Vacuum provides quantum advantage to otherwise simulatable architectures

Vacuum provides quantum advantage to otherwise simulatable architectures

Cameron Calcluth [1,*] Alessandro Ferraro [2,3] and Giulia Ferrini [1]

[1] *Department of Microtechnology and Nanoscience (MC2), Chalmers University of Technology, SE-412 96 Göteborg, Sweden*
[2] *Centre for Theoretical Atomic, Molecular and Optical Physics, Queen's University Belfast, Belfast BT7 1NN, United Kingdom*
[3] *Dipartimento di Fisica "Aldo Pontremoli," Università degli Studi di Milano, I-20133 Milan, Italy*

(Received 1 June 2022; accepted 9 May 2023; published 15 June 2023)

We consider a computational model composed of ideal Gottesman-Kitaev-Preskill stabilizer states, Gaussian operations including all rational symplectic operations and all real displacements, and homodyne measurement. We prove that such architecture is classically efficiently simulatable by explicitly providing an algorithm to calculate the probability density function of the measurement outcomes of the computation. We also provide a method to sample when the circuits contain conditional operations. This result is based on an extension of the celebrated Gottesman-Knill theorem, via introducing proper stabilizer operators for the code at hand. We conclude that the resource enabling quantum advantage in the universal computational model considered by Baragiola *et al.* [Phys. Rev. Lett. **123**, 200502 (2019)], composed of a subset of the elements given above augmented with a provision of vacuum states, is indeed the vacuum state.

DOI: 10.1103/PhysRevA.107.062414

I. INTRODUCTION

Identifying the physical resources underlying quantum advantage, i.e., yielding the ability of quantum computers to solve computational problems faster than classical computers, is of crucial importance for the design of meaningful architectures for quantum computation (QC) [1]. Often, the resource depends on the model. For example, for architectures over finite-dimensional systems, Clifford circuits are resourceless from a computational standpoint, since they are efficiently simulatable [2–4] until a so-called magic resource is provided, such as the T-state, which allows universal quantum computation to be performed [5,6]. Similarly, for infinite-dimensional continuous-variable (CV) systems, Gaussian circuits are efficiently simulatable [7–9] and to promote them to universal QC specific non-Gaussian resources [10,11] have to be provided, such as the cubic-phase state [12,13], or Gottesman-Kitaev-Preskill (GKP) states [14,15]. The cost of producing these enabling resources with sufficient quality generally requires a significant overhead and their distinct features are typically complex and in stark contrast with respect to the elements of the corresponding simulatable architectures. For example, T-states and cubic-phase states are nonstabilizer and non-Gaussian, respectively. It is a natural question to ask: Are resources always complex and costly to produce?

In this work, we provide a specific example of a CV quantum computing architecture that is classically efficiently simulatable, and that becomes universal by adding the vacuum state. The latter state is widely regarded as the simplest quantum state of a bosonic field, and in particular it is a Gaussian state. The architecture considered is based on stabilizer GKP states, Gaussian operations including conditional displacements and homodyne detection. By taking inspiration from stabilizer methods developed for discrete-variable (DV) systems [2–4,16,17], we prove that this class of circuits is classically efficiently simulatable for rational symplectic operations and arbitrary continuous displacement, thereby significantly extending [18] the class of Gaussian operations that was previously known to be simulatable in combination with GKP states [19,20]. This result is obtained despite the fact that GKP states are highly non-Gaussian and their Wigner function is highly negative [12,15,21], and hence the standard theorems based on Gaussianity [7] or on the positivity of quasiprobability distributions [8,9,22] cannot be applied. We then leverage on the results of Ref. [14], where the same architecture combined with the vacuum (or a thermal) state was shown to be universal for quantum computation, to conclude that the vacuum provides quantum advantage.

The paper is structured as follows. In Sec. II we provide an introduction to the circuit class that we demonstrate to be efficiently simulatable. In Sec. III we provide an analytic method to evaluate the probability density function (PDF) of the introduced circuit class. Then in Sec. IV we provide an algorithm to evaluate the PDF of the circuit and show that it is classically efficient. We also extend our result to include adaptive circuits and show that GKP-encoded Clifford circuits are included in the simulatable class. We then demonstrate in Sec. V that these results are sufficient to conclude that the vacuum is a resource for quantum advantage in the context of the simulatable model we consider. In Sec. VI we also extend

*calcluth@gmail.com

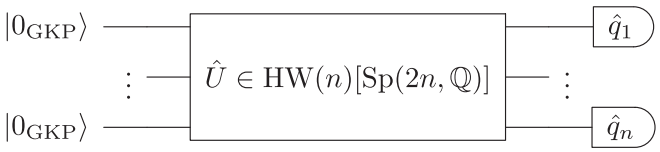

FIG. 1. Schematics of the circuit class considered. In input, there are ideal GKP stabilizer states, such as the 0-logical state. The operations considered are the semidirect product of the rational symplectic operations and the Heisenberg-Weyl group. Multimode homodyne detection follows.

this result to show that realistic GKP states can be considered resourceful in the context of this model. Finally, we provide conclusions and open questions in Sec. VII.

II. GAUSSIAN CIRCUITS WITH STABILIZER GKP STATES

In this section we introduce the circuit class considered in this work, which we later show to be efficiently simulatable.

We consider the circuits shown in Fig. 1, where the input states are n ideal GKP states encoding pure stabilizer states. Without loss of generality, we can consider each mode to be in the 0-logical encoded GKP state, which has a wave function in position representation given by [12]

$$\psi_{0,L}(x) = \langle \hat{q} = x|0_{\mathrm{GKP}}\rangle = \sum_m \delta(2m\sqrt{\pi} - x); \tag{1}$$

the total multimode input state can be compactly indicated by

$$|\mathbf{0}_{\mathrm{GKP}}\rangle = |0_{\mathrm{GKP}}\rangle^{\otimes n}. \tag{2}$$

The input state is stabilized by any combination of the operators $e^{2i\sqrt{\pi}\hat{p}_j}$, $e^{i\sqrt{\pi}\hat{q}_j}$ with any integer power. This means that the action of these operators, or any combination of them, on the state will have the effect of the identity, e.g.,

$$e^{2i\sqrt{\pi}\hat{p}_j}|\mathbf{0}_{\mathrm{GKP}}\rangle = |\mathbf{0}_{\mathrm{GKP}}\rangle \quad \forall j \in \{1, \ldots, n\}, \tag{3}$$

$$e^{i\sqrt{\pi}\hat{q}_j}|\mathbf{0}_{\mathrm{GKP}}\rangle = |\mathbf{0}_{\mathrm{GKP}}\rangle \quad \forall j \in \{1, \ldots, n\}. \tag{4}$$

The operations we consider in this work are those which belong to the group $\mathrm{HW}(n)[\mathrm{Sp}(2n, \mathbb{Q})]$ which is the semidirect product [23] of the Heisenberg-Weyl group $\mathrm{HW}(n)$ and the rational symplectic group $\mathrm{Sp}(2n, \mathbb{Q})$. The Heisenberg-Weyl group $\mathrm{HW}(n)$ consists of all real phase-space displacements of the form $e^{ic_j\hat{q}_j}$ and $e^{-id_j\hat{p}_j}$ for $c_j, d_j \in \mathbb{R}$ and $j \in \{1, \ldots, n\}$.

The rational symplectic group $\mathrm{Sp}(2n, \mathbb{Q})$ is the rational subgroup of the symplectic group $\mathrm{Sp}(2n, \mathbb{R})$ over the reals. It consists of all symplectic operations parameterized by a $2n \times 2n$ symplectic matrix such that all its elements are rational numbers. The set of rational symplectic operations is dense in the set of real symplectic operations. We provide a proof of this fact in Appendix A. Note, however, that the density of the rational symplectic matrices should be regarded as a mathematical property characterizing the extent of the class of simulatable operations. It does not imply that the probability distributions obtained with operations parameterized by operations that are outside the set (e.g., in its closure) are necessarily simulatable. For later convenience, we will denote a symplectic matrix M by square subblocks of equal dimension:

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \tag{5}$$

Gaussian operations can always be expressed as a unitary operator $\hat{U}$ in terms of symplectic operations and phase-space displacements [24,25]. The following operations form a generating set of all Gaussian operations:

$$\left\{e^{ic_j\hat{q}_j}, e^{i\theta_j(\hat{q}_j^2+\hat{p}_j^2)/2}, e^{-i\ln s_j(\hat{q}_j\hat{p}_j+\hat{p}_j\hat{q}_j)/2}, e^{-i\hat{q}_j\hat{p}_k}\right\}, \tag{6}$$

where $c_j \in \mathbb{R}$, $\theta_j \in [0, 2\pi)$, $s_j \in \mathbb{R}$, and $j, k \in \{1, \ldots, n\}$. These generators and also any combination of them will be shown to be simulatable so long as θ_j and s_j are chosen such that $\cos\theta_j, \sin\theta_j, s_j \in \mathbb{Q}$ for all j. We will also show that adaptivity can be included as a feature of the class of circuits that can be efficiently simulated.

The circuits we consider are measured using homodyne detection, which, without loss of generality, we can restrict to position measurements. The measurement outcomes of the circuit in Fig. 1 will therefore have a probability density function (PDF), denoted $f_{\mathrm{PD}}(\hat{\mathbf{q}} = \mathbf{x})$, expressed as

$$f_{\mathrm{PD}}(\hat{\mathbf{q}} = \mathbf{x}) = |\langle \hat{\mathbf{q}} = \mathbf{x}|\hat{U}|\mathbf{0}_{\mathrm{GKP}}\rangle|^2. \tag{7}$$

When measuring the output modes, a quantum computer will provide outputs $\mathbf{x}$ selected with probabilities specified by the f_{PD} in Eq. (7).

As we will clarify in Sec. V, the circuit elements (including adaptive operations) composing the universal model stemming from Ref. [14] all belong to our class of circuits except for the vacuum.

III. SIMULATION METHOD FOR GKP CIRCUITS

In order to assess the simulatability of the circuits outlined in the previous section, we introduce a method to evaluate the PDF of the circuit presented in Fig. 1. This method involves tracking the Heisenberg evolution of the measurement operators and then using the stabilizers of the input states to evaluate the PDF. We first provide an overview of the problem statement and a summary of the contents of the following subsections, which contain details of the proof.

A general Gaussian operation $\hat{U}$ belonging to $\mathrm{HW}(n)[\mathrm{Sp}(2n, \mathbb{Q})]$ transforms, in the Heisenberg picture, the measurement operators $\hat{q}_j$ according to [7,26]

$$\hat{Q}_j = \hat{U}^\dagger\hat{q}_j\hat{U} = \sum_i a_i^{(j)}\hat{q}_i + b_i^{(j)}\hat{p}_i + c_j, \tag{8}$$

where the coefficients $a_i^{(j)} = A_{i,j}$ and $b_i^{(j)} = B_{i,j}$ are elements of the blocks of the symplectic matrix M as defined in Eq. (5). The vector $\vec{c} \in \mathbb{R}^n$, with elements c_j, describes the displacement in position. As we now prove, these circuits can be simulated in the strong sense by calculating the PDF. The PDF given in Eq. (7) can be written in the Heisenberg picture using Eq. (8) as

$$f_{\mathrm{PD}}(\hat{\mathbf{Q}} = \mathbf{x}) = \langle \mathbf{0}_{\mathrm{GKP}}|\left(\prod_j |\hat{Q}_j = x_j\rangle\langle\hat{Q}_j = x_j|\right)|\mathbf{0}_{\mathrm{GKP}}\rangle. \tag{9}$$

Our method is based on two main observations. First, by inserting the GKP stabilizers $e^{2i\sqrt{\pi}\hat{p}_j}$ and $e^{i\sqrt{\pi}\hat{q}_j}$ into the expression (9), we can identify a periodicity relation of the PDF. Second, we can manufacture bespoke additional stabilizers, in terms of the Heisenberg measurement operators, of the form

$$g(\vec{l}) = e^{i\phi(\vec{l})}\prod_j e^{i\sqrt{\pi}l_j\hat{Q}_j}, \tag{10}$$

where $\vec{l}$ is an n-vector of real coefficients l_j and $\phi(\vec{l})$ is a phase factor chosen such that $g(\vec{l})$ is a stabilizer. By inserting this bespoke stabilizer into the PDF, it is possible to identify a second constraint that provides the nonzero values of the PDF. Together, these two constraints uniquely identify the PDF.

In Sec. III A we demonstrate how to derive the periodicity condition on the PDF, from the symplectic matrix M. In Sec. III B we demonstrate how to identify the nonzero points of the PDF. Finally, in Sec. III C we demonstrate that these two conditions are sufficient to construct the PDF of the circuit. A reader uninterested in the technical derivations may proceed directly to Eq. (52), whereby we provide the explicit PDF of the circuit shown in Fig. 1. This PDF will provide sufficient information to understand the next Sec. IV, whereby we provide the algorithm to simulate these circuits.

A. Periodicity of the PDF

In this subsection we will evaluate a periodicity condition that will provide a restriction on the PDF of the circuits considered. This periodicity condition informs us of the points of the PDF for which the values of the PDF are equal. The PDF, as given in Eq. (9), can equivalently be written as

$$f_{\rm PD}(\hat{\mathbf{Q}}=\mathbf{x}) = \langle \mathbf{0}_{\rm GKP}|\left(\prod_j \delta(\hat{Q}_j - x_j)\right)|\mathbf{0}_{\rm GKP}\rangle, \tag{11}$$

whereby we have rewritten the measurement operator as a delta function,

$$\delta(\hat{Q}_j - x_j) = \int ds e^{is(\hat{Q}_j - x_j)}. \tag{12}$$

Similarly to the original Gottesman-Knill theorem for qubits [2,4], by inserting stabilizers into this PDF on the right-hand-side of the delta function, and then using commutation relations to move the stabilizers to the left-hand side, we find two expressions for the PDF which are equivalent. These two expressions correspond to two separate points on the PDF, implying that the PDF is equal at these points. We start by considering the commutation of a general stabilizer with the measurement projection operators. We would like to calculate how the stabilizers $e^{2i\sqrt{\pi}\hat{p}_k}$ and $e^{i\sqrt{\pi}\hat{q}_k}$ commute with the general measurement projector, given in Eq. (12).

