Fermion Sampling: a robust quantum computational advantage scheme using fermionic linear optics and magic input states

Michał Oszmaniec,[1] Ninnat Dangniam,[1] Mauro E.S. Morales,[2] and Zoltán Zimborás[3,4,5]

[1] *Center for Theoretical Physics, Polish Academy of Sciences, Al. Lotników 32/46, 02-668 Warszawa, Poland*[*]

[2] *Centre for Quantum Computation and Communication Technology, Centre for Quantum Software and Information, University of Technology Sydney, NSW 2007, Australia*

[3] *Wigner Research Centre for Physics, H-1121, Budapest, Hungary*[†]

[4] *MTA-BME Lendület Quantum Information Theory Research Group Budapest, Hungary*

[5] *Mathematical Institute, Budapest University of Technology and Economics, H-1111, Budapest, Hungary*

Fermionic Linear Optics (FLO) is a restricted model of quantum computation which in its original form is known to be efficiently classically simulable. We show that, when initialized with suitable input states, FLO circuits can be used to demonstrate quantum computational advantage with strong hardness guarantees. Based on this, we propose a quantum advantage scheme which is a fermionic analogue of Boson Sampling: Fermion Sampling with magic input states.

We consider in parallel two classes of circuits: particle-number conserving (passive) FLO and active FLO that preserves only fermionic parity and is closely related to Matchgate circuits introduced by Valiant. Mathematically, these classes of circuits can be understood as fermionic representations of the Lie groups $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$. This observation allows us to prove our main technical results. We first show anticoncentration for probabilities in random FLO circuits of both kind. Moreover, we prove robust average-case hardness of computation of probabilities. To achieve this, we adapt the worst-to-average-case reduction based on Cayley transform, introduced recently by Movassagh [1], to representations of low-dimensional Lie groups. Taken together, these findings provide hardness guarantees comparable to the paradigm of Random Circuit Sampling.

Importantly, our scheme has also a potential for experimental realization. Both passive and active FLO circuits are relevant for quantum chemistry and many-body physics and have been already implemented in proof-of-principle experiments with superconducting qubit architectures. Preparation of the desired quantum input states can be obtained by a simple quantum circuit acting independently on disjoint blocks of four qubits and using 3 entangling gates per block. We also argue that due to the structured nature of FLO circuits, they can be efficiently certified using resources scaling polynomially with the system size.

I. INTRODUCTION

Universal fault-tolerant quantum computers are expected to exceed capabilities of classical computers in many applications including optimization problems, simulation of many-body quantum systems, machine learning and code-breaking. However, practical requirements for implementations of quantum algorithms generally require the noise level to be below a certain stringent threshold and an encoding of logical qubits into a large number of physical qubits [2]. Despite the impressive progress made along the road to realize a large-scale fault tolerant quantum computer as shown in the proof-of-principle demonstrations of error correction [3] and fault tolerance [4], what we have at present and in the near future are NISQ devices [5]: noisy, intermediate-scale quantum processors having of the order of tens or hundreds of qubits.

It is then of upmost importance to identify problems and tasks for which such imperfect quantum computers could demonstrate computational advantage over their classical counterparts. Broadly speaking, such demonstrations fall into two categories: (i) proposals that are potentially practically useful but for which

[*] oszmaniec@cft.edu.pl

[†] zimboras.zoltan@wigner.hu

there is little rigorous evidence for the quantum advantage [6, 7], and (ii) proposals that come with a rigorous justification from the side of complexity theory [8] but are not necessary useful for any practical purpose.

On the side of potential near-term applications, one of the leading candidates to demonstrate quantum speedup are variational quantum algorithms [9–12]. These routines use low-depth parametric quantum circuits and employ a classical optimizer when solving relevant problems. The targeted problems typically originate from combinatorial optimization [13], machine learning [14–16] and quantum chemistry [17, 18]. Importantly, these algorithms have been already implemented in proof-of-principle experiments in superconducting qubits for non-planar MAX-CUT problem [19] and variational computations for quantum chemistry [7, 20, 21].

