “spoof” the ground truth distribution.

An important drawback of this approach is that ruling out adversarial models and samplers with respect to the ground truth gives no information about how close this model is to the ideal squeezed state model. This opens the door to classical algorithms that reproduce the results of the experiments by exploiting the noise in the ground truth [20]. This issue can be avoided by verifying GBS implementations using the ideal squeezed state model directly. In the next section we argue how we could do this using the linear cross-entropy between GBS models.

III. LINEAR CROSS-ENTROPY SCORE FOR GBS VALIDATION

Let $\mathbf{A}$ and $\mathbf{B}$ be two different models for the same GBS setup. We define the linear cross-entropy between $\mathbf{A}$ and $\mathbf{B}$, for a given total number of detected photons N , as

$$\text{LXE}(\mathbf{A}, \mathbf{B}; N) = \sum_{\mathbf{n} \in K(N)} \frac{\Pr(\mathbf{n}|\mathbf{A}) \Pr(\mathbf{n}|\mathbf{B})}{\Pr(N|\mathbf{A}) \Pr(N|\mathbf{B})}, \quad (4)$$

where $K(N) = \{\mathbf{n} \mid \sum_{k=1}^M n_k = N\}$ and

$$\Pr(N|\mathbf{A}) = \sum_{\mathbf{n} \in K(N)} \Pr(\mathbf{n}|\mathbf{A}) \quad (5)$$

is the probability of detecting a total of N photons given model $\mathbf{A}$.

The linear cross-entropy belongs to a class of multiplicative measures of similarity between probability distributions that are collectively referred to as *cross-entropy measures* [3]. These *sample-efficient* measures (i.e., measures that can be estimated using polynomially many experimental samples) have been widely used for verifying quantum advantage claims in the field of quantum random sampling (see, for instance, Refs. [9,21]). We are interested in using $\text{LXE}(\mathbf{A}, \mathbf{B}; N)$ to assess the correlation between the ideal squeezed state model of a GBS implementation and the real distribution of the experimental samples.

The definition of $\text{LXE}(\mathbf{A}, \mathbf{B}; N)$ closely resembles the definition of the *linear cross-entropy benchmark* [3,21], a quantity that, despite having some limitations [23], has been extensively used for the validation of RCS implementations. Roughly speaking, RCS consists of repeatedly applying cycles of randomly selected one- and two-qubit gates over a set of input qubits and then measuring their final states. The action of all the gates is represented by a unitary matrix $\mathbf{U}$, which can be approximated by a Haar-random unitary when the depth of the circuit (i.e., the number of cycles) is sufficiently large. The outcome of the measurement is a bit string, i.e., a sequence of 0s and 1s. Sampling from the ideal probability distribution of the outcomes $\mathbf{s}$ of an RCS implementation, $P_{\mathbf{U}}(\mathbf{s})$, is considered to be a computationally hard task whose cost grows exponentially with the number of input qubits and the depth of the circuit. Let $Q_{\mathbf{U}}(\mathbf{s})$ be the real distribution of the bit strings $\mathbf{s}$. Then, the XEB reads [3]

$$\mathcal{F}(Q_{\mathbf{U}}, P_{\mathbf{U}}) = 2^N \sum_{\mathbf{s}} Q_{\mathbf{U}}(\mathbf{s}) P_{\mathbf{U}}(\mathbf{s}) - 1, \quad (6)$$

where N is the number of input qubits and the sum is over the set of all possible bit strings of length N . Note that this expression can be seen as a normalized, shifted version of the linear cross-entropy between two models of the same RCS implementation.

The definition of $\mathcal{F}(Q_{\mathbf{U}}, P_{\mathbf{U}})$ is such that we can identify two reference values for a *typical* instance of RCS: if $Q_{\mathbf{U}}(\mathbf{s}) = P_{\mathbf{U}}(\mathbf{s})$, $\mathbb{E}_{\mathbf{U}}[\mathcal{F}(Q_{\mathbf{U}}, P_{\mathbf{U}})] \approx 1$. If $Q_{\mathbf{U}}(\mathbf{s}) = 1/2^N$ (that is, the uniform distribution over bit strings), $\mathbb{E}_{\mathbf{U}}[\mathcal{F}(Q_{\mathbf{U}}, P_{\mathbf{U}})] = 0$ [3,21]. Here, $\mathbb{E}_{\mathbf{U}}[\cdot]$ indicates an average over the Haar measure of the unitary group. The presence of errors in experimental implementations of RCS leads to experimental samples with probability distributions that are uncorrelated with the ideal distribution,

and that are exponentially close to the uniform distribution over bit strings [21,22,24]. This implies that noisy implementations of RCS generally obtain values of the XEB close to zero. Moreover, obtaining an XEB satisfying $\mathcal{F}(Q_U, P_U) > b/2^N$, with $b > 1$, is considered to be a computationally hard task [3]. Thus, demonstrating quantum advantage for RCS implementations amounts to showing that the estimation of $\mathcal{F}(Q_U, P_U)$ using experimental samples is sufficiently different from zero.

There is no evidence that GBS architectures present the same sensibility to losses as RCS implementations. This makes the definition of a measure as decisive as the XEB for the validation of GBS experiments elusive. Nevertheless, one can use the idea of identifying reference values for *typical* instances of GBS as a tool for the verification of quantum advantage claims. Indeed, in the spirit of the XEB, it is possible to use the average values (over Haar-random unitaries) of normalized versions of the linear cross-entropy between the ideal squeezed state model and the most commonly used adversarial models and samplers in order to obtain these reference values. We could consider, among the most widely used adversarial models, those associated with GBS setups using thermal, squashed, or distinguishable squeezed states [8–10,17]. In addition to these, we could use classical algorithms that mimic the marginals, up to a certain order, of the ideal GBS distribution as adversarial samplers [9,18]. The validation of quantum advantage would then amount to comparing how much a given GBS implementation *scores* with respect to the other models and samplers. Note that this approach makes no use of the ground truth distribution of the corresponding GBS experiment and, consequently, it is not necessary to make any assumptions about the hardness of sampling from it.

In the remainder of this section, we workout the details of the definition of this normalized, Haar-averaged version of the linear cross-entropy, which we refer to as the *linear cross-entropy score* (LXE score). Only one additional feature will be included in this definition: we focus on the asymptotic behavior of the linear cross-entropy as $M \rightarrow \infty$. We do this to take into account the fact that the arguments justifying the complexity of GBS commonly require the setups to have a large number of modes, growing quadratically with the mean number of photons in the input squeezed states [5]. Moreover, by virtue of Levy's lemma [32], one would expect that, as M increases, typical instances of GBS will obtain values of the LXE score closer to the mean.

Following the definition of the XEB, we associate the first reference value of the LXE score with the value that would be obtained by the uniform distribution over the sample space over which the linear cross-entropy is defined. Unlike in RCS, the entire sample space of detection patterns in GBS is infinite dimensional. This is why Eq. (4) is defined for sets of samples with the same total

number of detected photons. The first reference value of the LXE score is related to a GBS model that leads to a uniform probability distribution for each sector of N . Let us call such a model $\mathbf{A}_{\text{uni}}$. We can readily note that $\Pr(\mathbf{n}|\mathbf{A}_{\text{uni}}) = f(|\mathbf{n}|)$, where $f(x)$ is a real-valued function satisfying $\sum_{N=0}^{\infty} f(N) = 1$, and $0 \leq f(N) \leq 1$ for all N , while $|\mathbf{n}| = \sum_{k=1}^M n_k$. This implies that, for an arbitrary model $\mathbf{B}$,

$$\begin{aligned} \text{LXE}(\mathbf{A}_{\text{uni}}, \mathbf{B}; N) &= \frac{f(N)}{\Pr(\mathbf{n}|\mathbf{A}_{\text{uni}})} \sum_{\mathbf{n} \in K(N)} \frac{\Pr(\mathbf{n}|\mathbf{B})}{\Pr(N|\mathbf{B})} \\ &= \frac{f(N)}{\sum_{\mathbf{n} \in K(N)} f(|\mathbf{n}|)} \\ &= \left(\sum_{\mathbf{n} \in K(N)} 1 \right)^{-1} \\ &= |K(N)|^{-1}, \end{aligned} \quad (7)$$

where $|K(N)|$ is the number of elements in $K(N)$. This value is equivalent to the number of weak M compositions of N , i.e., the number of ordered partitions of N having M parts (with some of the parts allowed to be zero). It can be shown that $|K(N)| = \binom{M+N-1}{N}$ [33,34]. We use $|K(N)|^{-1}$ as a normalization factor for the linear cross-entropy between any two models, thus setting the first reference value of the score to 1. It is worth mentioning that this same normalization term was used for the definition of other cross-entropy measures in Refs. [9,20].

Even though we defined $\mathbf{A}_{\text{uni}}$ according only to the properties of its corresponding probability distribution, it is important to keep in mind that this model can truly be associated with a GBS setup. It can be shown (see Appendix A) that GBS setups using identical thermal states at the input of every mode of a lossless interferometer lead to probability distributions that are uniform for every sector of the total number of detected photons.

With the normalization factor in place, we may now express the LXE score for a model $\mathbf{B}$ as

$$s(\mathbf{B}; N) = \lim_{M \rightarrow \infty} \binom{M+N-1}{N} \mathbb{E}_{\mathbf{U}}[\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{B}; N)]. \quad (8)$$

Although this definition is adequate for finding reference values corresponding to some adversarial models, the validation of a set of experimental or adversarial samples requires an estimate of the LXE score rather than an analytical computation. This is due to the fact that not every adversarial sampler has an associated GBS model and, moreover, we have no information about the actual probability distribution that the experimental samples follow. Consider a set of L samples $\{\mathbf{n}_k\}_{k=1}^L$ with the same total

number of detected photons N ; the estimated value of the score can be computed as

$$\bar{s}(N) = \mathcal{C}(\mathbf{A}_{\text{sqz}}, N) \frac{1}{L} \sum_{k=1}^L \Pr(\mathbf{n}_k | \mathbf{A}_{\text{sqz}}), \quad (9)$$

where

$$\mathcal{C}(\mathbf{A}_{\text{sqz}}, N) = \binom{M+N-1}{N} [\Pr(N | \mathbf{A}_{\text{sqz}})]^{-1}. \quad (10)$$

We can interpret the estimator $\bar{s}(N)$ as the average of the probabilities of each individual sample with respect to the probability distribution of the ideal model, multiplied by a normalization factor.

As mentioned before, the linear cross-entropy is a sample-efficient measure, and thus $\bar{s}(N)$ can be estimated using polynomially many samples. Other sample-efficient techniques, such as Bayesian testing or the heavy output generation test, typically require 10^3 to 10^4 samples per value of N to be determined [7–9, 17]. Because of the similarity between the computation of $\bar{s}(N)$ and these other validation techniques, we can expect that $\bar{s}(N)$ can also be estimated using this same number of samples range.

All the probabilities involved in the estimate of the score should be computed using a unitary matrix that is closely related to the actual subunitary matrix that describes the action of the lossy interferometer used in the experiment. If the GBS implementation is programmable, one can have access to information about the ideal (lossless) configurations of all the gates (i.e., all the beam splitters and phase shifters) used in the experiment. One then determines $\bar{s}(N)$ using the unitary matrix describing the action of all these ideal, unitary gates.

If the experiment has limited programmability and we only have access to the square subunitary matrix $\mathbf{T}$ describing the lossy interferometer, we can find a unitary matrix associated with $\mathbf{T}$ using its singular value decomposition [30]. Indeed, we can always write $\mathbf{T} = \mathbf{U}_1 \mathbf{D} \mathbf{U}_2^\dagger$, where $\mathbf{U}_1$, $\mathbf{U}_2$ are unitary and $\mathbf{D}$ is a diagonal matrix whose entries are the singular values of $\mathbf{T}$, which, in turn, are related to the transmission losses in the experiment. If we had no losses, we would be able to replace $\mathbf{D}$ by $\mathbb{I}_M$ and obtain the unitary transmission matrix $\mathbf{U}_1 \mathbf{U}_2^\dagger$. On this account, we can interpret $\mathbf{U}_1 \mathbf{U}_2^\dagger$ as the closest unitary matrix to $\mathbf{T}$, thus making it a reasonable choice for the computation of the LXE score.

However, it is important to mention that even if a given GBS implementation is not fully programmable, the authors of the experiment will be able to describe their ideal intended computation, i.e., they will have knowledge of the unitary $\mathbf{U}$ associated with their implementation.

The definition of the LXE score can be readily generalized to include GBS models with non-Gaussian noise. As mentioned in Sec. II, these models cannot be completely defined by a matrix of the form (1). However, if

we have complete knowledge of the probability distribution associated with a given non-Gaussian model, we can still use Eq. (8) to compute the LXE score; we need only replace $\Pr(\mathbf{n} | \mathbf{B})$ and $\Pr(N | \mathbf{B})$ in the definition of the linear cross-entropy by the adequate expressions of the probability distributions of interest. If we do not have complete knowledge of the probability distribution, but we have a set of samples associated with the non-Gaussian model, we can still use Eq. (9) to estimate the score.

We associate the second reference value of the LXE score with the value that we would obtain if the real distribution of the experimental samples were $\Pr(\mathbf{n} | \mathbf{A}_{\text{sqz}})$. The analytical computation of this *ideal score* will be the subject of the next section.

IV. LXE SCORE FOR THE IDEAL SQUEEZED STATE MODEL

Consider a GBS implementation where the first R of the M input modes of the interferometer receive identical single-mode squeezed states with squeezing parameter r , while the remaining $M - R$ modes receive the vacuum state. The matrix $\mathbf{A}_{\text{sqz}}$ describing this setup reads [1, 2]

$$\mathbf{A}_{\text{sqz}} = \tanh(r) \mathbf{V} \oplus \mathbf{V}^*, \quad (11)$$

where we define

$$\mathbf{V} = \mathbf{U} \boldsymbol{\zeta} \mathbf{U}^\dagger, \quad \boldsymbol{\zeta} = \mathbb{I}_R \oplus \mathbf{0}_{M-R} \quad (12)$$

(we explicitly indicate the size of the null matrix for clarity). The main result that we prove in this work states that

$$s(\mathbf{A}_{\text{sqz}}; 2N) = \frac{4^N (N!)^2}{(2N)!} \left[\frac{(R-2)!!}{(R+2N-2)!!} \right]^2 \sum_{\ell=1}^{2N} c_\ell R^\ell, \quad (13)$$

where the $\{c_\ell\}$ are non-negative coefficients.

Unlike the ideal XEB reference value, which remains constant no matter the number of qubits in the random circuit, the ideal LXE score varies for each sector of the total number of detected photons. This, however, does not mean that $s(\mathbf{A}_{\text{sqz}}; 2N)$ cannot be used as a tool for validation of GBS implementations. Indeed, we need only determine how different the scores of other models or samplers (which might also depend on N) are from the reference curve established by the ideal squeezed state model.

A few definitions must be set in place before expressing how to compute the coefficients $\{c_\ell\}$. Let $\mathbf{j} = (j_1, \dots, j_{2N})$ be a fixed sequence of *different* indices. We define the permutation $\Omega_{\mathbf{k}} \in S_{2N}$ (where we recall that S_m stands for the

symmetric group of degree m) by its action on $\mathbf{j}$ as

$$\Omega_{\mathbf{k}}[j_1, \dots, j_{2N}] = \bigoplus_{a=1}^N \bigoplus_{p=1}^{k_a} \omega_a[(j_{2v_{a-1}+2a(p-1)+1}, \dots, j_{2v_{a-1}+2ap})], \quad (14)$$

where $v_a = \sum_{p=1}^a p k_p$, $v_0 \equiv 0$, and the permutation $\omega_a \in S_{2a}$ (with $2a \leq 2N$) is defined by its action on a sequence $(g_1, \dots, g_{2a})$ as $\omega_a[(g_1, g_2, \dots, g_{2a-1}, g_{2a})] = (g_2, g_3, \dots, g_{2a}, g_1)$. Moreover, let $\varrho \in S_{4N}$, and, following Ref. [35], let $\Gamma(\varrho)$ be an undirected graph whose vertices are $\{1, \dots, 4N\}$, and whose edges are $\{(2k-1, 2k) \mid k \in \{1, \dots, 2N\}\}$ and $\{[\varrho(2k-1), \varrho(2k)] \mid k \in \{1, \dots, 2N\}\}$ (see Fig. 2 for an illustration of this definition). Then,

$$c_\ell = \sum_{\mathbf{k}^{(c)} \in \mathbf{I}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \times \sum_{\sigma \in S_{2N}} b_\ell[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})], \quad (15)$$

where $\mathbf{k}^{(c)}$ is a vector of N non-negative integers that satisfy $k_1 + 2k_2 + \dots + Nk_N = N$ (we define $\mathbf{l}^{(c)}$ in an analogous way), and

$$b_\ell(\mathbf{g}, \mathbf{h}) = |\{\varrho \in S_{4N} \mid \mathbf{h} = \varrho(\mathbf{g}) \text{ and } \Gamma(\varrho) \text{ has } \ell \text{ connected components}\}|. \quad (16)$$

Throughout the rest of this section, we explain in detail how to obtain the result in Eq. (13), and we justify the definitions in Eqs. (14) to (16).

We divide our calculation of the ideal score into the following stages.

- (1) Express the linear cross-entropy as an integral over a number of real parameters. This form will have the advantage of not depending on the measurement outcomes $\mathbf{n}$.
- (2) Write $\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; N)$ as a polynomial in the entries of $\mathbf{U}$. This will prove useful when computing the average over the Haar measure of the unitary group.
- (3) Compute the integral over the real parameters.
- (4) Calculate the average over Haar-random unitaries as $M \rightarrow \infty$.

As a final stage, we gather all the results of the previous steps and complete the computation of the ideal score

A. Integral form of the linear cross-entropy

Let $\mathbf{A}$ and $\mathbf{B}$ be two models for the same GBS setup. Adding the probabilities of every possible detection pattern

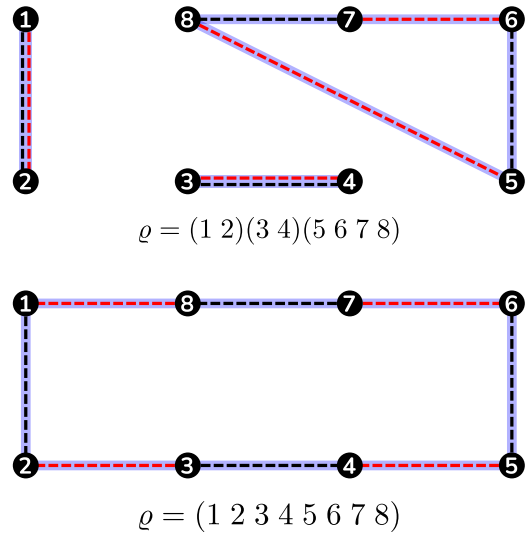


FIG. 2. Illustration of the definition of the undirected graphs $\Gamma(\varrho)$ for $4N = 8$. The vertices of the graph are represented by numbered black circles. Edges corresponding to $\{(2k-1, 2k) \mid k \in \{1, \dots, 2N\}\}$ are shown as black dashed lines, while edges corresponding to $\{[\varrho(2k-1), \varrho(2k)] \mid k \in \{1, \dots, 2N\}\}$ are shown as red dashed lines. Each connected component of the graph is highlighted with a light blue, thick line. The top graph corresponds to the permutation, written in cycle notation, $\varrho = (1\ 2)(3\ 4)(5\ 6\ 7\ 8)$. This permutation transforms the set of indices $\mathbf{g} = (g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8)$ as $\varrho(\mathbf{g}) = (g_2, g_1, g_4, g_3, g_6, g_7, g_8, g_5)$, and has a total of three connected components. The bottom graph corresponds to the permutation $\varrho = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$, which transforms $\mathbf{g}$ as $\varrho(\mathbf{g}) = (g_2, g_3, g_4, g_5, g_6, g_7, g_8, g_1)$. In this case there is only one connected component.

we can see that

$$\sum_{\mathbf{n}} \Pr(\mathbf{n}|\mathbf{A}) = \sum_{\mathbf{m}} \Pr(\mathbf{m}|\mathbf{B}) = 1,$$

which implies that

$$\sum_{\mathbf{n}, \mathbf{m}} \Pr(\mathbf{n}|\mathbf{A}) \Pr(\mathbf{m}|\mathbf{B}) = 1.$$

We can recast this expression in terms of the hafnian using Eq. (2):

$$\sum_{\mathbf{n}, \mathbf{m}} \frac{\text{haf}[\mathbf{A}_{\mathbf{n}}]}{\mathbf{n}!} \frac{\text{haf}[\mathbf{B}_{\mathbf{m}}]}{\mathbf{m}!} = \frac{1}{\Pr(\mathbf{0}|\mathbf{A}) \Pr(\mathbf{0}|\mathbf{B})}. \quad (17)$$

Define the matrix

$$\mathbf{D}(\boldsymbol{\phi}) = \text{diag}(e^{i\phi_1}, \dots, e^{i\phi_M}), \quad (18)$$

where $\boldsymbol{\phi} = (\phi_1, \dots, \phi_M)$ is a vector of real parameters with $\phi_k \in [0, 2\pi]$ for all k , and let $\mathbf{W}(\boldsymbol{\phi}) = \mathbf{D}(\boldsymbol{\phi}) \oplus \mathbf{D}(\boldsymbol{\phi})$. Note that $\mathbf{W}^*(\boldsymbol{\phi}) = \mathbf{W}(-\boldsymbol{\phi})$. Transforming matrices $\mathbf{A}$ and $\mathbf{B}$

in Eq. (17) according to $\mathbf{A} \rightarrow \alpha \mathbf{W}(\phi) \mathbf{A} \mathbf{W}(\phi)$ and $\mathbf{B} \rightarrow \beta \mathbf{W}^*(\phi) \mathbf{B} \mathbf{W}^*(\phi)$, where $\alpha, \beta \in [0, 1]$, we obtain (we drop the explicit dependence of matrices on ϕ in order to shorten the notation)

$$\sum_{\mathbf{n}, \mathbf{m}} \frac{\text{haf}[\alpha(\mathbf{WAW})_{\mathbf{n}}]}{\mathbf{n}!} \frac{\text{haf}[\beta(\mathbf{W}^* \mathbf{B} \mathbf{W}^*)_{\mathbf{m}}]}{\mathbf{m}!} = q(\alpha, \phi, \mathbf{A}) q(\beta, -\phi, \mathbf{B}), \quad (19)$$

where

$$q(\alpha, \phi, \mathbf{A}) = [\det(\mathbb{I}_{2M} - \alpha \mathbf{X} \mathbf{W} \mathbf{A} \mathbf{W})]^{-1/2} = [\det(\mathbb{I}_{2M} - \alpha \mathbf{\Omega} \mathbf{A})]^{-1/2} \quad (20)$$

and $\mathbf{\Omega}(\phi) = \mathbf{W}(\phi) \mathbf{X} \mathbf{W}(\phi)$ [36].

We can factorize the matrices inside the hafnian as $(\mathbf{WAW})_{\mathbf{n}} = \bar{\mathbf{W}}_{\mathbf{n}} \mathbf{A}_{\mathbf{n}} \bar{\mathbf{W}}_{\mathbf{n}}$, where $\bar{\mathbf{W}}_{\mathbf{n}}$ is a diagonal matrix obtained from $\mathbf{W}$ by repeating n_k times the entry $e^{i\phi_k}$ (see Appendix A for a proof of this statement). For instance, let $M = 2$ and $\mathbf{W} = \text{diag}(e^{i\phi_1}, e^{i\phi_2}, e^{i\phi_1}, e^{i\phi_2})$. If $\mathbf{n} = (1, 2)$ then $\bar{\mathbf{W}}_{\mathbf{n}} = \text{diag}(e^{i\phi_1}, e^{i\phi_2}, e^{i\phi_2}, e^{i\phi_1}, e^{i\phi_2}, e^{i\phi_2})$. Note that $\bar{\mathbf{W}}_{\mathbf{n}}$ has size $2|\mathbf{n}| \times 2|\mathbf{n}|$, where $|\mathbf{n}| = \sum_{k=1}^M n_k$.

This factorization, in turn, allows us to use the following property of the hafnian [31]: for any symmetric $m \times m$ matrix $\mathbf{O}$ and a diagonal matrix $\mathbf{S} = \text{diag}(s_1, \dots, s_m)$,

$$\text{haf}[\mathbf{SOS}] = \left(\prod_{k=1}^m s_k \right) \text{haf}[\mathbf{O}]. \quad (21)$$

We have

$$\begin{aligned} \text{haf}[\alpha(\mathbf{WAW})_{\mathbf{n}}] &= \text{haf}[\alpha \bar{\mathbf{W}}_{\mathbf{n}} \mathbf{A}_{\mathbf{n}} \bar{\mathbf{W}}_{\mathbf{n}}] \\ &= \alpha^{|\mathbf{n}|} \prod_{k=1}^{2|\mathbf{n}|} (\bar{\mathbf{W}}_{\mathbf{n}})_{k,k} \text{haf}[\mathbf{A}_{\mathbf{n}}]. \end{aligned} \quad (22)$$

Noting that $\prod_{k=1}^{2|\mathbf{n}|} (\bar{\mathbf{W}}_{\mathbf{n}})_{k,k} = \prod_{k=1}^M e^{2in_k \phi_k} = e^{2i\mathbf{n} \cdot \phi}$, we obtain

$$\text{haf}[\alpha(\mathbf{WAW})_{\mathbf{n}}] = \alpha^{|\mathbf{n}|} e^{2i\mathbf{n} \cdot \phi} \text{haf}[\mathbf{A}_{\mathbf{n}}]. \quad (23)$$

Using the same argument, it can be shown that $\text{haf}[\beta(\mathbf{W}^* \mathbf{B} \mathbf{W}^*)_{\mathbf{m}}] = \beta^{|\mathbf{m}|} e^{-2i\mathbf{m} \cdot \phi} \text{haf}[\mathbf{B}_{\mathbf{m}}]$. Substituting these expressions into Eq. (19), we obtain

$$\begin{aligned} q(\alpha, \phi, \mathbf{A}) q(\beta, -\phi, \mathbf{B}) \\ = \sum_{\mathbf{n}, \mathbf{m}} \alpha^{|\mathbf{n}|} \beta^{|\mathbf{m}|} e^{2i(\mathbf{n}-\mathbf{m}) \cdot \phi} \frac{\text{haf}[\mathbf{A}_{\mathbf{n}}]}{\mathbf{n}!} \frac{\text{haf}[\mathbf{B}_{\mathbf{m}}]}{\mathbf{m}!}. \end{aligned} \quad (24)$$

Integrating both sides of the last equation with respect to $d\phi = d\phi_1 \cdots d\phi_M$, and taking into account the fact that

$$\int_0^{2\pi} e^{2i(\mathbf{n}-\mathbf{m}) \cdot \phi} d\phi = (2\pi)^M \delta_{\mathbf{m}, \mathbf{n}},$$

where $\delta_{\mathbf{m}, \mathbf{n}} = \delta_{m_1, n_1} \cdots \delta_{m_M, n_M}$, we can write

$$\begin{aligned} \frac{1}{(2\pi)^M} \int_0^{2\pi} q(\alpha, \phi, \mathbf{A}) q(\beta, -\phi, \mathbf{B}) d\phi \\ = \sum_{N=0}^{\infty} \alpha^N \beta^N \sum_{\mathbf{n} \in K(N)} \frac{\text{haf}[\mathbf{A}_{\mathbf{n}}]}{\mathbf{n}!} \frac{\text{haf}[\mathbf{B}_{\mathbf{n}}]}{\mathbf{n}!}, \end{aligned} \quad (25)$$

where we have taken into account the fact that we can decompose the sum over all possible detection patterns as $\sum_{\mathbf{n}} = \sum_{N=0}^{\infty} \sum_{\mathbf{n} \in K(N)}$.

By repeatedly differentiating with respect to α and β , and then evaluating at $\alpha = \beta = 0$, we can single out the sum involving only the elements of $K(N)$. The result of this procedure reads

$$\begin{aligned} \frac{1}{(2\pi)^M} \int_0^{2\pi} \frac{\partial^N q(\alpha, \phi, \mathbf{A})}{\partial \alpha^N} \frac{\partial^N q(\beta, -\phi, \mathbf{B})}{\partial \beta^N} \Big|_{\alpha=0, \beta=0} d\phi \\ = (N!)^2 \sum_{\mathbf{n} \in K(N)} \frac{\text{haf}[\mathbf{A}_{\mathbf{n}}]}{\mathbf{n}!} \frac{\text{haf}[\mathbf{B}_{\mathbf{n}}]}{\mathbf{n}!}. \end{aligned} \quad (26)$$

We may readily observe that the previous expression leads to the definition of the linear cross-entropy; we need only include the vacuum probabilities for both models and the term $\text{Pr}(N|\mathbf{A}) \text{Pr}(N|\mathbf{B})$. Putting all these pieces together, we obtain the final expression of the integral form:

$$\begin{aligned} \text{LXE}(\mathbf{A}, \mathbf{B}; N) \\ = \frac{1}{(2\pi)^M} \mathcal{D}(\mathbf{A}, \mathbf{B}; N) \\ \times \int_0^{2\pi} \frac{\partial^N q(\alpha, \phi, \mathbf{A})}{\partial \alpha^N} \frac{\partial^N q(\beta, -\phi, \mathbf{B})}{\partial \beta^N} \Big|_{\alpha=0, \beta=0} d\phi \end{aligned} \quad (27)$$

with

$$\mathcal{D}(\mathbf{A}, \mathbf{B}; N) = \frac{1}{(N!)^2} \frac{\text{Pr}(\mathbf{0}|\mathbf{A}) \text{Pr}(\mathbf{0}|\mathbf{B})}{\text{Pr}(N|\mathbf{A}) \text{Pr}(N|\mathbf{B})}. \quad (28)$$

Although it may seem that the determination of $\text{Pr}(N|\mathbf{A}) \text{Pr}(N|\mathbf{B})$, and therefore $\mathcal{D}(\mathbf{A}, \mathbf{B}; N)$, requires knowledge of all detection patterns in $K(N)$, by using similar arguments to those that led to Eq. (24), it can be shown that

$$\mathcal{D}(\mathbf{A}, \mathbf{B}; N) = \left[\frac{\partial^N q(\alpha, \mathbf{0}, \mathbf{A})}{\partial \alpha^N} \frac{\partial^N q(\beta, \mathbf{0}, \mathbf{B})}{\partial \beta^N} \Big|_{\alpha=0, \beta=0} \right]^{-1}. \quad (29)$$

A detailed proof of this statement can be found in Appendix A.

We now turn our attention to the task of finding an expression for $q(\alpha, \phi, \mathbf{A})$ that allows us to readily compute its partial derivatives with respect to α . We do this by recasting $q(\alpha, \phi, \mathbf{A})$ into a power series in α .

Note that $\mathbb{I}_{2M} - \alpha \Omega \mathbf{A} = \exp[\log(\mathbb{I}_{2M} - \alpha \Omega \mathbf{A})]$, and recall the relation $\det[\exp(\mathbf{A})] = \exp[\text{tr}(\mathbf{A})]$ [we use $\text{tr}(\cdot)$ to indicate the trace of a matrix, while $\text{Tr}(\cdot)$ indicates the trace of an operator]. Using the Taylor series expansion $\log(1+x) = \sum_{l=1}^{\infty} (-1)^{l+1} x^l / l$, we may write $q(\alpha, \phi, \mathbf{A})$ as

$$q(\alpha, \phi, \mathbf{A}) = \exp \left[\sum_{l=1}^{\infty} y_l \frac{\alpha^l}{l} \right], \quad y_l = \frac{1}{2} \text{tr}[(\Omega \mathbf{A})^l], \quad (30)$$

where the ϕ dependence of every y_l is through $\Omega = \Omega(\phi)$. Details about the convergence of this series expansion for a wide number of GBS models, including the ideal squeezed state model, can also be found in Appendix A.