This can be calculated by using the Baker-Campbell-Hausdorff (BCH) formula [27,28] for linear combinations of quadrature operators

$$e^{\hat{X}+\hat{Y}+\frac{1}{2}[\hat{X},\hat{Y}]} = e^{\hat{X}}e^{\hat{Y}} \tag{13}$$

$$\Rightarrow e^{\hat{X}}e^{\hat{Y}} = e^{\hat{Y}}e^{\hat{X}}e^{[\hat{X},\hat{Y}]}, \tag{14}$$

valid for the case in which the operators $\hat{X}$ and $\hat{Y}$ commute with their commutator. The commutation between the measurement projector in Eq. (12) and each stabilizer can be evaluated using Eq. (14) by first evaluating how the terms commute, without integration. For the stabilizer containing $\hat{p}_k$ we find

$$\begin{aligned} e^{is(\hat{Q}_j-x)}e^{2i\sqrt{\pi}\hat{p}_k} &= e^{2i\sqrt{\pi}\hat{p}_k}e^{is(\hat{Q}_j-x)}e^{[is(\hat{Q}_j-x),2i\sqrt{\pi}\hat{p}_k]} \\ &= e^{-2s\sqrt{\pi}a_k^{(j)}i}e^{2i\sqrt{\pi}\hat{p}_k}e^{is(\hat{Q}_j-x)}, \end{aligned} \tag{15}$$

whereas, for the stabilizer containing $\hat{q}_k$, we find

$$\begin{aligned} e^{is(\hat{Q}_j-x)}e^{i\sqrt{\pi}\hat{q}_k} &= e^{i\sqrt{\pi}\hat{q}_k}e^{is(\hat{Q}_j-x)}e^{[is(\hat{Q}_j-x),i\sqrt{\pi}\hat{q}_k]} \\ &= e^{s\sqrt{\pi}b_k^{(j)}i}e^{i\sqrt{\pi}\hat{q}_k}e^{is(\hat{Q}_j-x)}. \end{aligned} \tag{16}$$

The first of these relations, Eq. (15), allows us to calculate the commutation between the measurement projection operator and any integer $m_k \in \mathbb{Z}$ power of the momentum stabilizer $e^{2im_k\sqrt{\pi}\hat{p}_k}$,

$$\begin{aligned} \delta(\hat{Q}_j - x_j)e^{2im_k\sqrt{\pi}\hat{p}_k} &= \int ds e^{-2m_k s\sqrt{\pi}a_k^{(j)}i}e^{2im_k\sqrt{\pi}\hat{p}_k}e^{is(\hat{Q}_j-x_j)} \\ &= e^{2im_k\sqrt{\pi}\hat{p}_k}\delta\left(\hat{Q}_j - x_j - 2m_k\sqrt{\pi}a_k^{(j)}\right). \end{aligned} \tag{17}$$

The second relation (16) provides us with a similar relation for any integer $m'_k \in \mathbb{Z}$ power of the position stabilizer $e^{im'_k\sqrt{\pi}\hat{q}_k}$,

$$\delta(\hat{Q}_j - x_j)e^{-im'_k\sqrt{\pi}\hat{q}_k} = e^{-im'_k\sqrt{\pi}\hat{q}_k}\delta\left(\hat{Q}_j - x_j - m'_k\sqrt{\pi}b_k^{(j)}\right). \tag{18}$$

Now, inserting all the stabilizers

$$e^{2\sqrt{\pi}im_1\hat{p}_1}e^{-\sqrt{\pi}im'_1\hat{q}_1}\ldots e^{2\sqrt{\pi}im_n\hat{p}_n}e^{-\sqrt{\pi}im'_n\hat{q}_n} \tag{19}$$

into the right-hand side of the full PDF given by Eq. (11), and using the commutation relations to move the stabilizers to the left-hand side, we find that the PDF at $\vec{x}$ is equal to the PDF at the displaced point $\hat{x}'$, which can be expressed as

$$x_j \to x'_j = x_j + \sqrt{\pi}\sum_k 2a_k^{(j)}m_k + b_k^{(j)}m'_k. \tag{20}$$

We also note that this periodicity condition can equivalently be written in terms of

$$\vec{x}' = \vec{x} + 2\sqrt{\pi}\begin{pmatrix} A & \frac{1}{2}B\end{pmatrix}\begin{pmatrix}\vec{m}\\ \vec{m}'\end{pmatrix}, \tag{21}$$

where $\vec{m}$ and $\vec{m}'$ are each n-dimensional vectors of integers. This form of the periodicity relation will be useful when combining the two conditions in Sec. III C. This provides us with the first condition for the form of the PDF. In the following subsection, we derive the second condition, which informs us of the set of points at which the PDF is nonzero.

B. Set of nonzero points

To evaluate the nonzero points of the PDF, we construct bespoke stabilizers from the Heisenberg measurement operators. Although this step varies notably from the conventional Gottesman-Knill theorem for DV systems, we can adopt a comparable approach to the DV theorem once such stabilizers have been identified. Specifically, we insert the stabilizers into the PDF and derive a set of equalities with respect to a set of

points $\vec{x}$. These equalities lead to a contradiction unless the value of the PDF is only nonzero at this set of points.

We begin by identifying stabilizers of the set of input 0-logical states, $|\mathbf{0}_{\mathrm{GKP}}\rangle$, expressed in terms of the Heisenberg measurement operators $\hat{Q}_j$. To do so, we first define an operator $g(\vec{l})$, which will become a stabilizer for the input 0-logical states under certain conditions. Considering a generic vector $\vec{l} \in \mathbb{Q}^n$ and a generic real function $\phi(\vec{l}) : \mathbb{Q}^n \to \mathbb{R}$, the operator is defined as

$$\begin{aligned} g(\vec{l}) &= e^{i\phi(\vec{l})} \prod_j e^{i\sqrt{\pi} l_j \hat{Q}_j} \\ &= e^{i\phi(\vec{l})} e^{i\sqrt{\pi}\sum_j l_j [\sum_k (A_{j,k}\hat{q}_k + B_{j,k}\hat{p}_k) + c_j]} \\ &= e^{i\phi(\vec{l})} e^{i\sqrt{\pi}\vec{l}\cdot\vec{c}} \prod_k e^{i\sqrt{\pi}(\sum_j l_j A_{j,k})\hat{q}_k + i\sqrt{\pi}(\sum_j l_j B_{j,k})\hat{p}_k} \\ &= e^{i\phi(\vec{l})} e^{i\sqrt{\pi}\vec{l}\cdot\vec{c}} \prod_{k=1}^{n} e^{i\sqrt{\pi}(\vec{l}^T A)_k \hat{q}_k + i\sqrt{\pi}(\vec{l}^T B)_k \hat{p}_k}. \end{aligned} \tag{22}$$

Using the BCH formula given in Eq. (13) we find that each term in the product can be expressed as

$$e^{i\sqrt{\pi}(\vec{l}^T A)_k \hat{q}_k} e^{i\sqrt{\pi}(\vec{l}^T B)_k \hat{p}_k} e^{\frac{i}{2}\pi (\vec{l}^T A)_k (\vec{l}^T B)_k}, \tag{23}$$

and we can therefore express the operator as

$$g(\vec{l}) = e^{i\phi(\vec{l})} e^{i\sqrt{\pi}\vec{l}\cdot\vec{c}} e^{\frac{i}{2}\pi \vec{l}^T A B^T \vec{l}} \prod_{k=1}^{n} e^{i\sqrt{\pi}(\vec{l}^T A)_k \hat{q}_k} e^{i\sqrt{\pi}(\vec{l}^T B)_k \hat{p}_k}. \tag{24}$$

We find that by choosing $\phi(\vec{l})$ to be

$$\phi(\vec{l}) = -\tfrac{1}{2}\pi \vec{l}^T A B^T \vec{l} - \sqrt{\pi}\vec{l}\cdot\vec{c} \tag{25}$$

this operator will have the form

$$g(\vec{l}) = \prod_k e^{i\sqrt{\pi}(\vec{l}^T A)_k \hat{q}_k} e^{i\sqrt{\pi}(\vec{l}^T B)_k \hat{p}_k}. \tag{26}$$

Hence, $g(\vec{l})$ will be a stabilizer of $|\mathbf{0}_{\mathrm{GKP}}\rangle$ whenever

$$\begin{aligned} (A^T \vec{l})_k &= 0 \mod 1, \\ (B^T \vec{l})_k &= 0 \mod 2. \end{aligned} \tag{27}$$

Inserting the stabilizer $g(\vec{l})$ into the equation of the PDF, given in Eq. (11), we have an equality between the PDF in its original form, and the PDF with the inserted stabilizer. Specifically, by inserting the stabilizer between the Heisenberg-evolved position quadrature basis states and the 0-logical GKP states, we find that the stabilizer will act on the basis states as

$$\begin{aligned} & g(\vec{l}) \prod_j |\hat{Q}_j = x_j\rangle\langle\hat{Q}_j = x_j| \\ &= e^{i\phi(\vec{l})} \prod_j e^{i\sqrt{\pi} l_j x_j} |\hat{Q}_j = x_j\rangle\langle\hat{Q}_j = x_j|, \end{aligned} \tag{28}$$

where the choice of $\vec{l}$ is constrained by Eq. (27) and $\phi(\vec{l})$ is of the form given in Eq. (25). Furthermore, given that we know that the PDF will be equal, with or without the inserted stabilizer, we find that

$$\begin{aligned} & \langle\mathbf{0}_{\mathrm{GKP}}| \left(\prod_j |\hat{Q}_j = x_j\rangle\langle\hat{Q}_j = x_j| \right) |\mathbf{0}_{\mathrm{GKP}}\rangle \\ &= e^{i\phi(\vec{l})} \prod_j e^{i\sqrt{\pi} l_j x_j} \langle\mathbf{0}_{\mathrm{GKP}}|\hat{Q}_j = x_j\rangle\langle\hat{Q}_j = x_j|\mathbf{0}_{\mathrm{GKP}}\rangle. \end{aligned} \tag{29}$$

This equality can be true only if the term involving the phase equals one, or the PDF itself is zero. Hence, the nonzero points $\vec{x}$ of the PDF satisfy the equation

$$\sqrt{\pi}\vec{l}^T\vec{x} - \tfrac{1}{2}\pi \vec{l}^T A B^T \vec{l} - \sqrt{\pi}\vec{l}\cdot\vec{c} = 0 \mod 2\pi \tag{30}$$

for all possible choices of $\vec{l}$ which satisfies Eq. (27). If, on the other hand, we choose a different point $\vec{x}$, that does not satisfy this constrained equation, the equality will result in a contradiction unless the PDF is zero at these values of $\vec{x}$. We can therefore reduce the problem of identifying the nonzero points to finding solutions $\vec{x}$ of Eq. (30) constrained by Eq. (27). We now provide a short summary of the steps required to solve Eq. (30) given Eq. (27), provided that A and B both contain all rational elements. The full details are provided in Appendix B.

To solve this constrained equation we first find the allowed vectors $\vec{l}$. This can be achieved by introducing the matrix S, which is defined as

$$S = \begin{pmatrix} A^T \\ \frac{1}{2}B^T \end{pmatrix}. \tag{31}$$

Then, the constraint on the allowed values of $\vec{l}$ is given by $S\vec{l} = \vec{b}$ where $\vec{b}$ is a vector of $2n$ integers. The Moore-Penrose pseudoinverse S^+ provides a method to find solutions of the form $\vec{l} = S^+\vec{b}$ [29–31]. The solutions of $\vec{l}$ can be found by first finding the Smith decomposition [31–33] of the matrix σS, where σ is the smallest integer for which the elements of the matrix σS are all integers. Note that this step assumes that the symplectic matrix, and therefore also S, is rational. We provide broader requirements for the symplectic matrix in Appendix C and discuss the relationships between these classes of simulatable operations in Appendix D. Next, using the Smith decomposition of $\sigma S = VDU$ we identify which integer choices of $\vec{b}$ will provide valid solutions of $\vec{l}$. We find that the vectors $\vec{l}$ can be expressed as [34]

$$\vec{l} = R\vec{m}, \tag{32}$$

where $\vec{m}$ is any choice of an n-vector of integers and R is an $n \times n$ invertible rational matrix, defined as

$$R = S^+ V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix}. \tag{33}$$

We can then rewrite Eq. (30) as a system of linear equations of the form

$$\frac{1}{\sqrt{\pi}} R^T (\vec{x} - \vec{c}) = \vec{t} \mod 2, \tag{34}$$

where $\vec{t}$ is the main diagonal of the matrix $T = \frac{1}{2}R^T A B^T R$. This form, Eq. (34), allows us to evaluate the solution to the constrained equation as

$$\vec{x} = \sqrt{\pi} R^{-T} (\vec{t} + 2\vec{m}) + \vec{c}. \tag{35}$$

Therefore, provided that the symplectic matrix is rational, we have identified that the PDF is nonzero exclusively at these points.

Combined with the insight from the previous subsection, we have now identified both a periodicity relation and the set of nonzero points of the PDF. In the following subsection, we use both these results to demonstrate that the PDF assumes the same value at all the nonzero points, i.e., those identified in Eq. (35).

C. Constructing the PDF of the circuit

We now show that the PDF is specified completely by the periodicity relation and the points at which the PDF is nonzero. For this to hold, two conditions are required. First, we need to ensure that any nonzero point displaced by the periodicity relations always results in another nonzero point. Second, we need to ensure that any nonzero point can be reached by another nonzero point using the periodicity relations.

We begin with the first condition and show that for any valid solution $\vec{x}$ we also get a valid solution if it is displaced according to the periodicity constraint. Namely, we can check that any point specified by the periodicity constraint is included in the allowed points.