The paradigm of quantum computational advantage [22, 23] (also known as supremacy) offers a complementary perspective and aims to develop schemes showing computational advantage of restricted-purpose quantum machines under minimal theoretical assumptions while minimising hardware requirements. Importantly, given the current status of complexity theory, a rigorous separation of the power of quantum and classical computers cannot be made without plausible assumptions such as the non-collapse of the polynomial hierarchy (a weaker version of $\mathrm{P} \neq \mathrm{NP}$). Current quantum advantage schemes are usually based on the problem of sampling, i.e., the task of generating samples of a distribution generated by a given quantum circuit or a specifically tuned devices (see, however, [24] for an alternative proposal involving *relation problems* that challenges classical computers in the playground of shallow circuits). The first candidate for demonstration of quantum computational supremacy was Boson Sampling [25] that proposed to sample from photonic networks that were initialized in single-photon photon states of several modes. Subsequent sampling proposals include the IQP sampling [26, 27], the Random Circuit Sampling [1, 28, 29], the quantum Fourier sampling [30] and many other schemes [31, 32] that usually operate on multiqubit systems that undergo evolutions under restricted gate sets (there exist, however, other proposals that use Gaussian states [33, 34] or atomic systems [32, 35]).

Random circuit sampling (RCS), as the name implies, is the task of sampling from the output distribution of a randomly selected quantum circuit. RCS has been recently experimentally demonstrated in a system of 53 superconducting qubits arranged in the planar layout, and using random two-qubit-local circuits of depth 20 [36]. Beside its experimental feasibility in current NISQ architectures, this quantum advantage proposal also enjoys strong hardness guarantees based on two technical results available for random quantum circuits: a worst-to-average-case reduction of the hardness of computing the output probabilities [1, 29] and anticoncentration [37, 38].

Independently of RCS, the original proposal of Boson Sampling received a lot of interest due to the experimental progress in the field of integrated photonics [39]. Currently, the state-of-the-art experiments involve 14 indistinguishable photons in 20 modes [40], while a recent work [41] reported demonstration of Gaussian Boson Sampling (i.e., a variant of Boson Sampling with Gaussian input states) using 50 squeezed states at the input of a 100 mode photonic network. While worst-to-average-case reduction (at least for the exact computation of the probabilities) was available for the Boson Sampling [25], the anticoncentration property remains unproven for this scheme. Interestingly, neither of the theoretical guarantees are currently in place for Gaussian Boson Sampling.

In this work, we propose a quantum advantage scheme based on a fermionic analogue of Boson Sampling: Fermion Sampling with magic input states. In our scheme a suitable input state $|\Psi_{\mathrm{in}}\rangle$ in $d = 4N$ fermionic modes is transformed via Fermionic Linear Optical (FLO) transformation V, and is measured using particle-number resolving detectors (see Figure 1). We consider in parallel two classes of circuits: particle-number conserving (passive) FLO and active FLO that preserves only the fermionic parity [42, 43] and is closely related to Matchgate circuits introduced by Valiant [44]. Mathematically, these classes of circuits can be understood as fermionic representations of the Lie groups $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$. This observation allows us to prove our main technical results. We first show anticoncentration for probabilities in random FLO circuits of both kind. Moreover, we prove robust average-case hardness of computation of probabilities. To achieve this we adapt the worst-to-average-case reduction based on Cayley transform [1] to our scenario, when instead of the defining representation of the unitary group one considers higher dimensional representations of low-dimensional Lie groups. Taken together, these findings give hardness guarantees matching that of the paradigm of RCS [1, 29]. We also argue that, due to the structural properties of FLO gates, one can efficiently certify them with resource scaling polynomially with the system size.

We argue that our scheme is feasible to realize experimentally. While experimental realization of linear-optical transformation in systems of *real* fermionic systems is usually hard because of Coulomb interaction (see however [45]), we make use of the fact that this class of operations is relevant for performing quantum chemistry and many-body simulations on a quantum computer [21, 46–48]. Specifically, after a standard Jordan-Wigner encoding of qubits into fermions, our sampling proposal becomes readily implementable by restricted set of gates and layouts native to superconducting qubit architecture used in simulations of quantum chemistry [49]. Compared to the RCS implementation of arbitrary FLO transformation requires depth scaling proportional to N. In this encoding magic input states can be prepared using 3 entangling gates per each and every disjoint block of four qubits and particle-number measurements are realized via standard computational basis measurement (see Figure 1) .