In the form of Eq. (30), $q(\alpha, \phi, \mathbf{A})$ becomes the generating function of the *cycle index* of the symmetric group Z_n [33,37,38], which leads to the expression

$$q(\alpha, \phi, \mathbf{A}) = \sum_{n=0}^{\infty} Z_n(y_1, \dots, y_n) \alpha^n, \quad (31)$$

where

$$Z_n(y_1, \dots, y_n) = \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^n \frac{1}{k_a!} \frac{1}{a^{k_a}} \prod_{a=1}^n y_a^{k_a}, \quad (32)$$

and the sum extends over all possible $\mathbf{k} = (k_1, \dots, k_n)$ whose non-negative, integer components satisfy the constraint $k_1 + 2k_2 + \dots + nk_n = n$ (we use the notation $\mathbf{k}^{(c)}$ to indicate the constraint over the components of $\mathbf{k}$).

We can now readily see that

$$\left. \frac{\partial^N q(\alpha, \phi, \mathbf{A})}{\partial \alpha^N} \right|_{\alpha=0} = N! Z_N[\mathbf{y}(\phi, \mathbf{A})], \quad (33)$$

where we have defined the vector $\mathbf{y}(\phi, \mathbf{A}) = (y_1, \dots, y_N)$ in order to make explicit the dependence of the $\{y_k\}$ on ϕ and $\mathbf{A}$. Using this expression, we can recast the linear cross-entropy as

$$\begin{aligned} \text{LXE}(\mathbf{A}, \mathbf{B}; N) &= \frac{1}{(2\pi)^M} \bar{\mathcal{D}}(\mathbf{A}, \mathbf{B}; N) \\ &\times \int_0^{2\pi} Z_N[\mathbf{y}(\phi, \mathbf{A})] Z_N[\mathbf{y}(-\phi, \mathbf{B})] d\phi \end{aligned} \quad (34)$$

with

$$\bar{\mathcal{D}}(\mathbf{A}, \mathbf{B}; N) = (N!)^2 \mathcal{D}(\mathbf{A}, \mathbf{B}; N). \quad (35)$$

B. LXE as a polynomial in the entries of Haar-random unitaries

Consider now the ideal squeezed state model $\mathbf{A}_{\text{sqz}}$. From the definition of $q(\alpha, \phi, \mathbf{A})$ we can see that

$$\begin{aligned} q(\alpha, \mathbf{0}, \mathbf{A}_{\text{sqz}}) &= \{\det[\mathbb{I}_{2M} - \alpha \tanh(r) \mathbf{X}(\mathbf{V} \oplus \mathbf{V}^*)]\}^{-1/2} \\ &= \{\det[\mathbb{I}_M - \alpha^2 \tanh^2(r) \boldsymbol{\xi}]\}^{-1/2} \\ &= [1 - \alpha^2 \tanh^2(r)]^{-R/2}, \end{aligned} \quad (36)$$

where we remind the reader that the squeezed states are sent in the first R modes of the interferometer. Expanding this expression in a Taylor series about $\alpha = 0$, we can prove the relation

$$\left. \frac{\partial^{2N} q(\alpha, \mathbf{0}, \mathbf{A}_{\text{sqz}})}{\partial \alpha^{2N}} \right|_{\alpha=0} = (2N)! \tanh^{2N}(r) \binom{R/2 + N - 1}{N}. \quad (37)$$

Note that the derivatives for odd N identically vanish when evaluated at $\alpha = 0$. This is due to the fact that squeezed states have support only over Fock states with an even number of photons and, moreover, we are considering a lossless (i.e., energy-conserving) interferometer. Using Eq. (37), we reach the result

$$\bar{\mathcal{D}}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N) = \frac{1}{\tanh^{4N}(r)} \binom{R/2 + N - 1}{N}^{-2}. \quad (38)$$

For the general case of $\phi \neq \mathbf{0}$, we can write

$$\begin{aligned} q(\alpha, \phi, \mathbf{A}_{\text{sqz}}) &= \det[\mathbb{I}_{2M} - \alpha \tanh(r) \Omega(\mathbf{V} \oplus \mathbf{V}^*)]^{-1/2} \\ &= \det[\mathbb{I}_M - \alpha^2 \tanh^2(r) \mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*]^{-1/2}, \end{aligned} \quad (39)$$

which can be recast in the form of Eq. (31) as

$$q(\alpha, \phi, \mathbf{A}_{\text{sqz}}) = \sum_{n=0}^{\infty} Z_n(u_1, \dots, u_n) \tanh^{2n}(r) \alpha^{2n}, \quad (40)$$

where $u_k = \frac{1}{2} \text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^k]$. Each u_k depends on ϕ through $\mathbf{D} = \mathbf{D}(\phi)$. Just as before, we can readily see that the derivatives of $q(\alpha, \phi, \mathbf{A}_{\text{sqz}})$ are different from zero when evaluated at $\alpha = 0$ only if N is even. Defining the vector $\mathbf{u}(\phi, \mathbf{U}) = (u_1, \dots, u_N)$, these derivatives can be expressed as

$$\left. \frac{\partial^{2N} q(\alpha, \phi, \mathbf{A}_{\text{sqz}})}{\partial \alpha^{2N}} \right|_{\alpha=0} = (2N)! \tanh^{2N}(r) Z_N[\mathbf{u}(\phi, \mathbf{U})], \quad (41)$$

where Z_N is given in Eq. (32). We can therefore compute $\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)$ using the relation

$$\begin{aligned} \text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N) &= \frac{1}{(2\pi)^M} \binom{R/2 + N - 1}{N}^{-2} \\ &\times \int_0^{2\pi} Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})] Z_N[\mathbf{u}(-\boldsymbol{\phi}, \mathbf{U})] d\boldsymbol{\phi}. \end{aligned} \quad (42)$$

The definition of the $\{u_k\}$ as traces of powers of matrix $\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*$ implies that they can be expanded as polynomials in the entries of matrices $\mathbf{V}$, $\mathbf{D}$, and their complex conjugates. Consequently, the integrand in Eq. (42) will also be a polynomial in the entries of these matrices. The dependence of each term in the expansion on the entries of $\mathbf{V}$ will have the general structure $V_{g_1, g_2} \cdots V_{g_{2l-1}, g_{2l}} V_{h_1, h_2}^* \cdots V_{h_{2m-1}, h_{2m}}^*$, where $\mathbf{g} = (g_1, \dots, g_{2l})$ and $\mathbf{h} = (h_1, \dots, h_{2m})$ are sequences of indices that take values in subsets of $\{1, \dots, M\}$. These terms can be recast as polynomials in the entries of matrix $\mathbf{U}$:

$$\begin{aligned} V_{g_1, g_2} \cdots V_{g_{2l-1}, g_{2l}} V_{h_1, h_2}^* \cdots V_{h_{2m-1}, h_{2m}}^* \\ = \sum_{\boldsymbol{\mu}, \mathbf{v}} \zeta_{\boldsymbol{\mu}} \zeta_{\mathbf{v}} \mathcal{U}(\mathbf{g}, \bar{\boldsymbol{\mu}} \mid \mathbf{h}, \bar{\mathbf{v}}). \end{aligned} \quad (43)$$

Here the indices in $\boldsymbol{\mu} = (\mu_1, \dots, \mu_l)$, $\mathbf{v} = (v_1, \dots, v_m)$ take values in $\{1, \dots, M\}$, so $\sum_{\boldsymbol{\mu}} \equiv \sum_{\mu_1=1}^M \cdots \sum_{\mu_l=1}^M$, and $\bar{\boldsymbol{\mu}} = (\mu_1, \mu_1, \dots, \mu_l, \mu_l)$, $\bar{\mathbf{v}} = (v_1, v_1, \dots, v_m, v_m)$. We conveniently write

$$\zeta_{\boldsymbol{\mu}} = \zeta_{\mu_1} \cdots \zeta_{\mu_l} \quad (44)$$

with the $\{\zeta_k\}$ the diagonal entries of $\boldsymbol{\zeta}$, and

$$\begin{aligned} \mathcal{U}(\mathbf{g}, \bar{\boldsymbol{\mu}} \mid \mathbf{h}, \bar{\mathbf{v}}) &= U_{g_1, \mu_1} U_{g_2, \mu_1} \cdots U_{g_{2l-1}, \mu_l} U_{g_{2l}, \mu_l} \\ &\times U_{h_1, v_1}^* U_{h_2, v_1}^* \cdots U_{h_{2m-1}, v_m}^* U_{h_{2m}, v_m}^*. \end{aligned} \quad (45)$$

Consider the sequences $\mathbf{j} = (j_1, \dots, j_{2N})$ and $\mathbf{j}' = (j'_1, \dots, j'_{2N})$, where $j_k, j'_l \in \{1, \dots, M\}$ for all k, l . Moreover, consider the permutation $\Omega_{\mathbf{k}} \in S_{2N}$ defined in Eq. (14),

$$\begin{aligned} \Omega_{\mathbf{k}}[(j_1, \dots, j_{2N})] \\ = \bigoplus_{a=1}^N \bigoplus_{p=1}^{k_a} \omega_a[(j_{2v_{a-1}+2a(p-1)+1}, \dots, j_{2v_{a-1}+2ap})], \end{aligned}$$

where, let us recall, $v_a = \sum_{p=1}^a p k_p$, $v_0 \equiv 0$, and the permutation ω_a transforms the sequence $(g_1, \dots, g_{2a})$ as

$\omega_a[(g_1, g_2, \dots, g_{2a-1}, g_{2a})] = (g_2, g_3, \dots, g_{2a}, g_1)$. Then, we can write (see Appendix B for details)

$$\begin{aligned} \text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N) &= \binom{R/2 + N - 1}{N}^{-2} \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ &\times \sum_{\mathbf{j}, \mathbf{j}'} I(\mathbf{j}, \mathbf{j}') \sum_{\boldsymbol{\mu}, \mathbf{v}} \zeta_{\boldsymbol{\mu}} \zeta_{\mathbf{v}} \\ &\times \mathcal{U}[\mathbf{j} \oplus \mathbf{j}', \bar{\boldsymbol{\mu}} \mid \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}}(\mathbf{j}'), \bar{\mathbf{v}}] \end{aligned} \quad (46)$$

with

$$I(\mathbf{j}, \mathbf{j}') = \frac{1}{(2\pi)^M} \int_0^{2\pi} \exp \left[\sum_{m \in \mathbf{j}, n \in \mathbf{j}'} 2i(\phi_m - \phi_n) \right] d\boldsymbol{\phi}. \quad (47)$$

C. Integrating the phases away

By inspection of Eq. (47) we can recognize that $I(\mathbf{j}, \mathbf{j}')$ will vanish whenever the sum inside the exponential is different from zero. Indeed, for this case, there must be at least one term of the form $e^{2iz\phi_p}$ for some nonzero integer z and some $p \in \mathbf{j}$ or $\mathbf{j}'$ that is not canceled out and, when integrated with respect to $d\phi_p$, makes the whole integral vanish. When the sum inside the exponential is equal to zero, $I(\mathbf{j}, \mathbf{j}') = 1$. We may then think of $I(\mathbf{j}, \mathbf{j}')$ as an indicator function that, given a fixed $\mathbf{j}$, allows us to keep track of all the ways we can set $\mathbf{j}'$ in order to make the sum inside the exponential vanish. Furthermore, note that the sum inside the exponential will be identically zero whenever $\mathbf{j}'$ is a permutation of $\mathbf{j}$. Since $\mathbf{j}$ might have indices with repeated values, we must take into account the fact that only the *different* permutations that take $\mathbf{j}$ into $\mathbf{j}'$ should be identified by $I(\mathbf{j}, \mathbf{j}')$.

In Appendix C we describe how to use the previous considerations to write Eq. (47) in terms of Kronecker deltas. The final result reads

$$\begin{aligned} I(\mathbf{j}, \mathbf{j}') &= \sum_{\Lambda \in \mathcal{Q}[\mathbf{j}]} \frac{1}{\Lambda!} F(\mathbf{j}', \mathbf{j}[\Lambda, \{j_{\lambda}\}]) \left[\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_{\lambda}, f} \right] \\ &\times \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_{\lambda}, j_{\mu}}). \end{aligned} \quad (48)$$

In this expression Λ represents a *set partition* of $\mathbf{j}$, i.e., a collection of nonempty, mutually disjoint subsets of $\mathbf{j}$ (which are usually called *blocks*), whose union is equal to $\mathbf{j}$; $\mathcal{Q}[\mathbf{j}]$ is the set of all partitions of $\mathbf{j}$. The set $\{j_{\lambda}\}$, which depends on a given partition Λ , is called the set of *representative indices* of Λ , and is constructed by choosing one element, any element, of each block $\lambda \in \Lambda$.

The sequence of indices $\mathbf{j}[\Lambda, \{j_{\lambda}\}]$ is constructed from $\mathbf{j}$ and Λ by using the following prescription: take a partition $\Lambda \in \mathcal{Q}[\mathbf{j}]$ and choose a representative index j_{λ} for

each block $\lambda \in \Lambda$; then replace all the elements in $\mathbf{j}$ that belong to the same block λ by the corresponding representative index j_λ . For example, consider $\mathbf{j} = (j_1, j_2, j_3, j_4)$ and $\Lambda = \{\{j_1, j_3\}, \{j_2, j_4\}\}$. Let $\{j_3, j_2\}$ be the representative indices of the partition; then $\mathbf{j}[\Lambda, \{j_3, j_2\}] = (j_3, j_2, j_3, j_2)$.

Note that the number of representative indices is equal to the number of blocks in Λ . Let $|\lambda|$ denote the length (i.e., the number of elements) of each block $\lambda \in \Lambda$; then $\Lambda! = \prod_{\lambda \in \Lambda} |\lambda|!$.

For two sequences of indices $\mathbf{g} = (g_1, \dots, g_m)$ and $\mathbf{h} = (h_1, \dots, h_m)$, $F(\mathbf{h}, \mathbf{g})$ is defined as

$$F(\mathbf{h}, \mathbf{g}) = \sum_{\sigma \in S_m} \prod_{a=1}^m \delta_{h_a, \sigma(g_a)}, \quad (49)$$

where the $\{\sigma(g_a)\}$ stand for the components of $\sigma(\mathbf{g})$.

Combining Eqs. (46) and (48), and after a careful manipulation of all the Kronecker deltas involved (see Appendix C for details), we can express the LXE as

$$\begin{aligned} \text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N) &= \binom{R/2 + N - 1}{N}^{-2} \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a + l_a}} \\ &\times \sum_{\Lambda \in \mathcal{Q}[\mathbf{j}]} \sum_{\text{diff. } \{j_\lambda\}} \sum_{\sigma \in S_{2N}} \frac{1}{\Lambda!} \\ &\times \sum_{\mu, \nu} \zeta_\mu \zeta_\nu \mathcal{U}[\mathbf{j}_\Lambda \oplus \sigma(\mathbf{j}_\Lambda), \bar{\mu} \mid \Omega_{\mathbf{k}}(\mathbf{j}_\Lambda) \\ &\oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_\Lambda), \bar{\nu}], \end{aligned} \quad (50)$$

where we introduce the short notation $\mathbf{j}_\Lambda \equiv \mathbf{j}[\Lambda, \{j_\lambda\}]$, and $\sigma \circ \tau$ indicates the composition of permutations. The subscript $\text{diff. } \{j_\lambda\}$ indicates that the sum must be done over representative indices taking *different* values in $\{1, \dots, M\}$.

D. Average over the Haar-random unitaries in the asymptotic limit

Following the result in Eq. (50), we can see that computing the average value of $\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)$ over Haar-random unitaries amounts to calculating the expected value of the polynomial

$$\sum_{\mu, \nu} \zeta_\mu \zeta_\nu \mathcal{U}[\mathbf{j}_\Lambda \oplus \sigma(\mathbf{j}_\Lambda), \bar{\mu} \mid \Omega_{\mathbf{k}}(\mathbf{j}_\Lambda) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_\Lambda), \bar{\nu}]. \quad (51)$$

This task can be tackled by using Weingarten calculus [25, 39].

We use two key results concerning the Weingarten calculus for the unitary group. The statements of these theorems, adapted to the notation we have used throughout

the article, can be found in Appendix D. The first of these results can be found in Lemma 3 of Ref. [35], and allows us to write

$$\begin{aligned} \mathbb{E}_{\mathbf{U}} \{ \mathcal{U}[\mathbf{j}_\Lambda \oplus \sigma(\mathbf{j}_\Lambda), \bar{\mu} \mid \Omega_{\mathbf{k}}(\mathbf{j}_\Lambda) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_\Lambda), \bar{\nu}] \} \\ = \sum_{\varrho, \tau \in S_{4N}} \Delta\{\Omega_{\mathbf{k}}(\mathbf{j}_\Lambda) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_\Lambda) \mid \varrho[\mathbf{j}_\Lambda \oplus \sigma(\mathbf{j}_\Lambda)]\} \\ \times \Delta[\bar{\nu} \mid \tau(\bar{\mu})] \text{Wg}_{4N}(\varrho^{-1} \circ \tau; M), \end{aligned} \quad (52)$$

where $\Delta[\mathbf{g} \mid \mathbf{h}] = \prod_{a=1}^m \delta_{g_a, h_a}$ and $\text{Wg}_m(\sigma; M)$ stands for the *Weingarten function* for the unitary group $U(M)$ [25, 39].

Combining Eqs. (51) and (52) we obtain

$$\begin{aligned} \sum_{\mu, \nu} \zeta_\mu \zeta_\nu \mathbb{E}_{\mathbf{U}} \{ \mathcal{U}[\mathbf{j}_\Lambda \oplus \sigma(\mathbf{j}_\Lambda), \bar{\mu} \mid \Omega_{\mathbf{k}}(\mathbf{j}_\Lambda) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_\Lambda), \bar{\nu}] \} \\ = \sum_{\varrho \in \bar{S}_\Lambda} \sum_{\tau \in S_{4N}} \text{Wg}_{4N}(\varrho^{-1} \circ \tau; M) f(\zeta, \tau), \end{aligned} \quad (53)$$

where $\bar{S}_\Lambda \subseteq S_{4N}$ depends on Λ , σ , $\mathbf{k}$, and $\mathbf{l}$, and is defined as

$$\bar{S}_\Lambda = \{ \varrho \in S_{4N} \mid \varrho[\mathbf{j}_\Lambda \oplus \sigma(\mathbf{j}_\Lambda)] = \Omega_{\mathbf{k}}(\mathbf{j}_\Lambda) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_\Lambda) \}. \quad (54)$$

Let us note that $\bar{S}_\Lambda$ is nonempty, since $\Omega_{\mathbf{k}} \oplus \Omega_{\mathbf{l}} \in \bar{S}_\Lambda$. On the other hand,

$$f(\zeta, \tau) = \sum_{\mu} \sum_{\substack{\nu \text{ such that} \\ \bar{\nu} = \tau(\bar{\mu})}} \zeta_\mu \zeta_\nu. \quad (55)$$

Note that $\text{Wg}_{4N}(\varrho^{-1} \circ \tau; M)$ does not depend on the specific values of the indices in $\mathbf{j}_\Lambda$. Rather, through its dependence on the permutations $\varrho \in \bar{S}_\Lambda$, it is determined by the *structure* of $\mathbf{j}_\Lambda$, i.e., by the number of different $\{j_\lambda\}$ and their positions within the sequence.

Since we are interested in the expected value of the linear cross-entropy as $M \rightarrow \infty$, we can focus on the asymptotic behavior of the Weingarten function, which is the subject of the second key result that we use in this section. According to Corollary 2.7 of Ref. [40], as $M \rightarrow \infty$, we can write

$$\begin{aligned} \text{Wg}_{4N}(\varrho^{-1} \circ \tau; M) &= \text{Moeb}(\varrho^{-1} \circ \tau) \frac{1}{M^{4N + \|\varrho^{-1} \circ \tau\|}} \\ &+ \mathcal{O}(M^{-4N - \|\varrho^{-1} \circ \tau\| - 2}), \end{aligned} \quad (56)$$

where $\text{Moeb}(\sigma)$ is the Möbius function (see Appendix D for its definition) and $\|\sigma\|$ denotes the minimum number of transpositions in which we can write σ .

Since $\|\varrho^{-1} \circ \tau\| \geq 0$, we can recognize that the leading order term in the asymptotic expansion in Eq. (56)

decays at least as fast as M^{-4N} . Taking into account the facts that, when $\tau = \varrho$, $\|\varrho^{-1} \circ \tau\| = \|e_{4N}\| = 0$ and $\text{Moeb}(\varrho^{-1} \circ \tau) = \text{Moeb}(e_{4N}) = 1$, with e_{4N} the identity permutation in S_{4N} , we can write the asymptotic form of Eq. (53) as

$$\sum_{\mu, \nu} \zeta_{\mu} \zeta_{\nu} \mathbb{E}_{\mathbf{U}}[\mathcal{U}[\mathbf{j}_{\Lambda} \oplus \sigma(\mathbf{j}_{\Lambda}), \bar{\mu} \mid \Omega_{\mathbf{k}}(\mathbf{j}_{\Lambda}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}_{\Lambda}), \bar{\nu}]] \\ = \sum_{\varrho \in \tilde{S}_{\Lambda}} f(\zeta, \varrho) M^{-4N} + \mathcal{O}(M^{-4N-1}). \quad (57)$$

Bringing together the results in Eqs. (57) and (50) we obtain the following expression for the average value of $\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)$:

$$\mathbb{E}_{\mathbf{U}}[\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)] \\ = \left(\frac{R/2 + N - 1}{N} \right)^{-2} \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ \times \sum_{\Lambda \in \mathcal{Q}[\mathbf{j}]} \sum_{\sigma \in S_{2N}} \frac{1}{\Lambda!} \\ \times \sum_{\text{diff. } \{j_{\lambda}\}} \left(\sum_{\varrho \in \tilde{S}_{\Lambda}} f(\zeta, \varrho) M^{-4N} + \mathcal{O}(M^{-4N-1}) \right), \quad (58)$$

where we were able to move the sum over different $\{j_{\lambda}\}$ past the sum over $\sigma \in S_{2N}$ and the term $1/\Lambda!$ because neither of them depends on the specific values that the $\{j_{\lambda}\}$ take.

In fact, there are no longer any terms in Eq. (58) that depend on the specific values of these indices. Indeed, as we argued before, the sum over permutations in $\tilde{S}_{\Lambda}$, as well as the terms of order $\mathcal{O}(M^{-4N-1})$, will depend only on the structure of $\mathbf{j}_{\Lambda}$, which is determined by Λ . Consequently, we can make the replacement

$$\sum_{\text{diff. } \{r_{\lambda}\}} \rightarrow \frac{M!}{(M - N_{\Lambda})!} = M^{N_{\Lambda}} + \mathcal{O}(M^{N_{\Lambda}-1}), \quad (59)$$

where N_{Λ} is the number of different $\{j_{\lambda}\}$, i.e., the number of blocks in Λ . This allows us to write

$$\sum_{\text{diff. } \{j_{\lambda}\}} \left(\sum_{\varrho \in \tilde{S}_{\Lambda}} f(\zeta, \varrho) M^{-4N} + \mathcal{O}(M^{-4N-1}) \right) \\ = \sum_{\varrho \in \tilde{S}_{\Lambda}} f(\zeta, \varrho) M^{-4N+N_{\Lambda}} + \mathcal{O}(M^{-4N+N_{\Lambda}-1}). \quad (60)$$

Given that $1 \leq N_{\Lambda} \leq 2N$, with $N_{\Lambda} = 2N$ for $\Lambda = \{\{j_1\}, \dots, \{j_{2N}\}\}$, we can see that the leading term in the asymptotic expansion of the average LXE decays as M^{-2N} .

On this account, and keeping in mind that $\Lambda! = 1$ for the leading term, we may write Eq. (58) as

$$\mathbb{E}_{\mathbf{U}}[\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)] \\ = \left(\frac{R/2 + N - 1}{N} \right)^{-2} \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ \times \left(\sum_{\sigma \in S_{2N}} \sum_{\varrho \in \tilde{S}} f(\zeta, \varrho) M^{-2N} + \mathcal{O}(M^{-2N-1}) \right), \quad (61)$$

where

$$\tilde{S} = \{\varrho \in S_{4N} \mid \varrho[\mathbf{j} \oplus \sigma(\mathbf{j})] = \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})\}. \quad (62)$$

E. Final expression of the ideal LXE score

Recall that in the definition of the LXE score given in Eq. (8) there is one extra term that depends on the number of modes M , namely, the normalization factor

$$\binom{M + 2N - 1}{2N} = \frac{\Gamma(M + 2N)}{\Gamma(2N + 1)\Gamma(M)}.$$

For a fixed $2N$, $\Gamma(M + 2N)/\Gamma(M) \sim M^{2N}$ as $M \rightarrow \infty$, so we can write the following asymptotic expression for the binomial coefficient:

$$\binom{M + 2N - 1}{2N} \sim \frac{M^{2N}}{(2N)!}. \quad (63)$$

On these grounds, and noting that

$$\left(\frac{R/2 + N - 1}{N} \right) = \frac{1}{2^N N!} \frac{(R + 2N - 2)!!}{(R - 2)!!},$$

we are now able to write

$$s(\mathbf{A}_{\text{sqz}}; 2N) = \lim_{M \rightarrow \infty} \binom{M + 2N - 1}{2N} \\ \times \mathbb{E}_{\mathbf{U}}[\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)] \\ = \frac{4^N (N!)^2}{(2N)!} \left[\frac{(R - 2)!!}{(R + 2N - 2)!!} \right]^2 \\ \times \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ \times \sum_{\sigma \in S_{2N}} \sum_{\varrho \in \tilde{S}} f(\zeta, \varrho). \quad (64)$$

At this point we may take into account the fact that the entries of the diagonal matrix ζ satisfy $\zeta_a = 1$ for $1 \leq a \leq$

R , and $\zeta_a = 0$ otherwise. This allows us to see that

$$f(\zeta, \varrho) = \sum_{\mu \in [R]^{2N}} \sum_{\substack{\nu \in [R]^{2N} \\ \text{such that } \bar{\nu} = \varrho(\bar{\mu})}} 1, \quad (65)$$

where the symbol $\mu \in [R]^{2N}$ indicates that each μ_a , $a = 1, \dots, 2N$, takes values in the set $[R] = \{1, \dots, R\}$. According to Lemma 6 of Ref. [35], the sum in the last expression satisfies the relation

$$\sum_{\mu \in [R]^{2N}} \sum_{\substack{\nu \in [R]^{2N} \\ \text{such that } \bar{\nu} = \varrho(\bar{\mu})}} 1 = R^{\ell(\varrho)}, \quad (66)$$

where $\ell(\varrho)$ is the *length of the coset type* of ϱ [25,35].

In order to understand the meaning of $\ell(\varrho)$, let us state the definition of the *coset type* of a permutation given in Ref. [25] (see Fig. 3 for an example). Let $\sigma \in S_{2m}$. We can assign to this permutation an *undirected graph* $\Gamma(\sigma)$, whose vertices are $1, 2, \dots, 2m$, and whose edges are defined by $\{(2k-1, 2k) \mid k \in \{1, \dots, m\}\}$ and $\{[\sigma(2k-1), \sigma(2k)] \mid k \in \{1, \dots, m\}\}$. Note that there are a total of $2m$ edges, and each vertex lies in exactly two edges. This implies that the *connected components* of the graph have an even number of edges [25]. Call the lengths of such connected components $2\eta_1, 2\eta_2, \dots, 2\eta_l$ and arrange them so that $\eta_1 \geq \eta_2 \geq \dots \geq \eta_l \geq 1$. Then, $\eta(\sigma) = (\eta_1, \eta_2, \dots, \eta_l)$ is an *integer partition* of m , and is called the *coset type* of σ . The length of the coset type of σ will then be the length of the partition $\eta(\sigma)$, or, equivalently, the number of connected components in graph $\Gamma(\sigma)$.

According to the previous definition, we can see that $1 \leq \ell(\varrho) \leq 2N$, which in turn allows us to write

$$\sum_{\varrho \in \bar{S}} f(\zeta, \varrho) = \sum_{\varrho \in \bar{S}} R^{\ell(\varrho)} = \sum_{\ell=1}^{2N} b_\ell R^\ell, \quad (67)$$

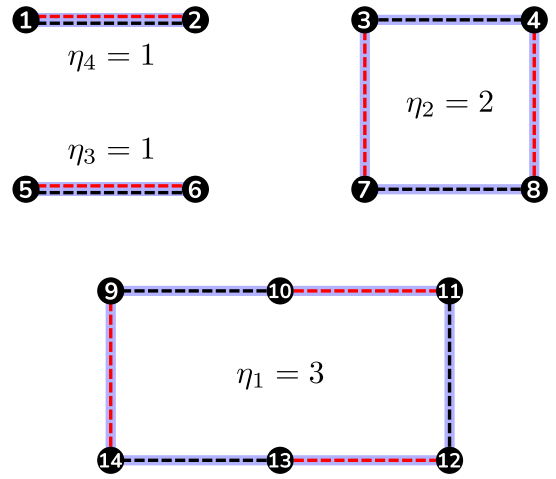
where

$$b_\ell \equiv b_\ell[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})] \quad (68)$$

is the number of permutations $\varrho \in S_{4N}$ that take $\mathbf{j} \oplus \sigma(\mathbf{j})$ into $\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})$, and whose coset type has length ℓ [or, equivalently, whose associated graphs $\Gamma(\varrho)$ have ℓ connected components].

Combining Eqs. (64) and (67), and defining [see Eq. (15)]

$$c_\ell = \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \times \sum_{\sigma \in S_{2N}} b_\ell[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})], \quad (69)$$



$$\sigma = (1\ 2)(3)(4\ 7\ 6\ 8\ 5)(9\ 10\ 11\ 12\ 13\ 14)$$

FIG. 3. Illustration of the definition of the coset type of σ for $\sigma = (1\ 2)(3)(4\ 7\ 6\ 8\ 5)(9\ 10\ 11\ 12\ 13\ 14)$. Note that σ is an element of S_{2m} with $m = 7$. The vertices of the undirected graph $\Gamma(\sigma)$ are represented by numbered black circles. Edges of the form $(2k-1, 2k)$, that correspond to the set $\{(1, 2), (3, 4), (5, 6), (7, 8), (9, 10), (11, 12), (12, 14)\}$, are drawn with black dashed lines. Edges of the form $[\sigma(2k-1), \sigma(2k)]$ are obtained after the application of σ over the pairs $(2k, 2k-1)$ and correspond to the set $\{(2, 1), (3, 7), (4, 8), (6, 5), (10, 11), (12, 13), (14, 9)\}$. These edges are shown as red dashed lines. Each connected component of the graph is highlighted with a light blue, thick line. As can be seen, there are a total of four connected components, all of them cycles, with lengths $2\eta_b$, $b = 1, 2, 3, 4$. This implies that the coset type of σ is $\eta(\sigma) = (3, 2, 1, 1)$, and its length is $\ell(\sigma) = 4$. We can readily check that $\eta(\sigma)$ is an integer partition of $m = 7$.

we finally obtain the result stated in Eq. (13), at the very beginning of this section:

$$s(\mathbf{A}_{\text{sqz}}; 2N) = \frac{4^N (N!)^2}{(2N)!} \left[\frac{(R-2)!!}{(R+2N-2)!!} \right]^2 \sum_{\ell=1}^{2N} c_\ell R^\ell.$$

V. LXE SCORE FOR THE IDEAL SQUEEZED STATE MODEL WITH DIFFERENT SQUEEZING PARAMETERS

We can readily generalize the methods presented in the last section to determine the ideal score for GBS setups that use input squeezed states with different squeezing parameters.

Suppose that the first R modes of the interferometer receive single-mode squeezed states with squeezing parameters $\{r_k\}$, $k \in \{1, \dots, R\}$, while the remaining $M - R$ modes receive the vacuum state. The matrix $\mathbf{A}'_{\text{sqz}}$ describing this setup can be written as (see Appendix A)

$$\mathbf{A}'_{\text{sqz}} = \mathbf{V} \oplus \mathbf{V}^*, \quad (70)$$

where $\mathbf{V} = \mathbf{U}\boldsymbol{\zeta}'\mathbf{U}^T$, with $\boldsymbol{\zeta}' = \tanh(\mathbf{r}) \oplus \mathbf{0}_{M-R}$ and $\tanh(\mathbf{r}) = \text{diag}[\tanh(r_1), \dots, \tanh(r_R)]$.