If we take a point specified by

$$\frac{1}{\sqrt{\pi}}\vec{x}^{(1)} = (R^T)^{-1}(\vec{t} + 2\vec{m}) + \vec{c} \tag{36}$$

and displace it according to the periodicity relation provided in Eq. (21), the new point should also satisfy this constraint. Here, to distinguish the vectors of integers in Eq. (21) and Eq. (36), we relabel the arbitrary choice of integers in Eq. (21), given as vectors $\vec{m}$ and $\vec{m}'$, as $\vec{k}$ and $\vec{k}'$, respectively. Given a displacement, specified by $\vec{k}$ and $\vec{k}'$, we find a new point

$$\frac{1}{\sqrt{\pi}}\vec{x}^{(2)} = (R^T)^{-1}(\vec{t} + 2\vec{m}) + 2\begin{pmatrix} A & \frac{1}{2}B \end{pmatrix}\begin{pmatrix} \vec{k} \\ \vec{k}' \end{pmatrix} + \vec{c}. \tag{37}$$

For the first condition to hold, this new point must also be a nonzero point of the PDF and should satisfy the system of linear equations defining the nonzero points, given in Eq. (34). This can be checked by inserting $\vec{x}^{(2)}$ into the left-hand side of that equation,

$$\begin{aligned} &\frac{1}{\sqrt{\pi}}R^T(\vec{x}^{(2)} - \vec{c}) \\ &\quad = R^T\left[(R^T)^{-1}(\vec{t} + 2\vec{m}) + 2\begin{pmatrix} A & \frac{1}{2}B \end{pmatrix}\begin{pmatrix} \vec{k} \\ \vec{k}' \end{pmatrix}\right] \\ &\quad = \vec{t} + 2\vec{m} + 2R^T\left(A\vec{k} + \frac{1}{2}B\vec{k}'\right), \end{aligned} \tag{38}$$

which we expect to evaluate to $\vec{t} + 2\vec{m}'$, where $\vec{m}'$ is a different n-vector of integers. This can be shown by inspecting each element of the vector that is given as the third term of Eq. (38). We label this vector as $\vec{w}$,

$$\vec{w} = 2R^T\left(A\vec{k} + \tfrac{1}{2}B\vec{k}'\right). \tag{39}$$

The elements of this vector can be found by multiplying its transpose with the unit vector

$$w_i = \vec{w}^T\vec{e}_i = 2\left(\vec{k}^T A^T R + \tfrac{1}{2}\vec{k}'^T B^T R\right)\vec{e}_i. \tag{40}$$

We know from Eq. (32) that for any n-dimensional vector of integers $\vec{k}$ there exists an allowed value of $\vec{l}$ as

$$\vec{l} = R\vec{k}. \tag{41}$$

Choosing $\vec{k}$ to be the basis vector $\vec{k} = \vec{e}^{(i)}$, which is zero in all entries except at i, we can identify one choice of $\vec{l}$, parameterized by i, that corresponds to the element of the vector $\vec{k}$, chosen to be nonzero, as

$$\vec{l}^{(i)} = R\vec{e}_i. \tag{42}$$

We can then write the ith element of the vector $\vec{w}$ in Eq. (39) as

$$w_i = 2\left(\vec{k}^T A^T \vec{l}^{(i)} + \tfrac{1}{2}\vec{k}'^T B^T \vec{l}^{(i)}\right). \tag{43}$$

Furthermore for any allowed $\vec{l}$, including the choice $\vec{l}^{(i)}$ we have

$$\begin{aligned} (A^T\vec{l})_i &= 0 \mod 1, \\ (B^T\vec{l})_i &= 0 \mod 2. \end{aligned} \tag{44}$$

The term in brackets in Eq. (43) must be an integer, and so w_i must be an even integer. This means that

$$\vec{w} = 2\tilde{\vec{m}} \tag{45}$$

for some n-dimensional vector of integers $\tilde{\vec{m}}$ and hence

$$\frac{1}{\sqrt{\pi}}R^T\vec{x}^{(2)} = \vec{t} + 2\vec{m} + \vec{w} = \vec{t} + 2\vec{m}', \tag{46}$$

which is of the same form as Eq. (34). This implies that any nonzero point displaced using the periodicity condition also satisfies the constrained equation specifying the nonzero points. We have therefore demonstrated that the first condition introduced in this subsection does indeed hold.

For the second condition, we need to demonstrate that any nonzero point can be reached using the periodicity relations.

This can be proven by specifying a center point as

$$\vec{x}^{(0)} = \sqrt{\pi}(R^T)^{-1}\vec{t} \tag{47}$$

and demonstrating that it can be displaced to any other nonzero point of the form

$$\vec{x}^{(1)} = \sqrt{\pi}(R^T)^{-1}(\vec{t} + 2\vec{m}) \tag{48}$$

using only displacements of the form given by Eq. (21). This is equivalent to saying that for any choice of $\vec{m}$, there exists some $\vec{k}, \vec{k}'$ such that

$$\begin{aligned} \sqrt{\pi}(R^T)^{-1}(\vec{t} + 2\vec{m}) = \sqrt{\pi}(R^T)^{-1}\vec{t} + 2\sqrt{\pi}S^T\begin{pmatrix} \vec{k} \\ \vec{k}' \end{pmatrix} \\ \Rightarrow (R^T)^{-1}\vec{m} = S^T\begin{pmatrix} \vec{k} \\ \vec{k}' \end{pmatrix}. \end{aligned} \tag{49}$$

We can solve this equation using the pseudoinverse to find potential solutions of the form

$$\begin{pmatrix} \vec{k} \\ \vec{k}' \end{pmatrix} = (S^T)^+ (R^T)^{-1} \vec{m}. \tag{50}$$

As with any pseudoinverse, we can check whether this solution is a valid solution by evaluating whether the original linear equation holds under the solution. That is, we check

$$S^T (S^T)^+ (R^T)^{-1} \vec{m} = (S^+ S)^T (R^T)^{-1} \vec{m} = (R^T)^{-1} \vec{m}, \tag{51}$$

which means that this solution is one possible valid solution. Note there exist infinite more solutions, but we do not need to find an expression for all of these. We have shown that no matter which nonzero point we are interested in, i.e., $\vec{x}^{(1)}$, there will be at least one way—and, in fact, infinite ways—to get to that point from the center point $\vec{x}^{(0)}$. This completes the proof of the second condition, introduced in this subsection.

We have therefore shown that both conditions hold, meaning that any nonzero point displaced by the periodicity relations results in another nonzero point and that any nonzero point can be reached from any other nonzero point. This implies that the value of the PDF is equal for all the nonzero points specified in Eq. (35).

This allows us to write the full and exact PDF of the multimode measurement, in terms of these allowed points, as

$$f_{\mathrm{PD}}(\vec{x}) = \sum_{\vec{m} \in \mathbb{Z}^n} \delta(\vec{x} - \sqrt{\pi} R^{-T} (\vec{t} + 2\vec{m}) - \vec{c}). \tag{52}$$

As we will show, this method to evaluate the PDF can be implemented with an efficient algorithm, namely, an algorithm whose complexity increases at most polynomially with respect to the number of modes. The algorithm for computing this PDF, along with its complexity analysis, is provided in Sec. IV.

IV. EFFICIENT ALGORITHM FOR THE SIMULATION OF GKP CIRCUITS

In this section we provide an explicit algorithm to evaluate the PDF of the circuit shown in Fig. 1 and derive some notable consequences of this result.

Efficient classical computation of the PDF of a quantum circuit is referred to as strong simulation. We begin with a presentation of the algorithm to efficiently simulate the circuits shown in Fig. 1 in Sec. IV A in the strong sense. We, therefore, extend the simulatable class to all real displacements and all rational symplectic operations as opposed to a restricted set [35]. Furthermore, the size of the set of simulatable operations does not depend on the number of modes measured, as was the case in Ref. [20].

The complementary notion of weak simulatability means instead that a classical computer can efficiently sample the outcomes of the circuit [36]. Weak simulation is sufficient to conclude that a quantum circuit will not provide quantum advantage, as a quantum computer will, in any case, produce outcomes selected from the PDF. Following the argument of Ref. [36], and assuming the capability of sampling from the set of integers, we will demonstrate in Sec. IV B that by restricting to weak simulation, we can further extend the class of simulatable circuits shown in Fig. 1. This extended class includes adaptive circuits, whereby intermediate measurement outcomes can affect future operations.

We will later use these results to demonstrate that the routine introduced in Ref. [14]—whereby the vacuum and GKP states are used to perform universal quantum computation—is efficiently simulatable when the vacuum is removed. This circuit is adaptive and contains GKP-encoded Clifford operations.

With this motivation, we demonstrate in Sec. IV C that GKP-encoded Clifford operations are included in the set of simulatable operations that we present in this work. As a consequence, we can also now simulate all encoded qubit stabilizer GKP states as input states, in the same sense as the Gottesman-Knill theorem [2–4]. This was not possible using our previous method [20]. Together, these results provide us with all the tools required to demonstrate in the later Sec. V that the vacuum is indeed the resource for quantum advantage in circuits composed of input GKP stabilizer states followed by Gaussian operations and homodyne measurement.

Finally, to demonstrate the practical implementation of the algorithm, we provide an example of evaluating the PDF of a simple circuit in Sec. IV D.

A. Algorithm to evaluate the PDF

We now provide the algorithm to calculate the PDF of a general circuit shown in Fig. 1 by using the result of the previous section. We will also provide an analysis of the computational time required to evaluate the PDF.

To express the PDF in Eq. (52) given the symplectic matrix M, given in block form as defined in Eq. (5), and the vector of displacement $\vec{c}$, we need to evaluate R^{-T} and $\vec{t}$. The matrix R^{-T} is given in terms of S^T and V, where V is the unimodular matrix arising from the Smith decomposition of σS. The vector $\vec{t}$ can be evaluated from V.

First, we identify the matrix S, by simply writing it in terms of the block components A, B as it is given in Eq. (31). To find the matrix V we first need to calculate the lowest common multiple of all the denominators of the elements S. Formally we could write

$$\sigma = \mathrm{lcm}(\mathrm{den}(S)), \tag{53}$$

where $\mathrm{den}(\cdot)$ evaluates the denominator of all matrix elements and $\mathrm{lcm}(\cdot)$ evaluates the lowest common multiple of all matrix elements.

Then we multiply the matrix S by σ to produce an integer matrix σS. We can perform a Smith normal form decomposition on this matrix to identify the $2n \times 2n$ unimodular matrix V, the $2n \times n$ diagonal matrix D and the $n \times n$ unimodular matrix U,

$$\sigma S = V D U. \tag{54}$$

We can discard the matrices D, U.

The transpose inverse of R can be directly evaluated as

$$R^{-T} = S^T V^{-T} \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} = \begin{pmatrix} A & \frac{1}{2} B \end{pmatrix} V^{-T} \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix}. \tag{55}$$

Furthermore, the matrix T can be calculated from V as

$$T = V^{(11)T} V^{(21)}, \tag{56}$$

and the vector $\vec{t}$ is simply the diagonal entries of T. The PDF is then given by Eq. (52).

To summarize, this algorithm consists of the following steps:

(1) Evaluate the matrix S from M
(2) Identify the integer σ from Eq. (53)
(3) Multiply every element of S by σ
(4) Find the matrix V from the Smith decomposition of σS
(5) Find the inverse-transpose of V
(6) Evaluate R^{-T} from S^T, V^{-T}
(7) Evaluate $\vec{t}$ from V

We can assume that the $2n \times 2n$ symplectic matrix M is stored as a matrix of numerators M^{num} and a matrix of denominators M^{den} such that $M = M^{\text{num}} \oslash M^{\text{den}}$, where $\oslash$ denotes element-wise division.

Step 1 consists of a truncation of the $2n \times 2n$ matrix M followed by matrix multiplication of the denominator matrix M^{den}, which in the worst case requires $O(n^3)$ operations [37].

Step 2 consists of finding the lowest common multiple of every element in M^{den}. There are $(2n)^2$ integer entries of this matrix $M^{\text{den}}_{i,j}$. We can find the lowest common multiple of two integers α, β by using the greatest common divisor

$$\text{lcm}(\alpha, \beta) = \frac{\alpha\beta}{\text{gcd}(\alpha, \beta)} \tag{57}$$

and then calculate the lowest common divisor of more than two integers iteratively,

$$\text{lcm}(\alpha, \beta, \gamma) = \text{lcm}(\text{lcm}(\alpha, \beta), \gamma). \tag{58}$$

If we limit the number of digits of precision in each element of $M^{\text{den}}_{i,j}$ to k, we can identify that the calculation of the lowest common multiple of two integers of bit length k will require at most $O(k^2)$ operations [37,38]. The size of the bit string representing the lowest common multiple will be at most $2k$. Calculating the lowest common multiple of two numbers of size k, $2k$ has complexity in terms of the bit length of the smallest of the two numbers, k and so the complexity of calculating the next iteration will also be $O(k^2)$ and the resulting lowest common multiple of the three numbers will be $3k$. We need to repeat this iterative process n^2 times, and so the total time complexity will be in the worst case $O(n^2k^2)$ and the size of the integer σ will have at most n^2k bits.

Step 3 consists of multiplying every element of S by σ which will require $O(n^2)$ operations and the matrix σS will contain $2n^2$ elements each of maximum size $n^2k + k$. Therefore, the bit length of each element of σS is polynomial in the number of modes n considered.

Step 4 consists of finding a Smith normal form decomposition, which is polynomial in the size of the matrix S and the number of bits of each element [39], which we know from Step 3 is also polynomial in the number of modes n. Therefore Step 4 can be computed in polynomial time.

The remaining steps consist of linear algebra operations (i.e., matrix inversion, matrix multiplication, and matrix transposition) which are all known to be polynomial in the size of the matrices considered and the bit length of each element [37].

We can therefore conclude that the entire algorithm for evaluating the exact PDF of the circuit is polynomial in the number of modes n. This means that all rational symplectic operations and all continuous displacements in the circuits of the form in Fig. 1 are strongly simulatable.

In the following subsection, we will demonstrate that our result can be extended to include adaptive circuits, when restricting to weak simulation.

B. Adaptive circuits are weakly simulatable

While in the previous subsection we demonstrated that the class of circuits shown in Fig. 1 are strongly simulatable, we will now demonstrate that this class can be extended to adaptive circuits when restricting to weak simulation. Adaptive quantum circuits contain intermediate measurements that can then either be used as parameters in future operations or can be used in a classical subroutine to decide if or where Gaussian operations are applied.

Formally, we can express adaptive circuits as beginning with a unitary operation $\hat{U}_0$, acted on the input state, followed by a series of K operations and measurements of the form [36]

$$\hat{U}_j(x_1, \ldots, x_j) M_{i_j(x_1,\ldots,x_{j-1})}(x_j), \tag{59}$$

where $j \in \{1, \ldots, K\}$. After applying the initial unitary operation $\hat{U}_0$, we measure the mode i_1, which gives the result x_1. Next, we act with the operator $\hat{U}_1(x_1)$ which is parameterized by the previous measurement result x_1. Following this, we measure mode $i_2(x_1)$. The mode which is measured, i.e., i_2, may also depend on the previous measurement result x_1. This continues up to an arbitrary number K of sequences of operations and measurements.

We now demonstrate that it is possible to sample from the circuits we have shown to be simulatable, even when incorporating adaptivity, in polynomial time. By the same logic of Theorem 5 of Ref. [36] we can consider each measurement as a single run of a reduced circuit. That is, starting with the first measurement $M_{i_1}(x_1)$, where we measure the i_1th mode, we simulate the Gaussian circuit $\hat{U}_1$ acting on the input states, followed by a measurement on the i_1th mode. We know, from the previous subsection, that we can calculate the PDF of this circuit. Hence, we can also sample a random measurement outcome of this circuit.