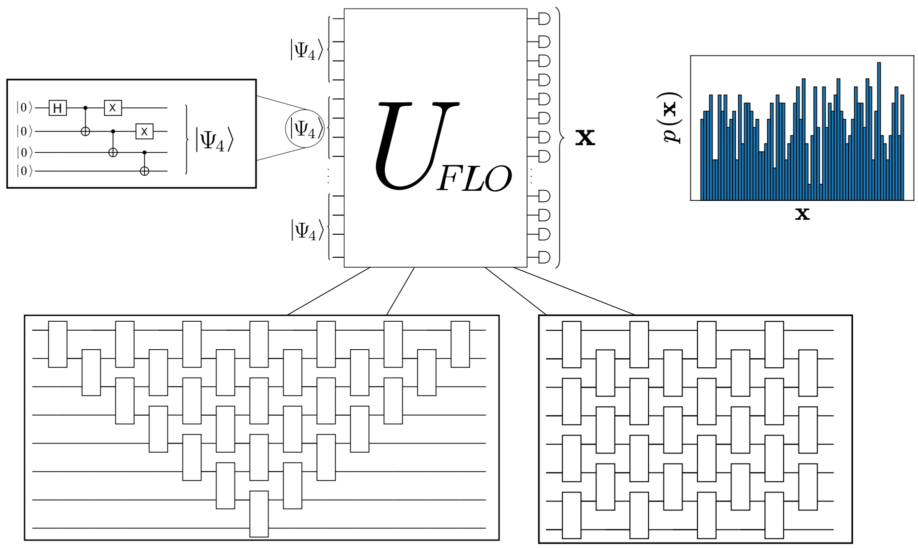

FIG. 1. The setup considered in our work. We run an FLO circuit U_{FLO} (passive or active) with input state $|\Psi_{\text{in}}\rangle = |\Psi_4\rangle^{\otimes N}$ and sample bitstrings $\mathbf{x}$ with the probability distribution $p(\mathbf{x})$ induced by the circuit. Using Jordan-Wigner transformation that encodes fermions in qubits, the state $|\Psi_4\rangle$ can be easily prepared as shown in the inset to the left. The decomposition of the circuits into elementary gate set can be realized by the fermionic analogues of existing layouts for linear optical networks [50, 51] as discussed in Appendix A.

Significance of our results and relation to prior work

Importance of the technical results for hardness of Fermion Sampling

A first step in establishing hardness of any quantum advantage proposal is showing hardness of sampling up to relative error. Sampling in relative error refers to the task in which a classical computer, given a classical description of the quantum process of interest (e.g., input states, arrangement of gates in the device, etc.), is challenged to efficiently sample from the probability distribution $\{q_{\mathbf{x}}\}$ that for every output $\mathbf{x}$ satisfies $|p_{\mathbf{x}} - q_{\mathbf{x}}| \leq \alpha p_{\mathbf{x}}$, where $\{p_{\mathbf{x}}\}$ is the true probability distribution produced by the device and $\alpha > 0$ is a constant. To establish hardness of sampling up to some relative error, it suffices to show that certain probabilities produced by the device are #P-hard to compute[1], assuming that polynomial hierarchy does not collapse. This hardness of quantum probabilities for specific circuits and outcomes (i.e., in the worst case) was proven long ago for circuit built from universal gates [53, 54]. For non universal models of quantum computation a standard technique for establishing #P-hardness of computation of probabilities is based on

[1] Informally, #P is the complexity class of counting solutions to problems that can be efficiently verified. For more details, see [52].

showing that a particular non-universal model becomes universal when postselection is allowed [25, 26, 32, 55–58]. Relative error approximation is however too strong to be a reasonable notion of approximation from the physical perspective. This is because even a very small amount of experimental noise can render very large relative error.