Models $\mathbf{A}'_{\text{sqz}}$ and $\mathbf{A}_{\text{sqz}}$ [which was defined in Eq. (11)] differ only in the definition of the diagonal matrix $\boldsymbol{\zeta}'$. This suggests that we can compute the ideal score associated with $\mathbf{A}'_{\text{sqz}}$ by making the replacement

$$\tanh(\mathbf{r})\boldsymbol{\zeta} \rightarrow \boldsymbol{\zeta}' = \tanh(\mathbf{r}) \oplus \mathbf{0}_{M-R},$$

while keeping all the procedures shown in Sec. IV mostly the same. Following this strategy, we can see that the change from $\mathbf{A}_{\text{sqz}}$ to $\mathbf{A}'_{\text{sqz}}$ will become manifest in two terms: the factor $\bar{D}(\mathbf{A}'_{\text{sqz}}, \mathbf{A}'_{\text{sqz}}, 2N)$ defined in Eq. (35), and the function $f(\boldsymbol{\zeta}', \tau)$ defined in Eq. (55).

To compute $\bar{D}(\mathbf{A}'_{\text{sqz}}, \mathbf{A}'_{\text{sqz}}, 2N)$, we note that, according to Eqs. (33) and (41),

$$\frac{1}{(2N)!} \frac{\partial^{2N} q(\alpha, \boldsymbol{\phi}, \mathbf{A}'_{\text{sqz}})}{\partial \alpha^{2N}} \Big|_{\alpha=0} = \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{1}{k_a!} \frac{1}{a^{k_a}} \prod_{a=1}^N u_a^{k_a}, \quad (71)$$

where $u_a = \frac{1}{2} \text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^a]$. When $\boldsymbol{\phi} = \mathbf{0}$, we have $\mathbf{D} = \mathbb{I}_M$, and so

$$u_a = \frac{1}{2} \text{tr}[(\mathbf{V} \mathbf{V}^*)^a] = \frac{1}{2} \text{tr}[(\boldsymbol{\zeta}')^{2a}] = \frac{1}{2} \sum_{k=1}^R \tanh^{2a}(r_k).$$

By defining

$$\varepsilon_a = \frac{1}{R} \sum_{k=1}^R \tanh^a(r_k), \quad (72)$$

where we note that $0 < |\varepsilon_a| < 1$ for all a and R , we can write $u_a = \frac{1}{2} \varepsilon_{2a} R$, and

$$\begin{aligned} \frac{1}{(2N)!} \frac{\partial^{2N} q(\alpha, \mathbf{0}, \mathbf{A}'_{\text{sqz}})}{\partial \alpha^{2N}} \Big|_{\alpha=0} &= \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{\varepsilon_{2a}^{k_a} R^{k_a}}{k_a! (2a)^{k_a}} \\ &= \sum_{\ell=1}^N d'_\ell R^\ell. \end{aligned} \quad (73)$$

The last equality above is obtained by noting that the non-negative integer components of $\mathbf{k} = (k_1, \dots, k_N)$ satisfy the constraint $k_1 + 2k_2 + \dots + Nk_N = N$. For each $\mathbf{k}$, the sum $\sum_{\mathbf{k}^{(c)}}$ will include a term proportional to $R^{k_1 + \dots + k_N}$, which can be at least R (for $k_N = 1$ and $k_a = 0$ for all $a \neq N$) and at most R^N (for $k_1 = N$ and $k_a = 0$ for all $a \neq 1$).

From Eq. (73), and using Eq. (29), we may write

$$\bar{D}(\mathbf{A}'_{\text{sqz}}, \mathbf{A}'_{\text{sqz}}, 2N) = \left(\sum_{\ell=1}^N d'_\ell R^\ell \right)^{-2}. \quad (74)$$

This expression leads to the following modified form of Eq. (64):

$$\begin{aligned} s(\mathbf{A}'_{\text{sqz}}; 2N) &= \frac{1}{(2N)!} \left(\sum_{\ell=1}^N d'_\ell R^\ell \right)^{-2} \\ &\times \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a + l_a}} \sum_{\sigma \in S_{2N}} \\ &\times \sum_{\varrho \in \bar{S}} f(\boldsymbol{\zeta}', \varrho) \end{aligned} \quad (75)$$

with $f(\boldsymbol{\zeta}', \varrho)$ now computed as

$$\begin{aligned} f(\boldsymbol{\zeta}', \varrho) &= \sum_{\boldsymbol{\mu}} \sum_{\substack{\mathbf{v} \text{ such that} \\ \bar{\mathbf{v}} = \varrho(\bar{\boldsymbol{\mu}})}} \zeta'_{\boldsymbol{\mu}} \zeta'_{\mathbf{v}} \\ &= \sum_{\boldsymbol{\mu} \in [R]^{2N}} \sum_{\substack{\mathbf{v} \in [R]^{2N} \\ \text{such that } \bar{\mathbf{v}} = \varrho(\bar{\boldsymbol{\mu}})}} \prod_{a=1}^{2N} \tanh(r_{\mu_a}) \tanh(r_{v_a}). \end{aligned} \quad (76)$$

In Appendix E, we prove that Eq. (76) reduces to

$$f(\boldsymbol{\zeta}', \varrho) = \left(\prod_{b \in \eta(\varrho)} \varepsilon_{2b} \right) R^{\ell(\varrho)}, \quad (77)$$

where, let us remind the reader, $\eta(\varrho)$ stands for the coset type of ϱ , and $\ell(\varrho)$ is the length of $\eta(\varrho)$ [or, equivalently, the number of connected components in the undirected graph $\Gamma(\varrho)$].

If we recall that $1 \leq \ell(\varrho) \leq 2N$, we can define the subset $\bar{S}_\ell \subset S_{4N}$ as

$$\begin{aligned} \bar{S}_\ell &= \{\varrho \in S_{4N} \mid \varrho[\mathbf{j} \oplus \sigma(\mathbf{j})] = \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}) \\ &\text{and } \Gamma(\varrho) \text{ has } \ell \text{ connected components}\}, \end{aligned} \quad (78)$$

and write

$$\sum_{\varrho \in \bar{S}} f(\boldsymbol{\zeta}', \varrho) = \sum_{\ell=1}^{2N} \left(\sum_{\varrho \in \bar{S}_\ell} \prod_{b \in \eta(\varrho)} \varepsilon_{2b} \right) R^\ell, \quad (79)$$

thus verifying that $\sum_{\varrho \in \bar{S}} f(\boldsymbol{\zeta}', \varrho)$ remains a polynomial of degree $2N$ in R .

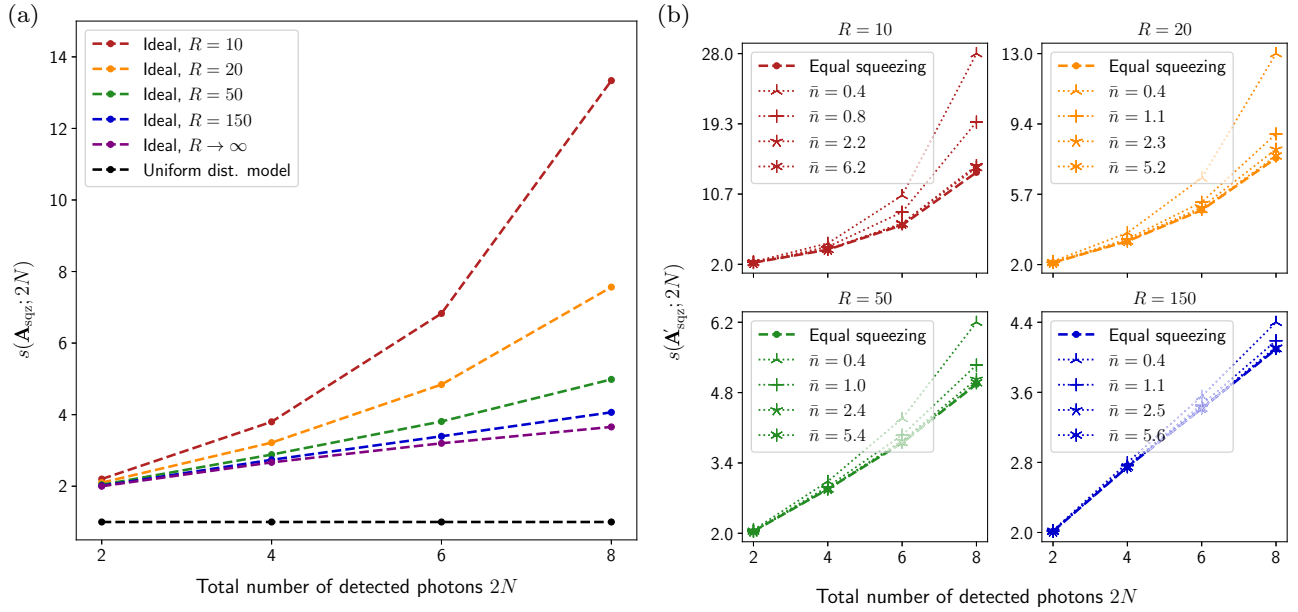


FIG. 4. (a) Ideal LXE score as a function of the total number of detected photons, $2N$. The purple dashed line shows the score for an ideal squeezed state model with no vacuum input modes (as indicated by the label $R \rightarrow \infty$). The black dashed line shows the score for model $\mathbf{A}_{\text{uni}}$, which leads to a uniform distribution over the sample space. The score for this model is identically 1 for every N . The remaining lines correspond to the ideal squeezed state model $\mathbf{A}_{\text{sqz}}$, where the first R modes receive identical single-mode squeezed states and the remaining $M - R$ modes receive the vacuum state. The red dashed line corresponds to $R = 10$, the orange dashed line to $R = 20$, the green dashed line to $R = 50$, and the blue dashed line to $R = 150$. (b) Ideal LXE score as a function of the total number of detected photons, $2N$, for GBS setups using input states with different squeezing parameters. The dotted lines were obtained by randomly selecting the squeezing parameters of the R input squeezed states. For each value of R , there are four sets of squeezing parameters, each of them identified by their corresponding mean number of photons $\bar{n} = (1/R) \sum_{k=1}^R \sinh^2(r_k)$. The dashed lines show the scores for the case of identical squeezing in the input modes. The red lines correspond to $R = 10$, the orange lines to $R = 20$, the green lines to $R = 50$, and the blue lines to $R = 150$.

Combining Eqs. (75) and (79) we obtain the final expression for the ideal LXE score for model $\mathbf{A}'_{\text{sqz}}$:

$$s(\mathbf{A}'_{\text{sqz}}; 2N) = \frac{1}{(2N)!} \left(\sum_{\ell=1}^N d'_\ell R^\ell \right)^{-2} \sum_{\ell=1}^{2N} c'_\ell R^\ell \quad (80)$$

with

$$c'_\ell = \sum_{\mathbf{k} \in \mathcal{S}_{2N}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\sigma \in \mathcal{S}_{2N}} \sum_{\ell \in \mathcal{S}_\ell} \prod_{b \in \eta(\ell)} \varepsilon_{2b}. \quad (81)$$

Again, in Appendix E, we prove that if $r_k = r$ for all $k \in \{1, \dots, R\}$, $s(\mathbf{A}'_{\text{sqz}}; 2N)$ becomes independent of r and we recover $s(\mathbf{A}_{\text{sqz}}; 2N)$ identically, showing the consistency between Eqs. (13) and (80).

The main difference between scores $s(\mathbf{A}_{\text{sqz}}; 2N)$ and $s(\mathbf{A}'_{\text{sqz}}; 2N)$ is that the latter shows an explicit dependence on the input squeezing parameters. In order to properly account for this dependence, we need not only determine the number of connected components in $\Gamma(\varrho)$, but also the lengths of all connected components in the graph.

Figure 4(b) shows scores $s(\mathbf{A}_{\text{sqz}}; 2N)$ and $s(\mathbf{A}'_{\text{sqz}}; 2N)$ as functions of $2N$ for $R \in \{10, 20, 50, 150\}$, and for different choices of the input squeezing parameters. Brute-force computation of the coefficients $\{c_\ell\}$ and $\{c'_\ell\}$ for values of $2N > 8$ proves to be difficult due to the increasing number of elements in set $\tilde{S}$. In view of this, we only show the exact computation of the scores for $2 \leq 2N \leq 8$. For each value of R , we randomly selected four sets of input squeezing parameters, making sure that every set had a different mean number of photons $\bar{n} = (1/R) \sum_{k=1}^R \sinh^2(r_k)$. For $R = 10$, we obtained $\bar{n} \in \{0.4, 0.8, 2.2, 6.2\}$; for $R = 20$, $\bar{n} \in \{0.4, 1.1, 2.3, 5.2\}$; for $R = 50$, $\bar{n} \in \{0.4, 1.0, 2.4, 5.4\}$; and for $R = 150$, $\bar{n} \in \{0.4, 1.1, 2.5, 5.6\}$. We computed the coefficients $\{c_\ell\}$ and $\{c'_\ell\}$ using the methods in the libraries Sympy [41] and graph-theory [42].

As can be seen, when we increase the value of $\bar{n}$, $s(\mathbf{A}'_{\text{sqz}}; 2N)$ approaches the score that would be obtained by a model that uses input states with the same squeezing parameter. Interestingly, $s(\mathbf{A}'_{\text{sqz}}; 2N)$ appears to approach $s(\mathbf{A}_{\text{sqz}}; 2N)$ more rapidly with increasing R . This suggests that, in the limit of large R , $s(\mathbf{A}'_{\text{sqz}}; 2N)$ will be approximately equal to the score of an ideal model with uniform squeezing, no matter the choice of the input squeezing

parameters. This behavior nicely connects with the results of the next section.

VI. LXE SCORE FOR THE IDEAL SQUEEZED STATE MODEL WITHOUT VACUUM INPUT MODES

An interesting instance of the ideal squeezed state model is obtained when $R = M$, i.e., when all the input modes in the interferometer receive single-mode squeezed states. The computation of the ideal score for this type of setup can be done by taking the limit as $R \rightarrow \infty$ of Eqs. (13) and (80).

Let us consider first the case of $s(\mathbf{A}_{\text{sqz}}; 2N)$, given in Eq. (13). For large R ,

$$\left[\frac{(R-2)!!}{(R+2N-2)!!} \right]^2 \sim R^{-2N}.$$

Thus, when taking the limit, the only nonvanishing contribution from the polynomial $\sum_{\ell} c_{\ell} R^{\ell}$ will be associated with the term $c_{2N} R^{2N}$. This allows us to write the ideal score as

$$s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N) = \lim_{R \rightarrow \infty} s(\mathbf{A}_{\text{sqz}}; 2N) = \frac{4^N (N!)^2}{(2N)!} c_{2N}. \quad (82)$$

In the case of $s(\mathbf{A}'_{\text{sqz}}; 2N)$, we have, from Eq. (80),

$$\left(\sum_{\ell=1}^N d'_{\ell} R^{\ell} \right)^{-2} \sim (d'_N)^{-2} R^{-2N},$$

when $R \rightarrow \infty$, which implies that the only nonvanishing contribution from the polynomial $\sum_{\ell} c'_{\ell} R^{\ell}$ will be associated with the term $c'_{2N} R^{2N}$. Then,

$$s(\mathbf{A}'_{\text{sqz}}; 2N) \sim \frac{1}{(2N)!} \frac{c'_{2N}}{(d'_N)^2}. \quad (83)$$

We can see in Eq. (73) that the only contribution to d'_N comes from a vector $\mathbf{k}$ satisfying $k_1 = N$ and $k_a = 0$ otherwise. This means that

$$d'_N = \frac{\varepsilon_2^{k_1}}{k_1! 2^{k_1}} = \frac{\varepsilon_2^N}{2^N N!}. \quad (84)$$

Following Eq. (81), we see that c'_{2N} is determined by computing the coset type of the permutations $\varrho \in \bar{S}_{2N}$. By definition, every $\varrho \in \bar{S}_{2N}$ has an associated graph $\Gamma(\varrho)$ with $2N$ connected components, which implies that every connected component in $\Gamma(\varrho)$ has length 2. This means that all $\varrho \in \bar{S}_{2N}$ have coset type $\eta(\varrho) = (1, \dots, 1)$, where

1 appears a total of $2N$ times. Consequently,

$$\sum_{\varrho \in \bar{S}_{2N}} \prod_{b \in \eta(\varrho)} \varepsilon_{2b} = \sum_{\varrho \in \bar{S}_{2N}} \prod_{a=1}^{2N} \varepsilon_2 = \varepsilon_2^{2N} |\bar{S}_{2N}|. \quad (85)$$

Recalling Eq. (78) and the definition of the coefficients b_{ℓ} given in Eq. (68), we can verify that

$$|\bar{S}_{2N}| = b_{2N} [\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})], \quad (86)$$

and, thus,

$$\begin{aligned} c'_{2N} &= \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\sigma \in S_{2N}} \varepsilon_2^{2N} |\bar{S}_{2N}| \\ &= \varepsilon_2^{2N} \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\sigma \in S_{2N}} b_{2N} \\ &= \varepsilon_2^{2N} c_{2N}. \end{aligned} \quad (87)$$

Combining Eqs. (83), (84), and (87), we conclude that

$$s(\tilde{\mathbf{A}}'_{\text{sqz}}; 2N) = \lim_{R \rightarrow \infty} s(\mathbf{A}'_{\text{sqz}}; 2N) = \frac{4^N (N!)^2}{(2N)!} c_{2N}, \quad (88)$$

i.e., the ideal score for a setup with no vacuum input modes will have the same value, whether we use input squeezed states with the same squeezing parameter or not.

The permutations $\varrho \in S_{4N}$ whose associated undirected graphs $\Gamma(\varrho)$ have $2N$ connected components constitute the *hyperoctahedral group* of degree $2N$, H_{2N} [35] (see Definition 1 in Appendix F). We may therefore say that the coefficient b_{2N} is the number of permutations in H_{2N} that take $\mathbf{j} \oplus \sigma(\mathbf{j})$ into $\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})$ for given $\mathbf{k}, \mathbf{l}$, and σ .

In Appendix F we prove that

$$c_{2N} = \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\sigma \in S_{2N}} b_{2N} = 1 \quad (89)$$

for every N , which implies that

$$s(\tilde{\mathbf{A}}'_{\text{sqz}}; 2N) = s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N) = \frac{4^N (N!)^2}{(2N)!}. \quad (90)$$

Figure 4(a) shows the values of scores $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$ and $s(\mathbf{A}_{\text{sqz}}; 2N)$ as functions of $2N$ for $R \in \{10, 20, 50, 150\}$. The computation of the coefficients $\{c_{\ell}\}$ becomes increasingly difficult for values of $2N > 8$ due to the sharp increase in the number of elements in $\bar{S}$. For this reason, we only show the scores for $2 \leq 2N \leq 8$. As can be seen, the value of the score for finite R is greater than the score of an ideal model with no vacuum input modes. For small

values of R , $s(\mathbf{A}_{\text{sqz}}; 2N)$ quickly diverges from $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$ when we increase $2N$. In contrast, for values of $R \sim 150$, $s(\mathbf{A}_{\text{sqz}}; 2N)$ seems to closely follow $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$. As shown in Fig. 4(b), this behavior can also be expected for models that use input squeezed states with different squeezing parameters.

Equation (90) is consistent with the ideal score found in a recent work by Ehrenberg *et al.* [26,27]. Their result was obtained by computing the first and second moments of the modulus squared of hafnians of random Gaussian matrices, which, according to the hiding conjecture [5,28,29], approximate the GBS distribution in the photon-collision-free limit. We did not use the hiding conjecture in our derivation of Eq. (90). However, defining the score in the limit $M \rightarrow \infty$ implies that our results are only valid in the photon-collision-free regime.

The analytical computation of the LXE score for setups that are not in the limit of $M \rightarrow \infty$ is beyond the scope of this work. However, we can study the behavior of the ideal score in this regime by numerically computing $\bar{s}_{\text{sqz}}(2N)$, as indicated in Eq. (9). Let us recall that $\bar{s}(N)$ is an estimator of the LXE score determined by computing the probabilities of a given set of samples with respect to an ideal squeezed state model. In the case of $\bar{s}_{\text{sqz}}(2N)$, the samples correspond to the ideal model itself. The procedure to determine $\bar{s}_{\text{sqz}}(2N)$ is the following. For a given value of M , generate a Haar-random unitary matrix. Using this unitary, generate a set of L samples from the probability distribution of the ideal squeezed state model, and compute their corresponding probabilities. All the samples must have $2N$ detected photons. Finally, compute estimator $\bar{s}_{\text{sqz}}(2N)$ using Eq. (9).

It is important to remember that sampling from the probability distribution of an ideal squeezed state model, as well as computing the corresponding probabilities, is a computationally hard task whose cost grows exponentially with the total number of detected photons in the samples. This means that the numerical computation of $\bar{s}_{\text{sqz}}(2N)$ is restricted, in practice, to low values of $2N$.

We numerically estimated $\bar{s}_{\text{sqz}}(2N)$ for GBS setups with $M \in \{50, 100, 200\}$. We chose these values of M because they are close to those used in recent experimental implementations of GBS [7–10]. We focused on ideal models with no vacuum input modes so we can compare the estimated scores with Eq. (90), which can be easily computed for $2N > 8$. We also considered input states with the same squeezing parameter, which was set so that the mean number of photons were $\bar{n} = 20$ for all three values of M . Therefore, $r = 0.60$ for $M = 50$, $r = 0.43$ for $M = 100$, and $r = 0.31$ for $M = 200$. Note, however, that the definition of $\mathbf{A}_{\text{sqz}}$ makes $\bar{s}_{\text{sqz}}(2N)$ independent of our choice of squeezing parameters. For each value of M , we generated ten Haar-random unitaries, and for each unitary, we generated $L = 1000$ samples per value of $2N$. We computed the scores for $10 \leq 2N \leq 26$. The generation

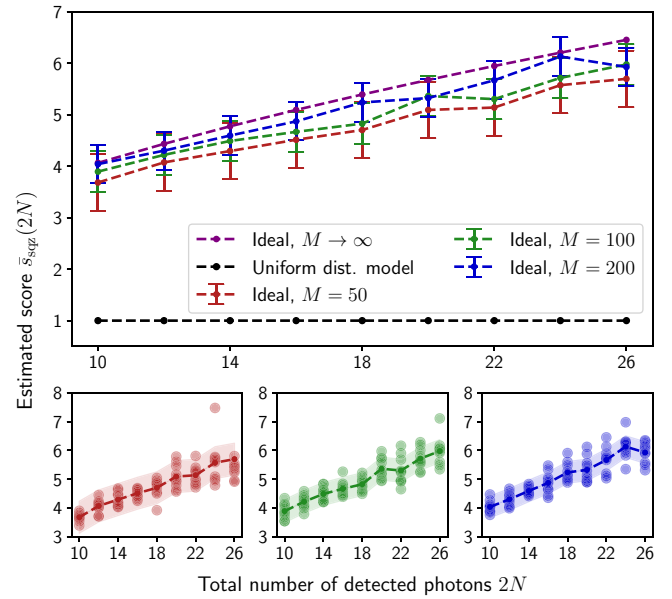


FIG. 5. Estimated score $\bar{s}_{\text{sqz}}(2N)$ as a function of $2N$. The violet dashed line corresponds to the score of an ideal model with $M \rightarrow \infty$. The black dashed line corresponds to a model that leads to a uniform distribution over the sample space. The remaining lines show the average estimated score $\langle \bar{s}_{\text{sqz}}(2N) \rangle$: the red dashed line corresponds to $M = 50$, the green dashed line to $M = 100$, and the blue dashed line to $M = 200$. Error bars show the uncertainty in the estimation of the average score. The colored circles shown in the small plots at the bottom indicate the values of $\bar{s}_{\text{sqz}}(2N)$ for each of the ten Haar-random unitaries used in the calculation of the corresponding average. The estimation of each of these values was done using $L = 1000$ samples. The shaded regions indicate how many unitaries obtain values of the score within the error of the estimated average value.

of all Haar-random unitaries and samples, as well as the computation of the probabilities of each individual sample, were done using the methods in the library `thewalrus` [43].

Figure 5 shows the results of the computation of $\bar{s}_{\text{sqz}}(2N)$ as a function of $2N$. The colored circles in the small figures at the bottom represent the values of $\bar{s}_{\text{sqz}}(2N)$ for each of the ten Haar-random unitaries. The dashed lines with error bars correspond to the average of these values, which we denote $\langle \bar{s}_{\text{sqz}}(2N) \rangle$. As was mentioned below Eq. (9), the estimated score can be interpreted as the average of the probabilities of each individual sample (with respect to the ideal model) multiplied by a constant. Consequently, the error of each $\bar{s}_{\text{sqz}}(2N)$ corresponds to the standard error of the mean. The uncertainty of $\langle \bar{s}_{\text{sqz}}(2N) \rangle$, which leads to the error bars shown in Fig. 5, is computed through error propagation.

We can see that the average estimated score, for all the values of M considered, closely resembles the analytical result in the limit of $M \rightarrow \infty$. Indeed, the relative

difference between $\langle \bar{s}_{\text{sqz}}(2N) \rangle$ and $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$,

$$\Delta(2N) = \frac{s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N) - \langle \bar{s}_{\text{sqz}}(2N) \rangle}{s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)} \times 100\%, \quad (91)$$

satisfies $8.12\% \leq \Delta(2N) \leq 13.57\%$ for $M = 50$, $4.17\% \leq \Delta(2N) \leq 10.82\%$ for $M = 100$, and $0.58\% \leq \Delta(2N) \leq 8.16\%$ for $M = 200$.

Interestingly, $\langle \bar{s}_{\text{sqz}}(2N) \rangle$ approaches $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$ more rapidly for small values of $2N$, while $\langle \bar{s}_{\text{sqz}}(2N) \rangle$ and $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$ seem to diverge for large $2N$. The divergence is faster the smaller M is. This suggests that the range of total detected photons for which $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$ will be a good approximation of $\bar{s}_{\text{sqz}}(2N)$ depends on the number of modes considered. One condition to ensure that the GBS distribution is in the photon-collision-free regime is that the mean number of photons $\bar{n}$ satisfies $\bar{n} \in o(\sqrt{M})$ [5,28,29]. Since $\bar{n}$ determines the range of $2N$ in which it is more likely to find experimental samples, and considering that Eq. (90) is only valid in the collision-free limit, we may say that $s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N)$ will be a good approximation of $\bar{s}_{\text{sqz}}(2N)$ for a range of total detected photons satisfying $2N \in o(\sqrt{M})$.

We can also see that most of the estimated $\bar{s}_{\text{sqz}}(2N)$ take values within the uncertainty of the average estimated score, even for a number of modes as low as $M = 50$. This confirms that typical GBS implementations obtain ideal scores that are close to the average over Haar-random unitaries.

To conclude this section, we numerically investigate the score that would be obtained by GBS setups with transmission losses. This study would give us an idea of how sensitive the LXE score is to the presence of noise. To do this, we consider a simple model in which the input squeezed states are sent through single-mode loss channels before entering a Haar-random unitary interferometer. We consider that there are no vacuum input modes, that all input states have the same squeezing, and that all loss channels have the same transmission parameter, η . When the transmission losses are high, the state of the light after the single-mode loss channel can be approximated by a squashed state [17]. We use a squashed state model where all input states have the same mean number of photons to investigate the case of extreme losses. The details on how obtain matrices $\mathbf{A}_{\text{loss}}$ and $\mathbf{A}_{\text{sqz}}$ associated with the lossy squeezed state and squashed state models can be found in Appendix A.

It is worth mentioning that the squashed states are classical Gaussian states [17], and thus sampling from the probability distribution of model $\mathbf{A}_{\text{sqz}}$ can be done efficiently. The lossy squeezed states used in model $\mathbf{A}_{\text{loss}}$ are not classical states. However, it has been shown that sampling from $\mathbf{A}_{\text{loss}}$ when transmission losses are high can be done with reasonable classical hardware resources (for

models with hundreds of modes, millions of samples can be generated in the order of an hour using contemporary supercomputers) [20]. For both models, the calculation of probabilities with respect to model $\mathbf{A}_{\text{sqz}}$ is still computationally hard. Therefore, the numerical computation of the estimators will also be restricted to low values of $2N$.

We numerically estimated $\bar{s}_{\text{loss}}(2N)$ and $\bar{s}_{\text{sqz}}(2N)$ for a GBS setup with $M = 200$. We considered transmission parameters $\eta \in \{0.5, 0.7, 0.9\}$, and set the squeezing parameter of the input states to $r = 0.31$. The mean number of photons for the squashed state model was $\bar{n} = 20$. Here, we also find that the definition of model $\mathbf{A}_{\text{sqz}}$ makes $\bar{s}_{\text{sqz}}(2N)$ independent of our choice of $\bar{n}$. For each of these cases, we generated ten Haar-random unitaries, and for each unitary, we generated $L = 1000$ samples per value of $2N$. We computed the scores for $2N$ between 4 and 24.

Figure 6 shows the computed values of $\bar{s}_{\text{loss}}(2N)$ and $\bar{s}_{\text{sqz}}(2N)$ as functions of $2N$. Just as before, the colored circles in the figures at the bottom represent the values of estimators for each of the ten Haar-random unitaries. The dashed lines with error bars correspond to $\langle \bar{s}_{\text{loss}}(2N) \rangle$ and $\langle \bar{s}_{\text{sqz}}(2N) \rangle$. The error of each $\bar{s}_{\text{loss}}(2N)$ and $\bar{s}_{\text{sqz}}(2N)$ corresponds to the standard error of the mean, and the uncertainty of the corresponding averages is computed through error propagation.

As can be seen, the values of $\langle \bar{s}_{\text{loss}}(2N) \rangle$ are significantly lower than those corresponding to the estimated ideal score. We find that the relative difference between $\langle \bar{s}_{\text{loss}}(2N) \rangle$ and $\langle \bar{s}_{\text{sqz}}(2N) \rangle$ satisfies $29.15\% \leq \Delta(2N) \leq 43.06\%$ for $\eta = 0.9$, $51.31\% \leq \Delta(2N) \leq 62.02\%$ for $\eta = 0.7$, and $52.03\% \leq \Delta(2N) \leq 69.07\%$ for $\eta = 0.5$. For the squashed state model, the difference is even more striking. The relative difference between $\langle \bar{s}_{\text{sqz}}(2N) \rangle$ and $\langle \bar{s}_{\text{sqz}}(2N) \rangle$ satisfies $75.96\% \leq \Delta(2N) \leq 82.53\%$, and we can readily note that the estimated $\bar{s}_{\text{sqz}}(2N)$ take values close to 1 for all the unitaries used in the computation. Finally, we confirm that most of the estimated $\bar{s}_{\text{loss}}(2N)$ and $\bar{s}_{\text{sqz}}(2N)$ take values within the uncertainty of the average estimated score. This demonstrates that typical GBS implementations with transmission losses also obtain LXE scores that are close to the average over Haar-random unitaries.