Next, we simulate a new circuit consisting of the operation

$$\hat{U}_1(x_1)\hat{U}_0 \tag{60}$$

using the measurement outcome of the previous simulation, to decide the Gaussian operation $\hat{U}(x_1)$. Measurement of i_1 and $i_2(x_1)$ will give a PDF of the form

$$f_{\text{PD}}(x_1, x_2) \tag{61}$$

for which we can input the simulated measurement outcome x_1 of the previous simulation, in order to get a PDF in terms of only x_2. Again, simulating a single measurement outcome of x_2 allows us to continue this procedure for the rest of the measurements of the circuit. Therefore the outcome of any adaptive Gaussian circuit, for which the nonadaptive circuits are strongly simulatable, is weakly simulatable.

As a complementary result—albeit, not necessary to reach the conclusions of this paper—we also show, in Appendix E, that it is also possible to efficiently simulate the outcomes of adaptive circuits with modulo homodyne measurement.

In order to prove the result in Sec. V, that the vacuum is a resource for quantum advantage, we must also show that adaptive circuits containing GKP-encoded Clifford operations are efficiently simulatable. In the following subsection, we demonstrate that this is indeed the case.

C. Clifford circuits are contained in the rational symplectic operations

We now demonstrate that GKP-encoded Clifford circuits are contained within the set of operations that we have shown to be efficiently simulatable. Qubit Clifford circuits consist of stabilizer qubit states, acted on by Clifford operations, followed by measurement in a stabilizer basis. Without loss of generality, we can consider these circuits to be initialized in 0 eigenstates of the Pauli $\hat{Z}$ operator, followed by Clifford operations and measured in the $\hat{Z}$ basis. Encoding these circuits into the GKP formalism gives circuits which consist of states initialized as 0-logical GKP states, acted on by encoded Clifford operations, followed by homodyne measurement in the position basis.

The Clifford operations acting over n modes can be described in terms of the following set of generators

$$\left\{e^{i\hat{q}_j^2/2}, \hat{F}_j, e^{-i\hat{q}_j\hat{p}_k} : j,k \in \{1,\dots,n\}\right\}, \tag{62}$$

where the Fourier transform is defined as

$$\hat{F}_j = e^{i\pi(\hat{q}_j^2+\hat{p}_j^2)/4}. \tag{63}$$

Note that in the case of the qubit encoding, it is not necessary to introduce phase-space displacements, as the required displacements can be produced by combinations of the symplectic operations.

Inspecting the symplectic form of each of these operators provides a description of the symplectic matrices of all Clifford group operations. Analyzing the generators of single-mode Clifford group operations we have

$$\hat{F} : \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{64}$$

$$e^{i\hat{q}_j^2/2} : \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \tag{65}$$

$$e^{-i\hat{q}_j\hat{p}_j} : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{66}$$

By considering any combination of these operations we will clearly obtain only integer matrices.

The set of qubit Clifford operations can therefore be described as at least a subset of integer symplectic operations. Integer symplectic operations are contained within the class of rational symplectic operations. Therefore, all encoded qubit Clifford circuits are simulatable by our method.

This concludes our analysis of the types of circuits which are simulatable with our method. That is, adaptive circuits consisting of input stabilizer GKP states, rational symplectic operations including GKP-encoded Clifford operations and real displacements, and homodyne measurement are all simulatable.

In the case of nonadaptive circuits, efficient strong simulation can be performed, whereby the PDF is evaluated efficiently. In the following subsection, we will apply this result to demonstrate the strong simulation of a simple circuit.

D. Simple example

We present an example of calculating the PDF of a simple circuit. We have specifically chosen a circuit that contains a vector $\vec{t}$ not equal to zero. We consider the circuit

$$\hat{U} = C_X F_1 P_1^2 F_1, \tag{67}$$

where P is the phase gate. Note that $F_1 P_1^2 F_1 = X_1$ which means we would expect the action of this operator on two encoded qubits states to be $C_X X_1 |0_{\mathrm{GKP}}\rangle|0_{\mathrm{GKP}}\rangle = |1_{\mathrm{GKP}}\rangle|1_{\mathrm{GKP}}\rangle$.

We can calculate its effect on the position measurement modes $\hat{q}_1$ and $\hat{q}_2$ as

$$\hat{Q}_1 = \hat{U}^\dagger \hat{q}_1 \hat{U} = -\hat{q}_1 + 2\hat{p}_1 \tag{68}$$

and

$$\hat{Q}_2 = \hat{U}^\dagger \hat{q}_2 \hat{U} = -\hat{q}_1 + 2\hat{p}_1 + \hat{q}_2, \tag{69}$$

from which we can inspect

$$A = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}. \tag{70}$$

We can explicitly write the matrix S as

$$S = \begin{pmatrix} A^T \\ \frac{1}{2}B^T \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}. \tag{71}$$

We then find the lowest common denominator of all the fractions of S. However, in this case, $\sigma = 1$ since we already have all integers. We can then calculate the Smith decomposition of $\sigma S = S$, which is given by

$$S = VDU \tag{72}$$

with

$$V = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$
$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{73}$$

We can also calculate the pseudoinverse of S as

$$S^+ = \begin{pmatrix} -\frac{1}{2} & -1 & \frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \tag{74}$$

from which we can calculate R as

$$R = S^+ V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{75}$$

and R^{-T} as

$$R^{-T} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{76}$$

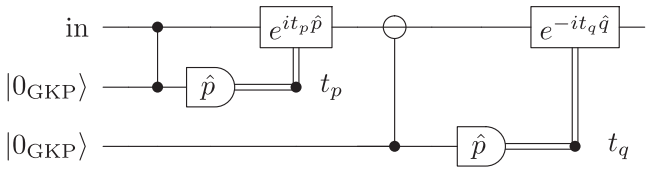

FIG. 2. Circuit gadget implementing $\hat{K}_{\mathrm{EC}}(\mathbf{t})$. Mode 1 is the top mode, which takes an input state and outputs a modified state. Modes 2 and 3 below are auxiliary modes which have a fixed input and once measured can be discarded. We use the notation of Ref. [40] whereby the controlled gate with the symbol $\ominus$ denotes the inverse of the SUM gate, namely, $e^{i\hat{q}_3\hat{p}_1}$. The measurement outcomes are denoted as t_p and t_q.

Furthermore we can find T as

$$\begin{aligned} T &= \frac{1}{2}R^T A B^T R \\ &= \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}2 & 2\\ 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \\ &= \begin{pmatrix}-1 & -1\\ -1 & -1\end{pmatrix}, \end{aligned} \tag{77}$$

which gives the vector $\vec{t}$ of the diagonal elements of T as

$$\vec{t} = (-1 \quad -1)^T. \tag{78}$$

This allows us to express the PDF, which is given by

$$f_{\mathrm{PD}}(\vec{x}) = \sum_{\vec{m}\in\mathbb{Z}^n} \delta(\vec{x} - \sqrt{\pi}(R^T)^{-1}(\vec{t} + 2\vec{m})). \tag{79}$$

The PDF can be expressed in terms of each vector element of $\vec{x}$ as

$$\begin{aligned} f_{\mathrm{PD}}(\vec{x}) = &\sum_{m_1,m_2\in\mathbb{Z}} \delta(x_1 + \sqrt{\pi} - 2\sqrt{\pi}m_1) \\ &\times \delta(x_2 + \sqrt{\pi} - 2\sqrt{\pi}m_2). \end{aligned} \tag{80}$$

This is equivalent to measuring $|1_{\mathrm{GKP}}\rangle$ in both modes, as we would expect, given the encoded circuit.

The results from this section provide us with the tools required to conclude the main result given in the following section, i.e., that the vacuum is the resource for quantum advantage in the context of this otherwise simulatable model.

V. VACUUM YIELDS QUANTUM ADVANTAGE

We now derive a notable consequence of the findings in the previous section, when combined with the results reported in Ref. [14]. There the circuit depicted in Fig. 2 is used as the central resource to achieve magic-state distillation, and in turn fault-tolerant universality of an otherwise simulatable (GKP-encoded) stabilizer computation. This circuit is composed of input GKP states $|0_{\mathrm{GKP}}\rangle$, an additional CV input state (possibly the vacuum), GKP-encoded Clifford operations, homodyne measurements, displacements, and classical feed-forward of measurement results (Fig. 2). Such a circuit gadget has the effect to implement the Kraus operator $\hat{K}_{\mathrm{EC}}(\mathbf{t}) = \hat{\Pi}_{\mathrm{GKP}}\hat{V}(-\mathbf{t})$, where $\hat{V}(-\mathbf{t}) = e^{it_q\hat{p}}e^{-it_p\hat{q}}$ and $\hat{\Pi}_{\mathrm{GKP}}$ is the projection operator onto the GKP subspace. This has the effect of "error correcting" the additional input state by projecting it onto the computational subspace of the GKP code. When the additional input state is the vacuum, this results in GKP-encoded magic states, except for a zero-measure set of the measurement outcomes t_q, t_p.

Performing this gadget across multiple modes with multiple additional vacuum states will provide a number of different states which each have a high fidelity to a magic H-type state.

This gadget is adaptive, and, once the auxiliary modes are measured, they can be discarded. Within the gadget, the measurement values are used to shift the input state in position and momentum. Furthermore, the measurement outcomes give an indication of which H-type state the output state is closest to. We can use these measurement results to decide a Gaussian operation which shifts the state close to the target $|\mathrm{H}_{\mathrm{GKP}}\rangle$ state.

If we have k copies of this gadget we will have produced k different states which each has a high fidelity to the $|\mathrm{H}_{\mathrm{GKP}}\rangle$ state. We can then apply the twirling operation to each state, which for qubits is a probabilistic Clifford operation (hence implementable by a probabilistic Gaussian operation), which projects each state onto the H axis of the Bloch sphere. These k states are nonidentical and so require adaptive depolarizing operations, which are again probabilistic Clifford operations, to make all these k states identical [41]. These adaptive probabilistic Clifford operations will adjust each state to match the state with the lowest fidelity to the target H state. These operations are adaptive since they require knowledge of each state, which can be constructed from the values of t_q, t_p measured for each gadget.

Now we have k identical copies of states which have fidelity above the threshold for magic state distillation. The magic state distillation algorithm [5,6] involves Clifford operations, adaptive Clifford operations, and probabilistic Clifford operations. Therefore, the total algorithm to produce a H-type state from the vacuum and GKP states requires the following resources: input GKP states, input vacuum states, adaptive Clifford operations, probabilistic Clifford operations, and homodyne measurements.

Now, consider the same procedure where instead of the vacuum state as the additional input, we have only 0-logical (or another stabilizer) GKP states.

We know from this work that circuits involving GKP states, adaptive Clifford operations, probabilistic Clifford operations, and homodyne measurements are weakly simulatable. Hence, the concatenation of all these operations, including the gadget in Fig. 2, belongs to the class of circuits that we have shown to be classically efficiently simulatable, if the supply of initial vacua is not included at the input of the circuit. Therefore, in the context of the model of Ref. [14], ideal stabilizer GKP states, homodyne measurement, displacements, and classical feed-forward of measurement outcomes are to be regarded as free operations, in the sense that they provide a simulatable model.

However, if we add the vacuum to this otherwise simulatable model, we find that it is promoted to universal quantum computation. We can thus conclude that the vacuum can be considered a resource for quantum advantage in this model. Note that this conclusion was not possible to draw from Ref. [14] solely, because the model considered, even

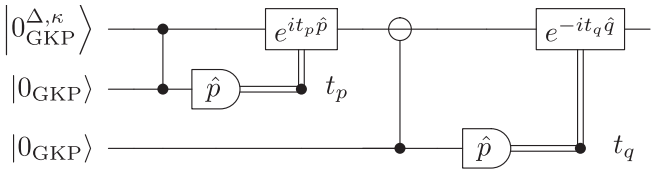

FIG. 3. The error-correcting circuit from Fig. 2 implementing $\hat{K}_{\mathrm{EC}}(\mathbf{t})$, acting on an additional input nonideal GKP state parameterized by Δ, κ. Note that the control gate with the symbol $\ominus$ at the target is the inverse of the SUM gate, namely, $e^{i\hat{q}_3\hat{p}_1}$ [40].

excluding the additional vacuum state, was not proven to be classically efficiently simulatable therein.

The intuition behind this result is that, as already noticed in Ref. [14], the interaction with the vacuum through an entangling operation takes the GKP states outside of the computational subspace spanned by the GKP logical codewords. Measurements followed by feed-forward and displacement project the unmeasured system back onto the GKP-encoded computational subspace, now in a magic state (apart from measurement outcomes which represent a zero-measure set in the set of all possible real measurement outcomes).

In the following section, we will extend this argument to demonstrate that realistic GKP states can also be considered a resource for quantum advantage in the context of this model.

VI. REALISTIC GKP STATES ARE A RESOURCE FOR QUANTUM ADVANTAGE

Following the result of the previous section, we now demonstrate that realistic GKP states can also be considered a resource for quantum advantage. Using a realistic (i.e., finitely squeezed) GKP state as the additional input state of the gadget in Fig. 1, instead of the vacuum, also produces a magic state with fixed probability, dependent on the squeezing of the realistic GKP state.

We now explicitly compute the outcome of the circuit in Fig. 3. Here the additional input state, to be combined with ideal GKP states, is not the vacuum state, but instead a GKP state with variable squeezing. Note that the case of vacuum is reobtained with a very good approximation by taking the limit of no squeezing in the GKP state. We will then compute the fidelity of the output state with the closest magic $|H\rangle$-type state.

The nonideal GKP state can be defined as [12]

$$\psi_{0,L(\Delta,\kappa)}(x) = \langle x|0^{\Delta,\kappa}_{\mathrm{GKP}}\rangle \times \propto \sum_{s\in\mathbb{Z}} e^{-2\kappa^2 s^2\pi} e^{-(x-2s\sqrt{\pi})^2/2\Delta^2}. \tag{81}$$

The output of the circuit of Fig. 3 will be a state of the form

$$|\psi\rangle \propto \hat{\Pi}_{\mathrm{GKP}} e^{it_q\hat{p}} e^{-it_p\hat{q}} |0^{\Delta,\kappa}_{\mathrm{GKP}}\rangle, \tag{82}$$

which can be expressed in terms of the coefficients

$$c_0 = \langle 0_{\mathrm{GKP}}|e^{it_q\hat{p}} e^{-it_p\hat{q}}|0^{\Delta,\kappa}_{\mathrm{GKP}}\rangle,$$
$$c_1 = \langle 1_{\mathrm{GKP}}|e^{it_q\hat{p}} e^{-it_p\hat{q}}|0^{\Delta,\kappa}_{\mathrm{GKP}}\rangle, \tag{83}$$

which can be normalized as

$$\bar{c}_0 = \frac{c_0}{\sqrt{c_0^2 + c_1^2}},$$
$$\bar{c}_1 = \frac{c_1}{\sqrt{c_0^2 + c_1^2}}. \tag{84}$$

The fidelity of this state with each of the $|H\rangle$-type states can be calculated in terms of these normalized coefficients. That is, for each $|H\rangle$-type state $|H\rangle = a_0|0\rangle + a_1|1\rangle$ we calculate the fidelity

$$F(|H\rangle, |\psi\rangle) = \left|\langle H| \frac{1}{\sqrt{c_0^2 + c_1^2}}(c_0|0\rangle + c_1|1\rangle)\right|^2 = \frac{|a_0c_0 + a_1c_1|^2}{|c_0^2 + c_1^2|}. \tag{85}$$

The resulting fidelity of the output state, given the input GKP state with various levels of squeezing Δ, is shown in Fig. 4. The figure ordering should then be maintained as it is now.