A more realistic notion of approximate sampling is based on additive error [25, 59] in which classical computer is supposed to efficiently produce samples from probability distribution $\{q_{\mathbf{x}}\}$ satisfying $\sum_{\mathbf{x}} |p_{\mathbf{x}} - q_{\mathbf{x}}| \leq \epsilon$, where ϵ is the error parameter. Establishing hardness for additive error approximate sampling is however much more challenging then in the case of relative error. Assuming non-collapse of the polynomial hierarchy, the currently existing techniques [25, 27, 59] establish this hardness using Stockmayer approximate counting algorithm [60] and by relying on two technical properties of a given quantum advantage proposal: (i) anti-concentration of outcome probabilities, and (ii) #P-hardness of relative error approximate computation of outcome probabilities on average. Anti-concentration refers to property that probability amplitudes $p_{\mathbf{x}}(V)$ are typically not too small, compered to their average value, for random circuits V defining a given quantum advantage proposal. Anticoncentration property has been shown in several schemes [27, 31, 35, 38, 57], while for others, including Fourier Sampling [30] and Boson Sampling [25] it remains unproven. On the other hand average-case #P- hardness of relative error approximate computation of $p_{\mathbf{x}}(V)$ has not been proven to date for the existing quantum advantage proposals. There however exist intermediate results that support it in the form of average-case #P-hardness of *exact* computation of $p_{\mathbf{x}}(V)$ for Boson Sampling [25], RCS [29] and related schemes [35]. These works adopt the polynomial interpolation technique from [25] and to prove worst-to-average-case hardness reduction. This reduction has been recently improved by Movassagh [1] for RCS who showed that it is average-case #P-hard to approximate $p_{\mathbf{x}}(V)$ in additive error $\exp(-\Theta(N^{4.5}))$, where N is the number of qubits.

In this work, in order to justify computational hardness of the proposed Fermion Sampling scheme we prove the following results

- i Anticoncentration of probabilities $p_{\mathbf{x}}(V)$ in the output of the scheme for both passive and active FLO circuits initialized in magic states.
- ii Robust worst-to-average-case hardness reduction for computation of probabilities for passive and active FLO circuits initialized in magic states up to error $\exp(-\Theta(N^6))$.

Instrumental to our proofs is the fact that active and passive FLO circuits are representations of the low-dimensional (of dimensions scaling polynomially with the number of fermionic modes d) Lie groups $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$ respectively. For the anticoncentration property, we do not use the 2-design property (which is not satisfied for FLO unitaries), but instead prove it relying on specific group-theoretic properties of FLO circuits. For the worst-to-average case reduction, we follows the state-of-the-art technique by Movassagh [1], which utilizes Cayley path to construct a low-degree rational interpolation between the worst-case and average-case circuits, while generalizing it in two significant directions. First, while the interpolation in [1] is performed directly using physical circuits, ours is performed at the level of group elements which are then represented as circuits (see Fig. 2) Secondly, while [1] applies the interpolation to local one- and two-qubit gates that constitute the circuit, we directly apply it to a global circuit while maintaining the low-degree nature of the rational functions, which is required for the robust reduction.

These results put Fermion Sampling at the comparable level as RCS [1, 29] in terms of state-of-the-art hardness guarantees, surpassing that of Boson Sampling. The advantage of our scheme compared to RCS is that FLO circuits can be efficiently certified due to their low-dimensional structural properties. The apparent disadvantage is the size of the required circuits - RCS can be implemented in depth $\sqrt{N}$ [28, 38] while our scheme requires depth of the structured circuit scaling like N.

Comparison with Boson Sampling

Boson Sampling [25], the first quantum advantage proposal based on sampling, relies on the fact that the probability amplitudes of indistinguishable bosons initially prepared in a Fock state and passing through linear-optical network, can be expressed via matrix permanents. Computation of permanent is know to be #P- hard in the worst case [52]. In contrast, the analogous amplitudes for fermions are given by the