These results show that the presence of transmission losses in GBS setups do not necessarily bring the LXE score to values close to those obtained by models that lead to a uniform distribution over the sample space. Indeed, only for situations in which the transmission losses are higher than 50% does the score of a lossy squeezed state model approach the value of 1. However, we note that losses as low as 10% seem to define a reference value that is easily distinguishable from that of the ideal model. This will prove useful at the moment of verifying real-world GBS implementations, as we can define clearly delimited regions associated with certain values

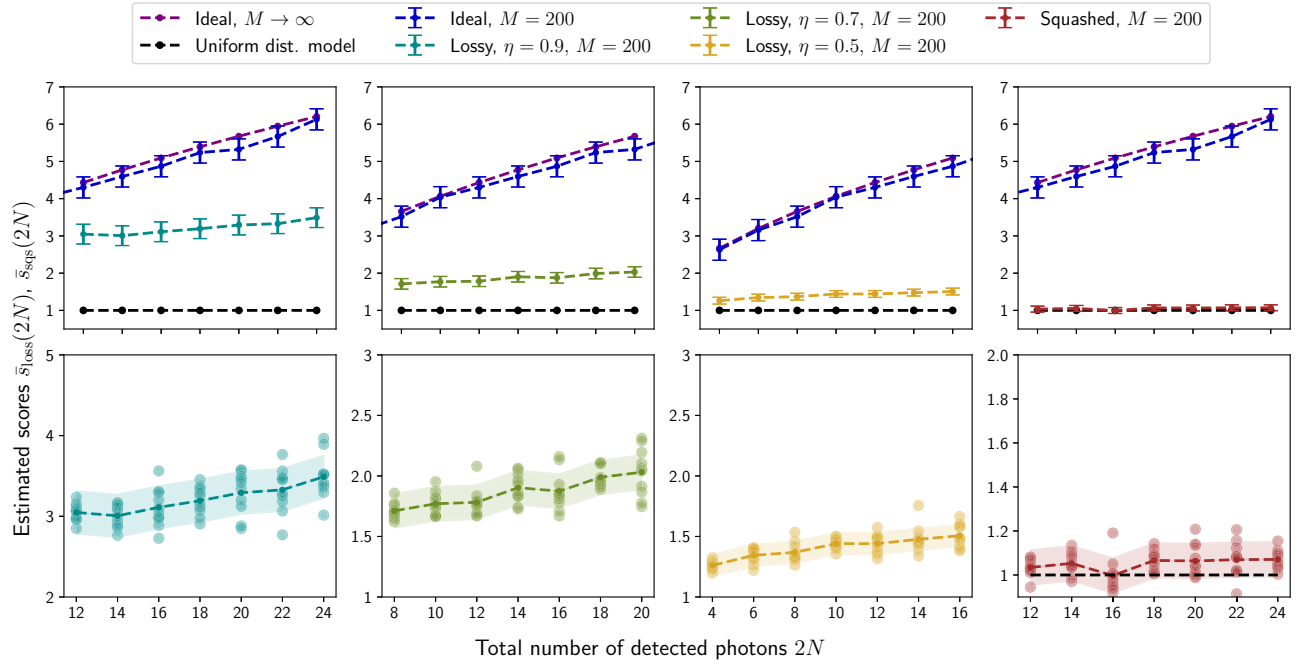


FIG. 6. Estimated scores $\bar{s}_{\text{loss}}(2N)$ and $\bar{s}_{\text{sqs}}(2N)$ as functions of $2N$. The violet dashed line corresponds to the score of an ideal model with $M \rightarrow \infty$. The black dashed line corresponds to a model that leads to a uniform distribution over the sample space. The dark blue dashed line with error bars corresponds to the average estimated score of an ideal model with $M = 200$. The remaining lines show the average estimated scores $\langle \bar{s}_{\text{loss}}(2N) \rangle$ and $\langle \bar{s}_{\text{sqs}}(2N) \rangle$: the teal dashed line corresponds to a lossy squeezed state model with $\eta = 0.9$, the olive green dashed line to $\eta = 0.7$, the dark yellow dashed line to $\eta = 0.5$, and the dark red line to the squashed state model. Error bars show the uncertainty in the estimation of the average score. The colored circles shown in the plots at the bottom indicate the values of $\bar{s}_{\text{loss}}(2N)$ and $\bar{s}_{\text{sqs}}(2N)$ for each of the ten Haar-random unitaries used in the calculation of the corresponding average. The estimation of each of these values was done using $L = 1000$ samples. The shaded regions indicate how many unitaries obtain values of the score within the error of the estimated average value.

of the transmission loss and then determine in which of them lies the score associated with a set of experimental samples. A more thorough study of the LXE score for models with transmission losses, as well as other types of Gaussian and non-Gaussian noise, is needed in order to completely determine the reference values delimiting these regions.

We also bring attention to the fact that the squashed state model obtains estimated scores very close to 1. These models have proven to be good classical adversaries of recent GBS implementations, performing as good as, and sometimes better than, the ground truth in a number of validation tests [17]. Therefore, it would be valuable to determine the analytical value of the LXE score for the squashed model, and verify if it is identically 1.

The definition of analytical reference values corresponding to noisy models will be of central importance for the use of the LXE score as a GBS validation metric. However, we also need determine if obtaining a score greater than a given reference value is a computationally hard task or not. In this way, we would be certain that the LXE score is a good witness of quantum computational advantage. Future studies on the LXE score also need to focus on this subject.

VII. DISCUSSION

In this work, we proposed using the LXE score as a tool for validating quantum advantage claims in the context of GBS. Taking inspiration from the definition of the linear XEB used for the validation or RCS implementations, we defined the LXE score as a normalized version of the linear cross-entropy between two GBS models, one of them being the ideal squeezed state model, averaged over the Haar measure of the unitary group, and evaluated at the limit of a large number of modes. The key idea of the verification strategy consists in finding reference values of the LXE score (corresponding to the ideal squeezed state model, known classical models, and adversarial samplers) and compare them with the estimated score obtained by the outcomes of a given GBS experiment. Using this comparison, we can assess how far a GBS implementation is from its corresponding typical, ideal model.

Following the definition of the LXE score, we identified two of its reference values. The first one corresponding to a GBS setup leading to a uniform probability distribution for each sector of the total number N of detected photons in the experimental samples. The second one is associated

with a GBS implementation using a lossless interferometer that receives single-mode squeezed states in the first R of its M input modes, and the vacuum in the rest of them. The first reference value follows directly from the normalization of the LXE score and is equal to 1. In addition to this, we found two expressions for the second reference value as a function of R and N : Eq. (13) for the case of input states having the same squeezing parameter, and Eq. (80) for input states with different squeezing parameters. It is worth mentioning that even if the ideal value of the LXE score is not constant with N (unlike its RCS counterpart), the validation strategy remains sound; we need only compare the estimated score of the experimental outcomes with respect to the reference curve set by the ideal squeezed state model.

An important feature of the expression we found for the ideal LXE score is that part of its dependence on R can be written as a polynomial of degree $2N$ in this variable. The corresponding coefficients can be computed by counting the number of undirected graphs, associated with certain permutations, with a given number of connected components. When we consider setups that use input states with different squeezing parameters, the coefficients also depend on the lengths of the connected components of the graph. This property of the ideal score closely resembles a recent result by Ehrenberg *et al.* [26,27] concerning a study on anticoncentration in GBS. In their work, they developed a graph-theoretical technique to compute the first and second moments of the output GBS distribution in the photon-collision-free regime. They found that the second moment of the distribution can be expressed as a polynomial of degree $2N$ in R , with coefficients computed by counting how many graphs have a specific number of connected components. Moreover, they found an expression for the LXE score of an ideal squeezed state model that uses input states with the same squeezing parameter in terms of the first and second moments [27].

Our expression for the ideal LXE score, in the case of equal squeezing, and that of Ehrenberg *et al.* are very similar. The main difference is that their results rely on the GBS hiding conjecture [5,28,29], which states that, in the photon-collision-free regime, the distribution of the symmetric product of Haar-random unitary matrices closely approximates the distribution of the symmetric product of complex Gaussian random matrices. In contradistinction, our results rely on the distribution of Haar-random unitaries in the asymptotic limit. Additionally, the definition and origin of the graphs pertinent to our computation of the ideal score differ from those used in Refs. [26,27]. At this time, more work is required in order to find the relation between the graph-theoretical technique of Ehrenberg *et al.* and the computation of the coefficients defined in Eq. (15). While our results provide a complete description to determine the ideal LXE score, we must also acknowledge that a more detailed analysis of Eqs. (15), (16), and

(81) is needed in order to make the computation of the score better suited for the validation of real-world GBS implementations.

When considering setups with no vacuum input modes, i.e., setups with $R = M$, we found a simple expression for the ideal score as a function of $2N$ [see Eq. (90)]. We also proved that this equation holds whether we use input squeezed states with different squeezing parameters or not. We compared this result, which was obtained taking the limit as $M \rightarrow \infty$, with numerical estimations of the ideal score for setups with $M \in \{50, 100, 200\}$. We found that, for all M , the analytical expression closely approximates the estimated scores in a range of $2N$ between 10 and 26. However, we noted that this approximation worsens for increasing $2N$. We argue that the reason behind this is that, being defined for $M \rightarrow \infty$, our expression for the ideal score is only valid in the photon-collision-free regime. Since in this limit the mean number of photons satisfies $\bar{n} \in o(\sqrt{M})$, we expect Eq. (90) to be a good approximation of the estimated score, for a given M , for a range of $2N$ satisfying $2N \in o(\sqrt{M})$.

We also computed the estimated score for a squashed state model, and for a simple GBS model that includes transmission losses. We found that the presence of these types of loss does not necessarily lead to scores that rapidly approach the value of 1. However, transmission losses as low as 10% lead to an estimated score that is notably different from the reference value set by an ideal model. On the other hand, we found that the estimated score of the squashed state model is surprisingly close to 1. These findings suggest that computing the score for different values of the transmission loss, as well as for classical models such as the squashed state model, is a viable way of defining reference values that will allow us to assess how far a given GBS implementation is from its corresponding ideal model.

Additional work is required to analytically determine the score of noisy and classical GBS models, as well as to prove whether the score of the squashed state model is identically 1 or not. It would also be highly relevant to provide sufficient evidence to decide if obtaining a score sufficiently close to that of the ideal model (or sufficiently different from those of classical models) is a computationally hard task or not. Our future studies of the LXE score will follow these directions.

The use of the LXE score will greatly benefit the field of GBS verification. Since we have defined the score using an ideal model instead of the ground truth, the validation of GBS implementations using this metric will not rely on providing evidence that the outcomes of the experiment follow its expected theoretical distribution (of which, additionally, we do not know if it is computationally hard to sample). Verifying directly against the ideal model will also shield the validation procedure from classical techniques that directly intend to simulate the ground truth. In

view of this, we believe that obtaining a high LXE score constitutes a stricter test that current and future GBS implementations should consider when providing evidence in support of quantum advantage claims.

In addition, since the computation of probability amplitudes for pure Gaussian states requires the calculation of hafnians of matrices half the size of those used in the computation of probabilities of mixed states, the estimation of the LXE score can be done for a range of N that is approximately twice as large as those considered in the validation of recent GBS implementations [7–10]. This represents a considerable improvement on the verification of GBS experiments.

Moreover, given that estimating the LXE score relies on the computation of probability amplitudes of pure states, our validation technique is protected against “spoofing” attacks that rely on efficiently simulating lossy GBS implementations, postselecting samples with high probabilities in the ground truth (i.e., with heavy outcomes), and then computing cross-entropy measures that are also defined with respect to the ground truth [19] (thus obtaining higher scores than the experimental samples). A direct simulation of an ideal GBS experiment is computationally as hard as the computation of the LXE score [44], so “spoofing” our validation strategy using heavy outputs in the ideal distribution is unlikely.

Note added. After publication of a first version of this work on arXiv, we became aware of a second article by Ehrenberg *et al.* [27], which included an expression for the ideal LXE score in terms of moments of the GBS distribution. We now include references to this work in the main text.

All data used in the computation of the results shown in Figs. 4 to 6 are available from Zenodo [45]. The corresponding code is available online [46].

ACKNOWLEDGMENTS

We acknowledge support from the Ministère de l’Économie et de l’Innovation du Québec and the Natural Sciences and Engineering Research Council of Canada (NSERC). H.dG. would like to thank NSERC. N.Q. and H.dG. would also like to thank ACFAS for partial support of this project. This research was enabled in part by support provided by the Digital Research Alliance of Canada.

APPENDIX A: COMPILATION OF RESULTS FOR THE COMPUTATION OF THE INTEGRAL FORM OF THE LXE

In this appendix we present the proofs of some of the results used in the computation of the integral form of the LXE. We also show that a GBS setup using identical thermal states as input of all modes of a lossless interferometer

leads to a probability distribution that is uniform for each sector of the total number of detected photons.

We begin by proving, in a slightly more general fashion, the factorization $(\mathbf{WAW})_{\mathbf{n}} = \bar{\mathbf{W}}_{\mathbf{n}} \mathbf{A}_{\mathbf{n}} \bar{\mathbf{W}}_{\mathbf{n}}$ used in the derivation of Eq. (22).

Proposition 1. *Let $\mathbf{M} = (M_{j,k})_{j,k=1}^P$ be a complex $P \times P$ matrix, and let $\mathbf{n} = (n_1, \dots, n_P)$ be a vector whose entries are non-negative integers. Define matrix $\mathbf{M}_{(\mathbf{n})}$ as the matrix obtained from taking the k th row and column of $\mathbf{M}$ and repeating it n_k times. This matrix is an $N \times N$ block matrix (with $N = \sum_{k=1}^P n_k$) of the form $\mathbf{M}_{(\mathbf{n})} = (\mathbf{B}_{p,q})_{q,p=1}^P$, where the blocks $\mathbf{B}_{p,q}$ have size $n_p \times n_q$ and their corresponding entries are all equal to $N_{q,p}$. Furthermore, let $\mathbf{R}, \mathbf{L}$ be $P \times P$ complex diagonal matrices of the form $\mathbf{R} = \text{diag}(r_1, \dots, r_P)$, $\mathbf{L} = \text{diag}(l_1, \dots, l_P)$. Then $(\mathbf{LMR})_{(\mathbf{n})} = \bar{\mathbf{L}}_{(\mathbf{n})} \mathbf{M}_{(\mathbf{n})} \bar{\mathbf{R}}_{(\mathbf{n})}$, where $\bar{\mathbf{R}}_{(\mathbf{n})} = \bigoplus_{k=1}^P r_k \mathbb{I}_{n_k}$ and $\bar{\mathbf{L}}_{(\mathbf{n})} = \bigoplus_{k=1}^P l_k \mathbb{I}_{n_k}$ with $\mathbb{I}_{n_k}$ the identity matrix of size $n_k \times n_k$.*

Proof. The entries of $\mathbf{LMR}$ can be written as $(\mathbf{LMR})_{j,k} = l_j M_{j,k} r_k$. Also, suppose that $\mathbf{D}$ is an $S \times T$ matrix whose entries are all equal to xCy , where x, y, C are complex numbers. We can see that such a matrix can be written in the form $\mathbf{D} = (x \mathbb{I}_S) C (y \mathbb{I}_T)$, where $\mathbf{C}$ is an $S \times T$ matrix whose entries are all equal to C . According to the definition, $(\mathbf{LMR})_{(\mathbf{n})} = (\mathbf{K}_{p,q})_{p,q=1}^P$, where the entries of the $n_p \times n_q$ blocks are all equal to $l_p M_{p,q} r_q$, which implies that $\mathbf{K}_{p,q} = (l_p \mathbb{I}_{n_p}) \mathbf{B}_{p,q} (r_q \mathbb{I}_{n_q})$. From this expression, we can define the block diagonal matrices $\bar{\mathbf{R}}_{(\mathbf{n})} = \bigoplus_{k=1}^P r_k \mathbb{I}_{n_k}$ and $\bar{\mathbf{L}}_{(\mathbf{n})} = \bigoplus_{k=1}^P l_k \mathbb{I}_{n_k}$ and check that $(\mathbf{LMR})_{(\mathbf{n})} = \bar{\mathbf{L}}_{(\mathbf{n})} \mathbf{M}_{(\mathbf{n})} \bar{\mathbf{R}}_{(\mathbf{n})}$. ■

The relation $(\mathbf{WAW})_{\mathbf{n}} = \bar{\mathbf{W}}_{\mathbf{n}} \mathbf{A}_{\mathbf{n}} \bar{\mathbf{W}}_{\mathbf{n}}$ can be recovered by observing that $\mathbf{A}_{\mathbf{n}} = \mathbf{A}_{(\mathbf{n} \oplus \mathbf{n})}$.

We now prove that $\Pr(N|\mathbf{A})$ can be computed by repeated differentiation of $q(\alpha, \mathbf{0}, \mathbf{A})$.

Proposition 2. *For any GBS model $\mathbf{A}$,*

$$\Pr(N|\mathbf{A}) = \frac{1}{N!} \Pr(\mathbf{0}|\mathbf{A}) \left. \frac{\partial^N q(\alpha, \mathbf{0}, \mathbf{A})}{\partial \alpha^N} \right|_{\alpha=0}, \quad (\text{A1})$$

where $q(\alpha, \mathbf{0}, \mathbf{A}) = [\det(\mathbb{I}_{2M} - \alpha \mathbf{XA})]^{-1/2}$ is a specialization of Eq. (20).

Proof. Let us begin with the relation $1 = \sum_{\mathbf{n}} \Pr(\mathbf{n}|\mathbf{A})$, where the sum extends over all possible detection patterns. In terms of the hafnian, this relation can be written as

$$\frac{1}{\Pr(\mathbf{0}|\mathbf{A})} = \sum_{N=0}^{\infty} \sum_{\mathbf{n} \in K(N)} \frac{1}{\mathbf{n}!} \text{haf}[\mathbf{A}_{\mathbf{n}}]. \quad (\text{A2})$$

Making the replacement $\mathbf{A} \rightarrow \alpha \mathbf{A}$, we can use the property $\text{haf}[\alpha \mathbf{A}_n] = \alpha^{|\mathbf{n}|} \text{haf}[\mathbf{A}_n]$ to write

$$q(\alpha, \mathbf{0}, \mathbf{A}) = \sum_{N=0}^{\infty} \alpha^N \left(\sum_{\mathbf{n} \in K(N)} \frac{1}{\mathbf{n}!} \text{haf}[\mathbf{A}_n] \right). \quad (\text{A3})$$

By repeatedly differentiating with respect to α we find that

$$\frac{1}{N!} \frac{\partial^N q(\alpha, \mathbf{0}, \mathbf{A})}{\partial \alpha^N} \Big|_{\alpha=0} = \sum_{\mathbf{n} \in K(N)} \frac{1}{\mathbf{n}!} \text{haf}[\mathbf{A}_n], \quad (\text{A4})$$

which implies that

$$\Pr(N|\mathbf{A}) = \frac{1}{N!} \Pr(\mathbf{0}|\mathbf{A}) \frac{\partial^N q(\alpha, \mathbf{0}, \mathbf{A})}{\partial \alpha^N} \Big|_{\alpha=0}. \quad (\text{A5})$$

This completes the proof. $\blacksquare$

From this result we can readily see that

$$\begin{aligned} \mathcal{D}(\mathbf{A}, \mathbf{B}; N) &= \frac{1}{(N!)^2} \frac{\Pr(\mathbf{0}|\mathbf{A}) \Pr(\mathbf{0}|\mathbf{B})}{\Pr(N|\mathbf{A}) \Pr(N|\mathbf{B})} \\ &= \left[\frac{\partial^N q(\alpha, \mathbf{0}, \mathbf{A})}{\partial \alpha^N} \frac{\partial^N q(\beta, \mathbf{0}, \mathbf{B})}{\partial \beta^N} \Big|_{\alpha=0, \beta=0} \right]^{-1}. \end{aligned} \quad (\text{A6})$$

For the remaining demonstrations of this section, we need to give a more detailed description of the GBS models introduced in Sec. II.

When we consider input single-mode Gaussian states and a lossless interferometer represented by a Haar-random unitary matrix, matrix $\mathbf{A}$ will have the general structure

$$\mathbf{A} = \begin{pmatrix} \mathbf{V} & \mathbf{Y} \\ \mathbf{Y}^* & \mathbf{V}^* \end{pmatrix}, \quad (\text{A7})$$

where $\mathbf{V} = \mathbf{U} \boldsymbol{\lambda} \mathbf{U}^T$ is a symmetric matrix, and $\mathbf{Y} = \mathbf{U} \boldsymbol{\mu} \mathbf{U}^\dagger$ is Hermitian. Matrices $\boldsymbol{\lambda}$, $\boldsymbol{\mu}$ are defined as $\boldsymbol{\lambda} = \text{diag}(\lambda_1, \dots, \lambda_M)$, $\boldsymbol{\mu} = \text{diag}(\mu_1, \dots, \mu_M)$, where the $\{\lambda_k\}$ and $\{\mu_k\}$ are real parameters that can be written in terms of the entries of the *real covariance matrix* of the input single-mode Gaussian states as

$$\lambda_k = \frac{1}{1 + 2\sigma_p^{(k)}/\hbar} - \frac{1}{1 + 2\sigma_x^{(k)}/\hbar}, \quad (\text{A8})$$

$$\mu_k = 1 - \left(\frac{1}{1 + 2\sigma_x^{(k)}/\hbar} + \frac{1}{1 + 2\sigma_p^{(k)}/\hbar} \right). \quad (\text{A9})$$

Recall that the entries of the real covariance matrix $\boldsymbol{\sigma}$ of an M -mode, nondisplaced Gaussian state are computed as $\sigma_{j,k} = \frac{1}{2} \langle \{\hat{r}_j, \hat{r}_k\} \rangle$, where the $\{\hat{r}_k\}$ are the components of the

operator vector $\hat{\mathbf{r}} = (\hat{x}_1, \dots, \hat{x}_M, \hat{p}_1, \dots, \hat{p}_M)$ with $\hat{x}_k, \hat{p}_k$ the quadrature operators of mode k . For a single-mode Gaussian state, we can write $\sigma_x^{(k)} = \langle \hat{x}^2 \rangle$ and $\sigma_p^{(k)} = \langle \hat{p}^2 \rangle$. Note that we can neglect the nondiagonal entries $\sigma_{x,p}^{(k)} = \sigma_{p,x}^{(k)} = \frac{1}{2} \langle \{\hat{x}, \hat{p}\} \rangle$ because these can be obtained from a diagonal covariance matrix via a local rotation (i.e., a local phase shift), which can be absorbed into the unitary operator describing the interferometer [47]. Using $\sigma > 0$, it follows that $\sigma_x^{(k)}, \sigma_p^{(k)} > 0$ for all k .

For a GBS setup that uses identical thermal states with the mean number of photons $\bar{n}$ as input of all the modes of the interferometer, we have $\sigma_x^{(k)} = \sigma_p^{(k)} = \hbar(2\bar{n} + 1)/2$ for all k , which implies that $\lambda_k = 0$, $\mu_k = \bar{n}/(1 + \bar{n})$ for all k . This leads to the following form of matrix $\mathbf{A}_{\text{thm}}$:

$$\mathbf{A}_{\text{thm}} = \frac{\bar{n}}{\bar{n} + 1} \begin{pmatrix} \mathbf{0} & \mathbb{I}_M \\ \mathbb{I}_M & \mathbf{0} \end{pmatrix} = \frac{\bar{n}}{\bar{n} + 1} \mathbf{X}. \quad (\text{A10})$$

We may now prove that this model leads to a uniform probability distribution for each sector of the total number of detected photons.

Proposition 3. *It holds that*

$$\Pr(\mathbf{n}|\mathbf{A}_{\text{thm}}) = \Pr(\mathbf{0}|\mathbf{A}_{\text{thm}}) \left(\frac{\bar{n}}{\bar{n} + 1} \right)^{|\mathbf{n}|}. \quad (\text{A11})$$

Proof. Note that

$$(\mathbf{A}_{\text{thm}})_{\mathbf{n}} = \frac{\bar{n}}{\bar{n} + 1} \begin{pmatrix} \mathbf{0} & (\mathbb{I}_M)_{(\mathbf{n})} \\ (\mathbb{I}_M)_{(\mathbf{n})} & \mathbf{0} \end{pmatrix}, \quad (\text{A12})$$

where $\mathbf{M}_{(\mathbf{n})}$ is the matrix obtained by taking the k th row and column of $\mathbf{M}$ and repeating it n_k times. In the special case of $\mathbb{I}_M$ it can be seen that $(\mathbb{I}_M)_{(\mathbf{n})} = \bigoplus_{k=1}^M \mathbf{1}_{n_k}$, where $\mathbf{1}_m$ is an $m \times m$ matrix whose entries are all equal to 1.

Taking into account Eq. (A12), we can write

$$\begin{aligned} \text{haf}[(\mathbf{A}_{\text{thm}})_{\mathbf{n}}] &= \left(\frac{\bar{n}}{\bar{n} + 1} \right)^{|\mathbf{n}|} \text{haf} \left[\begin{pmatrix} \mathbf{0} & (\mathbb{I}_M)_{(\mathbf{n})} \\ (\mathbb{I}_M)_{(\mathbf{n})} & \mathbf{0} \end{pmatrix} \right] \\ &= \left(\frac{\bar{n}}{\bar{n} + 1} \right)^{|\mathbf{n}|} \text{per}[(\mathbb{I}_M)_{(\mathbf{n})}] \\ &= \left(\frac{\bar{n}}{\bar{n} + 1} \right)^{|\mathbf{n}|} \mathbf{n}!, \end{aligned} \quad (\text{A13})$$

where $\text{per}[\cdot]$ stands for the permanent of a matrix, and we have used the relation

$$\text{haf} \left[\begin{pmatrix} \mathbf{0} & \mathbf{G} \\ \mathbf{G}^T & \mathbf{0} \end{pmatrix} \right] = \text{per}[\mathbf{G}] \quad (\text{A14})$$

for any $m \times m$ matrix $\mathbf{G}$. Moreover, we have used the relation $\text{per}[\bigoplus_{k=1}^M \mathbf{1}_{n_k}] = \prod_{k=1}^M n_k! = \mathbf{n}!$ [31]. It directly

follows that

$$\Pr(\mathbf{n}|\mathbf{A}_{\text{thm}}) = \Pr(\mathbf{0}|\mathbf{A}_{\text{thm}}) \left(\frac{\bar{n}}{\bar{n}+1} \right)^{|\mathbf{n}|}. \quad (\text{A15})$$

This completes the proof. $\blacksquare$

We conclude this section by proving the convergence of the series expansion that leads to Eq. (30). Recall that $q(\alpha, \phi, \mathbf{A}) = [\det(\mathbb{I}_{2M} - \alpha \mathbf{\Omega A})]^{-1/2}$. By noting that $\mathbb{I}_{2M} - \alpha \mathbf{\Omega A} = \exp[\log(\mathbb{I}_{2M} - \alpha \mathbf{\Omega A})]$, and using the relation $\det[\exp(\mathbf{A})] = \exp[\text{tr}(\mathbf{A})]$, we can write

$$q(\alpha, \phi, \mathbf{A}) = \exp \left\{ -\frac{1}{2} \text{tr}[\log(\mathbb{I}_{2M} - \alpha \mathbf{\Omega A})] \right\}. \quad (\text{A16})$$

We now use $\log(1+x) = \sum_{l=1}^{\infty} (-1)^{l+1} x^l / l$, which converges for $|x| < 1$, to write

$$q(\alpha, \phi, \mathbf{A}) = \exp \left[-\frac{1}{2} \text{tr} \left(\sum_{l=1}^{\infty} -\frac{\alpha^l}{l} (\mathbf{\Omega A})^l \right) \right]. \quad (\text{A17})$$

This expression directly yields Eq. (30). We now focus on the series inside the trace.

Proposition 4. *The power series*

$$\sum_{l=1}^{\infty} \frac{\alpha^l}{l} (\mathbf{\Omega A})^l \quad (\text{A18})$$

converges for every GBS model $\mathbf{A}$ of the form (A7) provided that $|\alpha| < 1$.

Proof. Let us take the spectral norm of the power series and write

$$\begin{aligned} \left\| \sum_{l=1}^{\infty} \frac{\alpha^l}{l} (\mathbf{\Omega A})^l \right\|_2 &\leq \sum_{l=1}^{\infty} \left\| \frac{\alpha^l}{l} (\mathbf{\Omega A})^l \right\|_2 \\ &= \sum_{l=1}^{\infty} \frac{|\alpha|^l}{l} \|(\mathbf{\Omega A})^l\|_2 \\ &\leq \sum_{l=1}^{\infty} \frac{|\alpha|^l}{l} \|\mathbf{\Omega A}\|_2^l \\ &= \sum_{l=1}^{\infty} \frac{|\alpha|^l}{l} \|\mathbf{W X W A}\|_2^l. \end{aligned} \quad (\text{A19})$$

Note that $\mathbf{W X} = \mathbf{X W}$. Moreover $\|\mathbf{W}^2\|_2 = 1$ since $\mathbf{W}$ is unitary. We therefore have

$$\begin{aligned} \left\| \sum_{l=1}^{\infty} \frac{\alpha^l}{l} (\mathbf{\Omega A})^l \right\|_2 &\leq \sum_{l=1}^{\infty} \frac{|\alpha|^l}{l} \|\mathbf{W}^2 \mathbf{X A}\|_2^l \\ &\leq \sum_{l=1}^{\infty} \frac{|\alpha|^l}{l} \|\mathbf{X A}\|_2^l. \end{aligned} \quad (\text{A20})$$

According to Eq. (A7), we can recast $\mathbf{X A}$ as

$$\mathbf{X A} = \mathbf{F G F}^\dagger, \quad \mathbf{F} = \begin{pmatrix} \mathbf{U}^* & \mathbf{0} \\ \mathbf{0} & \mathbf{U} \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} \mu & \lambda \\ \lambda & \mu \end{pmatrix}, \quad (\text{A21})$$

where $\mathbf{F}$ is also unitary. This allows us to see that $\|\mathbf{X A}\|_2 = \|\mathbf{G}\|_2$. Since $\mathbf{G}$ is real and symmetric, its singular values are the absolute values of its eigenvalues. These, in turn, can be proven to be

$$\left\{ 1 - \frac{2}{1 + 2\sigma_x^{(k)}/\hbar}, 1 - \frac{2}{1 + 2\sigma_p^{(k)}/\hbar} \right\}. \quad (\text{A22})$$

Because $\sigma_x^{(k)}, \sigma_p^{(k)} > 0$ for all k , these eigenvalues lie in the interval $(-1, 1)$, which implies that $\|\mathbf{G}\|_2 < 1$. We conclude that

$$\left\| \sum_{l=1}^{\infty} \frac{\alpha^l}{l} (\mathbf{\Omega A})^l \right\|_2 < \sum_{l=1}^{\infty} \frac{|\alpha|^l}{l}. \quad (\text{A23})$$

For $|\alpha| < 1$, $\sum_{l=1}^{\infty} |\alpha|^l / l$ converges to $-\log(1 - |\alpha|)$. Therefore, the series in Eq. (A18) converges for $|\alpha| < 1$. $\blacksquare$

The specific case of the ideal squeezed state model is obtained for $2\sigma_x^{(k)}/\hbar = e^{2r_k}$, $2\sigma_p^{(k)}/\hbar = e^{-2r_k}$, with r_k the squeezing parameter at mode k , for $1 \leq k \leq R$ and $\sigma_x^{(k)} = \sigma_p^{(k)} = \hbar/2$ otherwise. This implies that $\mu_k = 0$ for all k , while $\lambda_k = \tanh(r_k)$ for $1 \leq k \leq R$ and zero otherwise.

For single-mode squeezed states passing through single-mode loss channels before entering the interferometer (like those used in the transmission loss model of Sec. VI), we have $2\sigma_x^{(k)}/\hbar = \eta_k e^{2r_k} + (1 - \eta_k)$ and $2\sigma_p^{(k)}/\hbar = \eta_k e^{-2r_k} + (1 - \eta_k)$, with η_k the transmission parameter of the loss channel at mode k , for $1 \leq k \leq R$ and $\sigma_x^{(k)} = \sigma_p^{(k)} = \hbar/2$ otherwise. This implies that

$$\begin{aligned} \mu_k &= \frac{\eta_k(1 - \eta_k) \sinh^2(r_k)}{1 + \eta_k(2 - \eta_k) \sinh^2(r_k)}, \\ \lambda_k &= \frac{\eta_k \sinh(r_k) \cosh(r_k)}{1 + \eta_k(2 - \eta_k) \sinh^2(r_k)} \end{aligned} \quad (\text{A24})$$

for $1 \leq k \leq R$, and $\mu_k = \lambda_k = 0$ otherwise. Note that we can recover the ideal squeezed state model from these equations by setting $\eta_k = 1$ for all k .

Finally, the squashed state model (see also Sec. VI) is obtained for $2\sigma_x^{(k)}/\hbar = 1 + 4\bar{n}_k$, $2\sigma_p^{(k)}/\hbar = 1$, with $\bar{n}_k$ the mean number of photons at mode k , for $1 \leq k \leq R$ and $\sigma_x^{(k)} = \sigma_p^{(k)} = \hbar/2$ otherwise. This implies that $\mu_k = \lambda_k = \bar{n}_k / (1 + 2\bar{n}_k)$ for $1 \leq k \leq R$, and $\mu_k = \lambda_k = 0$ otherwise.