The PDF of the measurement outcomes can be calculated, as in [14], as $f_{\mathrm{PD}}(\mathbf{t}) \propto c_0^2 + c_1^2$, which is then normalized over a region periodic in $2\sqrt{\pi}$ in both t_q and t_p. The probability of obtaining a state with fidelity higher than a certain threshold F^* can then be calculated numerically by calculating the fidelities for each value of t_q, t_p and integrating over the $f_{\mathrm{PD}}(\mathbf{t})$ for those values at which $F > F*$.

In Fig. 5 we plot the probability of obtaining a magic $|H\rangle$-type state in the output of the circuit in Fig. 3 above a given threshold fidelity, for different values of the squeezing parameter Δ.

We see that the squeezing parameter in the auxiliary state of the circuit in Fig. 3 inversely quantifies the resourcefulness of the auxiliary state.

This result can be understood by interpreting the vacuum as the zero-squeezing limit of a GKP state. The zero-squeezing limit corresponds to setting $\Delta = \kappa = 1$. In this case, we obtain from the expression of the finitely squeezed GKP state in the position representation

$$|0^{\Delta,\kappa}_{\mathrm{GKP}}\rangle \propto \sum_{s\in\mathbb{Z}} \int dq e^{-2s^2\pi} e^{-(q-2s\sqrt{\pi})^2/2}|q\rangle. \tag{86}$$

Then, calculating the fidelity with the vacuum state, $|\emptyset\rangle = \pi^{-1/4}\int dq e^{-q^2/2}|q\rangle$ gives

$$\left|\langle\emptyset|0^{\Delta,\kappa}_{\mathrm{GKP}}\rangle\right|^2 = 0.999993. \tag{87}$$

This high fidelity value explains in particular why, using the zero-squeezing limit of a GKP state, we obtain the plot in Fig. 4, third panel, that is indistinguishable for the naked eye from that of Ref. [14] obtained using input vacuum.

This allows us to interpret the value Δ as interpolating from a free state, the ideal 0-logical GKP state, corresponding to infinite squeezing, and with which no magic state can be generated, to a maximally resourceful state, namely, the vacuum, corresponding to zero squeezing.

We can therefore conclude that in the context of this model, realistic GKP states are also resourceful for quantum advantage. The realistic GKP states required for magic state

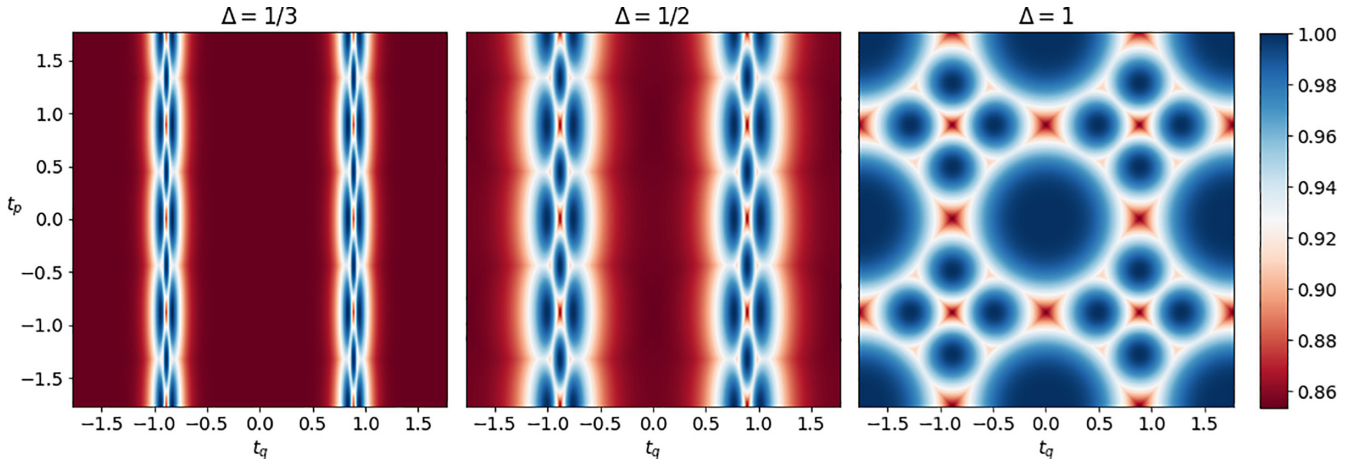

FIG. 4. Fidelity of the output state of the error correcting circuit in Fig. 3 with the closest H-type magic state, for the various possible measurement outcomes t_q and t_p. Note that in the limit $\Delta \to 1$ the finitely squeezed GKP state at the input in Fig. 3 is approximately equivalent to the vacuum state, yielding agreement of panel 3 with Ref. [14].

distillation can have any noninfinite squeezing; in other words, there is no threshold required to distill a magic state.

VII. CONCLUSIONS

First, we have demonstrated that circuits with input GKP states acted on with arbitrary displacements and rational [42] symplectic operations, and measured with homodyne detection are classically efficiently simulatable. This result extends the classes of circuits previously known to be simulatable and can be understood as a CV analog to the Gottesman-Knill theorem [2–4]. The Gottesman-Knill theorem provides a method to simulate circuits involving qubits initialized in ideal input qubit stabilizer states acted on by Clifford operations and measured in the computational basis. Meanwhile, our result provides a method to simulate ideal GKP states acted on by Gaussian operations and measured with homodyne detection.

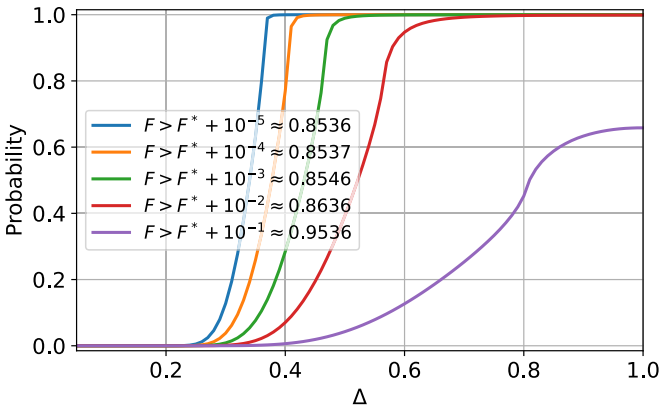

FIG. 5. Probability of producing, as output of the circuit in Fig. 3, a magic state $|\psi\rangle$ with a given fidelity $F = |\langle H|\psi\rangle|^2$ to the nearest target magic state $|H\rangle$ when the additional input state is a GKP state with squeezing level $\Delta = \kappa$. Note that in the other modes we still assume ideal GKP states in logical state 0. Also note that $\Delta \to 1$ is approximately equivalent to the vacuum state. $F^* = \frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.8536$ is the threshold for magic state distillation [6,14].

Second, this result in combination to those of Ref. [14] leads to the counterintuitive interpretation of the vacuum, or realistic GKP states with any finite squeezing, as a resource for universality. Here we can draw an analogy to DV magic state distillation [5], where it is known that "noisy" pure states that are close to (but not exactly) the points corresponding to the stabilizer states on the Bloch sphere act as a resource for universal QC [6]. Similarly, in the circuits we have considered, introducing noise in the form of vacuum or realistic GKP states promotes the circuit class we consider to universality by allowing one to produce and distill magic states.

The question of whether realistic GKP states in all modes (possibly with different squeezing levels), combined with Gaussian operations, yield a simulatable or universal model is still open. Our analysis in Sec. VI, showing that a combination of ideal and realistic GKP states yields a universal model, can be seen as a first attempt to provide an answer to this question. Therein, squeezing quantifies inversely the resourcefulness of finitely squeezed GKP states, when these are combined with infinitely squeezed GKP states, in terms of their ability of producing output GKP magic states. This leads us to speculate that, even in a more realistic model with input highly squeezed GKP states, the vacuum will retain its character as a resource, boosting the magic content at the output of the circuit.

Our work also opens the question as to whether the methodology introduced to compute the PDF, based on imposing stabilizer conditions, can be also used for other types of circuits, for which input states admit a stabilizer representation.

ACKNOWLEDGMENTS

We acknowledge useful discussions with Laura García-Álvarez and Ben Q. Baragiola. G.F. and C.C. acknowledge support from the Vetenskapsrådet (Swedish Research Council) Grant QuACVA and the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT).

APPENDIX A: THE SET OF RATIONAL MATRICES IS DENSE IN THE REALS

In this Appendix, we will prove that $\mathrm{Sp}(2n,\mathbb{Q})$ is dense on $\mathrm{Sp}(2n,\mathbb{R})$. This is equivalent [43] to showing that the closure of the rational symplectic group $\mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q}))$ is the real symplectic group $\mathrm{Sp}(2n,\mathbb{R})$, i.e., $\mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q}))=\mathrm{Sp}(2n,\mathbb{R})$.

We provide an overview of the steps of this proof taken from Ref. [44]. First note that the symplectic group defined over any field $\mathrm{Sp}(2n,\mathbb{F})$ is generated by the set of symplectic transvections, $H_{\mathbb{F}}$ [45]. This set consists of maps $\xi_{\alpha,\vec{u}}$ with $\alpha\in\mathbb{F}$ and $\vec{u}\in\mathbb{F}^2$, which transforms any arbitrary vector $\vec{v}\in\mathbb{F}^{2n}$ as

$$\xi_{\alpha,\vec{u}}(\vec{v})=\vec{v}+\alpha B(\vec{v},\vec{u})\vec{u}, \tag{A1}$$

where B is the alternating bilinear form [44,46].

The set of generators of the rational symplectic group can therefore be written as

$$H_{\mathbb{Q}}=\{\xi_{\alpha,\vec{u}}:\alpha\in\mathbb{Q},\vec{u}\in\mathbb{Q}^{2n}\}, \tag{A2}$$

while the set of generators of the real symplectic group can be written as

$$H_{\mathbb{R}}=\{\xi_{\alpha,\vec{u}}:\alpha\in\mathbb{R},\vec{u}\in\mathbb{R}^{2n}\}. \tag{A3}$$

For any chosen generator in the set of generators for the real symplectic group, $\xi_{\alpha,\vec{u}}\in H_{\mathbb{R}}$, it is possible to find an arbitrarily close generator from the set of generators of the rational symplectic group $\xi_{\alpha',\vec{u}'}\in H_{\mathbb{Q}}$. We can demonstrate this by evaluating the norm of the difference of these generators [44] and showing that it is possible to find for any $\xi_{\alpha,\vec{u}}$ and $\xi_{\alpha',\vec{u}'}$ a norm such that

$$||\xi_{\alpha',\vec{u}'}(\vec{v})-\xi_{\alpha,\vec{u}}(\vec{v})||=||\alpha' B(\vec{v},\vec{u}')\vec{u}'-\alpha B(\vec{v},\vec{u})\vec{u}||\leqslant\epsilon. \tag{A4}$$

Choosing $\vec{u}'=\vec{u}+\vec{u}_\epsilon$ and $\alpha'=\alpha+\alpha_\epsilon$ we can make use of the triangle inequality [47] to find

$$\begin{aligned}
&||\xi_{\alpha',\vec{u}'}(\vec{v})-\xi_{\alpha,\vec{u}}(\vec{v})||\\
&\quad=||\alpha' B(\vec{v},\vec{u}+\vec{u}_\epsilon)(\vec{u}+\vec{u}_\epsilon)-\alpha B(\vec{v},\vec{u})\vec{u}||\\
&\quad=||(\alpha+\alpha_\epsilon)(B(\vec{v},\vec{u}_\epsilon)+B(\vec{v},\vec{u}))(\vec{u}+\vec{u}_\epsilon)-\alpha B(\vec{v},\vec{u})\vec{u}||\\
&\quad\leqslant|\alpha B(\vec{v},\vec{u}_\epsilon)|\cdot||\vec{u}||+|\alpha B(\vec{v},\vec{u}_\epsilon)|\cdot||\vec{u}_\epsilon||\\
&\qquad+|\alpha B(\vec{v},\vec{u})|\cdot||\vec{u}_\epsilon||+|\alpha_\epsilon B(\vec{v},\vec{u}_\epsilon)|\cdot||\vec{u}||\\
&\qquad+|\alpha_\epsilon B(\vec{v},\vec{u})|\cdot||\vec{u}||+|\alpha_\epsilon B(\vec{v},\vec{u}_\epsilon)|\cdot||\vec{u}_\epsilon||\\
&\qquad+|\alpha_\epsilon B(\vec{v},\vec{u})|\cdot||\vec{u}_\epsilon||.
\end{aligned} \tag{A5}$$

Note that we can write $\vec{u}_\epsilon=\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}$ where $\vec{u}_\epsilon^{\,\mathbb{1}}$ is the unit vector containing the direction of $\vec{u}_\epsilon$, $|\vec{u}_\epsilon^{\,\mathbb{1}}|=1$, and the magnitude $\epsilon_{\vec{u}}\in\mathbb{R}$ is small, $\epsilon_{\vec{u}}\ll 1$.