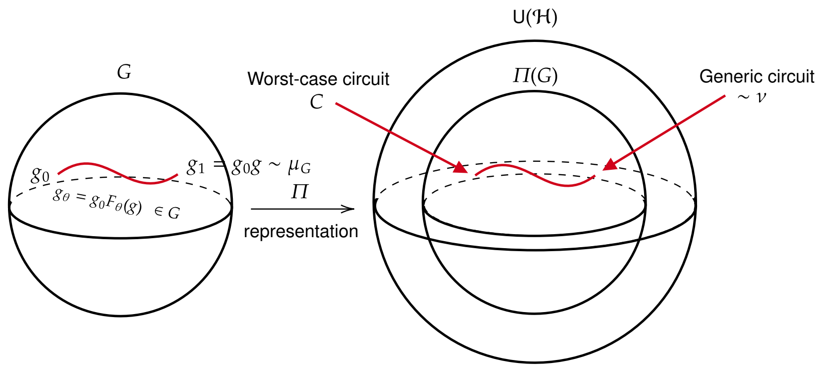

FIG. 2. Π is a group representation from G to (a subgroup $\Pi(G)$ of) the group $\mathrm{U}(\mathcal{H})$ of all quantum circuits on Hilbert space $\mathcal{H}$ (typically of exponential dimension). The Cayley path $g_\theta = g_o F_\theta(g) \in G$ gives a rational interpolation between a fixed element g_0 and $g_1 = g_0 g$. This gives rise to a rational interpolation between circuits $C \coloneqq \Pi(g_0)$ and $\Pi(g_0)\Pi(g) = \Pi(g_0 g)$. To carry out worst-to-average-case reduction we would consider g_0 to be group element corresponding to the worst-case circuit C while g will be chosen to be a *generic* element of the Lie group G.

determinant, which can be computed efficiently. Physically, this difference in complexity can be attributed to the fact that bosonic Focks states are *non-Gaussian* bosonic states, while their fermionic counterparts are in fact fermionic Gaussian states [61]. Thus, to make a closer the analogy with Boson Sampling, we define our Fermion Sampling using *non-Gaussian* input states $|\Psi_{\mathrm{in}}\rangle = |\Psi_4\rangle^{\otimes N}$, where $|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$. This state can be prepared easily on a quantum computer but at the same time can be expressed as an exponential sum of orthogonal Fock states. This is sufficient to guarantee hardness of the corresponding probability amplitudes. It was shown by Ivanov and Gurvitz [62, 63] that if $|\Psi_{\mathrm{in}}\rangle$ is transformed via particle-number preserving (passive) FLO transformation, the probability amplitudes are related to *mixed discriminants* of matrices, which is known to be #P-hard, because they can be efficiently reduced to permanent. In the context of active FLO transformations, auxiliary states $|\Psi_4\rangle$ are known to promote this class of transformations to universality [64] (see also [65]), which can be used to show #P-hardness of probabilities arising form active FLO circuits initialized with such non-Gaussian states. We conclude the comparison with boson sampling by clarifying the role of the measurements used. Our proposal uses fermionic particle-number measurements which are themselves fermionic Gaussian. This differentiates Fermion Sampling from Boson Sampling schemes. This includes Gaussian Boson Sampling [66] in which bosonic squeezed states (that are bosonic Gaussian) are transformed using linear optics, and finally measured using (non-Gaussian) particle-number detectors. In that proposal non-Gaussian character of the particle-number measurement is crucial for hardness [67].

Relation to Fermionic Quantum Computation

Quantum computing with (active) FLO circuits has received significant attention over the years. While FLO circuits with unentangled input states and measurements are efficiently simulable classically, they constitute a "maximally classical" subset of quantum circuits in the sense that an addition of any non-FLO unitary allows one to reach any unitary on the relevant Hilbert space [68]. Thus, similar to Clifford circuits, FLO circuits with additional resources constitute an interesting model of universal quantum computing [61, 64]. Here we review what the most important results about computational power of FLO circuits and their extensions. Common notions of simulation in the literature falls into two classes of strong and weak simulations: strong simulation refers to the ability to compute the the marginal probability of any chosen outcome, whereas weak simulation refers to the ability to sample from the output probability distribution. Strong classical simulability of FLO circuits can be traced back to the work of Valiant [44] in which he introduced so-called matchgates for the purpose of studying algorithms for graphs. Assuming computational-basis input states and measurements, circuits of nearest neighbor (n.n) matchgates in 1D layout can be strongly simulated on a classical computer in polynomial time, even with adaptive measurement in the computational basis [42]. Soon after the introduction of matchgates, their classical simulability was connected to exact solvability in physics as n.n matchgate circuits can be mapped to evolutions of non-interacting fermions via the Jordan-Wigner transformation [42, 43] and extended to classical simulability of dissipative FLO and non-unitary matchgates [69, 70]. The geometric locality restriction is non-trivial as matchgate computation becomes quantum universal when the n.n condition is lifted [71] or the linear chain of qubits is replaced by more general graphs [72].