APPENDIX B: INDEX STRUCTURE OF THE LXE

In this appendix we show how to obtain Eq. (46) and we motivate the definition of permutation Ω_k . Let us start by recalling that $\text{LXE}(\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N)$ is expressed as an integral of $Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})]Z_N[\mathbf{u}(-\boldsymbol{\phi}, \mathbf{U})]$ with respect to $d\boldsymbol{\phi}$, where

$$Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})] = \sum_{\mathbf{k}(c)} \prod_{a=1}^N \frac{1}{k_a!} \prod_{a=1}^N u_a^{k_a}, \quad (\text{B1})$$

$u_a = \frac{1}{2} \text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^a]$, $\mathbf{V} = \mathbf{U} \boldsymbol{\xi} \mathbf{U}^T$, and u_a depends on $\boldsymbol{\phi}$ through $\mathbf{D} = \mathbf{D}(\boldsymbol{\phi})$. In what follows, we express $Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})]$ in terms of the entries of $\mathbf{V}$.

Note that the entries of $\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*$ can be written as

$$(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)_{j_1 j_3} = \sum_{j_2=1}^M e^{2i(\phi_{j_1} + \phi_{j_2})} V_{j_1 j_2} V_{j_2 j_3}^* \quad (\text{B2})$$

with $\{j_k\}$ denoting a set of dummy indices. Using this expression, we can readily see that

$$[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^2]_{j_1 j_5} = \sum_{j_2 j_3 j_4} e^{2i(\phi_{j_1} + \phi_{j_2} + \phi_{j_3} + \phi_{j_4})} V_{j_1 j_2} V_{j_2 j_3} V_{j_3 j_4} V_{j_4 j_5}^*, \quad (\text{B3})$$

or, for a general power l ,

$$[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l]_{j_1 j_{2l+1}} = \sum_{j_2, \dots, j_{2l}} e^{2i(\phi_{j_1} + \dots + \phi_{j_{2l}})} V_{j_1 j_2} \dots V_{j_{2l-1} j_{2l}} V_{j_{2l} j_{2l+1}}^* \dots V_{j_2 j_3}^* \dots V_{j_{2l} j_{2l+1}}^*. \quad (\text{B4})$$

Taking the trace of $(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l$ we obtain

$$\text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l] = \sum_{j_1, \dots, j_{2l}} e^{2i(\phi_{j_1} + \dots + \phi_{j_{2l}})} V_{j_1 j_2} \dots V_{j_{2l-1} j_{2l}} V_{j_{2l} j_1}^* \dots V_{j_2 j_3}^* \dots V_{j_{2l} j_1}^*. \quad (\text{B5})$$

Let us gather all the dummy indices in the sequence $\mathbf{j}_{1,2l} = (j_1, \dots, j_{2l})$. Note that the subscripts in $\mathbf{j}$ indicate the labels of the first and last dummy indices. We define $\omega_l \in S_{2l}$ as the permutation that transforms $(j_1, j_2, \dots, j_{2l-1}, j_{2l})$ into $(j_2, j_3, \dots, j_{2l}, j_1)$: $\omega_l(\mathbf{j}_{1,2l}) = (j_2, j_3, \dots, j_{2l}, j_1)$. Furthermore, let us define $V[\mathbf{j}_{1,2l}] \equiv V_{j_1 j_2} \dots V_{j_{2l-1} j_{2l}}$ and $V^*[\omega_l(\mathbf{j}_{1,2l})] \equiv V_{j_2 j_3}^* \dots V_{j_{2l} j_1}^*$. Then, we can recast Eq. (B5) as

$$\text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l] = \sum_{j_1, \dots, j_{2l}} E(\mathbf{j}_{1,2l}) V[\mathbf{j}_{1,2l}] V^*[\omega_l(\mathbf{j}_{1,2l})], \quad (\text{B6})$$

where $E(\mathbf{j}_{1,2l}) = \exp[2i(\phi_{j_1} + \dots + \phi_{j_{2l}})]$.

Defining a second sequence of dummy indices $\mathbf{j}'_{1,2l} = (j'_1, \dots, j'_{2l})$, we can readily see that $V[\mathbf{j}_{1,2l}] V[\mathbf{j}'_{1,2l}] = V[\mathbf{j}_{1,2l} \oplus \mathbf{j}'_{1,2l}]$, with analogous relations holding for $V^*[\cdot]$ and $E[\cdot]$. These properties come in handy when computing powers of $\text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l]$. Indeed, consider the expression

$$\begin{aligned} & \{\text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l]\}^2 \\ &= \sum_{j_1, \dots, j_{2l}} \sum_{j'_1, \dots, j'_{2l}} E(\mathbf{j}_{1,2l}) E(\mathbf{j}'_{1,2l}) V[\mathbf{j}_{1,2l}] V[\mathbf{j}'_{1,2l}] \\ & \quad \times V^*[\omega_l(\mathbf{j}_{1,2l})] V^*[\omega_l(\mathbf{j}'_{1,2l})]. \end{aligned} \quad (\text{B7})$$

Renaming each dummy index j'_k as $j'_k \rightarrow j_{2l+k}$, and using the direct sum properties of V , V^* , and E , we can write

$$\begin{aligned} \{\text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l]\}^2 &= \sum_{j_1, \dots, j_{4l}} E(\mathbf{j}_{1,4l}) V[\mathbf{j}_{1,4l}] \\ & \quad \times V^*[\omega_l(\mathbf{j}_{1,2l}) \oplus \omega_l(\mathbf{j}_{2l+1,4l})]. \end{aligned} \quad (\text{B8})$$

Applying this same procedure a given number of times, say k_l times, we obtain

$$\begin{aligned} \{\text{tr}[(\mathbf{D}^2 \mathbf{V} \mathbf{D}^2 \mathbf{V}^*)^l]\}^{k_l} &= \sum_{j_1, \dots, j_{2lk_l}} E(\mathbf{j}_{1,2lk_l}) V[\mathbf{j}_{1,2lk_l}] \\ & \quad \times V^* \left[\bigoplus_{p=1}^{k_l} \omega_l(\mathbf{j}_{2l(p-1)+1,2lp}) \right]. \end{aligned} \quad (\text{B9})$$

From the definition of u_a , we can see that Eq. (B9) allows us to directly express $u_a^{k_l}$ in terms of the entries of $\mathbf{V}$ for an arbitrary value of a . The next step is to use Eq. (B9) to compute the product $\prod_{a=1}^N u_a^{k_l}$. The strategy is completely analogous to that used to obtain Eq. (B9): we define a set of primed dummy indices and make the product of two different sums, then rename the primed indices, and finally make the direct sum of the sequences of indices involved.

Consider, for example, the product $u_1^{k_1} u_2^{k_2}$:

$$\begin{aligned} u_1^{k_1} u_2^{k_2} &= \frac{1}{2^{k_1+k_2}} \sum_{j_1, \dots, j_{2k_1}} E(\mathbf{j}_{1,2k_1}) V[\mathbf{j}_{1,2k_1}] \\ & \quad \times V^* \left[\bigoplus_{p=1}^{k_1} \omega_1(\mathbf{j}_{2(p-1)+1,2p}) \right] \\ & \quad \times \sum_{j'_1, \dots, j'_{4k_2}} E(\mathbf{j}'_{1,4k_2}) V[\mathbf{j}'_{1,4k_2}] \\ & \quad \times V^* \left[\bigoplus_{p=1}^{k_2} \omega_2(\mathbf{j}'_{4(p-1)+1,4p}) \right]. \end{aligned} \quad (\text{B10})$$

Changing the dummy indices j'_b as $j'_b \rightarrow j_{2k_1+b}$, we can rewrite Eq. (B10) as

$$u_1^{k_1} u_2^{k_2} = \frac{1}{2^{k_1+k_2}} \sum_{j_1, \dots, j_{2k_1+4k_2}} E(\mathbf{j}_{1,2k_1+4k_2}) V[\mathbf{j}_{1,2k_1+4k_2}] \\ \times V^* \left[\bigoplus_{p=1}^{k_1} \omega_1(\mathbf{j}_{2(p-1)+1,2p}) \right. \\ \left. \times \bigoplus_{p=1}^{k_2} \omega_2(\mathbf{j}_{2k_1+4(p-1)+1,2k_1+4p}) \right]. \quad (\text{B11})$$

Applying this same process for the remaining $\{u_a\}$, we obtain the general expression

$$\prod_{a=1}^N u_a^{k_a} = \frac{1}{2^{k_1+\dots+k_N}} \sum_{j_1, \dots, j_{2N}} E(\mathbf{j}_{1,2N}) V[\mathbf{j}_{1,2N}] \\ \times V^* \left[\bigoplus_{a=1}^N \bigoplus_{p=1}^{k_a} \omega_a(\mathbf{j}_{2v_{a-1}+2a(p-1)+1,2v_{a-1}+2ap}) \right], \quad (\text{B12})$$

where we have used $k_1 + 2k_2 + \dots + Nk_N = N$ and defined $v_a = \sum_{p=1}^a pk_p$, $v_0 \equiv 0$.

Write $\mathbf{j} \equiv \mathbf{j}_{1,2N} = (j_1, \dots, j_{2N})$. Moreover, let $\Omega_{\mathbf{k}} \in S_{2N}$ act on $\mathbf{j}$ as

$$\Omega_{\mathbf{k}}(\mathbf{j}) = \Omega_{\mathbf{k}}[(j_1, \dots, j_{2N})] \\ = \bigoplus_{a=1}^N \bigoplus_{p=1}^{k_a} \omega_a(\mathbf{j}_{2v_{a-1}+2a(p-1)+1,2v_{a-1}+2ap}) \\ = \bigoplus_{a=1}^N \bigoplus_{p=1}^{k_a} \omega_a[(j_{2v_{a-1}+2a(p-1)+1}, \dots, j_{2v_{a-1}+2ap})]. \quad (\text{B13})$$

Then, we can express Eq. (B12) in the form

$$\prod_{a=1}^N u_a^{k_a} = \frac{1}{2^{k_1+\dots+k_N}} \sum_{\mathbf{j}} E(\mathbf{j}) V[\mathbf{j}] V^*[\Omega_{\mathbf{k}}(\mathbf{j})], \quad (\text{B14})$$

where $\sum_{\mathbf{j}} \equiv \sum_{j_1=1}^M \dots \sum_{j_{2N}=1}^M$. This result allows us to readily write $Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})]$ in the form

$$Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})] = \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \sum_{\mathbf{j}} E(\mathbf{j}) V[\mathbf{j}] V^*[\Omega_{\mathbf{k}}(\mathbf{j})]. \quad (\text{B15})$$

Going one step further, we can obtain the expansion of $Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})] Z_N[\mathbf{u}(-\boldsymbol{\phi}, \mathbf{U})]$ in terms of V and V^* :

$$Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})] Z_N[\mathbf{u}(-\boldsymbol{\phi}, \mathbf{U})] = \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ \times \sum_{\mathbf{j}, \mathbf{j}'} E(\mathbf{j}) E^*(\mathbf{j}') V[\mathbf{j} \oplus \mathbf{j}'] \\ \times V^*[\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}}(\mathbf{j}')]. \quad (\text{B16})$$

Recall now that Eq. (43) allows us to write monomials in the entries of $\mathbf{V}$ and $\mathbf{V}^*$ as polynomials in the entries of $\mathbf{U}$ and $\mathbf{U}^*$:

$$V[\mathbf{g}] V^*[\mathbf{h}] = V_{g_1, g_2} \dots V_{g_{2l-1}, g_{2l}} V_{h_1, h_2}^* \dots V_{h_{2m-1}, h_{2m}}^* \\ = \sum_{\boldsymbol{\mu}, \mathbf{v}} \zeta_{\boldsymbol{\mu}} \zeta_{\mathbf{v}} \mathcal{U}(\mathbf{g}, \bar{\boldsymbol{\mu}} \mid \mathbf{h}, \bar{\mathbf{v}}) \quad (\text{B17})$$

with the dummy indices in $\boldsymbol{\mu} = (\mu_1, \dots, \mu_l)$ and $\mathbf{v} = (v_1, \dots, v_m)$ taking values in $\{1, \dots, M\}$, and $\bar{\boldsymbol{\mu}} = (\mu_1, \mu_1, \dots, \mu_l, \mu_l)$, $\bar{\mathbf{v}} = (v_1, v_1, \dots, v_m, v_m)$. As per Eq. (44), $\zeta_{\boldsymbol{\mu}} = \zeta_{\mu_1} \dots \zeta_{\mu_l}$, with $\{\zeta_k\}$ the diagonal entries of $\boldsymbol{\zeta}$; and

$$\mathcal{U}(\mathbf{g}, \bar{\boldsymbol{\mu}} \mid \mathbf{h}, \bar{\mathbf{v}}) = U_{g_1, \mu_1} U_{g_2, \mu_1} \dots U_{g_{2l-1}, \mu_l} U_{g_{2l}, \mu_l} \\ \times U_{h_1, v_1}^* U_{h_2, v_1}^* \dots U_{h_{2m-1}, v_m}^* U_{h_{2m}, v_m}^*. \quad (\text{B18})$$

We can now recast Eq. (B16) as

$$Z_N[\mathbf{u}(\boldsymbol{\phi}, \mathbf{U})] Z_N[\mathbf{u}(-\boldsymbol{\phi}, \mathbf{U})] \\ = \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\mathbf{j}, \mathbf{j}'} E(\mathbf{j}) E^*(\mathbf{j}') \\ \times \sum_{\boldsymbol{\mu}, \mathbf{v}} \zeta_{\boldsymbol{\mu}} \zeta_{\mathbf{v}} \mathcal{U}[\mathbf{j} \oplus \mathbf{j}', \bar{\boldsymbol{\mu}} \mid \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}}(\mathbf{j}'), \bar{\mathbf{v}}]. \quad (\text{B19})$$

Integrating the previous equation with respect to $d\boldsymbol{\phi}$, multiplying by $\left(\frac{(R/2)+N-1}{N}\right)^{-2}$, and defining

$$I(\mathbf{j}, \mathbf{j}') = \frac{1}{(2\pi)^M} \int_0^{2\pi} E(\mathbf{j}) E^*(\mathbf{j}') d\boldsymbol{\phi} \\ = \frac{1}{(2\pi)^M} \int_0^{2\pi} \exp \left[\sum_{m \in \mathbf{j}, n \in \mathbf{j}'} 2i(\phi_m - \phi_n) \right] d\boldsymbol{\phi}, \quad (\text{B20})$$

we obtain the expression of LXE($\mathbf{A}_{\text{sqz}}, \mathbf{A}_{\text{sqz}}; 2N$) presented in Eq. (46).

APPENDIX C: INTEGRAL OVER PHASES

Consider the integral

$$I(\mathbf{j}, \mathbf{j}') = \frac{1}{(2\pi)^M} \int_0^{2\pi} \exp \left[\sum_{m \in \mathbf{j}, n \in \mathbf{j}'} 2i(\phi_m - \phi_n) \right] d\phi, \quad (\text{C1})$$

where we see $\mathbf{j}, \mathbf{j}'$ as sequences of variables taking values in $\{1, \dots, M\}$. Recall that $\phi_k \in [0, 2\pi]$ for all k and $d\phi = d\phi_1 \cdots d\phi_M$.

Let us turn our attention to the term inside the exponential:

$$2i \sum_{m \in \mathbf{j}} \phi_m - 2i \sum_{n \in \mathbf{j}'} \phi_n. \quad (\text{C2})$$

As mentioned in the main text, if this sum is nonzero, there must be at least one $p \in \mathbf{j}$ or $p \in \mathbf{j}'$ such that

$$2i \sum_{m \in \mathbf{j}} \phi_m - 2i \sum_{n \in \mathbf{j}'} \phi_n = 2iz\phi_p + \text{other terms}, \quad (\text{C3})$$

where z is a nonzero integer. This expression represents the fact that the sum is unbalanced. Since the exponential can be factorized, we can focus on the integral involving ϕ_p only:

$$\begin{aligned} \int_0^{2\pi} e^{2iz\phi_p} d\phi_p &= \frac{1}{2iz} e^{2iz\phi_p} \Big|_0^{2\pi} \\ &= \frac{1}{2iz} [(e^{2i\pi})^{2z} - 1] = \frac{1}{2iz} (1 - 1) = 0. \end{aligned} \quad (\text{C4})$$

This means that the entirety of the integral is zero whenever the sum inside the exponential is different from zero. If the exponent is zero, we can readily see that the integral is equal to 1:

$$\frac{1}{(2\pi)^M} \int_0^{2\pi} \exp(0) d\phi = \frac{1}{(2\pi)^M} (2\pi)^M = 1. \quad (\text{C5})$$

When considering the sum inside the exponential as a function of the variables $\mathbf{j}$ and $\mathbf{j}'$, we can recognize that we can make it vanish whenever $\mathbf{j}'$ is a permutation of $\mathbf{j}$ (this ensures the balance in the summations). This is the case even if we find that some of the $\{j_k\}$ have repeated values, which is allowed given the fact that all of them take values in the same set. The task now is to find a function of $\mathbf{j}$ and $\mathbf{j}'$ that is unity for any event that makes the sum in the exponential equal to zero, and that vanishes identically otherwise. The integral will then be equal to this function.

Let us start by considering that all the indices in $\mathbf{j}$ take different values. Note that this makes the indices

in $\mathbf{j}'$ take different values as well. Consider a permutation $\sigma \in S_{2N}$. We can see that the function $F_\sigma(\mathbf{j}', \mathbf{j}) = \delta_{j'_1, \sigma(j_1)} \cdots \delta_{j'_{2N}, \sigma(j_{2N})}$, with $\delta_{j,k}$ the usual Kronecker delta, vanishes whenever $\mathbf{j}' \neq \sigma(\mathbf{j})$, and is equal to one otherwise. Summing over all the permutations in S_{2N} , we obtain a function that is equal to 1 whenever $\mathbf{j}'$ is a permutation, any permutation, of $\mathbf{j}$, and vanishes otherwise:

$$F(\mathbf{j}', \mathbf{j}) = \sum_{\sigma \in S_{2N}} F_\sigma(\mathbf{j}', \mathbf{j}) = \sum_{\sigma \in S_{2N}} \prod_{a=1}^{2N} \delta_{j'_a, \sigma(j_a)}. \quad (\text{C6})$$

This is the value of $I(\mathbf{j}, \mathbf{j}')$ when all the indices in $\mathbf{j}$ take different values.

When some of the $\{j_k\}$ have the same values as others, the situation becomes slightly more involved. To address this problem, it is convenient to first translate the phrase “there are some indices having the same value as others” into a sequence of repeated dummy indices taken from $\mathbf{j}$. We can do this by considering the following procedure. First, identify all the indices in $\mathbf{j}$ that have the same value and gather them in individual sets, one for each different value that the indices take. The result of this step is a set of subsets of $\mathbf{j}$. For instance, consider $2N = 6$, so $\mathbf{j} = (j_1, j_2, j_3, j_4, j_5, j_6)$, and let us suppose that we are in a situation where $j_1 = j_4 = j_3$, $j_2 = j_5$, and $j_1 \neq j_2 \neq j_6$. After gathering the indices that have the same values, we obtain the set $\{\{j_1, j_3, j_4\}, \{j_2, j_5\}, \{j_6\}\}$. We may recognize that this procedure is equivalent to finding a *partition* of $\mathbf{j}$ (i.e., a collection of nonempty, mutually disjoint subsets of $\mathbf{j}$, usually called blocks, whose union is equal to $\mathbf{j}$), where all the indices within each block of the partition take the same value. Next, we select one index within each block and replace all the indices in $\mathbf{j}$ that belong to the same block by this *representative index*. In our example, let us choose j_1, j_2 , and j_6 as representatives. After the replacement of indices belonging to the same block, we obtain the sequence $\mathbf{g} = (j_1, j_2, j_1, j_1, j_2, j_6)$. This procedure can be applied for any situation where we have repeated indices. Note that selecting different representative indices leads to different $\mathbf{g}$. However, no matter the choice of representatives, the resulting $\mathbf{g}$ represent the same *situation*.

Having found a sequence $\mathbf{g}$ associated with a specific case of repeated indices, let us return to finding a function that vanishes whenever $\mathbf{j}'$ is not a *unique permutation* of $\mathbf{g}$, and is unity otherwise. We could consider the function $F(\mathbf{j}', \mathbf{g})$, but we can readily observe that the sum $\sum_{\sigma \in S_{2N}}$ is overcounting the different permutations of $\mathbf{g}$, i.e., there are multiple permutations in S_{2N} that, when applied to $\mathbf{g}$, lead to the same result. This implies that if $\mathbf{j}' \neq \sigma(\mathbf{j})$, we obtain $F(\mathbf{j}', \mathbf{g}) = 0$, but when $\mathbf{j}' = \sigma(\mathbf{j})$, we generally do not obtain $F(\mathbf{j}', \mathbf{g}) = 1$. Fortunately, we can solve this issue in a simple manner: we normalize $F(\mathbf{j}', \mathbf{g})$ using the number of times the unique permutations of $\mathbf{g}$

are being overcounted. This number is the same for every distinct permutation, and depends only on the *multiplicities* of the indices appearing in $\mathbf{g}$. Let $\{j_k\}_{k \in \Theta}$, where $\Theta \subset \{1, \dots, 2N\}$, be the different dummy indices that appear in $\mathbf{g}$, and let each j_k appear t_k times within the sequence. Then the number of times each unique permutation of $\mathbf{g}$ is being overcounted by $\sum_{\sigma \in S_{2N}} \prod_{k \in \Theta} t_k!$.

On this account, we can see that the function

$$\left(\prod_{k \in \Theta} \frac{1}{t_k!} \right) F(\mathbf{j}', \mathbf{g}) = \prod_{k \in \Theta} \frac{1}{t_k!} \sum_{\sigma \in S_{2N}} \prod_{a=1}^{2N} \delta_{j'_a, \sigma(g_a)} \quad (\text{C7})$$

vanishes whenever $\mathbf{j}'$ is not a unique permutation of $\mathbf{g}$, and is equal to 1 otherwise. This is the result of $I(\mathbf{j}, \mathbf{j}')$ when we have a situation of repeated indices represented by $\mathbf{g}$.

We are now two steps away from finding a general expression for $I(\mathbf{j}, \mathbf{j}')$. The first of these consists in finding a systematic way of computing all the possible $\mathbf{g}$, i.e., a systematic way of identifying all the events with repeated indices. We already gave a hint of how to do this when we explained how to construct $\mathbf{g}$; the key is to use the partitions of $\mathbf{j}$. Indeed, since the procedure of grouping indices in $\mathbf{j}$ that have the same values naturally leads to a partition of $\mathbf{j}$, we can invert the process and assign to each possible partition a sequence $\mathbf{g}$ representing an event with repeated indices. The procedure is the following. Consider a partition Λ of $\mathbf{j}$. We think of all the indices within each block $\lambda \in \Lambda$ as having the same value. The corresponding $\mathbf{g}$ is constructed by choosing a representative index j_λ for each λ , and then replacing all the j_k in $\mathbf{j}$ that belong to the same λ by the corresponding j_λ . For clarity, we introduce the notation $\mathbf{g} \equiv \mathbf{j}[\Lambda, \{j_\lambda\}]$.

Now, note that the degeneracy of each $\{j_\lambda\}$ is equal to the length, $|\lambda|$, of each block (i.e., the number of elements in each block). This allows us to write the normalization factor of $F(\mathbf{j}', \mathbf{j}[\Lambda, \{j_\lambda\}])$ as $\Lambda! = \prod_{\lambda \in \Lambda} |\lambda|!$. Moreover, the event where all the indices in $\mathbf{j}$ take different values is represented by the partition $\Lambda_0 = \{\{j_1\}, \dots, \{j_{2N}\}\}$ (one index per block). For this partition, $\Lambda_0! = 1$.

Since each partition Λ of $\mathbf{j}$ gives us a unique way of grouping the indices $\{j_k\}$ in different blocks, each Λ leads to a $\mathbf{j}[\Lambda, \{j_\lambda\}]$ representing a unique event with repeated indices. Note, however, that each Λ is associated with several $\mathbf{j}[\Lambda, \{j_\lambda\}]$ differing only on the choice of representative indices $\{j_\lambda\}$. Nevertheless, all of these sequences represent the same unique situation where there are indices taking the same value as others.

The final step for finding an expression for $I(\mathbf{j}, \mathbf{j}')$ consists in constructing a function of $\mathbf{j}$ and $\mathbf{j}[\Lambda, \{j_\lambda\}]$ that is equal to 1 only when we have a situation of repeated indices represented by $\mathbf{j}[\Lambda, \{j_\lambda\}]$, and vanishes otherwise. We need this in order to single out the contributions of each unique Λ to the integral. The event that we need to identify can be equivalently written as “when all the indices

in $\lambda \in \Lambda$ are equal to j_λ , and all the $\{j_\lambda\}$ are different from each other.” This phrase can be readily written in terms of Kronecker deltas as

$$\left[\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_\lambda, f} \right] \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu}). \quad (\text{C8})$$

We may now bring together Eqs. (C6) to (C8); sum over all the possible ways of identifying events with repeated indices, i.e., sum over the set of all partitions of $\mathbf{j}$, $\mathcal{Q}[\mathbf{j}]$; and finally write $I(\mathbf{j}, \mathbf{j}')$ as [see Eq. (48)]

$$I(\mathbf{j}, \mathbf{j}') = \sum_{\Lambda \in \mathcal{Q}[\mathbf{j}]} \frac{1}{\Lambda!} F(\mathbf{j}', \mathbf{j}[\Lambda, \{j_\lambda\}]) \left[\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_\lambda, f} \right] \times \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu}). \quad (\text{C9})$$

It is worth mentioning that in the subscript $\Lambda \in \mathcal{Q}[\mathbf{j}]$, $\mathbf{j}$ should be viewed as a collection of fixed indices, or objects, whose sole purpose is to determine all the possible partitions of a set with $2N$ elements. Thus, in this subscript, we must not replace any j_k by one of its possible values $\{1, \dots, M\}$. The reason behind this is that the sum over partitions was included only as a way to index a series of events concerning the variables $\{j_k\}$.

To conclude this section, let us turn our attention to the reorganization of sums that leads to Eq. (50). Let $h(\mathbf{j}, \mathbf{j}')$ be an arbitrary function of $\mathbf{j}$ and $\mathbf{j}'$, and consider the expression

$$\sum_{\mathbf{j}, \mathbf{j}'} h(\mathbf{j}, \mathbf{j}') I(\mathbf{j}, \mathbf{j}') = \sum_{\mathbf{j}, \mathbf{j}'} \sum_{\Lambda \in \mathcal{Q}[\mathbf{j}]} \frac{1}{\Lambda!} h(\mathbf{j}, \mathbf{j}') F(\mathbf{j}', \mathbf{j}[\Lambda, \{j_\lambda\}]) \times \left[\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_\lambda, f} \right] \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu}), \quad (\text{C10})$$

where we recall that $\sum_{\mathbf{j}} = \sum_{j_1=1}^M \dots \sum_{j_{2N}=1}^M$.

Choose an arbitrary partition $\Lambda \in \mathcal{Q}[\mathbf{j}]$, and let us focus on the term

$$T = \sum_{\mathbf{j}, \mathbf{j}'} h(\mathbf{j}, \mathbf{j}') F(\mathbf{j}', \mathbf{j}[\Lambda, \{j_\lambda\}]) \left[\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_\lambda, f} \right] \times \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu}). \quad (\text{C11})$$

Following the definition of $F(\mathbf{j}', \mathbf{j}[\Lambda, \{j_\lambda\}])$ in terms of Kronecker deltas, we can replace the sum over indices $\mathbf{j}'$ by a sum over permutations $\sigma \in S_{2N}$ and, moreover, we can

make the transformation $\mathbf{j}' \rightarrow \sigma(\mathbf{j}[\Lambda, \{j_\lambda\}])$:

$$T = \sum_{\mathbf{j}} \sum_{\sigma \in S_{2N}} h\{\mathbf{j}, \sigma(\mathbf{j}[\Lambda, \{j_\lambda\}])\} \left[\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_\lambda, f} \right] \times \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu}). \quad (\text{C12})$$

The term $\prod_{\lambda \in \Lambda} \prod_{f \in \lambda} \delta_{j_\lambda, f}$ allows us to make the transformation $\mathbf{j} \rightarrow \mathbf{j}[\Lambda, \{j_\lambda\}]$, and to turn the sum over $\mathbf{j}$ into a sum only over the values of the representative indices $\{j_\lambda\}$. We can write

$$T = \sum_{\{j_\lambda\}} \sum_{\sigma \in S_{2N}} h\{\mathbf{j}[\Lambda, \{j_\lambda\}], \sigma(\mathbf{j}[\Lambda, \{j_\lambda\}])\} \times \prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu}). \quad (\text{C13})$$

Finally, the product of deltas $\prod_{(\lambda \neq \mu) \in \Lambda} (1 - \delta_{j_\lambda, j_\mu})$ ensures that we focus only on the terms where the representative indices take different values. Then, T will read

$$T = \sum_{\text{diff. } \{j_\lambda\}} \sum_{\sigma \in S_{2N}} h\{\mathbf{j}[\Lambda, \{j_\lambda\}], \sigma(\mathbf{j}[\Lambda, \{j_\lambda\}])\}. \quad (\text{C14})$$

Summing all the contributions from different partitions, we reach the result

$$\sum_{\mathbf{j}, \mathbf{j}'} h(\mathbf{j}, \mathbf{j}') I(\mathbf{j}, \mathbf{j}') = \sum_{\Lambda \in \mathcal{Q}[\mathbf{j}]} \sum_{\text{diff. } \{j_\lambda\}} \sum_{\sigma \in S_{2N}} \frac{1}{\Lambda!} h\{\mathbf{j}[\Lambda, \{j_\lambda\}], \sigma(\mathbf{j}[\Lambda, \{j_\lambda\}])\}. \quad (\text{C15})$$

Equation (50) is obtained by applying this result to

$$h(\mathbf{j}, \mathbf{j}') = \sum_{\mu, \nu} \zeta_\mu \zeta_\nu \mathcal{U}[\mathbf{j} \oplus \mathbf{j}', \bar{\mu} \mid \Omega_k(\mathbf{j}) \oplus \Omega_l(\mathbf{j}'), \bar{\nu}]. \quad (\text{C16})$$

APPENDIX D: WEINGARTEN CALCULUS

In this appendix we gather the two key theorems regarding the Weingarten calculus that we used in Sec. IV D.

Proposition 5 (Lemma 3 of Ref. [35]). *Let $\mathbf{U}$ be an $M \times M$ Haar-distributed unitary matrix, and let $\mathbf{j} = (j_1, \dots, j_n)$, $\boldsymbol{\mu} = (\mu_1, \dots, \mu_n)$, $\mathbf{j}' = (j'_1, \dots, j'_n)$, and $\boldsymbol{\mu}' = (\mu'_1, \dots, \mu'_n)$ be four sequences of indices in $[M] = \{1, \dots, M\}$ (i.e., each index can take values from 1 to M).*

If $m = n$,

$$\mathbb{E}_{\mathbf{U}}[\mathcal{U}(\mathbf{j}, \boldsymbol{\mu} \mid \mathbf{j}', \boldsymbol{\mu}')] = \sum_{\substack{\varrho \in S_n \\ \mathbf{j}' = \varrho(\mathbf{j})}} \sum_{\substack{\tau \in S_n \\ \boldsymbol{\mu}' = \tau(\boldsymbol{\mu})}} W_{\mathbf{g}_n}(\varrho^{-1} \circ \tau; M), \quad (\text{D1})$$

and it vanishes otherwise. Here,

$$\mathcal{U}(\mathbf{j}, \boldsymbol{\mu} \mid \mathbf{j}', \boldsymbol{\mu}') = U_{j_1, \mu_1} \cdots U_{j_n, \mu_n} U_{j'_1, \mu'_1}^* \cdots U_{j'_n, \mu'_n}^* \quad (\text{D2})$$

and $W_{\mathbf{g}_n}(\sigma; M)$ is the Weingarten function for the unitary group $U(M)$ [25, 35]. The sums extend over all permutations ϱ, τ in the symmetric group of degree n , S_n , such that $\mathbf{j}' = \varrho(\mathbf{j})$ and $\boldsymbol{\mu}' = \tau(\boldsymbol{\mu})$.