This allows us to write

$$B(\vec{v},\vec{u}_\epsilon)=\epsilon_u B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big). \tag{A6}$$

Therefore, for any chosen $7\epsilon\in\mathbb{R}$, we can ensure that the distance is less than 7ϵ by ensuring each term is smaller than ϵ,

$$\big|\alpha B\big(\vec{v},\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\leqslant\epsilon, \tag{A7}$$

$$\big|\alpha B\big(\vec{v},\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}||\leqslant\epsilon, \tag{A8}$$

$$|\alpha B(\vec{v},\vec{u})|\cdot\big|\big|\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big|\big|\leqslant\epsilon, \tag{A9}$$

$$\big|\alpha_\epsilon B\big(\vec{v},\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\leqslant\epsilon, \tag{A10}$$

$$|\alpha_\epsilon B(\vec{v},\vec{u})|\cdot||\vec{u}||\leqslant\epsilon, \tag{A11}$$

$$\big|\alpha_\epsilon B\big(\vec{v},\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot\big|\big|\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big|\big|\leqslant\epsilon, \tag{A12}$$

$$|\alpha_\epsilon B(\vec{v},\vec{u})|\cdot\big|\big|\epsilon_u\vec{u}_\epsilon^{\,\mathbb{1}}\big|\big|\leqslant\epsilon, \tag{A13}$$

which is equivalent to

$$\big|\epsilon_u\alpha B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\leqslant\epsilon, \tag{A14}$$

$$\big|\alpha\epsilon_u B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot\epsilon_u\leqslant\epsilon, \tag{A15}$$

$$|\alpha B(\vec{v},\vec{u})|\epsilon_u\leqslant\epsilon, \tag{A16}$$

$$\big|\alpha_\epsilon\epsilon_u B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\leqslant\epsilon, \tag{A17}$$

$$|\alpha_\epsilon B(\vec{v},\vec{u})|\cdot||\vec{u}||\leqslant\epsilon, \tag{A18}$$

$$\big|\alpha_\epsilon\epsilon_u B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot\epsilon_u\leqslant\epsilon, \tag{A19}$$

$$|\alpha_\epsilon B(\vec{v},\vec{u})|\cdot\epsilon_u\leqslant\epsilon. \tag{A20}$$

These can be rearranged into conditions

$$\epsilon_u\leqslant\epsilon/\big[\big|\alpha B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\big], \tag{A21}$$

$$\epsilon_u^2\leqslant\epsilon/\big|\alpha B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|, \tag{A22}$$

$$\epsilon_u\leqslant\epsilon/|\alpha B(\vec{v},\vec{u})|, \tag{A23}$$

$$\alpha_\epsilon\epsilon_u\leqslant\epsilon/\big[\big|B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\big], \tag{A24}$$

$$\alpha_\epsilon\leqslant\epsilon/[|B(\vec{v},\vec{u})|\cdot||\vec{u}||], \tag{A25}$$

$$\alpha_\epsilon\epsilon_u^2\leqslant\epsilon/\big|B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|, \tag{A26}$$

$$\alpha_\epsilon\epsilon_u\leqslant\epsilon/|B(\vec{v},\vec{u})| \tag{A27}$$

and can be further simplified to the conditions

$$\epsilon_u\leqslant\epsilon/\big[\big|\alpha B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|\cdot||\vec{u}||\big], \tag{A28}$$

$$\epsilon_u\leqslant\sqrt{\epsilon/\big|\alpha B\big(\vec{v},\vec{u}_\epsilon^{\,\mathbb{1}}\big)\big|}, \tag{A29}$$

$$\epsilon_u\leqslant\epsilon/|\alpha B(\vec{v},\vec{u})|, \tag{A30}$$

$$\alpha_\epsilon\leqslant 1/\alpha, \tag{A31}$$

$$\alpha_\epsilon\leqslant\epsilon/[|B(\vec{v},\vec{u})|\cdot||\vec{u}||]. \tag{A32}$$

For any $\alpha,\vec{u},\vec{v}$ it is always possible to find $\alpha',\vec{u}'$ for which $\alpha_\epsilon,\epsilon_u\in\mathbb{R}$ are arbitrarily close to 0 such that all these inequalities hold. This follows from the fact that the rational numbers are dense on the reals [48].

We can therefore say that $H_{\mathbb{Q}}$ is dense on the set $H_{\mathbb{R}}$, which can be expressed in terms of the closure of the set of rational generators $\mathrm{cl}(H_{\mathbb{Q}})=H_{\mathbb{R}}$.

Furthermore, we know that $H_{\mathbb{Q}}\subseteq\mathrm{Sp}(2n,\mathbb{Q})$, which implies that [43] $\mathrm{cl}(H_{\mathbb{Q}})\subseteq\mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q}))$ and hence the

generators of $H_{\mathbb{R}}$ are all members of the closure of the rational symplectic group; i.e., $H_{\mathbb{R}} \subseteq \mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q}))$. Since all the generators of $\mathrm{Sp}(2n,\mathbb{R})$ are members of $\mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q}))$, then $\mathrm{Sp}(2n,\mathbb{R}) \subseteq \mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q}))$.

Finally, using the fact that $\mathrm{Sp}(2n,\mathbb{Q}) \subseteq \mathrm{Sp}(2n,\mathbb{R})$, we have $\mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q})) \subseteq \mathrm{Sp}(2n,\mathbb{R})$. This means that $\mathrm{cl}(\mathrm{Sp}(2n,\mathbb{Q})) = \mathrm{Sp}(2n,\mathbb{R})$ and the symplectic group over the rationals is dense on the symplectic group over the reals.

APPENDIX B: SOLUTION TO THE CONSTRAINED LINEAR EQUATION

In this Appendix, we solve the constrained equation introduced in Sec. IV, which provides the solution for the set of allowed points of the PDF. Specifically, we find the solution of Eq. (30) given the constraint of Eq. (27):

$$\begin{aligned} &\sqrt{\pi}\vec{l}^T\vec{x} - \tfrac{1}{2}\pi\vec{l}^T AB^T\vec{l} - \sqrt{\pi}\vec{l}\cdot\vec{c} = 0 \mod 2\pi, \\ &\text{s.t.} \quad \begin{aligned} (A^T\vec{l})_k &= 0 \mod 1, \\ (B^T\vec{l})_k &= 0 \mod 2. \end{aligned} \end{aligned} \tag{B1}$$

To solve this equation, we begin by identifying a method to evaluate the possible values of the vector $\vec{l}$.

First, in Sec. B 1, we express the constraint as an overdetermined system of linear equations, that has solutions dependent on a projection matrix $1 - SS^+$. In Sec. B 2 we demonstrate that this projection matrix is rational, given that the symplectic matrix is rational. Together, these results allow us to provide the solutions to $\vec{l}$ in Sec. B 3. Then in Sec. B 4 we demonstrate that given the solutions of $\vec{l}$, we can express the constrained equation in Eq. (B1) as set of unconstrained linear equations. Finally, in Sec. B 5 we provide the solution of these unconstrained equations, which are also the solutions to the constrained equation given in Eq. (B1).

1. Expressing the constraint as a linear system of equations

We first identify a method to express the constraining terms defined in Eq. (B1) as a system of overdetermined linear equations. We demonstrate that the solutions of $\vec{l}$ can be expressed in terms of the pseudoinverse of a matrix S, which is dependent on A and B, and a new vector $\vec{b}$, which will be solved in the following subsections. To begin, we combine the constraining terms into one equation of the form

$$\begin{pmatrix} A^T \\ B^T \end{pmatrix}\vec{l} = \begin{pmatrix} 0 \mod 1 \\ \vdots \\ 0 \mod 1 \\ 0 \mod 2 \\ \vdots \\ 0 \mod 2 \end{pmatrix}. \tag{B2}$$

We now introduce a matrix S which is defined in terms of the two matrices A and B as

$$S = \begin{pmatrix} A^T \\ \frac{1}{2}B^T \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}\bar{S}, \tag{B3}$$

where we also introduce the matrix $\bar{S}$, which is the transpose of the first n rows of the symplectic matrix M,

$$\bar{S} = \begin{pmatrix} A^T \\ B^T \end{pmatrix}. \tag{B4}$$

We introduce the vector $\vec{b}$ which is a $2n$-vector of integers. This allows us to express the constraint on $\vec{l}$ as

$$S\vec{l} = \vec{b}. \tag{B5}$$

This gives an overdetermined system of linear equations and does not necessarily always have a solution. Whether the system has solutions or not depends on which integers are chosen in $\vec{b}$.

The columns of S are linearly independent. This can be seen by considering the fact that the determinant of the symplectic matrix is $\det M = 1$ which means that it has linearly independent rows [49]. Hence, the matrix $\bar{S}$ will have linearly independent columns. Furthermore, the matrix which converts $\bar{S}$ to S is a full rank $2n \times 2n$ matrix. Hence, the rank of S will be the same as the rank of $\bar{S}$; i.e., it will have rank n which means the columns must be linearly independent [34,50].

We can express the solutions of $\vec{l}$ in terms of the Moore-Penrose pseudoinverse [29–31], which is a generalization of the matrix inverse. For any matrix S there exists a pseudoinverse S^+ even if the matrix does not have a true inverse. A $2n \times n$ rectangular matrix S with linearly independent columns has rank n [50]. The pseudoinverse S^+ is defined such that $S^+S = \mathbb{1}$. The pseudoinverse of S can be found in terms of the pseudoinverse of the rank n matrix $\bar{S}$ as [51]

$$S^+ = \bar{S}^+\begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}^+ = \bar{S}^+\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \tag{B6}$$

where we have used the fact that the pseudoinverse of a nonsingular matrix is equal to its inverse [31].

This gives potential solutions of $\vec{l}$ in the form

$$\vec{l} = S^+\vec{b}, \tag{B7}$$

but if this system is unsolvable for a given $\vec{b}$ then the pseudoinverse will not provide a valid solution to $\vec{l}$. For it to be valid it must satisfy the original equation [31]

$$S\vec{l} = SS^+\vec{b} = \vec{b}, \tag{B8}$$

which gives the constraint on the integers $\vec{b}$ as

$$SS^+\vec{b} = \vec{b}. \tag{B9}$$

We can write this constraint as

$$(SS^+ - 1)\vec{b} = 0 \quad \Rightarrow \quad (1 - SS^+)\vec{b} = 0. \tag{B10}$$

Finding the values of $\vec{b}$ which satisfy this equation also informs us of all the possible choices of $\vec{l}$ which satisfy the constraining equation. This is equivalent to finding the eigenvectors of the projection matrix $1 - SS^+$ which have eigenvalues equal to zero. To solve this equation, we will demonstrate that the projection matrix $1 - SS^+$ has a convenient eigenvalue decomposition, provided that it is a rational matrix. We first prove that this matrix is rational in the following section, given that the symplectic matrix is rational, and then we will proceed to find its eigenvectors.

2. The projector is rational

In this subsection, we will analyze the $2n \times 2n$ projection matrix $1 - SS^+$ and demonstrate that it contains all rational elements. We then use the expression to find the pseudoinverse of a matrix with linearly independent columns, to identify the pseudoinverse of $\bar{S}$ as [31]

$$\bar{S}^+ = (\bar{S}^T \bar{S})^{-1} \bar{S}^T. \tag{B11}$$

Note that $1 - SS^+$ will be rational if SS^+ is rational. Inspecting

$$\bar{S}^+ = (AA^T + BB^T)^{-1}(A \quad B), \tag{B12}$$

we can see that as long as A, B are rational, the matrix $(AA^T + BB^T)$ will be rational. The inverse of a rational matrix will also be rational, and so $\bar{S}^+$ will also be rational. Therefore we know S^+ is rational. This also implies that $1 - SS^+$ is a matrix of rational elements.

3. Evaluation of the allowed parameters provided by the constraint

As shown in the previous subsection, the matrix $1 - SS^+$ consists of all rational elements. In this subsection, we will demonstrate that it has an eigenvector decomposition of the form

$$1 - SS^+ = V \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{1} \end{pmatrix} V^{-1}, \tag{B13}$$

where V is a unimodular matrix, also known as a unit matrix [31]. The definition of a unimodular matrix is one that contains all integers and has determinant 1 [32]. This decomposition then be used to find the solutions of $\vec{b}$ in Eq. (B10) and therefore also $\vec{l}$ in Eq. (B7).

To find such V for a given matrix $1 - SS^+$ we can first find the Smith decomposition of the matrix σS. We use the integer σ to multiply every element of matrix S to an integer. The integer σ can be found to be the lowest common multiple of all of the denominators of S. The Smith decomposition is given by

$$\sigma S = VDU \quad \Rightarrow \quad S = \sigma^{-1} VDU, \tag{B14}$$

where V is a $2n \times 2n$ unimodular matrix, U is a $n \times n$ unimodular matrix. D is a diagonal $2n \times n$ matrix which has the same rank as S, which has rank n. The Smith decomposition algorithm will order the diagonal elements of D in descending order. We can therefore assume that D has n nonzero entries along the diagonal. The remaining entries in the matrix D will be 0.

Furthermore, we can identify the pseudoinverse of S as

$$S^+ = \sigma U^{-1} D^+ V^{-1}, \tag{B15}$$

where we have used that the pseudoinverse of the product of two matrices AB is $(AB)^+ = B^+ A^+$ [52]. This gives a convenient expression for SS^+

$$SS^+ = VDD^+ V^{-1} \tag{B16}$$

and the projector

$$1 - SS^+ = 1 - VDD^+ V^{-1} = V(1 - DD^+)V^{-1}. \tag{B17}$$

As D is a matrix of integer entries along the diagonal, its pseudoinverse, D^+, can be found by taking the inverse of each nonzero element along the diagonal and then transposing [31]. Therefore we can find DD^+ by inspecting its form,

$$\begin{pmatrix} D_{1,1} & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \dots & D_{n,n} \\ 0 & \dots & 0 \\ 0 & \vdots & 0 \\ 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} D_{1,1}^{-1} & \dots & 0 & 0 & \dots & 0 \\ 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & \dots & D_{n,n}^{-1} & 0 & \dots & 0 \end{pmatrix}, \tag{B18}$$

which means that

$$DD^+ = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & 0 \end{pmatrix}. \tag{B19}$$

From this, we can immediately identify

$$1 - DD^+ = \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{1} \end{pmatrix}, \tag{B20}$$

and we can express the projector as

$$1 - SS^+ = 1 - VDD^+ V^{-1} = V \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{1} \end{pmatrix} V^{-1} \tag{B21}$$

as we had anticipated. This form is an eigenvalue decomposition of the matrix $1 - SS^+$. The integer eigenvectors of $1 - SS^+$ are given as the columns of V. The first n columns correspond to eigenvectors with eigenvalue 0 and the remaining n columns correspond to eigenvectors with eigenvalue 1. We can therefore construct any integer eigenvector with eigenvalue 0 as [34]

$$\vec{b} = V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} \vec{m}. \tag{B22}$$

Note that in general the decomposition matrices U, V of the Smith decomposition are not necessarily unique. However, the complete set of eigenvectors $\vec{b}$ will be the same regardless of which decomposition matrix V is found [34].

The allowed values of $\vec{l}$ can therefore be calculated in terms of the values of $\vec{b}$ using Eq. (B7), which can be expressed in terms of the n-vector $\vec{m}$ as

$$\vec{l} = S^+ \vec{b} = S^+ V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} \vec{m} = R\vec{m}, \tag{B23}$$

where we have introduced the $n \times n$ matrix R as

$$R = S^+ V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix}. \tag{B24}$$

Given these solutions for the vector $\vec{l}$, we can solve the constrained equation, given in Eq. (B1), to find the allowed values of $\vec{x}$.