Note that we can write

$$\sum_{\substack{\varrho \in S_n \\ \mathbf{j}' = \varrho(\mathbf{j})}} \sum_{\substack{\tau \in S_n \\ \boldsymbol{\mu}' = \tau(\boldsymbol{\mu})}} W_{\mathbf{g}_n}(\varrho^{-1} \circ \tau; M) \quad (\text{D3})$$

$$= \sum_{\varrho \in S_n} \sum_{\tau \in S_n} \Delta[\mathbf{j}' \mid \varrho(\mathbf{j})] \Delta[\boldsymbol{\mu}' \mid \tau(\boldsymbol{\mu})] W_{\mathbf{g}_n}(\varrho^{-1} \circ \tau; M) \quad (\text{D4})$$

with $\Delta[\mathbf{j}' \mid \varrho(\mathbf{j})] = \prod_{a=1}^n \delta_{j'_a, \varrho(j_a)}$, which corresponds to the form used in Eq. (52).

Proposition 6 (Corollary 2.7 of Ref. [40]). *We have*

$$M^{n+\|\sigma\|} W_{\mathbf{g}_n}(\sigma; M) = \text{Moeb}(\sigma) + \mathcal{O}(M^{-2}), \quad (\text{D5})$$

where $\|\sigma\|$ is the minimum number of transpositions in which we can write σ and

$$\text{Moeb}(\sigma) = \prod_{k=1}^l \text{Cat}(|\chi_k| - 1) (-1)^{|\chi_k| - 1} \quad (\text{D6})$$

is the Möbius function. In this expression, the $\{\chi_k\}$ are the disjoint cycles in the cycle decomposition of σ (i.e., we write $\sigma = \chi_1 \chi_2 \cdots \chi_l$), $|\chi_k|$ denotes the length of cycle χ_k , and $\text{Cat}(n) = (2n)!/[n!(n+1)!]$ stands for the n th Catalan number.

APPENDIX E: COMPUTATION OF THE LXE SCORE FOR THE IDEAL SQUEEZED STATE MODEL WITH DIFFERENT SQUEEZING PARAMETERS

In this appendix we complete the details of the computation of the ideal score for GBS setups using different squeezing parameters, and show that the resulting expression is consistent with the findings of Sec. IV.

Our main goal in this section is to prove that

$$\sum_{\mu \in [R]^{2N}} \sum_{\substack{\mathbf{v} \in [R]^{2N} \\ \text{such that } \bar{\mathbf{v}} = \varrho(\bar{\mu})}} \prod_{a=1}^{2N} \tanh(r_{\mu_a}) \tanh(r_{v_a}) = \left(\prod_{b \in \eta(\varrho)} \varepsilon_{2b} \right) R^{\ell(\varrho)}. \quad (\text{E1})$$

In order to do so, let us first briefly recall the definitions of all the terms involved in this relation. Here $\mu = (\mu_1, \dots, \mu_{2N})$, $\mathbf{v} = (v_1, \dots, v_{2N})$ are vectors whose integer components take values in the set $[R] = \{1, \dots, R\}$ (this is indicated by the symbols $\mu \in [R]^{2N}$, $\mathbf{v} \in [R]^{2N}$). Vector $\bar{\mu} = (\bar{\mu}_1, \dots, \bar{\mu}_{4N}) = (\mu_1, \mu_1, \dots, \mu_{2N}, \mu_{2N})$, and $\bar{\mathbf{v}}$ has an analogous definition. Let us remind the reader that R is the number of modes with a squeezed state at the input. The squeezing parameters of the input single-mode squeezed states are $\{r_k\}_{k=1}^R$. We denote by $\eta(\varrho)$ the coset type of $\varrho \in S_{4N}$, and by $\ell(\varrho)$ the length of $\eta(\varrho)$. Finally, ε_a is defined as

$$\varepsilon_a = \frac{1}{R} \sum_{k=1}^R \tanh^a(r_k). \quad (\text{E2})$$

Now, note that the second sum on the left-hand side of Eq. (E1) runs over values of $\mathbf{v}$ that satisfy the condition $\bar{\mathbf{v}} = \varrho(\bar{\mu})$. Along with the definitions of $\bar{\mathbf{v}}$ and $\bar{\mu}$, this condition allows us to write the relations

$$\bar{\mu}_{2k-1} = \bar{\mu}_{2k} = \mu_k, \quad k \in \{1, \dots, 2N\}, \quad (\text{E3})$$

$$\bar{\mu}_{\varrho(2k-1)} = \bar{\mu}_{\varrho(2k)} = v_k, \quad k \in \{1, \dots, 2N\}. \quad (\text{E4})$$

The second of these relations leads to two types of constraints: (i) a constraint that defines each v_k in terms of μ_k and ϱ ; and (ii) a constraint between different $\{\mu_k\}$, which comes from the relation $\bar{\mu}_{\varrho(2k-1)} = \bar{\mu}_{\varrho(2k)}$. This means that the final sum in Eq. (E1) will run over only a number of “free” $\{\tilde{\mu}_l\}$. In what follows, we determine how many of these free indices there are.

Let us recall that each $\varrho \in S_{4N}$ has an associated undirected graph, $\Gamma(\varrho)$, whose vertices are $\{1, \dots, 4N\}$, and whose edges are defined by the sets $\{(2k-1, 2k), k \in \{1, \dots, 2N\}\}$ and $\{[\varrho(2k-1), \varrho(2k)], k \in \{1, \dots, 2N\}\}$. Combined with relations (E3) and (E4), this definition implies that, for every edge in $\Gamma(\varrho)$, there will be an equality of the form $\bar{\mu}_{2k} = \bar{\mu}_{2k-1}$ or $\bar{\mu}_{\varrho(2k)} = \bar{\mu}_{\varrho(2k-1)}$. This, in turn, leads to the following result.

Proposition 7. *Let $a, b \in \{1, \dots, 4N\}$ and $a \neq b$; then $\bar{\mu}_a = \bar{\mu}_b$ if and only if vertices a and b are connected in $\Gamma(\varrho)$.*

Proof. If vertices a and b are connected in $\Gamma(\varrho)$ then there exists a sequence of vertices $\{v_1, v_2, \dots, v_p\}$, with $v_1 = a$, $v_p = b$, and $2 \leq p \leq 4N$, where v_k is adjacent to v_{k+1} , i.e., there is an edge connecting them, for all $k \in \{1, \dots, p-1\}$. The presence of an edge between v_k and v_{k+1} implies that $\bar{\mu}_{v_k} = \bar{\mu}_{v_{k+1}}$. Since these relations hold for every k , we can conclude that $\bar{\mu}_{v_1} = \bar{\mu}_{v_p}$, so $\bar{\mu}_a = \bar{\mu}_b$.

Suppose now that $\bar{\mu}_a = \bar{\mu}_b$. If there exists some $k \in \{1, \dots, 2N\}$ such that $a = 2k-1$, $b = 2k$ or $a = \varrho(2k-1)$, $b = \varrho(2k)$ (or the same relations but inverting the places of a and b), then a and b are connected. In any other case, we can find a new vertex v_2 adjacent to a that satisfies $\bar{\mu}_a = \bar{\mu}_{v_2}$, either by Eq. (E3) or Eq. (E4), and check if it is connected to b . If not, we can find a second vertex v_3 adjacent to v_2 but not to a (because every vertex lies in exactly two edges) that will satisfy $\bar{\mu}_a = \bar{\mu}_{v_2} = \bar{\mu}_{v_3}$; then we can verify whether it is adjacent to b or not. We can repeat this process until we find a sequence of adjacent vertices $\{v_2, \dots, v_{p-1}\}$ that satisfy $\bar{\mu}_a = \bar{\mu}_{v_2} = \dots = \bar{\mu}_b$. The existence of this sequence implies that a and b are connected in $\Gamma(\varrho)$. ■

Following this proposition, we can see that if $\bar{\mu}_a \neq \bar{\mu}_b$ then vertices a and b will belong to different connected components in $\Gamma(\varrho)$. Since every $\bar{\mu}_a$ is equal to some μ_k , with $k \in \{1, \dots, 2N\}$, this implies that there will be as many different (or free) $\{\tilde{\mu}_l\}$ as there are connected components in $\Gamma(\varrho)$. Therefore, we may say that the number of different $\{\tilde{\mu}_l\}$ is equal to the length of the coset type of ϱ , $\ell(\varrho)$.

In each connected component, an edge of the form $(2k-1, 2k)$ determines a single μ_k via the relation $\bar{\mu}_{2k-1} = \bar{\mu}_{2k} = \mu_k$. Edges of the form $[\varrho(2k-1), \varrho(2k)]$ determine which $\{\mu_k\}$ are equal to others. This implies that the number of repetitions, i.e., the degeneracy, of every free $\tilde{\mu}_l$ will be equal to the number of edges of the form $(2k-1, 2k)$ in its corresponding connected component. This number is equal to half the length of the connected component.

Let us recall the definition of the coset type of $\varrho \in S_{4N}$. Let $2\eta_1, 2\eta_2, \dots, 2\eta_\ell$, with $\eta_1 \geq \eta_2 \geq \dots \geq \eta_\ell \geq 1$, be the lengths of the different connected components in $\Gamma(\varrho)$. The coset type of ϱ is defined as $\eta(\varrho) = (\eta_1, \dots, \eta_\ell)$. As can be seen, η_l is half the length of the l th connected component of $\Gamma(\varrho)$, which, according to the argument given above, will be equal to the degeneracy of the free $\tilde{\mu}_l$ corresponding to that component. This means that we can determine the degeneracies of all $\{\tilde{\mu}_l\}$ by computing $\eta(\varrho)$.

We are now in the position to prove Eq. (E1). Taking into account the fact that each $\{v_k\}$ will be equal to some free $\tilde{\mu}_l$, we may write

$$\sum_{\mu \in [R]^{2N}} \sum_{\substack{\mathbf{v} \in [R]^{2N} \\ \text{such that } \bar{\mathbf{v}} = \varrho(\bar{\mu})}} \prod_{a=1}^{2N} \tanh(r_{\mu_a}) \tanh(r_{v_a})$$

$$\begin{aligned}
 &= \sum_{\{\tilde{\mu}_l\}} \prod_{a=1}^{\ell(\varrho)} \tanh^{2\eta_a}(r_{\tilde{\mu}_a}) \\
 &= \prod_{a=1}^{\ell(\varrho)} \sum_{\tilde{\mu}_a=1}^R \tanh^{2\eta_a}(r_{\tilde{\mu}_a}). \tag{E5}
 \end{aligned}$$

Recalling the definition of ε_a , we obtain

$$\prod_{a=1}^{\ell(\varrho)} \sum_{\tilde{\mu}_a=1}^R \tanh^{2\eta_a}(r_{\tilde{\mu}_a}) = \prod_{a=1}^{\ell(\varrho)} \varepsilon_{2\eta_a} R = \left(\prod_{b \in \eta(\varrho)} \varepsilon_{2b} \right) R^{\ell(\varrho)}. \tag{E6}$$

To conclude this appendix, we show that the result in Eq. (80) is consistent with Eq. (13). Suppose that $r_k = r$ for all $k \in \{1, \dots, R\}$; then $\varepsilon_a = \tanh^a(r)$ for every a . This allows us to see that

$$\prod_{b \in \eta(\varrho)} \varepsilon_{2b} = \tanh^{2\eta_1 + \dots + 2\eta_\ell}(r) = \tanh^{4N}(r), \tag{E7}$$

where we took into account the fact that, according to its definition, $\eta(\varrho)$ is an integer partition of $2N$ for all ϱ (therefore, $\eta_1 + \dots + \eta_\ell = 2N$). This allows us to recast Eq. (81) as

$$\begin{aligned}
 c'_\ell &= \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\sigma \in S_{2N}} \sum_{\varrho \in \tilde{S}_\ell} \tanh^{4N}(r) \\
 &= \tanh^{4N}(r) \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \sum_{\sigma \in S_{2N}} |\tilde{S}_\ell|. \tag{E8}
 \end{aligned}$$

Now recalling the definition of $|\tilde{S}_\ell|$ from Eq. (86),

$$|\tilde{S}_\ell| = b_\ell [\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})], \tag{E9}$$

and the definition of b_ℓ from Eq. (68), we can then write

$$\begin{aligned}
 c'_\ell &= \tanh^{4N}(r) \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\
 &\quad \times \sum_{\sigma \in S_{2N}} b_\ell [\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})] \\
 &= \tanh^{4N}(r) c_\ell. \tag{E10}
 \end{aligned}$$

On the other hand, we have

$$\begin{aligned}
 \sum_{\ell=1}^N d'_\ell R^\ell &= \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{\varepsilon_{2a}^{k_a} R^{k_a}}{k_a! (2a)^{k_a}} \\
 &= \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{\tanh^{2a}(r) R^{k_a}}{k_a! (2a)^{k_a}} \\
 &= \tanh^{2N}(r) \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{R^{k_a}}{k_a! (2a)^{k_a}}, \tag{E11}
 \end{aligned}$$

where we used the condition $k_1 + 2k_2 + \dots + Nk_N = N$. In order to continue, we need the following proposition.

Proposition 8. *It holds that*

$$\sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{R^{k_a}}{k_a! (2a)^{k_a}} = \binom{R/2 + N - 1}{N}. \tag{E12}$$

Proof. Note that

$$\sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{R^{k_a}}{k_a! (2a)^{k_a}} = Z_N \left(\frac{R}{2}, \frac{R}{2}, \dots, \frac{R}{2} \right), \tag{E13}$$

where Z_N is the cycle index of S_N [see Eq. (32)]:

$$Z_N(y_1, \dots, y_N) = \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! a^{k_a}} \prod_{a=1}^N y_a^{k_a}. \tag{E14}$$

Using the generating function of $Z_n(y_1, \dots, y_n)$ [33,38],

$$\exp \left[\sum_{l=1}^{\infty} y_l \frac{\alpha^l}{l} \right] = \sum_{n=0}^{\infty} Z_n(y_1, \dots, y_n) \alpha^n, \tag{E15}$$

we can write

$$\exp \left[\frac{R}{2} \sum_{l=1}^{\infty} \frac{\alpha^l}{l} \right] = \sum_{n=0}^{\infty} Z_n \left(\frac{R}{2}, \frac{R}{2}, \dots, \frac{R}{2} \right) \alpha^n. \tag{E16}$$

Assuming that $|\alpha| < 1$, we can write $\sum_{l=1}^{\infty} \alpha^l/l = -\log(1 - \alpha)$, and obtain

$$\begin{aligned}
 \exp \left[-\frac{R}{2} \log(1 - \alpha) \right] &= (1 - \alpha)^{-R/2} \\
 &= \sum_{n=0}^{\infty} Z_n \left(\frac{R}{2}, \frac{R}{2}, \dots, \frac{R}{2} \right) \alpha^n. \tag{E17}
 \end{aligned}$$

Taking into account the fact that

$$(1 - \alpha)^{-R/2} = \sum_{n=0}^{\infty} \binom{R/2 + n - 1}{n} \alpha^n, \quad (\text{E18})$$

we see that Eq. (E13) holds. $\blacksquare$

From this result, it follows that

$$\sum_{\ell=1}^N d'_\ell R^\ell = \tanh^{2N}(r) \binom{R/2 + N - 1}{N}. \quad (\text{E19})$$

Combining this relation with Eqs. (80) and (E11), we obtain

$$\begin{aligned} s(\mathbf{A}'_{\text{sqz}}; 2N) &= \frac{1}{(2N)!} \left(\sum_{\ell=1}^N d'_\ell R^\ell \right)^{-2} \sum_{\ell=1}^{2N} c'_\ell R^\ell \\ &= \frac{1}{(2N)!} \tanh^{-4N}(r) \binom{R/2 + N - 1}{N}^{-2} \\ &\quad \times \tanh^{4N}(r) \sum_{\ell=1}^{2N} c_\ell R^\ell \\ &= \frac{4^N (N!)^2}{(2N)!} \left[\frac{(R-2)!!}{(R+2N-2)!!} \right]^2 \sum_{\ell=1}^{2N} c_\ell R^\ell \\ &= s(\mathbf{A}_{\text{sqz}}; 2N). \end{aligned} \quad (\text{E20})$$

APPENDIX F: COMPUTATION OF THE LXE SCORE FOR THE IDEAL SQUEEZED STATE MODEL WITHOUT VACUUM INPUT MODES

In this appendix we present the details of the computation of the score for the ideal squeezed state model without vacuum input modes. Specifically, we prove that

$$\begin{aligned} \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ \times \sum_{\sigma \in S_{2N}} b_{2N}[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})] = 1, \end{aligned} \quad (\text{F1})$$

with b_{2N} defined in Eq. (16). This leads to the result

$$s(\tilde{\mathbf{A}}'_{\text{sqz}}; 2N) = s(\tilde{\mathbf{A}}_{\text{sqz}}; 2N) = \frac{4^N (N!)^2}{(2N)!}. \quad (\text{F2})$$

Let us recall that $b_{2N}[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})]$ is the number of permutations in the hyperoctahedral group of degree $2N$, $H_{2N} \subset S_{4N}$, that transform the sequence $\mathbf{j} \oplus \sigma(\mathbf{j})$ into $\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})$. Recall also that the indices $\mathbf{j} = (j_1, \dots, j_{2N})$ are all different.

We begin by recasting $b_{2N}[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})]$ into an expression that is independent of $\mathbf{j}$. Given two permutations $\sigma \in S_n$ and $\sigma' \in S_m$, their *direct sum* $\sigma \oplus \sigma' \in S_{m+n}$ is defined by its action on the sequence $(1, \dots, m+n)$ as

$$(\sigma \oplus \sigma')(k) = \begin{cases} \sigma(k), & k \in \{1, \dots, n\}, \\ \sigma'(k-n) + n, & k \in \{n+1, \dots, n+m\}, \end{cases} \quad (\text{F3})$$

i.e., $\sigma \oplus \sigma'$ acts as σ in the first n elements of a sequence, and as σ' in the remaining elements. From this definition, we can write the relations

$$\mathbf{j} \oplus \sigma(\mathbf{j}) = (e_{2N} \oplus \sigma)(\mathbf{j} \oplus \mathbf{j}), \quad (\text{F4})$$

$$\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j}) = (\Omega_{\mathbf{k}} \oplus \Omega_{\mathbf{l}}) \circ (e_{2N} \oplus \sigma)(\mathbf{j} \oplus \mathbf{j}), \quad (\text{F5})$$

where e_{2N} is the identity permutation in S_{2N} .

To shorten the notation, we denote the composition $\sigma \circ \tau$ of two permutations $\sigma, \tau \in S_n$ as $\sigma\tau$. Suppose now that $\varrho \in S_{4N}$ transforms $\mathbf{j} \oplus \sigma(\mathbf{j})$ into $\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})$. Then

$$\varrho(e_{2N} \oplus \sigma)(\mathbf{j} \oplus \mathbf{j}) = (\Omega_{\mathbf{k}} \oplus \Omega_{\mathbf{l}})(e_{2N} \oplus \sigma)(\mathbf{j} \oplus \mathbf{j}), \quad (\text{F6})$$

which implies that

$$\begin{aligned} &[(\Omega_{\mathbf{k}} \oplus \Omega_{\mathbf{l}})(e_{2N} \oplus \sigma)]^{-1} \varrho(e_{2N} \oplus \sigma)(\mathbf{j} \oplus \mathbf{j}) \\ &= [(e_{2N} \oplus \sigma^{-1})(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1}) \varrho(e_{2N} \oplus \sigma)](\mathbf{j} \oplus \mathbf{j}) \\ &= \mathbf{j} \oplus \mathbf{j}, \end{aligned} \quad (\text{F7})$$

where $(\sigma \oplus \tau)^{-1} = \sigma^{-1} \oplus \tau^{-1}$. This means that $(e_{2N} \oplus \sigma^{-1})(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1}) \varrho(e_{2N} \oplus \sigma)$ is a permutation that leaves the sequence $\mathbf{j} \oplus \mathbf{j}$ invariant.

Let $S^* \subset S_{4N}$ be defined as

$$S^* = \{\nu \in S_{4N} \mid \nu(\mathbf{j} \oplus \mathbf{j}) = \mathbf{j} \oplus \mathbf{j}\}. \quad (\text{F8})$$

Then, every permutation ϱ that takes $\mathbf{j} \oplus \sigma(\mathbf{j})$ into $\Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})$ can be written in the form

$$\varrho = (\Omega_{\mathbf{k}} \oplus \Omega_{\mathbf{l}})[(e_{2N} \oplus \sigma) \nu (e_{2N} \oplus \sigma^{-1})], \quad \nu \in S^*. \quad (\text{F9})$$

It can be easily shown that S^* forms a subgroup of S_{4N} . Indeed, the identity permutation $e_{4N} \in S_{4N}$ clearly leaves the sequence $\mathbf{j} \oplus \mathbf{j}$ invariant, so $e_{4N} \in S^*$. Let $\nu_1, \nu_2 \in S^*$; we have $\nu_1 \nu_2(\mathbf{j} \oplus \mathbf{j}) = \nu_1[\nu_2(\mathbf{j} \oplus \mathbf{j})] = \nu_1(\mathbf{j} \oplus \mathbf{j}) = \mathbf{j} \oplus \mathbf{j}$, which implies that $\nu_1 \nu_2 \in S^*$. We can show that $\nu_2 \nu_1 \in S^*$ in a completely analogous way. Finally, for any $\nu_1 \in S^*$, $\mathbf{j} \oplus \mathbf{j} = \nu_1^{-1} \nu_1(\mathbf{j} \oplus \mathbf{j}) = \nu_1^{-1}[\nu_1(\mathbf{j} \oplus \mathbf{j})] = \nu_1^{-1}(\mathbf{j} \oplus \mathbf{j})$, which implies that $\nu_1^{-1} \in S^*$.

The subset $S_\sigma^* \subset S_{4N}$ defined by

$$S_\sigma^* = \{\tau \in S_{4N} \mid \tau = (e_{2N} \oplus \sigma) \nu (e_{2N} \oplus \sigma^{-1}), \nu \in S^*\} \quad (\text{F10})$$

is also a subgroup of S_{4N} for every $\sigma \in S_{2N}$; it is the group of all permutations in S_{4N} that leave invariant the sequence $\mathbf{j} \oplus \sigma(\mathbf{j})$.

The permutations in S^* can only make the interchange $k \leftrightarrow k + 2N$ for $k \in \{1, \dots, 2N\}$. In this way we guarantee that $\mathbf{j} \oplus \mathbf{j}$ remains invariant. Thus, an arbitrary permutation in S^* will take a subset B of $\{1, \dots, 2N\}$, make the interchange $k \leftrightarrow k + 2N$ for all $k \in B$, and keep all the remaining elements in $\{1, \dots, 4N\}$ unchanged. We may then write every $\nu \in S^*$ as $\nu \equiv \nu_B$, where $B \in \mathcal{P}(\{1, \dots, 2N\})$ and

$\mathcal{P}(A)$ stands for the power set of A . Furthermore, we may write the action of ν_B over the sequence $(1, \dots, 4N)$ as

$$\nu_B(k) = \begin{cases} k, & k \notin B, \\ k + 2N, & k \in B, \\ k, & k - 2N \notin B \text{ and } k \in \{2N + 1, \dots, 4N\}, \\ k - 2N, & k - 2N \in B \text{ and } k \in \{2N + 1, \dots, 4N\}. \end{cases} \quad (\text{F11})$$

We can readily see that $|S^*| = |S_\sigma^*| = 2^{2N}$ for all $\sigma \in S_{2N}$, since there are as many ν_B as there are subsets of $\{1, \dots, 2N\}$. Moreover, we can write the action of permutations $\tau_B \in S_\sigma^*$ over sequence $(1, \dots, 4N)$ as

$$\begin{aligned} \tau_B(k) &= [(e_{2N} \oplus \sigma) \nu_B (e_{2N} \oplus \sigma^{-1})](k) \\ &= \begin{cases} k, & k \notin B, \\ \sigma(k) + 2N, & k \in B, \\ k, & \sigma^{-1}(k - 2N) \notin B \text{ and } k \in \{2N + 1, \dots, 4N\}, \\ \sigma^{-1}(k - 2N), & \sigma^{-1}(k - 2N) \in B \text{ and } k \in \{2N + 1, \dots, 4N\}. \end{cases} \end{aligned} \quad (\text{F12})$$

Having characterized the permutations in S^* and S_σ^* , let us return to the expression for ϱ given in Eq. (F9). In order to compute $b_{2N}[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}}\sigma(\mathbf{j})]$, we require that $\varrho = (\Omega_{\mathbf{k}} \oplus \Omega_{\mathbf{l}})\tau_B = \beta$ for some $\beta \in H_{2N}$. This implies that $\tau_B = (\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})\beta$, or, equivalently, $\tau_B \in (\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})H_{2N}$, i.e., τ_B must be an element of the *left coset* of H_{2N} corresponding to $\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1}$. On this account, determining the adequate ϱ amounts to finding the elements of $(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})H_{2N} \cap S_\sigma^*$. Then, we may write

$$b_{2N}[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}}\sigma(\mathbf{j})] = |(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})H_{2N} \cap S_\sigma^*|. \quad (\text{F13})$$

This is the $\mathbf{j}$ -independent expression of coefficients b_{2N} .

In the following we show how to compute $|(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})H_{2N} \cap S_\sigma^*|$ as a function of $\mathbf{k}$, $\mathbf{l}$, and σ . However, in order to do so, we need to prove a number of important intermediate results. The first of these results concerns the following definition.

Definition 1 (Hyperoctahedral group). *The hyperoctahedral group of degree n , $H_n \subset S_{2n}$, is the centralizer of the permutation $\Omega^* \in S_{2n}$ that transforms the sequence of indices $(g_1, \dots, g_{2n})$ as $\Omega^*[(g_1, g_2, \dots, g_{2n-1}, g_{2n})] = (g_2, g_1, \dots, g_{2n}, g_{2n-1})$ [48].*

Let us recall that the centralizer of a permutation $\tau \in S_m$ is the set of all permutations in S_m that commute with τ , i.e., $\{\varrho \in S_m \mid \varrho\tau = \tau\varrho\}$. As a product of disjoint transpositions, Ω^* reads $\Omega^* = (1\ 2)(3\ 4) \dots (2n-1\ 2n)$. Note that $(\Omega^*)^2 = e_{2n}$. The following proposition gives us a useful way of characterizing the elements of H_n .

Proposition 9. *We have $\sigma \in H_n$ if and only if, for every $p \in \{1, \dots, n\}$, there exists a $q \in \{1, \dots, n\}$ such that $\sigma(2p) = 2q$, $\sigma(2p-1) = 2q-1$ or $\sigma(2p) = 2q-1$, $\sigma(2p-1) = 2q$.*

Proof. Since H_n is the centralizer of Ω^* , $\sigma \in H_n$ if and only if $\Omega^*\sigma\Omega^* = \sigma$. Let us consider an arbitrary $p \in \{1, \dots, n\}$. We have

$$\begin{aligned} \sigma(2p) &= [\Omega^*\sigma\Omega^*](2p) = [\Omega^*\sigma](2p-1) \\ &= \Omega^*[\sigma(2p-1)]. \end{aligned} \quad (\text{F14})$$

Since σ is a bijection from $\{1, \dots, 2n\}$ to itself, there exists a unique $q \in \{1, \dots, n\}$ such that $\sigma(2p-1) = 2q$ or $\sigma(2p-1) = 2q-1$. In the first case we have

$$\sigma(2p) = \Omega^*[\sigma(2p-1)] = \Omega^*(2q) = 2q-1. \quad (\text{F15})$$

In the second case we obtain

$$\sigma(2p) = \Omega^*[\sigma(2p-1)] = \Omega^*(2q-1) = 2q. \quad (\text{F16})$$

On the other hand, suppose that $\sigma \in S_{2n}$ satisfies the condition that, for every $p \in \{1, \dots, n\}$, there exists a $q \in \{1, \dots, n\}$ such that $\sigma(2p) = 2q$, $\sigma(2p-1) = 2q-1$ or $\sigma(2p) = 2q-1$, $\sigma(2p-1) = 2q$. In the first case we have

$$[\Omega^* \sigma](2p) = \Omega^*[\sigma(2p)] = \Omega^*(2q) = 2q-1, \quad (\text{F17})$$

$$[\Omega^* \sigma](2p-1) = \Omega^*[\sigma(2p-1)] = \Omega^*(2q-1) = 2q, \quad (\text{F18})$$

$$[\sigma \Omega^*](2p) = \sigma[\Omega^*(2p)] = \sigma(2p-1) = 2q-1, \quad (\text{F19})$$

$$[\sigma \Omega^*](2p-1) = \sigma[\Omega^*(2p-1)] = \sigma(2p) = 2q. \quad (\text{F20})$$

Thus, $[\sigma \Omega^*](2p) = [\Omega^* \sigma](2p)$ and $[\sigma \Omega^*](2p-1) = [\Omega^* \sigma](2p-1)$. Since these relations hold for an arbitrary p , we conclude that $\sigma \Omega^* = \Omega^* \sigma$ and, consequently, $\sigma \in H_n$. For the second case, we may write

$$[\Omega^* \sigma](2p) = \Omega^*[\sigma(2p)] = \Omega^*(2q-1) = 2q, \quad (\text{F21})$$

$$[\Omega^* \sigma](2p-1) = \Omega^*[\sigma(2p-1)] = \Omega^*(2q) = 2q-1, \quad (\text{F22})$$

$$[\sigma \Omega^*](2p) = \sigma[\Omega^*(2p)] = \sigma(2p-1) = 2q, \quad (\text{F23})$$

$$[\sigma \Omega^*](2p-1) = \sigma[\Omega^*(2p-1)] = \sigma(2p) = 2q-1. \quad (\text{F24})$$

We conclude again that $[\sigma \Omega^*](2p) = [\Omega^* \sigma](2p)$ and $[\sigma \Omega^*](2p-1) = [\Omega^* \sigma](2p-1)$ for every p ; therefore, $\sigma \Omega^* = \Omega^* \sigma$ and $\sigma \in H_n$. ■

A useful interpretation of the previous proposition follows from analyzing the undirected graphs $\Gamma(\sigma)$ associated with the $\sigma \in H_n$. As mentioned in Sec. IV E, these graphs have n connected components with two edges (see Fig. 7). Since the first set of edges of $\Gamma(\sigma)$ is of the form $\{(2p-1, 2p) \mid p \in \{1, \dots, n\}\}$, the only way we can obtain n connected components is that the edges in the second set $\{[\sigma(2p-1), \sigma(2p)] \mid p \in \{1, \dots, n\}\}$ be of the form $(2q-1, 2q)$ or $(2q, 2q-1)$, with $q \in \{1, \dots, n\}$, for every p .

Next, we show how to determine the coset type of permutations $\Omega_k \in S_{2N}$. From their definition [Eq. (14)] we see that the Ω_k are written as a product of disjoint cycles of even length, where a cycle of length $2a$ appears a total of k_a times [note that the permutations $\omega_a \in S_{2a}$ defined just below Eq. (14) are precisely these cycles]. Moreover,

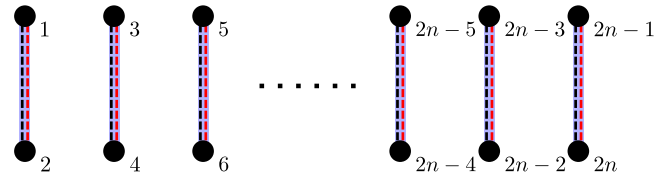


FIG. 7. Structure of the undirected graphs $\Gamma(\sigma)$ for $\sigma \in H_n$. The vertices of $\Gamma(\sigma)$ are represented by black circles. Edges corresponding to $\{(2p-1, 2p) \mid p \in \{1, \dots, n\}\}$ are shown as black dashed lines, while edges corresponding to $\{[\sigma(2p-1), \sigma(2p)] \mid p \in \{1, \dots, n\}\}$ are shown as red dashed lines. Each connected component of the graph is highlighted with a light blue, thick line. For $\Gamma(\sigma)$ to have n connected components, so that $\sigma \in H_n$, σ must keep together pairs of the form $(2q-1, 2q)$. This is the statement of Proposition 9.

all the elements within the cycles are consecutive. These features of Ω_k greatly facilitate the determination of its corresponding undirected graph $\Gamma(\Omega_k)$.

Proposition 10. *Permutation Ω_k has coset type $\eta(\Omega_k) = (N^{k_N}, \dots, 2^{k_2}, 1^{k_1})$, where a^{k_a} indicates that a appears k_a times in the partition $\eta(\Omega_k)$. For example, $(3^2, 1^4) \equiv (3, 3, 1, 1, 1, 1)$. If $k_a = 0$, the corresponding a does not appear in the partition. It follows that the length of the coset type of Ω_k is $\ell(\Omega_k) = \sum_{a=1}^N k_a$.*

Proof. Let us consider one of the cycles of length $2a$ that appear in the definition of Ω_k . This cycle acts over a sequence of consecutive indices of the form $(2q+1, \dots, 2q+2a)$, where we use $2q$ to label the beginning of this particular cycle. After applying Ω_k , this sequence transforms as $(2q+1, \dots, 2q+2a) \rightarrow \omega_a[(2q+1, \dots, 2q+2a)] = (2q+2, \dots, 2q+2a, 2q+1)$.

When constructing $\Gamma(\Omega_k)$ for this subset of vertices, we can see that the first set of edges of the graph has the form $\{(2q+1, 2q+2), \dots, (2q+2a-1, 2q+2a)\}$, while the second reads $\{[\omega_a(2q+1), \omega_a(2q+2)], \dots, [\omega_a(2q+2a-1), \omega_a(2q+2a)]\} = \{(2q+2, 2q+3), (2q+4, 2q+5), \dots, (2q+2a, 2q+1)\}$. These edges lead to a connected component of length $2a$ in $\Gamma(\Omega_k)$ (see Fig. 8).

Since all the cycles in Ω_k are disjoint, each cycle of length $2a$ leads to a different connected component of length $2a$ in $\Gamma(\Omega_k)$. Since there are k_a cycles of length $2a$ in Ω_k , there will be k_a connected components of length $2a$ in $\Gamma(\Omega_k)$. This implies that a will appear a total of k_a times in $\eta(\Omega_k)$, and thus $\eta(\Omega_k) = (N^{k_N}, \dots, 2^{k_2}, 1^{k_1})$. Note that, since $k_1 + 2k_2 + \dots + Nk_N = N$, $\eta(\Omega_k)$ will be, as expected, an integer partition of N . Finally, there will be a total of $k_1 + \dots + k_N$ connected components in $\Gamma(\Omega_k)$, so $\ell(\Omega_k) = \sum_{a=1}^N k_a$. ■

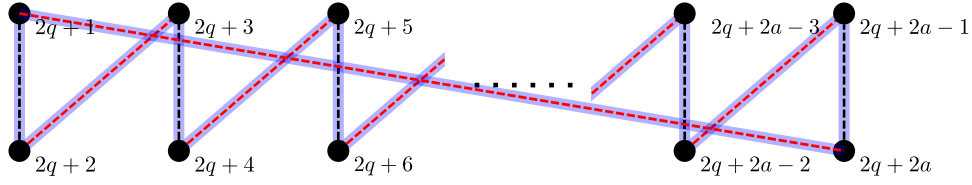


FIG. 8. Illustration of the connected component of $\Gamma(\Omega_k)$ corresponding to the vertices $(2q+1, \dots, 2q+2a)$ (black circles). Edges corresponding to $\{(2p-1, 2p) \mid p \in \{q+1, \dots, 2q+2a\}\}$ are shown as black dashed lines, while edges corresponding to $\{[\Omega_k(2p-1), \Omega_k(2p)] \mid p \in \{q+1, \dots, 2q+2a\}\} = \{[\omega_a(2p-1), \omega_a(2p)] \mid p \in \{q+1, \dots, 2q+2a\}\}$ are shown as red dashed lines. The connected component is highlighted by a light blue, thick line. As mentioned in the proof of Proposition 10, a cycle of length $2a$ acting over $(2q+1, \dots, 2q+2a)$ leads to a connected component of length $2a$ in $\Gamma(\Omega_k)$.

From the previous proposition, we can see that Ω_k and Ω_l will have different coset types whenever $k \neq l$.

We move on to stating two important results, one of them proved in Ref. [49], regarding coset types and left cosets.

Proposition 11 (Theorem 2.1 of Ref. [49]). (i) Two permutations $\sigma_1, \sigma_2 \in S_{2n}$ have the same coset type if and only if $\sigma_2 \in H_n \sigma_1 H_n$, that is, if and only if there exist $\tau_1, \tau_2 \in H_n$ such that $\sigma_2 = \tau_1 \sigma_1 \tau_2$.

(ii) Permutation $\sigma \in S_{2n}$ has the same coset type as σ^{-1} .

Proposition 12. If $\sigma_1 \in \sigma_2^{-1} H_n$ then σ_1 and σ_2 have the same coset type.

Proof. If $\sigma_1 \in \sigma_2^{-1} H_n$, then there exists $\tau \in H_n$ such that $\sigma_1 = \sigma_2^{-1} \tau$. Since H_n is a group, $e_{2n} \in H_n$, and thus we may write $\sigma_1 = e_{2n} \sigma_2^{-1} \tau$. This means that $\sigma_1 \in H_n \sigma_2^{-1} H_n$, which implies that σ_1 and σ_2^{-1} have the same coset type. Given that σ_2 and σ_2^{-1} have the same coset type, we conclude that σ_1 and σ_2 have the same coset type. ■

Equivalently, we may say that if $\sigma_1, \sigma_2 \in S_{2n}$ have different coset types then $\sigma_1 \notin \sigma_2^{-1} H_n$. Note that the converse

of Proposition 12 does not necessarily hold; the fact that σ_1 and σ_2 have the same coset type does not imply that $\sigma_1 \in \sigma_2^{-1} H_n$. As a direct consequence of Propositions 11 and 12, we obtain the following result, which will be of particular importance in our proof of Eq. (F1).

Proposition 13. Let $\sigma_1, \sigma_2, \tau \in S_{2n}$, and suppose that σ_1 and σ_2 have different coset types. Then $\tau \in \sigma_1^{-1} H_n$ implies that $\tau^{-1} \notin \sigma_2^{-1} H_n$.

Proof. If $\tau \in \sigma_1^{-1} H_n$, τ and τ^{-1} have the same coset type as σ_1 . Since σ_1 and σ_2 have different coset types, τ^{-1} and σ_2 will have different coset types, consequently, $\tau^{-1} \notin \sigma_2^{-1} H_n$. ■

We are now in the position to compute $|(\Omega_k^{-1} \oplus \Omega_l^{-1}) H_{2N} \cap S_\sigma^*|$ for the case $k \neq l$. A permutation $\tau_B \in S_\sigma^*$, corresponding to a subset $B \subseteq \{1, \dots, 2N\}$, will be an element of $(\Omega_k^{-1} \oplus \Omega_l^{-1}) H_{2N}$ if $(\Omega_k \oplus \Omega_l) \tau_B = \beta$ for $\beta \in H_{2N}$. This relation will set some constraints over B and σ . In order to find them, let us combine Eqs. (F3) and (F12), and express the action of β over pairs of the form $(2p-1, 2p)$, with $p \in \{1, \dots, 2N\}$, as

$$\beta(2p-1) = \begin{cases} \Omega_k(2p-1), & 2p-1 \notin B \text{ and } p \in \{1, \dots, N\}, \\ \Omega_l[\sigma(2p-1)] + 2N, & 2p-1 \in B \text{ and } p \in \{1, \dots, N\}, \\ \Omega_l(2p-2N-1) + 2N, & \sigma^{-1}(2p-2N-1) \notin B \text{ and } p \in \{N+1, \dots, 2N\}, \\ \Omega_k[\sigma^{-1}(2p-2N-1)], & \sigma^{-1}(2p-2N-1) \in B \text{ and } p \in \{N+1, \dots, 2N\}, \end{cases} \quad (\text{F25})$$

$$\beta(2p) = \begin{cases} \Omega_k(2p), & 2p \notin B \text{ and } p \in \{1, \dots, N\}, \\ \Omega_l[\sigma(2p)] + 2N, & 2p \in B \text{ and } p \in \{1, \dots, N\}, \\ \Omega_l(2p-2N) + 2N, & \sigma^{-1}(2p-2N) \notin B \text{ and } p \in \{N+1, \dots, 2N\}, \\ \Omega_k[\sigma^{-1}(2p-2N)], & \sigma^{-1}(2p-2N) \in B \text{ and } p \in \{N+1, \dots, 2N\}. \end{cases} \quad (\text{F26})$$

According to Proposition 9, $\beta \in H_{2N}$ if, for every $p \in \{1, \dots, 2N\}$, there exists a $q \in \{1, \dots, 2N\}$ such that $\beta(2p) = 2q$, $\beta(2p-1) = 2q-1$ or $\beta(2p) = 2q-1$, $\beta(2p-1) = 2q$. Keeping in mind that B^c is the complement of B , this condition allows us to draw the following conclusions.

- (1) Subset B must be nonempty because Ω_k, Ω_l are not, in general, elements of H_N , which would be necessary in order to have $\beta \in H_{2N}$.
- (2) When $p \in \{1, \dots, N\}$, it is necessary that either $2p-1, 2p \in B$ or $2p-1, 2p \notin B$, i.e., the pair $(2p-1, 2p)$ must remain together either in B or in B^c . Indeed, if $2p \in B$, but $2p-1 \notin B$, then $\beta(2p-1) = \Omega_k(2p-1) \in \{1, \dots, 2N\}$, while $\beta(2p) = \Omega_l[\sigma(2p)] + 2N \in \{2N+1, \dots, 4N\}$, which breaks the condition for β to be in H_{2N} . The case $2p-1 \in B, 2p \notin B$ yields to a similar conclusion.
- (3) When $p \in \{N+1, \dots, 2N\}$, it is necessary that either $\sigma^{-1}(2p-2N), \sigma^{-1}(2p-2N-1) \in B$ or $\sigma^{-1}(2p-2N), \sigma^{-1}(2p-2N-1) \notin B$. Just as before, if $\sigma^{-1}(2p-2N) \in B$, but $\sigma^{-1}(2p-2N-1) \notin B$, then $\beta(2p-1) = \Omega_l(2p-2N-1) + 2N \in \{2N+1, \dots, 4N\}$, while $\beta(2p) = \Omega_k[\sigma^{-1}(2p-2N)] \in \{1, \dots, 2N\}$, which implies that $\beta \notin H_{2N}$. The case $\sigma^{-1}(2p-2N-1) \in B, \sigma^{-1}(2p-2N) \notin B$ leads to a similar conclusion.
- (4) Assuming that the two conditions above hold, we require that B^c contains the pairs $(2p-1, 2p)$, with $p \in \{1, \dots, N\}$, for which $\Omega_k(2p-1) = 2q-1, \Omega_k(2p) = 2q$ or $\Omega_k(2p-1) = 2q, \Omega_k(2p) = 2q-1$ for some $q \in \{1, \dots, N\}$. Moreover, we require that B^c contains the pairs $[\sigma^{-1}(2p-2N-1), \sigma^{-1}(2p-2N)]$, with $p \in \{N+1, \dots, 2N\}$, for which $\Omega_l(2p-2N-1) = 2q'-1, \Omega_l(2p-2N) = 2q'$ or $\Omega_l(2p-2N-1) = 2q', \Omega_l(2p-2N) = 2q'-1$ for some $q' \in \{1, \dots, N\}$. In other words, the elements in B^c must correspond to transpositions in the cycle decomposition of both Ω_k and Ω_l . Recall that permutations Ω_k are defined as products of cycles of even length. The only possible cycles that naturally satisfy the condition described here are those of length 2, i.e., the transpositions.
- (5) We can guarantee that the elements in B^c correspond to transpositions in both Ω_k and Ω_l by constructing

B using the following prescription. There are k_1 transpositions (cycles of length 2) in Ω_k and the last element in $\{1, \dots, 2N\}$ that belongs to a transposition in Ω_k is precisely $2k_1$. Similarly, the last element in $\{1, \dots, 2N\}$ that belongs to a transposition in Ω_l is $2l_1$. Let $2p^* = \min(2k_1, 2l_1)$; then $B = \{2p^*+1, \dots, 2N\}$ contains all the elements in $\{1, \dots, 2N\}$ that correspond to cycles of length greater than 2 in both Ω_k and Ω_l . Note that B will also contain elements that correspond to some transpositions in Ω_k or Ω_l as long as $k_1 \neq l_1$. This construction ensures that the elements of B^c lead only to transpositions in both Ω_k and Ω_l .

- (6) The prescription given above is not the only way to construct B . Indeed, the only condition that B should satisfy is that it contains all the elements in $\{1, \dots, 2N\}$ that correspond to cycles of length greater than 2 in both Ω_k and Ω_l . This means that B can also contain any number of pairs of the form $(2p-1, 2p)$ that correspond to transpositions in Ω_k or Ω_l .
- (7) Let B satisfy item (5) or (6) above, and suppose that there is some $p \in \{N+1, \dots, 2N\}$ such that $\sigma^{-1}(2p-2N-1), \sigma^{-1}(2p-2N) \notin B$, but $2p-2N-1, 2p-2N \in B$. Then, in general, we cannot guarantee that $\beta(2p-1) = \Omega_l(2p-2N-1) + 2N, \beta(2p) = \Omega_l(2p-2N) + 2N$ will satisfy the conditions that let $\beta \in H_{2N}$. This is because most (or all) of the elements in B correspond to cycles of length greater than 2 in Ω_l . In order to avoid this, we demand that $\sigma^{-1}(B) = \sigma(B) = B$, i.e., the image of B under σ, σ^{-1} is B itself. In this way, the condition $\sigma^{-1}(2p-2N-1), \sigma^{-1}(2p-2N) \notin B$ will always correspond to a transposition in Ω_l . This constraints σ to have the form $\sigma = \bar{\sigma} \oplus \tilde{\sigma}$, where $\bar{\sigma} \in S_{2N-|B|}$ acts only over B^c , and $\tilde{\sigma} \in S_{|B|}$ acts only over B .

Following these considerations, we can recast Eqs. (F25) and (F26) as

$$\beta(2p-1) = \begin{cases} \bar{\Omega}_k(2p-1), & 2p-1 \notin B \text{ and } p \in \{1, \dots, N\}, \\ \tilde{\Omega}_l[\tilde{\sigma}(2p-1)] + 2N, & 2p-1 \in B \text{ and } p \in \{1, \dots, N\}, \\ \bar{\Omega}_l(2p-2N-1) + 2N, & 2p-2N-1 \notin B \text{ and } p \in \{N+1, \dots, 2N\}, \\ \tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p-2N-1)], & 2p-2N-1 \in B \text{ and } p \in \{N+1, \dots, 2N\}, \end{cases} \quad (\text{F27})$$

$$\beta(2p) = \begin{cases} \bar{\Omega}_k(2p), & 2p \notin B \text{ and } p \in \{1, \dots, N\}, \\ \tilde{\Omega}_l[\tilde{\sigma}(2p)] + 2N, & 2p \in B \text{ and } p \in \{1, \dots, N\}, \\ \bar{\Omega}_l(2p-2N) + 2N, & 2p-2N \notin B \text{ and } p \in \{N+1, \dots, 2N\}, \\ \tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p-2N)], & 2p-2N \in B \text{ and } p \in \{N+1, \dots, 2N\}, \end{cases} \quad (\text{F28})$$

where we used the decomposition of Ω_k and Ω_l as $\Omega_k = \tilde{\Omega}_k \oplus \tilde{\Omega}_k$, $\Omega_l = \tilde{\Omega}_l \oplus \tilde{\Omega}_l$ with $\tilde{\Omega}_k, \tilde{\Omega}_l \in S_{2N-|B|}$ and $\tilde{\Omega}_k, \tilde{\Omega}_l \in S_{|B|}$ ($\tilde{\Omega}_k, \tilde{\Omega}_l$ will be products of some of the transpositions of Ω_k and Ω_l , and $\tilde{\Omega}_k, \tilde{\Omega}_l$ will be products of the remaining cycles). Note also that $\tilde{\Omega}_k, \tilde{\Omega}_l \in H_{N-|B|/2}$.

We can now see that finding a way for β to be in H_{2N} is equivalent to finding a $\tilde{\sigma} \in S_{|B|}$ that satisfies the following two conditions simultaneously.

- (a) For every $2p-1, 2p \in B$, there exist $2q-1, 2q \in B$ such that $\tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p-1)] = 2q-1$, $\tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p)] = 2q$ or $\tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p-1)] = 2q$, $\tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p)] = 2q-1$.
- (b) For every $2p-1, 2p \in B$, there exist $2q'-1, 2q' \in B$ such that $\tilde{\Omega}_l[\tilde{\sigma}(2p-1)] = 2q'-1$, $\tilde{\Omega}_l[\tilde{\sigma}(2p)] = 2q'$ or $\tilde{\Omega}_l[\tilde{\sigma}(2p-1)] = 2q'$, $\tilde{\Omega}_l[\tilde{\sigma}(2p)] = 2q'-1$.

These statements are equivalent to having $\tilde{\Omega}_k \tilde{\sigma}^{-1}, \tilde{\Omega}_l \tilde{\sigma} \in H_{|B|/2}$, which may also be written as $\tilde{\sigma}^{-1} \in \tilde{\Omega}_k^{-1} H_{|B|/2}$ and $\tilde{\sigma} \in \tilde{\Omega}_l^{-1} H_{|B|/2}$. However, Proposition 13 forbids the existence of $\tilde{\sigma}$. Indeed, $\tilde{\Omega}_k$ and $\tilde{\Omega}_l$ have different coset types, and thus, according to Proposition 13, the conditions $\tilde{\sigma}^{-1} \in \tilde{\Omega}_k^{-1} H_{|B|/2}$, $\tilde{\sigma} \in \tilde{\Omega}_l^{-1} H_{|B|/2}$ cannot hold simultaneously.

To confirm that $\tilde{\Omega}_k$ and $\tilde{\Omega}_l$ have different coset types, recall that B is defined in such a way that it contains all the elements in $\{1, \dots, 2N\}$ that correspond to cycles of length greater than 2 in both Ω_k and Ω_l . Suppose for a moment that $k_1 = l_1$. In order to have $k \neq l$, there must be at least one $a \neq 1$ such that $k_a \neq l_a$, which implies that the number of connected components of length $2a$ in $\Gamma(\tilde{\Omega}_k)$ will be different from that of $\Gamma(\tilde{\Omega}_l)$, and thus $\tilde{\Omega}_k$ and $\tilde{\Omega}_l$ will have different coset types. If $k_1 \neq l_1$, B will contain at least one pair of elements that will correspond to a transposition in Ω_k , but not in Ω_l (or vice versa). This implies that $\Gamma(\tilde{\Omega}_k)$ and $\Gamma(\tilde{\Omega}_l)$ will differ by at least one connected component of length 2, and so $\tilde{\Omega}_k$ and $\tilde{\Omega}_l$ will have different coset types.

The following proposition is a direct consequence of the fact that conditions $\tilde{\sigma}^{-1} \in \tilde{\Omega}_k^{-1} H_{|B|/2}$, $\tilde{\sigma} \in \tilde{\Omega}_l^{-1} H_{|B|/2}$ cannot hold at the same time.

Proposition 14. *Let $k \neq l$; then $|(\Omega_k^{-1} \oplus \Omega_l^{-1})H_{2N} \cap S_\sigma^*| = 0$ for every $\sigma \in S_{2N}$.*

Proof. We have seen that in order for $\tau_B \in S_\sigma^*$, with $B \subseteq \{1, \dots, 2N\}$, to also be an element of $(\Omega_k^{-1} \oplus \Omega_l^{-1})H_{2N}$, Eqs. (F25) and (F26), later transformed into Eqs. (F27) and (F28), must hold. This can only happen if B contains all the elements in $\{1, \dots, 2N\}$ that correspond to cycles of length greater than 2 in both Ω_k and Ω_l . This, in turn, makes σ take the form $\sigma = \tilde{\sigma} \oplus \tilde{\sigma}$, where $\tilde{\sigma} \in S_{2N-|B|}$ and $\tilde{\sigma} \in S_{|B|}$. Moreover, no matter the choice of B , $\tilde{\sigma}$ must satisfy the conditions $\tilde{\sigma}^{-1} \in \tilde{\Omega}_k^{-1} H_{|B|/2}$, $\tilde{\sigma} \in \tilde{\Omega}_l^{-1} H_{|B|/2}$ simultaneously. However, as proved in Proposition (13), this

cannot happen because Ω_k and Ω_l , and, consequently, $\tilde{\Omega}_k$ and $\tilde{\Omega}_l$, have different coset types when $k \neq l$. Therefore, there is no $\tilde{\sigma} \in S_{|B|}$, and thus no $\sigma \in S_{2N}$, for which $\tau_B \in S_\sigma^*$ and $\tau_B \in (\Omega_k^{-1} \oplus \Omega_l^{-1})H_{2N}$. It follows that $|(\Omega_k^{-1} \oplus \Omega_l^{-1})H_{2N} \cap S_\sigma^*| = 0$ for every $\sigma \in S_{2N}$. ■

We now focus on the case $k = l$. Let us set $B = \{2k_1 + 1, \dots, 2N\}$, so that the elements in B^c correspond to all the transpositions in Ω_k (recall that B^c is the complement of B). We discuss possible modifications of B later on.

According to relations (F27) and (F28), in order to have $\beta \in H_{2N}$, we need $\tilde{\Omega}_k \tilde{\sigma}, \tilde{\Omega}_k \tilde{\sigma}^{-1} \in H_{N-k_1}$. We will see how these relations determine the possible $\tilde{\sigma}$ that we can use. First, note that $\tilde{\Omega}_k^2 \in H_{N-k_1}$. Indeed, let the sequence $(2q+1, \dots, 2q+2a)$ correspond to a cycle of length $2a$ in $\tilde{\Omega}_k$. After one application of $\tilde{\Omega}_k$, $(2q+1, \dots, 2q+2a)$ maps to $(2q+1, \dots, 2q+2a) \mapsto (2q+2, 2q+3, \dots, 2q+2a-1, 2q+2a, 2q+1)$. After a second application of the permutation, we have $(2q+1, \dots, 2q+2a) \mapsto (2q+3, 2q+4, \dots, 2q+2a-1, 2q+2a, 2q+1, 2q+2)$, which brings pairs of the form $(2p-1, 2p)$, with $p \in \{1, \dots, a\}$, back together. Since this holds for an arbitrary a , we see that $\tilde{\Omega}_k^2$ satisfies the conditions to be in H_{N-k_1} . In view of this, we see that $\tilde{\Omega}_k^{-2} \in H_{N-k_1}$, and thus $\tilde{\Omega}_k^{-2} \tilde{\Omega}_k \tilde{\sigma} = \tilde{\Omega}_k^{-1} \tilde{\sigma}^{-1} \in H_{N-k_1}$. Consequently, the conditions that $\tilde{\sigma}$ must satisfy can be written as $\tilde{\Omega}_k \tilde{\sigma}, \tilde{\sigma} \tilde{\Omega}_k \in H_{N-k_1}$.

Another interesting property of $\tilde{\Omega}_k$ is that every pair of the form $(2p-1, 2p)$, with $p \in \{k_1+1, \dots, N\}$, belongs to the same cycle in $\tilde{\Omega}_k$. This is because all the elements within the cycles of $\tilde{\Omega}_k$ are consecutive and, moreover, all of the cycles have even length. We use this fact to find the structure of $\tilde{\sigma}$.

Consider again the sequence $(2q+1, \dots, 2q+2a)$, corresponding to a cycle of length $2a$ in $\tilde{\Omega}_k$. Every element in this sequence can be written as $2q+2l-1$ or $2q+2l$ with $l \in \{1, \dots, a\}$. Therefore, every pair of the form $(2p-1, 2p)$ with elements in this sequence can be written as $(2q+2l-1, 2q+2l)$. This holds for every cycle in $\tilde{\Omega}_k$.

If $\tilde{\Omega}_k \tilde{\sigma} \in H_{N-k_1}$ then, for all $l \in \{1, \dots, a\}$, $\tilde{\Omega}_k[\tilde{\sigma}(2q+2l-1)] = 2q'+2l'-1$ and $\tilde{\Omega}_k[\tilde{\sigma}(2q+2l)] = 2q'+2l'$, or $\tilde{\Omega}_k[\tilde{\sigma}(2q+2l-1)] = 2q'+2l'$ and $\tilde{\Omega}_k[\tilde{\sigma}(2q+2l)] = 2q'+2l'-1$, with $2q'+1$ being the first element in another cycle of length $2a'$ in $\tilde{\Omega}_k$. Here $l' \in \{1, \dots, a'\}$. We can use these relations to find the action of $\tilde{\sigma}$ over the elements in $(2q+1, \dots, 2q+2a)$. We analyze these two possible conditions separately, and during this procedure we keep in mind that $\tilde{\sigma} \tilde{\Omega}_k \in H_{N-k_1}$ also holds.

Case 1: $\tilde{\Omega}_k[\tilde{\sigma}(2q+2l-1)] = 2q'+2l'-1$ and $\tilde{\Omega}_k[\tilde{\sigma}(2q+2l)] = 2q'+2l'$. The first of these relations implies that $\tilde{\sigma}(2q+2l-1) = \Omega_k^{-1}(2q'+2l'-1)$. Consequently, if $l' \neq 1$, $\tilde{\sigma}(2q+2l-1) = 2q'+2l'-2$. If $l' =$

1, $\tilde{\sigma}(2q + 2l - 1) = 2q' + 2a'$. The second of these relations implies that $\tilde{\sigma}(2q + 2l) = \Omega_k^{-1}(2q' + 2l') = 2q' + 2l' - 1$.

Moreover, we have $\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l - 1)] = \tilde{\sigma}(2q + 2l) = 2q' + 2l' - 1$, which, given that $\tilde{\sigma}\tilde{\Omega}_k \in H_{N-k_1}$, implies that

$$\begin{array}{c|c|c|c|c|c} p: & \cdots & 2q + 2l - 1 & 2q + 2l & 2q + 2l + 1 & \cdots \\ \hline \tilde{\sigma}(p): & \cdots & 2q' + 2l' - 2 & 2q' + 2l' - 1 & 2q' + 2l' & \cdots \end{array}. \quad (\text{F29})$$

The first and last elements of the cycles can be included in this structure by taking the addition and subtraction modulo a or a' .

Case 2: $\tilde{\Omega}_k[\tilde{\sigma}(2q + 2l - 1)] = 2q' + 2l'$ and $\tilde{\Omega}_k[\tilde{\sigma}(2q + 2l)] = 2q' + 2l' - 1$. The first relation implies that $\tilde{\sigma}(2q + 2l - 1) = \Omega_k^{-1}(2q' + 2l') = 2q' + 2l' - 1$. The second relation implies that $\tilde{\sigma}(2q + 2l) = \Omega_k^{-1}(2q' + 2l' - 1)$. If $l' = 1$, $\tilde{\sigma}(2q + 2l) = \Omega_k^{-1}(2q' + 1) = 2q' + 2a'$; otherwise, $\tilde{\sigma}(2q + 2l) = \Omega_k^{-1}(2q' + 2l' - 1) = 2q' + 2l' - 2$.

Moreover, we have $\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l - 1)] = \tilde{\sigma}(2q + 2l)$. Thus, considering that $\tilde{\sigma}\tilde{\Omega}_k \in H_{N-k_1}$, $\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l)] = 2q' + 2a' - 1$ for $l' = 1$, and $\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l)] = 2q' +$

$\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l)] = 2q' + 2l'$. If $l \neq a$, $\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l)] = \tilde{\sigma}(2q + 2l + 1) = 2q' + 2l'$. If $l = a$, $\tilde{\sigma}[\tilde{\Omega}_k(2q + 2l)] = \tilde{\sigma}(2q + 1) = 2q' + 2l'$. Therefore, $\tilde{\sigma}$ must have the structure

$2l' - 3$ for $l' \neq 1$. These relations lead to four results:

$$\sigma(2q + 2l + 1) = 2q' + 2l' - 3 \quad \text{for } l' \neq 1, l \neq a, \quad (\text{F30})$$

$$\sigma(2q + 1) = 2q' + 2l' - 3 \quad \text{for } l' \neq 1, l = a, \quad (\text{F31})$$

$$\sigma(2q + 2l + 1) = 2q' + 2a' - 1 \quad \text{for } l' = 1, l \neq a, \quad (\text{F32})$$

$$\sigma(2q + 1) = 2q' + 2a' - 1 \quad \text{for } l' = 1, l = a. \quad (\text{F33})$$

Gathering all these results, we find that $\tilde{\sigma}$ must have the structure

$$\begin{array}{c|c|c|c|c|c} p: & \cdots & 2q + 2l - 1 & 2q + 2l & 2q + 2l + 1 & \cdots \\ \hline \tilde{\sigma}(p): & \cdots & 2q' + 2l' - 1 & 2q' + 2l' - 2 & 2q' + 2l' - 3 & \cdots \end{array}, \quad (\text{F34})$$

where the first and last elements of the cycles can be included by taking the addition and subtraction modulo a or a' .

As we can see, the results of case 1 show that the image of $(2q + 1, \dots, 2q + 2a)$ under $\tilde{\sigma}$ corresponds to shifting the elements in $(2q' + 1, \dots, 2q' + 2a')$ while maintaining their ascending order. The results of case 2 show that we are also allowed to make shifts using a descending order of the elements within the cycles. The value of l' determines by how much $\tilde{\sigma}$ shifts the elements in $(2q' + 1, \dots, 2q' + 2a')$, while the value of q' determines which cycle corresponds to the image of $(2q + 1, \dots, 2q + 2a)$.

It is apparent that we need to have $a = a'$, so that every element in the sequence $(2q + 1, \dots, 2q + 2a)$ has an image in $(2q' + 1, \dots, 2q' + 2a')$. We can show that this is in fact a consequence of the relations $\tilde{\sigma}\tilde{\Omega}_k, \tilde{\sigma}^{-1}\tilde{\Omega}_k \in H_{N-k_1}$ (the second of these is obtained by noting that $\tilde{\Omega}_k\tilde{\sigma} \in H_{N-k_1}$ implies that $\tilde{\sigma}^{-1}\tilde{\Omega}_k^{-1} \in H_{N-k_1}$, which leads to $\tilde{\sigma}^{-1}\tilde{\Omega}_k^{-1}\tilde{\Omega}_k^2 = \tilde{\sigma}^{-1}\tilde{\Omega}_k \in H_{N-k_1}$).

Suppose that $a > a'$; then there must be some $l^* \in \{1, \dots, a\}$ such that $\tilde{\sigma}(2q + 2l^* - 1), \tilde{\sigma}(2q + 2l^*) \notin \{2q' + 1, \dots, 2q' + 2a'\}$, but $\tilde{\sigma}(2q + 2l^* - 3), \tilde{\sigma}(2q + 2l^* - 2) \in \{2q' + 1, \dots, 2q' + 2a'\}$. Let $\tilde{\sigma}(2q + 2l^* - 1) = r$, $\tilde{\sigma}(2q + 2l^*) = r'$. After applying $\tilde{\Omega}_k$ and $\tilde{\sigma}$ over $(2q + 1, \dots, 2q + 2a)$, we have

$$\begin{array}{c|c|c|c|c|c|c} p: & \cdots & 2q + 2l^* - 3 & 2q + 2l^* - 2 & 2q + 2l^* - 1 & 2q + 2l^* & \cdots \\ \hline \tilde{\Omega}_k(p): & \cdots & 2q + 2l^* - 2 & 2q + 2l^* - 1 & 2q + 2l^* & 2q + 2l^* + 1 & \cdots \\ \hline \tilde{\sigma}[\tilde{\Omega}_k(p)]: & \cdots & 2q' + 2l' + j & r & r' & \cdots & \cdots \end{array}$$

where $j \in \{1, \dots, a'\}$. We see that the image of the pair $(2q + 2l^* - 3, 2q + 2l^* - 2)$ is $(2q' + 2l' + j, r)$ under $\tilde{\sigma}\tilde{\Omega}_k$, and this breaks the condition $\tilde{\sigma}\tilde{\Omega}_k \in H_{N-k_1}$ because the companion of $2q' + 2l' + j$ should be an element of $\{2q' + 1, \dots, 2q' + 2a'\}$, but r is not. Consequently, we must have $a \leq a'$.