4. Expressing the constrained equation as a set of linear equations

We then would like to solve the equation

$$\sqrt{\pi}\vec{l}^T \vec{x} - \tfrac{1}{2}\pi \vec{l}^T AB^T \vec{l} - \sqrt{\pi}\vec{l} \cdot \vec{c} = 0 \mod 2\pi, \tag{B25}$$

for which we can, without loss of generality, set $\vec{c} = 0$ (because we can consider a different $\vec{c}$ to be a change of variables in $\vec{x}$) and it becomes

$$\vec{l}^T\left(\frac{1}{\sqrt{\pi}}\vec{x} - \frac{1}{2}AB^T\vec{l}\right) = 0 \mod 2. \tag{B26}$$

We consider the term

$$\tfrac{1}{2}\vec{l}^T AB^T\vec{l} = \vec{m}^T T\vec{m}, \tag{B27}$$

where we have defined the $n \times n$ matrix

$$\begin{aligned} T &= \frac{1}{2}R^T AB^T R \\ &= \frac{1}{2}(\mathbb{1} \quad 0)V^T(S^+)^T AB^T S^+ V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix}. \end{aligned} \tag{B28}$$

The matrix T will always give integer values. For proof of this consider the following. We know from Eq. (B9) and Eq. (B22) that

$$SS^+V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix}\vec{m} = V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix}\vec{m}, \tag{B29}$$

which must be true for all integer vectors $\vec{m}$. As a consequence we have

$$SS^+V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix} = V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix} \Rightarrow \begin{pmatrix}A^T\\\frac{1}{2}B^T\end{pmatrix}S^+V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix} = V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix}. \tag{B30}$$

We know that

$$S^+V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix} \tag{B31}$$

is an $n \times n$ matrix, so we must have

$$\begin{aligned} A^T S^+V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix} &= V^{(11)}, \\ \frac{1}{2}B^T S^+V\begin{pmatrix}\mathbb{1}\\0\end{pmatrix} &= V^{(21)}. \end{aligned} \tag{B32}$$

This means that from Eq. (B28) the matrix T can be succinctly written as

$$T = V^{(11)T}V^{(21)}. \tag{B33}$$

The matrix V is unimodular meaning that it consists of all integer elements. The block matrices $V^{(21)}, V^{(11)}$ must also be integer and the multiplication of two integer matrices is also integer. Hence, T is an integer matrix.

We can now solve Eq. (B26) which constrains the values of $\vec{x}$, which can be written in terms of Eq. (B23) and Eq. (B27) as

$$\frac{1}{\sqrt{\pi}}\vec{m}^T R^T\vec{x} - \vec{m}^T T\vec{m} = 0 \mod 2. \tag{B34}$$

This must be true for any chosen $\vec{m}$. We introduce the length-n basis vector $\vec{e}^{(j)}$ which has zero in all elements, except at element j for which it is 1,

$$\vec{e}^{(j)} = (0_1, \ldots, 0_{j-1}, 1_j, 0_{j+1}, \ldots, 0_n)^T. \tag{B35}$$

Choosing $\vec{m} = m_j\vec{e}^{(j)}$, for any integer $m_j \in \mathbb{Z}$, gives an equation of the form

$$\frac{1}{\sqrt{\pi}}m_j(R^T\vec{x})_j - m_j^2 T_{jj} = 0 \mod 2. \tag{B36}$$

The vector $\vec{m} = m_j\vec{e}^{(j)}$ will produce constraints for different choices of $m_j \in \{1, 2, 3, \ldots\}$ as

$$\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j - T_{jj} = 0 \mod 2, \tag{B37}$$

$$2\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j - 4T_{jj} = 0 \mod 2, \tag{B38}$$

$$3\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j - 9T_{jj} = 0 \mod 2, \tag{B39}$$

continuing for all integers m_j. We know that T_{jj} is an integer and so we inspect two cases. In the first case we consider when T_{jj} is an even integer. These constraints can then always be simplified to

$$m_j\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j = 0 \mod 2. \tag{B40}$$

Then using the fact that this must hold for any choice of m_j we identify that any integer m_j multiplied by $\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j$ is an even integer. This means that for even T_{jj} we have

$$\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j = 0 \mod 2. \tag{B41}$$

In the second case, for which T_{jj} is odd and so $T_{j,j} \mod 2 = 1$, the constraints can be simplified to

$$\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j - 1 = 0 \mod 2, \tag{B42}$$

$$2\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j = 0 \mod 2, \tag{B43}$$

$$3\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j - 1 = 0 \mod 2, \tag{B44}$$

which will be satisfied for all choices of m_j if and only if $\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j$ is an odd number. Hence, for odd T_{jj} we can write

$$\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j = 1 \mod 2. \tag{B45}$$

Combining these two cases we can express the two relations, which depend on whether T_{jj} is odd, i.e., $T_{jj} \mod 2 = 1$ or even, i.e., $T_{jj} \mod 2 = 0$, as

$$\frac{1}{\sqrt{\pi}}(R^T\vec{x})_j = T_{j,j} \mod 2. \tag{B46}$$

We can also attempt to select for combinations of these basis vectors. For example, we can choose $\vec{m} = m_i\vec{e}^{(i)} + m_j\vec{e}^{(j)}$ for different integers $m_i, m_j \in \mathbb{Z}$. These will give constraints of the form

$$\begin{aligned} \frac{1}{\sqrt{\pi}}m_i(R^T\vec{x})_i + \frac{1}{\sqrt{\pi}}m_j(R^T\vec{x})_j - m_j^2T_{jj} \\ - m_i^2T_{ii} - 2m_im_jT_{ij} \quad = 0 \mod 2, \end{aligned} \tag{B47}$$

but because we know that every element $T_{i,j}$ is an integer, this is equivalent to linear combinations of the constraints with a single $m_j \neq 0$. We already know that the constraints with

single $m_j \neq 0$ are satisfied, and so adding combinations of such constraints does not constrain the allowed values of $\vec{x}$ any further.

A valid solution can be found by solving

$$\frac{1}{\sqrt{\pi}} R^T \vec{x} = \vec{t} \mod 2, \tag{B48}$$

where $\vec{t}$ is an integer vector of the diagonal elements of T. Note that R^T is a $n \times n$ matrix given by

$$R^T = (\mathbb{1} \quad 0) V^T (S^+)^T. \tag{B49}$$

This system of equations will have infinite solutions. However, if R^T is invertible, then the system of equations can be solved by applying the inverse of R^T to the left of both sides of the equation.

5. Solutions of the constrained equation

To solve the set of linear equations we need to find the inverse of R. We first claim that the pseudoinverse is the inverse of R. R is given in Eq. (B24) so its pseudoinverse is

$$R^+ = (\mathbb{1} \quad 0) V^{-1} S. \tag{B50}$$

Now we can check that $R^+R = 1$ and $RR^+ = 1$. If this is true then we will know that R is invertible and $R^+ = R^{-1}$. First, we see that

$$R^+R = (\mathbb{1} \quad 0) V^{-1} S S^+ V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} \tag{B51}$$

and use Eq. (B16) and Eq. (B20) to write

$$\begin{aligned} R^+R &= (\mathbb{1} \quad 0) D D^+ \begin{pmatrix} 0 \\ \mathbb{1} \end{pmatrix} \\ &= (\mathbb{1} \quad 0) \begin{pmatrix} \mathbb{1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} \\ &= (\mathbb{1} \quad 0) \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} \\ &= \mathbb{1}. \end{aligned} \tag{B52}$$

Furthermore we can check RR^+ is equal to the identity

$$\begin{aligned} RR^+ &= S^+ V \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix} (\mathbb{1} \quad 0) V^{-1} S \\ &= S^+ V \begin{pmatrix} \mathbb{1} & 0 \\ 0 & 0 \end{pmatrix} V^{-1} S. \end{aligned} \tag{B53}$$

This time we replace the matrix with DD^+, using Eq. (B16) to find

$$\begin{aligned} RR^+ &= S^+ V D D^+ V^{-1} S \\ &= S^+ S S^+ S \\ &= \mathbb{1}, \end{aligned} \tag{B54}$$

where we have used that $S^+S = \mathbb{1}$.

This means that $RR^+ = R^+R = \mathbb{1}$ which implies that $R^{-1} = R^+$. Hence, we can write the inverse of R as

$$R^{-1} = (\mathbb{1} \quad 0) V^{-1} S \tag{B55}$$

and

$$R^{-T} = S^T V^{-T} \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix}. \tag{B56}$$

Finally, we can invert Eq. (B48) to identify the solutions to the constrained linear equation as

$$\vec{x} = \sqrt{\pi} R^{-T} (\vec{t} + 2\vec{m}). \tag{B57}$$

APPENDIX C: FURTHER EXTENDING THE CLASS OF SIMULATABLE OPERATIONS

In this Appendix, we will demonstrate that the class of symplectic operations simulatable using our method can be extended further than the rational symplectic matrices. Specifically, there are certain instances whereby the projector $1 - SS^+$, given in Eq. (B10), is rational even when the symplectic matrix is irrational.

To understand why, consider that any symplectic matrix can be expressed as [53]

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A_0 & 0 \\ C_0 & (A_0^T)^{-1} \end{pmatrix} \begin{pmatrix} X & Y \\ -Y & X \end{pmatrix}, \tag{C1}$$

where the second factor is an orthogonal symplectic matrix. Using $A = A_0 X$ and $B = A_0 Y$ we can write Eq. (B4) as

$$\bar{S} = \begin{pmatrix} X^T A_0^T \\ Y^T A_0^T \end{pmatrix}. \tag{C2}$$

We can also express its pseudoinverse, given in Eq. (B11), as

$$\begin{aligned} \bar{S}^+ &= \left(A_0 X X^T A_0^T + A_0 Y Y^T A_0^T\right)^{-1} (A_0 X \quad A_0 Y) \\ &= \left(A_0 A_0^T\right)^{-1} (A_0 X \quad A_0 Y). \end{aligned} \tag{C3}$$

The rationality of the projection matrix $1 - SS^+$ depends on the rationality of this matrix, which can be written as

$$\begin{aligned} \bar{S}\bar{S}^+ &= \begin{pmatrix} X^T A_0^T \\ Y^T A_0^T \end{pmatrix} \left(A_0 A_0^T\right)^{-1} (A_0 X \quad A_0 Y) \\ &= \begin{pmatrix} X^T A_0^T \\ Y^T A_0^T \end{pmatrix} \left(A_0^{-T} A_0^{-1}\right) (A_0 X \quad A_0 Y) \\ &= \begin{pmatrix} X^T X & X^T Y \\ Y^T X & Y^T Y \end{pmatrix}. \end{aligned} \tag{C4}$$

Therefore $1 - SS^+$ will be rational as long as each of the blocks of this matrix are rational. That is, the projector will be rational if all the elements of the matrices $X^T X, Y^T X$ are rational.

The projector can therefore in certain cases still be rational when the symplectic matrix is irrational. Namely, the matrix A_0 can be irrational while the projection matrix remains rational.

There are also certain cases where the individual matrices X, Y can be irrational while the projection matrix is rational. For example, consider the case that

$$X = \mathrm{diag}(\cos(\vec{\theta})), \tag{C5}$$

$$Y = \mathrm{diag}(\sin(\vec{\theta})). \tag{C6}$$

We can rewrite these diagonal block matrices in terms of the tangent of the angles

$$(X^T X)_{jj} = \cos^2(\theta_j) = \frac{1}{\tan^2(\theta_j)+1}, \tag{C7}$$

$$(X^T Y)_{jj} = \cos(\theta_j)\sin(\theta_j) = \frac{\tan(\theta_j)}{1+\tan^2(\theta_j)}, \tag{C8}$$

from which we see that the projection matrix will be rational whenever $\tan(\theta_j) \in \mathbb{Q}$ for all j.

Provided that the projection matrix in Eq. (B10) is rational, it is possible to identify nonzero points of the PDF, by virtue of Appendix B 3. The constraint of rational symplectic matrices can therefore be relaxed. However, for simplicity, we choose to restrict to rational symplectic matrices in this work.

APPENDIX D: RELATIONSHIPS BETWEEN THE CLASSES OF SIMULATABLE OPERATIONS

The class of operations which are shown to be efficiently simulatable in our work can be denoted by $\mathcal{D}$, which contains all operations deemed simulatable in Appendix C. For simplicity, throughout this work, we chose to denote the class of simulatable operations as those which belong to the class $\mathrm{HW}(n)[\mathrm{Sp}(2n,\mathbb{Q})]$, i.e., those for which the symplectic matrix is rational.

This class of operations $\mathrm{HW}(n)[\mathrm{Sp}(2n,\mathbb{Q})]$ contains, in particular, all GKP Clifford operations for encoded qudits of any dimension, as was proven in Sec. IV C.

We now recall and compare classes of operations that we demonstrated to be simulatable using different techniques in our previous work, Ref. [20], with those considered here. We previously demonstrated that circuits with input GKP states acted on by operations selected from a class $\mathcal{B}$ and measured in all modes with homodyne measurement are simulatable. This class was defined as

$$\mathcal{B} = \mathrm{HW}(n) \times \mathrm{DSp}(2n,\mathbb{R}) \tag{D1}$$

where

$$\mathrm{DSp}(2n,\mathbb{R}) = \left\{ \begin{pmatrix} A_0 & 0 \\ C_0 & (A_0^T)^{-1} \end{pmatrix} \begin{pmatrix} \mathrm{diag}(\cos\vec{\theta}) & \mathrm{diag}(\sin\vec{\theta}) \\ -\mathrm{diag}(\sin\vec{\theta}) & \mathrm{diag}(\cos\vec{\theta}) \end{pmatrix} : \det A_0 \neq 0, A_0^T = A_0, C_0^T A_0 = A_0^T C_0, \theta_j \in \Theta \right\} \tag{D2}$$

and

$$\Theta = \{\theta \in \mathbb{R} : \cot\theta = u/v \in \mathbb{Q}_{(2)}\} \cup \{0,\pi\}. \tag{D3}$$

The class $\mathcal{B}$ contains operations where the symplectic matrix can contain irrational elements, e.g., when $\theta_j = \pi/4$, despite satisfying the condition that $\cot\theta_j \in \mathbb{Q}_{(2)}$. This implies that $\mathcal{B} \not\subset \mathrm{HW}(n) \times \mathrm{Sp}(2n,\mathbb{Q})$.

In Appendix C we demonstrated that it is possible to extend the class of simulatable operations beyond the group $\mathrm{HW}(n) \times \mathrm{Sp}(2n,\mathbb{Q})$, to a larger set which we denote $\mathcal{D}$, and we show that $\mathcal{B} \subset \mathcal{D}$. This set contains all displacements $\mathrm{HW}(n)$ and all symplectic matrices such that $X^T X$ and $X^T Y$ are rational.