$p:$	$\dots$	$2q' + 2m^* - 3$	$2q' + 2m^* - 2$	$2q' + 2m^* - 1$	$2q' + 2m^*$	$\dots$
$\tilde{\Omega}_k(p):$	$\dots$	$2q' + 2m^* - 2$	$2q' + 2m^* - 1$	$2q' + 2m^*$	$2q' + 2m^* + 1$	$\dots$
$\sigma^{-1}[\tilde{\Omega}_k(p)]:$	$\dots$	$2q + 2l + j$	s	s'	$\dots$	$\dots$

where $j \in \{1, \dots, a\}$. Just as before, we see that the image under $\tilde{\sigma}^{-1}\tilde{\Omega}_k$ of the pair $(2q' + 2m^* - 3, 2q' + 2m^* - 2)$ is $(2q + 2l + j, s)$, which breaks the condition $\tilde{\sigma}^{-1}\tilde{\Omega}_k \in H_{N-k_1}$ because $2q + 2l + j$ should be paired with an element of $\{2q + 1, \dots, 2q + 2a\}$, not with $s \notin \{2q + 1, \dots, 2q + 2a\}$. We therefore conclude that $a = a'$, i.e., the image under $\tilde{\sigma}$ of any cycle of length $2a$ in $\tilde{\Omega}_k$ must correspond to another cycle of length $2a$ in $\tilde{\Omega}_k$.

Having found the structure of $\tilde{\sigma}$, we can easily count how many of them there are.

Proposition 15. *There are $\prod_{a=2}^N (2a)^{k_a} k_a!$ possible $\tilde{\sigma}$.*

Proof. As we just showed, the image under $\tilde{\sigma}$ of the elements within a cycle of length $2a$ in $\tilde{\Omega}_k$ corresponds to a shift of the elements within another cycle of length $2a$ in $\tilde{\Omega}_k$. For all of these cycles, there are a possible values of the shift [because there are a possible values of l' in Eqs. (F29) and (F34)]. Additionally, we can make each shift with the elements within the cycles having either an ascending or descending order [as also shown in Eqs. (F29) and (F34)]. Since there are k_a cycles of length $2a$ in $\tilde{\Omega}_k$, we have a total of $(2a)^{k_a}$ ways of choosing the shift and order of all of them. Moreover, as mentioned below Eq. (F34), q' determines the image of a given cycle. The number of possible q' is equal to the number of cycles of length $2a$, namely k_a , which means that there are $k_a!$ ways of choosing the images of all these cycles. This implies that there are a total of $(2a)^{k_a} k_a!$ ways of choosing the image under $\tilde{\sigma}$ of all the cycles of length $2a$ in $\tilde{\Omega}_k$. Since a is arbitrary, and we are only considering cycles of length greater than 2, we conclude that there are $\prod_{a=2}^N (2a)^{k_a} k_a!$ possible ways of choosing the image of $\tilde{\sigma}$. ■

Having found the number of possible $\tilde{\sigma}$ and their structure, we can focus on $\tilde{\sigma}$. This will also allow us to discuss possible modifications to B . As shown in Eqs. (F27) and (F28), once we choose $\tilde{\sigma}$ for $B = \{2k_1 + 1, \dots, 2N\}$, we have complete freedom in the choice of $\tilde{\sigma} \in S_{2k_1}$. This is because $\tilde{\sigma}$ plays no role in the computation of β . Indeed,

Suppose now that $a < a'$; then there must exist $m^* \in \{1, \dots, a'\}$ such that $\tilde{\sigma}^{-1}(2q' + 2m^* - 1), \tilde{\sigma}^{-1}(2q' + 2m^*) \notin \{2q + 1, \dots, 2q + 2a\}$, but $\tilde{\sigma}^{-1}(2q' + 2m^* - 3), \tilde{\sigma}^{-1}(2q' + 2m^* - 2) \in \{2q + 1, \dots, 2q + 2a\}$. Let $\tilde{\sigma}^{-1}(2q' + 2m^* - 1) = s, \tilde{\sigma}^{-1}(2q' + 2m^*) = s'$. After applying $\tilde{\Omega}_k$ and $\tilde{\sigma}^{-1}$ to $(2q' + 1, \dots, 2q' + 2a')$, we obtain

we needed $\tilde{\sigma}$ to “break” all the connected components of length greater than 2 in $\Gamma(\Omega_k)$, while we “hid” the action of $\tilde{\sigma}$ with our choice of B . We can now fix $\tilde{\sigma}$, so that $\sigma = \tilde{\sigma} \oplus \tilde{\sigma}$ keeps breaking the connected components of interest, and see if we can “reveal” some of the structure of $\tilde{\sigma}$ while keeping $\beta \in H_{2N}$.

If we extend B to include a pair of points $(2p - 1, 2p)$, with $p \in \{1, \dots, k_1\}$, computing β amounts to calculating $\tilde{\Omega}_k[\tilde{\sigma}(2p - 1)], \tilde{\Omega}_k[\tilde{\sigma}(2p)],$ and $\tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p - 1)], \tilde{\Omega}_k[\tilde{\sigma}^{-1}(2p)]$. Since $\tilde{\Omega}_k$ consists only of transpositions, in order to have $\beta \in H_{2N}$, we need the image of $(2p - 1, 2p)$ under $\tilde{\sigma}$ to be of the form $(2q - 1, 2q)$ or $(2q, 2q - 1)$, with $q \in \{1, \dots, k_1\}$. Similarly, the image of $(2p - 1, 2p)$ under $\tilde{\sigma}^{-1}$ must be of the form $(2q' - 1, 2q')$ or $(2q', 2q' - 1)$, with $q' \in \{1, \dots, k_1\}$. This means that we can extend B to include $(2p - 1, 2p)$ as long as this pair of points leads to a connected component of length 2 in $\Gamma(\tilde{\sigma})$. Note that extending B to include $(2p - 1, 2p)$ may imply that $\sigma(B) \neq B, \sigma^{-1}(B) \neq B$. However, since the pair $(2p - 1, 2p)$ leads to a connected component of length 2 in $\Gamma(\tilde{\sigma})$, we can guarantee that it will also lead to connected components of length 2 in $\Gamma(\tilde{\Omega}_k\tilde{\sigma}), \Gamma(\tilde{\Omega}_k\tilde{\sigma}^{-1})$, and thus $\Gamma(\Omega_k\sigma), \Gamma(\Omega_k\sigma^{-1})$, making β satisfy the conditions to be an element of H_{2N} . Consequently, given a specific $\tilde{\sigma}$, any modification of B will consist in appending pairs of the form $\{(2p - 1, 2p)\}$ that correspond to connected components of length 2 in $\Gamma(\tilde{\sigma})$. Note that the choice of including a given pair is independent of the choice of including any other pair.

The exact number of possible modifications of B , for given $\tilde{\sigma}$ and $\tilde{\sigma}$, will depend on the number of connected components of length 2 in $\Gamma(\tilde{\sigma})$. Let $\eta(\tilde{\sigma})$ be the coset type of $\tilde{\sigma}$, and let $\eta^{(1)}(\tilde{\sigma})$ be the number of 1s in $\eta(\tilde{\sigma})$, which is equivalent to the number of connected components of length 2 in $\Gamma(\tilde{\sigma})$. Each of these connected components will correspond to a pair $(2p - 1, 2p)$ with $p \in \{1, \dots, k_1\}$. For each pair, we can decide whether to include it in B or not. This means that we can modify B in $2^{\eta^{(1)}(\tilde{\sigma})}$ ways. This result allows us to state the following propositions.

Proposition 16. *We have $|(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{k}}^{-1})H_{2N} \cap S_{\sigma}^*| = 2^{\eta^{(1)}(\bar{\sigma})}$ if $\sigma = \bar{\sigma} \oplus \tilde{\sigma}$; otherwise, it vanishes. Here, $\bar{\sigma} \in S_{2k_1}$ acts over $\{1, \dots, 2k_1\}$, and $\eta^{(1)}(\bar{\sigma})$ is the number of 1s in the coset type of $\bar{\sigma}$. Permutation $\tilde{\sigma} \in S_{2N-2k_1}$ acts over $\{2k_1 + 1, \dots, 2N\}$ and has the form indicated by Eq. (F29) or (F34).*

Proof. We have seen that in order for $\tau_B \in S_{\sigma}^*$, with $B \subseteq \{1, \dots, 2N\}$, to also be an element of $(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{k}}^{-1})H_{2N}$, Eqs. (F25) and (F26), later transformed into Eqs. (F27) and (F28), must hold. By setting $B = \{2k_1 + 1, \dots, 2N\}$, we found that these equations are satisfied if $\sigma = \bar{\sigma} \oplus \tilde{\sigma}$, with $\bar{\sigma}$ acting over B^c and $\tilde{\sigma}$ over B . Moreover, $\tilde{\sigma}$ must be defined by Eq. (F29) or (F34). Fixing $\tilde{\sigma}$, we can modify B in order to include any number of pairs of the form $(2p - 1, 2p) \in \{1, \dots, 2N\}$ that correspond to connected components of length 2 in $\Gamma(\bar{\sigma})$. The total number of this type of connected components is equal to $\eta^{(1)}(\bar{\sigma})$, the number of 1s in the coset type of $\bar{\sigma}$. For each pair, we can choose whether to include it in B or not, which leads to a total of $2^{\eta^{(1)}(\bar{\sigma})}$ possible modifications to B . Therefore, there are $2^{\eta^{(1)}(\bar{\sigma})}$ possible τ_B for a given $\sigma = \bar{\sigma} \oplus \tilde{\sigma}$. ■

Proposition 17. *It holds that*

$$\sum_{\sigma \in S_{2N}} |(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{k}}^{-1})H_{2N} \cap S_{\sigma}^*| = \prod_{a=2}^N (2a)^{k_a} k_a! \sum_{\bar{\sigma} \in S_{2k_1}} 2^{\eta^{(1)}(\bar{\sigma})}. \quad (\text{F35})$$

Proof. The sum over all $\sigma \in S_{2N}$ reduces to a sum over permutations of the form $\sigma = \bar{\sigma} \oplus \tilde{\sigma}$ because the summand vanishes otherwise. For a given $\bar{\sigma}$, there are always $\prod_{a=2}^N (2a)^{k_a} k_a!$ possible $\tilde{\sigma}$, so we only need to sum over $\bar{\sigma}$. ■

Now that we have computed $|(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})H_{2N} \cap S_{\sigma}^*|$ as a function of $\mathbf{k}$, $\mathbf{l}$, and σ , we are almost ready to attack Eq. (F1). Combining all the results we have obtained so far, we can see that

$$\begin{aligned} & \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ & \times \sum_{\sigma \in S_{2N}} b_{2N}[\mathbf{j} \oplus \sigma(\mathbf{j}), \Omega_{\mathbf{k}}(\mathbf{j}) \oplus \Omega_{\mathbf{l}} \circ \sigma(\mathbf{j})] \\ & = \sum_{\mathbf{k}^{(c)}, \mathbf{l}^{(c)}} \prod_{a=1}^N \frac{1}{k_a! l_a! (2a)^{k_a+l_a}} \\ & \times \sum_{\sigma \in S_{2N}} |(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{l}}^{-1})H_{2N} \cap S_{\sigma}^*| \end{aligned}$$

$$\begin{aligned} & = \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right)^2 \\ & \times \sum_{\sigma \in S_{2N}} |(\Omega_{\mathbf{k}}^{-1} \oplus \Omega_{\mathbf{k}}^{-1})H_{2N} \cap S_{\sigma}^*| \\ & = \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right)^2 \prod_{a=2}^N k_a! (2a)^{k_a} \sum_{\bar{\sigma} \in S_{2k_1}} 2^{\eta^{(1)}(\bar{\sigma})} \\ & = \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=2}^N \frac{1}{k_a! (2a)^{k_a}} \right) \left(\frac{1}{2^{k_1} k_1!} \right)^2 \sum_{\bar{\sigma} \in S_{2k_1}} 2^{\eta^{(1)}(\bar{\sigma})}. \end{aligned} \quad (\text{F36})$$

In order to complete our proof, we need two additional results.

Proposition 18. *Let S_{2n} be the symmetric group of degree $2n$, and let $\eta^{(1)}(\sigma)$ stand for the number of 1s in the coset type of $\sigma \in S_{2n}$. Moreover, let α be a real parameter satisfying $|\alpha| < 1$. Then,*

$$\sum_{\sigma \in S_{2n}} 2^{\eta^{(1)}(\sigma)} = 2^{2n} n! \frac{d^n}{d\alpha^n} [e^{\alpha/2} (1 - \alpha)^{-1/2}] \Big|_{\alpha=0}. \quad (\text{F37})$$

Proof. Let H_{η} denote the set of permutations $\sigma \in S_{2n}$ that have coset type η . Since every σ has a unique coset type, it will belong to only one H_{η} . This allows us to write the sum over $\sigma \in S_{2n}$ in Eq. (F37) as

$$\sum_{\sigma \in S_{2n}} 2^{\eta^{(1)}(\sigma)} = \sum_{\eta \vdash n} |H_{\eta}| 2^{\eta^{(1)}}, \quad (\text{F38})$$

where $\eta \vdash n$ indicates that the sum is taken over all the integer partitions of n (recall that the coset type of a permutation in S_{2n} is an integer partition of n) and $\eta^{(1)}$ is the number of 1s in η .

Given a partition η of n , we can construct a vector of non-negative integers $\mathbf{k} = (k_1, \dots, k_n)$ whose components satisfy $k_1 + 2k_2 + \dots + nk_n = n$. Indeed, we need only define k_a as the multiplicity of a in η , i.e., k_a is the number of times a appears in η . This implies that

$$\sum_{\sigma \in S_{2n}} 2^{\eta^{(1)}(\sigma)} = \sum_{\eta \vdash n} |H_{\eta}| 2^{\eta^{(1)}} = \sum_{\mathbf{k}^{(c)}} |H_{\mathbf{k}}| 2^{k_1}, \quad (\text{F39})$$

where $\eta^{(1)} = k_1$ has been used, and we write $\mathbf{k}^{(c)}$ to indicate that the components of $\mathbf{k}$ are constrained.

According to Refs. [35,49], we have

$$|H_\eta| = |H_{\mathbf{k}}| = (2^n n!)^2 \prod_{a=1}^n \frac{1}{k_a! (2a)^{k_a}}, \quad (\text{F40})$$

which leads to the expression

$$\begin{aligned} \sum_{\sigma \in S_{2n}} 2^{\eta^{(1)}(\sigma)} &= (2^n n!)^2 \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^n \frac{1}{k_a! (2a)^{k_a}} \right)^{2^{k_1}} \\ &= (2^n n!) Z_n \left(1, \frac{1}{2}, \dots, \frac{1}{2} \right), \end{aligned} \quad (\text{F41})$$

where we recalled the definition of the cycle index of S_n [Eq. (32) in the main text]:

$$Z_n(y_1, \dots, y_n) = \sum_{\mathbf{k}^{(c)}} \prod_{a=1}^n \frac{1}{k_a! a^{k_a}} \prod_{a=1}^n y_a^{k_a}. \quad (\text{F42})$$

Using the generating function of $Z_n(y_1, \dots, y_n)$,

$$\exp \left[\sum_{l=1}^{\infty} y_l \frac{\alpha^l}{l} \right] = \sum_{n=0}^{\infty} Z_n(y_1, \dots, y_n) \alpha^n, \quad (\text{F43})$$

we can write

$$\begin{aligned} \exp \left[\alpha + \frac{1}{2} \sum_{l=2}^{\infty} \frac{\alpha^l}{l} \right] &= e^{\alpha/2} \exp \left[\frac{1}{2} \sum_{l=1}^{\infty} \frac{\alpha^l}{l} \right] \\ &= \sum_{n=0}^{\infty} Z_n \left(1, \frac{1}{2}, \dots, \frac{1}{2} \right) \alpha^n. \end{aligned} \quad (\text{F44})$$

Assuming that $|\alpha| < 1$, we can write $\sum_{l=1}^{\infty} \alpha^l/l = -\log(1 - \alpha)$, and obtain

$$\begin{aligned} e^{\alpha/2} \exp \left[-\frac{1}{2} \log(1 - \alpha) \right] &= e^{\alpha/2} (1 - \alpha)^{-1/2} \\ &= \sum_{n=0}^{\infty} Z_n \left(1, \frac{1}{2}, \dots, \frac{1}{2} \right) \alpha^n. \end{aligned} \quad (\text{F45})$$

Equation (F37) follows from repeatedly differentiating this expression with respect to α , and then evaluating at $\alpha = 0$. ■

Proposition 19. Let x be a real parameter. Then,

$$\sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^n \frac{1}{k_a! (2a)^{k_a}} \right)^{2^{k_1} x^{k_1}} = \frac{1}{n!} \sum_{m=0}^n \binom{n}{m} x^m g_{n-m}, \quad (\text{F46})$$

where g_m is defined by the relation

$$\begin{aligned} e^{-\beta/2} (1 - \beta)^{-1/2} &= \sum_{m=0}^{\infty} \frac{g_m}{m!} \beta^m, \\ g_m &= (-1/2)^m {}_2F_0(1/2, -m; ; 2), \end{aligned} \quad (\text{F47})$$

with $|\beta| < 1$ and ${}_2F_0(a, b; ; z)$ the hypergeometric function ${}_2F_0$.

Proof. We can readily note that

$$\sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^n \frac{1}{k_a! (2a)^{k_a}} \right)^{2^{k_1} x^{k_1}} = Z_n \left(x, \frac{1}{2}, \dots, \frac{1}{2} \right), \quad (\text{F48})$$

and thus we can use the generating function of Z_n to find an new expression for the left-hand side of Eq. (F46). We have

$$\begin{aligned} \exp \left[x\beta + \frac{1}{2} \sum_{l=2}^{\infty} \frac{\beta^l}{l} \right] &= e^{x\beta} e^{-\beta/2} \exp \left[\frac{1}{2} \sum_{l=1}^{\infty} \frac{\beta^l}{l} \right] \\ &= \sum_{n=0}^{\infty} Z_n \left(x, \frac{1}{2}, \dots, \frac{1}{2} \right) \beta^n. \end{aligned} \quad (\text{F49})$$

Using the equality $\sum_{l=1}^{\infty} \beta^l/l = -\log(1 - \beta)$ for $|\beta| < 1$, we can recast this expression as

$$e^{x\beta} e^{-\beta/2} (1 - \beta)^{-1/2} = \sum_{n=0}^{\infty} Z_n \left(x, \frac{1}{2}, \dots, \frac{1}{2} \right) \beta^n. \quad (\text{F50})$$

Consequently,

$$\begin{aligned} \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^n \frac{1}{k_a! (2a)^{k_a}} \right)^{2^{k_1} x^{k_1}} &= Z_n \left(x, \frac{1}{2}, \dots, \frac{1}{2} \right) \\ &= \frac{1}{n!} \frac{d^n}{d\beta^n} [e^{x\beta} e^{-\beta/2} (1 - \beta)^{-1/2}] \Big|_{\beta=0}. \end{aligned} \quad (\text{F51})$$

Now, let us expand $e^{x\beta}$ and $e^{-\beta/2} (1 - \beta)^{-1/2}$ as

$$e^{x\beta} = \sum_{m=0}^{\infty} \frac{x^m}{m!} \beta^m, \quad e^{-\beta/2} (1 - \beta)^{-1/2} = \sum_{m=0}^{\infty} \frac{g_m}{m!} \beta^m. \quad (\text{F52})$$

These expressions allow us to write

$$\begin{aligned} e^{x\beta} e^{-\beta/2} (1-\beta)^{-1/2} &= \left(\sum_{m=0}^{\infty} \frac{x^m}{m!} \beta^m \right) \left(\sum_{p=0}^{\infty} \frac{g_p}{p!} \beta^p \right) \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \left[\sum_{m=0}^n \binom{n}{m} x^m g_{n-m} \right] \beta^n, \end{aligned} \quad (\text{F53})$$

where we used the Leibniz formula for the product of two series [33,38] to obtain the last equality. Repeated differentiation with respect to β , and evaluation at $\beta = 0$, leads to Eq. (F46). ■

Using Proposition 18, we can recast the last line in Eq. (F36) as

$$\begin{aligned} \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=2}^N \frac{1}{k_a! (2a)^{k_a}} \right) \left(\frac{1}{2^{k_1} k_1!} \right)^2 \sum_{\bar{\sigma} \in S_{2k_1}} 2^{\eta^{(1)}(\bar{\sigma})} \\ = \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right) 2^{k_1} \frac{d^{k_1}}{d\alpha^{k_1}} [e^{\alpha/2} (1-\alpha)^{-1/2}] \Big|_{\alpha=0}. \end{aligned} \quad (\text{F54})$$

This expression leads to the following result.

Proposition 20. *It holds that*

$$\sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right) 2^{k_1} \frac{d^{k_1}}{d\alpha^{k_1}} [e^{\alpha/2} (1-\alpha)^{-1/2}] \Big|_{\alpha=0} = 1. \quad (\text{F55})$$

Proof. Let us define the differential operator

$$\mathcal{D}_\alpha = \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right) 2^{k_1} \frac{d^{k_1}}{d\alpha^{k_1}}, \quad (\text{F56})$$

which allows us to write

$$\begin{aligned} \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right) 2^{k_1} \frac{d^{k_1}}{d\alpha^{k_1}} [e^{\alpha/2} (1-\alpha)^{-1/2}] \Big|_{\alpha=0} \\ = \mathcal{D}_\alpha [e^{\alpha/2} (1-\alpha)^{-1/2}] \Big|_{\alpha=0}. \end{aligned} \quad (\text{F57})$$

Using Proposition 19, we can reorganize the sum that defines $\mathcal{D}_\alpha$ to obtain

$$\begin{aligned} \mathcal{D}_\alpha &= \sum_{\mathbf{k}^{(c)}} \left(\prod_{a=1}^N \frac{1}{k_a! (2a)^{k_a}} \right) 2^{k_1} \frac{d^{k_1}}{d\alpha^{k_1}} \\ &= \frac{1}{N!} \sum_{m=0}^N \binom{N}{m} g_{N-m} \frac{d^m}{d\alpha^m}. \end{aligned} \quad (\text{F58})$$

Expanding $e^{\alpha/2} (1-\alpha)^{-1/2}$ as

$$\begin{aligned} e^{\alpha/2} (1-\alpha)^{-1/2} &= \sum_{p=0}^{\infty} \frac{a_p}{p!} \alpha^p, \\ a_p &= \frac{(2p-1)!!}{2^p} {}_1F_1 \left(-p; \frac{1}{2} - p; \frac{1}{2} \right), \end{aligned} \quad (\text{F59})$$

where ${}_1F_1(a; b; c)$ denotes the confluent hypergeometric function of the first kind, we have

$$\begin{aligned} \mathcal{D}_\alpha [e^{\alpha/2} (1-\alpha)^{-1/2}] \Big|_{\alpha=0} &= \frac{1}{N!} \sum_{m=0}^N \binom{N}{m} g_{N-m} \frac{d^m}{d\alpha^m} \left(\sum_{p=0}^{\infty} \frac{a_p}{p!} \alpha^p \right) \Big|_{\alpha=0} \\ &= \frac{1}{N!} \sum_{m=0}^N \binom{N}{m} a_m g_{N-m}. \end{aligned} \quad (\text{F60})$$

Now, note that

$$\begin{aligned} [e^{\alpha/2} (1-\alpha)^{-1/2}] [e^{-\alpha/2} (1-\alpha)^{-1/2}] &= \left(\sum_{p=0}^{\infty} \frac{a_p}{p!} \alpha^p \right) \left(\sum_{m=0}^{\infty} \frac{g_m}{m!} \alpha^m \right) \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \left[\sum_{m=0}^n \binom{n}{m} a_m g_{n-m} \right] \alpha^n \\ &= (1-\alpha)^{-1}, \end{aligned} \quad (\text{F61})$$

which, combined with the fact that $(1-\alpha)^{-1} = \sum_{n=0}^{\infty} \alpha^n$ for $|\alpha| < 1$, allows us to conclude that

$$\mathcal{D}_\alpha [e^{\alpha/2} (1-\alpha)^{-1/2}] \Big|_{\alpha=0} = \frac{1}{N!} \sum_{m=0}^N \binom{N}{m} a_m g_{N-m} = 1 \quad (\text{F62})$$

for all N . ■

This concludes our proof of Eq. (F1).

-
- [1] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Gaussian boson sampling, *Phys. Rev. Lett.* **119**, 170501 (2017).
 - [2] R. Kruse, C. S. Hamilton, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Detailed study of Gaussian boson sampling, *Phys. Rev. A* **100**, 032326 (2019).
 - [3] D. Hangleiter and J. Eisert, Computational advantage of quantum random sampling, *Rev. Mod. Phys.* **95**, 035001 (2023).

- [4] N. Quesada, J. M. Arrazola, and N. Killoran, Gaussian boson sampling using threshold detectors, *Phys. Rev. A* **98**, 062322 (2018).
- [5] D. Grier, D. J. Brod, J. M. Arrazola, M. B. de Andrade Alonso, and N. Quesada, The complexity of bipartite Gaussian boson sampling, *Quantum* **6**, 863 (2022).
- [6] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, NY, USA, 2011), p. 333.
- [7] 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, *et al.*, Quantum computational advantage using photons, *Science* **370**, 1460 (2020).
- [8] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, *et al.*, Phase-programmable Gaussian boson sampling using stimulated squeezed light, *Phys. Rev. Lett.* **127**, 180502 (2021).
- [9] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, *et al.*, Quantum computational advantage with a programmable photonic processor, *Nature* **606**, 75 (2022).
- [10] Y.-H. Deng, Y.-C. Gu, H.-L. Liu, S.-Q. Gong, H. Su, Z.-J. Zhang, H.-Y. Tang, M.-H. Jia, J.-M. Xu, M.-C. Chen, *et al.*, Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage, *Phys. Rev. Lett.* **131**, 150601 (2023).
- [11] D. Hangleiter, M. Kliesch, J. Eisert, and C. Gogolin, Sample complexity of device-independently certified “quantum supremacy”, *Phys. Rev. Lett.* **122**, 210502 (2019).
- [12] M. Bentivegna, N. Spagnolo, C. Vitelli, D. J. Brod, A. Crespi, F. Flamini, R. Ramponi, P. Mataloni, R. Osellame, E. F. Galvão, *et al.*, Bayesian approach to boson sampling validation, *Int. J. Quantum Inf.* **12**, 1560028 (2015).
- [13] D. Phillips, M. Walschaers, J. Renema, I. Walmsley, N. Treps, and J. Sperling, Benchmarking of Gaussian boson sampling using two-point correlators, *Phys. Rev. A* **99**, 023836 (2019).
- [14] Y. Cardin and N. Quesada, Photon-number moments and cumulants of Gaussian states, *ArXiv:2212.06067*.
- [15] P. D. Drummond, B. Opanchuk, A. Dellios, and M. D. Reid, Simulating complex networks in phase space: Gaussian boson sampling, *Phys. Rev. A* **105**, 012427 (2022).
- [16] G. Bressanini, B. Seron, L. Novo, N. J. Cerf, and M. Kim, Gaussian boson sampling validation via detector binning, *ArXiv:2310.18113*.
- [17] J. Martínez-Cifuentes, K. Fonseca-Romero, and N. Quesada, Classical models may be a better explanation of the Jiuzhang 1.0 Gaussian boson sampler than its targeted squeezed light model, *Quantum* **7**, 1076 (2023).
- [18] B. Villalonga, M. Y. Niu, L. Li, H. Neven, J. C. Platt, V. N. Smelyanskiy, and S. Boixo, Efficient approximation of experimental Gaussian boson sampling, *ArXiv:2109.11525*.
- [19] C. Oh, L. Jiang, and B. Fefferman, Spoofing cross-entropy measure in boson sampling, *Phys. Rev. Lett.* **131**, 010401 (2023).
- [20] C. Oh, M. Liu, Y. Alexeev, B. Fefferman, and L. Jiang, Classical algorithm for simulating experimental Gaussian boson sampling, *Nat. Phys.* **20**, 1461 (2024).
- [21] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [22] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nat. Phys.* **14**, 595 (2018).
- [23] X. Gao, M. Kalinowski, C.-N. Chou, M. D. Lukin, B. Barak, and S. Choi, Limitations of linear cross-entropy as a measure for quantum advantage, *PRX Quantum* **5**, 010334 (2024).
- [24] A. M. Dalzell, N. Hunter-Jones, and F. G. Brandão, Random quantum circuits transform local noise into global white noise, *Commun. Math. Phys.* **405**, 78 (2024).
- [25] B. Collins, S. Matsumoto, and J. Novak, The Weingarten calculus, *ArXiv:2109.14890*.
- [26] A. Ehrenberg, J. T. Iosue, A. Deshpande, D. Hangleiter, and A. V. Gorshkov, Transition of anticoncentration in Gaussian boson sampling, *ArXiv:2312.08433*.
- [27] A. Ehrenberg, J. T. Iosue, A. Deshpande, D. Hangleiter, and A. V. Gorshkov, The second moment of hafnians in Gaussian boson sampling, *ArXiv:2403.13878*.
- [28] A. Deshpande, A. Mehta, T. Vincent, N. Quesada, M. Hinsche, M. Ioannou, L. Madsen, J. Lavoie, H. Qi, J. Eisert, *et al.*, Quantum computational advantage via high-dimensional Gaussian boson sampling, *Sci. Adv.* **8**, eabi7894 (2022).
- [29] A. Arkhipov and G. Kuperberg, The bosonic birthday paradox, *Geom. Topol. Monogr.* **18**, 10 (2012).
- [30] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Boca Raton, Florida, USA, 2017).
- [31] A. Barvinok, *Combinatorics and Complexity of Partition Functions* (Springer, Cham, Switzerland, 2016), Vol. 30.
- [32] M. Ledoux, *The Concentration of Measure Phenomenon* (American Mathematical Soc., Providence, Rhode Island, USA, 2001), Vol. 89.
- [33] L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions* (Springer Science & Business Media, Dordrecht, Holland, 1974).
- [34] P. Flajolet and R. Sedgewick, *Analytic Combinatorics* (Cambridge University Press, Cambridge, UK, 2009).
- [35] S. Matsumoto, General moments of matrix elements from circular orthogonal ensembles, *Random Matrices: Theory Appl.* **1**, 1250005 (2012).
- [36] To write the second line of this relation, we used Sylvester’s theorem, which states that if $\mathbf{A}$ and $\mathbf{B}$ are $m \times n$ and $n \times m$ matrices, respectively, such that $\mathbf{AB}$ and $\mathbf{BA}$ are trace class, then $\det(\mathbb{I}_m + \mathbf{AB}) = \det(\mathbb{I}_n + \mathbf{BA})$.
- [37] F. Roberts and B. Tesman, *Applied Combinatorics* (CRC Press, Boca Raton, Florida, USA, 2009).
- [38] H. S. Wilf, *Generatingfunctionology* (CRC Press, Wellesley, Massachusetts, USA, 2005).
- [39] B. Collins, Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability, *Int. Math. Res. Not.* **2003**, 953 (2003).

- [40] B. Collins and P. Śniady, Integration with respect to the haar measure on unitary, orthogonal and symplectic group, *Commun. Math. Phys.* **264**, 773 (2006).
- [41] A. Meurer, C. P. Smith, M. Paprocki, O. Čertík, S. B. Kirpichev, M. Rocklin, A. Kumar, S. Ivanov, J. K. Moore, S. Singh, *et al.*, Sympy: Symbolic computing in Python, *PeerJ Comput. Sci.* **3**, e103 (2017).
- [42] B. Madsen, Graph-theory, <https://github.com/root-11/graph-theory>, 2024.
- [43] B. Gupt, J. Izaac, and N. Quesada, The Walrus: A library for the calculation of hafnians, Hermite polynomials and Gaussian boson sampling, *J. Open Source Softw.* **4**, 1705 (2019).
- [44] N. Quesada, R. S. Chadwick, B. A. Bell, J. M. Arrazola, T. Vincent, H. Qi, R. García, *et al.*, Quadratic speed-up for simulating Gaussian boson sampling, *PRX Quantum* **3**, 010306 (2022).
- [45] <https://doi.org/10.5281/zenodo.13327744>.
- [46] https://github.com/polyquantique/lxe_score_for_gbs.
- [47] S. Rahimi-Keshari, A. P. Lund, and T. C. Ralph, What can quantum optics say about computational complexity theory?, *Phys. Rev. Lett.* **114**, 060501 (2015).
- [48] A. Islami, Symmetric functions as characters of hyperoctahedral group, Ph.D. thesis, York University, 2020.
- [49] I. G. Macdonald, *Symmetric Functions and Hall Polynomials* (Oxford University Press, New York, New York, USA, 1998).