In our previous work [20] we demonstrated that is possible to simulate another class $\mathcal{A}$ which consists of symplectic operations whereby the top row of the symplectic matrix has a specific structure. That matrix does not necessarily satisfy any constraints in the other elements, and so we cannot conclude that neither $\mathcal{D}$ nor $\mathrm{HW}(n) \times \mathrm{Sp}(2n,\mathbb{Q})$ contains $\mathcal{A}$.

We have included a figure, Fig. 6, to show the containment of each of these classes of operations, with respect to the previous classes identified in Ref. [20].

APPENDIX E: ADAPTIVE CIRCUITS WITH MODULAR HOMODYNE MEASUREMENTS

Although not required for the results of this paper, we provide an additional observation in this Appendix. We demonstrate how to efficiently sample from a circuit that makes use of modular measurements. This method involves producing random integers selected from a finite set of integers.

Quantum circuits involving GKP states often make use of modular homodyne measurements. These are measurements in position or momentum modulo some period. Formally we define some period $T/\sqrt{\pi} \in \mathbb{Q}$ such that the recorded measurement result in position or momentum, x_1, is recorded as $x_1 \mod T$. For example, Pauli $\hat{Z}$ measurements in the GKP framework [12] are measurements in position modulo $T = 2\sqrt{\pi}$. If the measurement result x_1 is closest to $x_1 \mod 2\sqrt{\pi} = 0$, the measurement corresponds to a measurement of the logical qubit state $|0\rangle$. If the measurement result x_1 is closest to $x_1 \mod 2\sqrt{\pi} = \sqrt{\pi}$, the measurement corresponds to a measurement of the logical qubit state $|1\rangle$.

An adaptive circuit with feed-forward operations that makes use of modular measurements will use the value of $x_1 \mod 2\sqrt{\pi}$ to determine future operations. In the case of Pauli $\hat{Z}$ measurements, we can define two possible operations which could be performed on the remaining modes, depending on which outcome is measured.

The PDF of a unitary nonadaptive operation U_0 followed by a measurement of mode 1 can be represented as

$$f_{\mathrm{PD}}(x_1) = \sum_{\vec{m}\in\mathbb{Z}^n} \delta(x_1 - \sqrt{\pi}((R^T)^{-1}(\vec{t}+2\vec{m}))_1 - c_1), \tag{E1}$$

which is equivalent to identifying that the possible measurement values of x_1 can be given by

$$x_1 = \sqrt{\pi}(R^{-T}(\vec{t}+2\vec{m}))_1 + c_1 \quad \forall \quad \vec{m} \in \mathbb{Z}^n. \tag{E2}$$

To identify the possible outcomes of $x_1 \mod \sqrt{\pi}k$, we calculate

$$x_1 \mod k\sqrt{\pi} = \sqrt{\pi}(R^{-T}(\vec{t}+2\vec{m}))_1 + c_1 \mod k\sqrt{\pi}. \tag{E3}$$

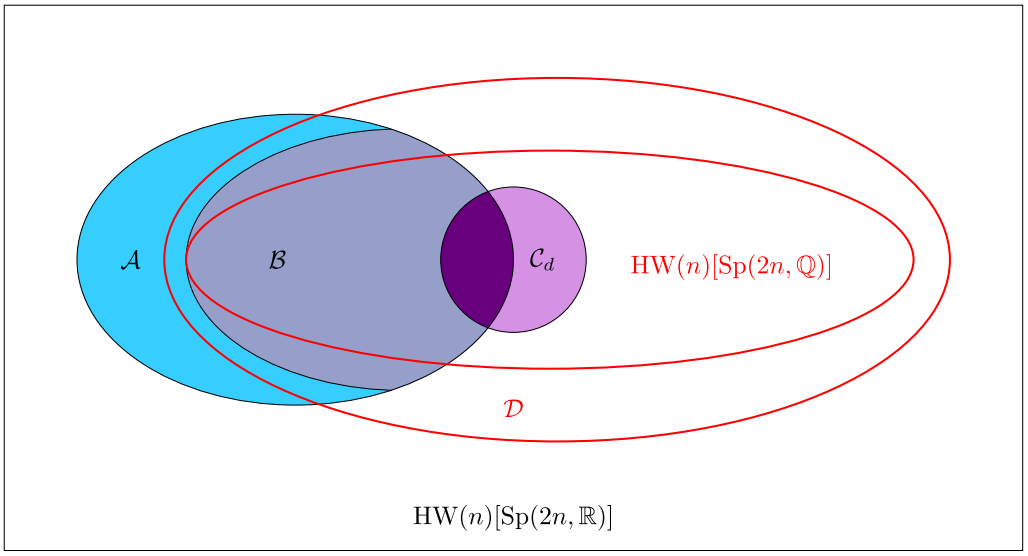

FIG. 6. The classes of circuits considered in this work and previous works. The class $\mathcal{C}_d$ refers to the Clifford group for dimension d. Classes $\mathcal{A}$ and $\mathcal{B}$ are defined in Ref. [20] as the class of operations which are simulatable for single-mode and multimode measurement, respectively. $\mathcal{A}, \mathcal{B}, \mathcal{C}_d$ are all contained within the set of Gaussian operations HW(n)[Sp$(2n, \mathbb{R})$]. The class HW(n)[Sp$(2n, \mathbb{Q})$] contains $\mathcal{C}_d$ but does not completely contain $\mathcal{A}$ nor $\mathcal{B}$. The class $\mathcal{D}$, as defined in this Appendix, contains $\mathcal{B}, \mathcal{C}_d$ but is not known to contain $\mathcal{A}$. Note that the size of each of these regions in the diagram is arbitrary.

The matrix R is rational, and so we can write [20]

$$((R^{-T})2\vec{m})_1 = \frac{u}{v}m^*, \tag{E4}$$

which reduces the random vector of integers to a single integer $m^* \in \mathbb{Z}$, and a period $\frac{u}{v} \in \mathbb{Q}$, which depends on the first row of the matrix R^{-T}.

This allows us to simplify the possible measurement outcomes to

$$\begin{aligned}\bar{x}_1 &= x_1 \mod k\sqrt{\pi} \\ &= \sqrt{\pi}(R^{-T}\vec{t})_1 + \sqrt{\pi}\frac{u}{v}m^* + c_1 \mod k\sqrt{\pi},\end{aligned} \tag{E5}$$

where we can restrict to at most vk possible outcomes parameterized by $\bar{m} \in \{0, 1, 2, vk-1\}$, which each occurs with equal probability. Simulation of measurement consists of choosing a random value of $\bar{m}$ from the finite set of possible integers.

Following the adaptive routine, we then choose a new operator $U_1(x_1)$ dependent on the measured value of x_1 and simulate the circuit $U_1(x_1)U_0$. This will provide us with points of the form

$$\begin{aligned}f_{\mathrm{PD}}(\vec{x}) = \sum_{\vec{m}} &\delta(x_1 - (\sqrt{\pi}R'^{-T}(\vec{t}' + 2\vec{m}') + \vec{c}')_1) \\ &\times \cdots \delta(x_n - (\sqrt{\pi}R'^{-T}(\vec{t}' + 2\vec{m}') + \vec{c}')_n).\end{aligned} \tag{E6}$$

Choosing $x_1 = \bar{x}_1$ and assuming no operations have been applied to the measured mode we have

$$\begin{aligned}f_{\mathrm{PD}}(\vec{x}) = \sum_{\vec{m}} &\delta\left(\frac{u}{v}\bar{m} - 2(R'^{-T}\vec{m}')_1\right) \\ &\times \ldots \delta(x_n - (\sqrt{\pi}R'^{-T}(\vec{t}' + 2\vec{m}') + \vec{c}')_n).\end{aligned} \tag{E7}$$

This expression can be simplified to a summation over $n-1$ integers.

[1] E. Chitambar and G. Gour, Rev. Mod. Phys. **91**, 025001 (2019).
[2] D. Gottesman, Ph.D. thesis, California Institute of Technology (1997), arXiv:quant-ph/9705052.
[3] D. Gottesman, in *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[6] B. W. Reichardt, Quant. Info. Proc. **4**, 251 (2005).
[7] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).
[8] A. Mari and J. Eisert, Phys. Rev. Lett. **109**, 230503 (2012).
[9] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, New J. Phys. **14**, 113011 (2012).
[10] F. Albarelli, M. G. Genoni, M. G. A. Paris, and A. Ferraro, Phys. Rev. A **98**, 052350 (2018).
[11] R. Takagi and Q. Zhuang, Phys. Rev. A **97**, 062337 (2018).
[12] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[13] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[14] B. Q. Baragiola, G. Pantaleoni, R. N. Alexander, A. Karanjai, and N. C. Menicucci, Phys. Rev. Lett. **123**, 200502 (2019).
[15] H. Yamasaki, T. Matsuura, and M. Koashi, Phys. Rev. Res. **2**, 023270 (2020).
[16] N. de Beaudrap, Quantum Inf. Comput. **13**, 73 (2013).

[17] V. Gheorghiu, Phys. Lett. A **378**, 505 (2014).

[18] Note that in the main text, we simplify the class of simulatable operations to those which have a rational symplectic matrix. However, the class of simulatable operations also includes those given in the multimode case of Ref. [20]. We provide the broader requirements of the class of simulatable symplectic matrices in Appendix C.

[19] L. García-Álvarez, C. Calcluth, A. Ferraro, and G. Ferrini, Phys. Rev. Res. **2**, 043322 (2020).

[20] C. Calcluth, A. Ferraro, and G. Ferrini, Quantum **6**, 867 (2022).

[21] L. García-Álvarez, A. Ferraro, and G. Ferrini, in *International Symposium on Mathematics, Quantum Theory, and Cryptography*, edited by T. Takagi, M. Wakayama, K. Tanaka, N. Kunihiro, K. Kimoto, and Y. Ikematsu (Springer, Singapore, 2021), pp. 79–92.

[22] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, Phys. Rev. X **6**, 021039 (2016).

[23] The Heisenberg-Weyl group HW(n) is a normal subgroup of the semidirect product of HW(n) and Sp($2n$, $\mathbb{Q}$), which we indicate by HW(n)[Sp($2n$, $\mathbb{Q}$)]. Indeed, the subgroup HW(n) is invariant under conjugation by any element of HW(n)[Sp($2n$, $\mathbb{Q}$)]. Therefore, the full group of simulatable operations is specified by the semidirect product of these two subgroups [54].

[24] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Naples, 2005).

[25] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, Boca Raton, FL, 2017).

[26] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, 2010).

[27] J. J. Sakurai and J. Napolitano, *Modern Quantum Mechanics*, 2nd ed. (Cambridge University Press, Cambridge, 2017).

[28] C. Gerry, P. Knight, and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, 2005).

[29] E. H. Moore, Bull. Amer. Math. Soc. **26**, 394 (1920).

[30] R. Penrose, Math. Proc. Cambridge Philos. Soc. **51**, 406 (1955).

[31] A. Ben-Israel and T. N. Greville, *Generalized Inverses: Theory and Applications* (Springer Science & Business Media, New York, 2003), Vol. 15.

[32] M. Newman, *Integral Matrices*, Pure and Applied Mathematics: A Series of Monographs and Textbooks (Academic Press, New York, 1972), Vol. 45.

[33] M. Newman, Linear Algebra Its Appl. **254**, 367 (1997).

[34] Integer eigenvectors of a rational matrix, Mathematics Stack Exchange, https://math.stackexchange.com/questions/4391454/integer-eigenvectors-of-a-rational-matrix/4391951 (2022).

[35] Alternative previous results [55,56] also exist for the simulation of CV circuits in the form of normalizer circuits. These results provide a numerical method to simulate nonadaptive normalizer circuits in the weak sense [36]; i.e., it is possible to sample the output of a nonadaptive circuit. However, adaptivity is required for magic state distillation, and so these results alone do not allow us to conclude that the vacuum is responsible for providing quantum advantage.

[36] R. Jozsa and M. Van Den Nest, Quantum Inf. Comput. **14**, 633 (2014).

[37] S. Arora and B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, Cambridge, 2009).

[38] R. A. Mollin, *Fundamental Number Theory with Applications* (Chapman and Hall/CRC, 2008).

[39] A. Storjohann, dissertation, Swiss Federal Institute of Technology, Zurich (2000).

[40] K. Noh, C. Chamberland, and F. G. S. L. Brandão, PRX Quantum **3**, 010315 (2022).

[41] B. Q. Baragiola, private communication (2022).

[42] Gaussian operations parameterized by irrational symplectic operations cannot in general be simulated with our method. We refer to our previous work [20], which demonstrates that when the symplectic matrix is irrational, the wave function of the transformed state corresponds to a periodic distribution which cannot be analytically reduced. Measuring in the position basis of a state which has been transformed by a general irrational symplectic matrix will have a PDF which will give random integer combinations of irrational numbers. Except for specific choices of irrational symplectic matrices, the measurement values will be randomly selected from a set dense on the real number line.

[43] F. H. Croom, *Principles of Topology* (Dover Publications, Mineola, NY, 2016).

[44] Is the symplectic group over the rationals dense on the symplectic group over the reals? Mathematics Stack Exchange, https://math.stackexchange.com/q/4510323/ (2022).

[45] E. Artin, *Geometric Algebra*, Wiley Classics Library (J. Wiley, New York, 1988).

[46] H. Weyl, *The Classical Groups: Their Invariants and Representations*, 2nd ed., Princeton Landmarks in Mathematics and Physics Mathematics (Princeton University Press, Princeton, 1946).

[47] D. Pedoe, *Geometry, a Comprehensive Course* (Dover Publications, New York, 1988).

[48] W. F. Trench, *Introduction to Real Analysis* (Prentice Hall/Pearson Education, Upper Saddle River, N.J., 2003).

[49] W. Greub, *Linear Algebra*, Graduate Texts in Mathematics (Springer, New York, 1975), Vol. 23.

[50] S. Roman, *Advanced Linear Algebra*, 3rd ed., Graduate Texts in Mathematics no. 135 (Springer, New York, 2007).

[51] G. H. Golub and C. F. V. Loan, *Matrix Computations*, 3rd ed. (John Hopkins University Press, Baltimore, 1996).

[52] T. N. E. Greville, SIAM Rev. **8**, 518 (1966).

[53] Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana **45**, 471 (1995).

[54] J. Bermejo-Vega, *Normalizer Circuits and Quantum Computation*, Technische Universität München, 2016.

[55] J. Bermejo-Vega, Ph.D. thesis, Technische Universität München Max-Planck-Institut für Quantenoptik, arXiv:1611.09274.

[56] J. Bermejo-Vega, Y. Lin, and M. Van den Nest, Quantum Inf. Comput. **16**, 0361 (2016).