When one considers arbitrary product input states, adaptive computation using FLO circuits with such inputs can be simulated classically [73]. This is in striking contrast to the case of Clifford circuits in which supplying single-qubit magic states and adaptive measurement in the computational basis suffices for universal quantum computation [74]. Since every fermionic state (or qubit state with a fixed parity) of fewer than 4 qubits is Gaussian [75, 76], FLO circuits with computational-basis measurement must be supplied with at least four-qubit magic input state to attain universality. The first example of such state is $|a_8\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ (which can be converted to $|\Psi_4\rangle$ used in our scheme, see the proof of Lemma 15) was introduced in [64] along with the corresponding state-injection scheme for universal quantum computation using Ising anyons. Much more general result was established in [65] where it was showed that all non-Gaussian states, when supplied in multiple copies, allow one to perform universal quantum computation. Finally, weak classical simulability of FLO circuits with noisy magic input states was studied in [76, 77],

Alternative to magic input states, adding an arbitrary non-FLO gate [61, 68, 78] (see also [79]), or entangled measurements such as non-destructive parity measurement [61, 80], also allows one to perform universal quantum computation. When the final measurement is restricted to only one qubit line and no adaptive measurement is allowed during the computation, the circuits are classically simulable in the strong sense even with magic input states. This result was first proven for an arbitrary product input state in [71] and observed to generalized to any product of $O(\log m)$-qubit states in [81]. Recently comprehensive investigation of the complexity landscape of FLO circuits with auxiliary resources are given in [81], which investigated the hardness of FLO circuits depending on: (i) whether the input is a product state or copies of entangled magic states, (ii) whether adaptive measurements are allowed, (iii) whether the final measurement is performed only on a single qubit or on all qubits. It was established there that strong simulation of FLO circuits is #P-hard in all cases considered except ones that are already known to be classically simulable [42, 71, 73]. Using the standard postselection argument [26], it is possible to show that weak simulation FLO circuits with magic input states and no adaptive measurement implies collapse of the polynomial hierarchy (see Appendix D). These scenario coincides with one of the settings considered in this work. However, in this work we are concerned with establishing hardness of Fermion Sampling up to additive error which, as explained earlier, is a property much harder to establish.

Organization of the paper.– First, in Section II we lay out basic notations and concepts, focusing mostly on the fermionic context. Then in Section III we formally define our quantum advantage proposal and give a high level overview of our results and their significance. We also present there arguments in favour of experimental feasibility of our scheme. In Section IV we discuss possible applications of our work and present future research directions. In the subsequent Section V we prove that output probabilities of FLO circuits initialized in suitable magic states anticoncentrate for generic active and passive FLO circuits. These results, together with known [62] worst-case #P hardness of probability distributions, is then used in Section VI to prove hardness of approximate Fermion Sampling. Section VII is devoted to the quantitative analysis of the Cayley path transformation for unitary and orthogonal groups. Section VIII focuses on polynomials associated to the probabilities in our FLO sampling scheme. In Section IX we use technical results form the two preceding parts to prove, following [1] worst-to-average-case reduction for hardness of computing probabilities in our quantum advantage scheme. In the final Section X we show that in the Jordan-Wigner encoding an unknown FLO unitary can be efficiently certified using resources scaling polynomially with the number of fermionic modes. The Appendix consists of four parts and contains auxiliary technical results. In Appendix A, we describe in detail the decomposition of an FLO circuits into elementary one- and two-qubit gates. In part B, we give details of the computations needed in the proof of anticoncentration of our results. In Appendix C, we prove a lemma concerning the stability of the FLO representations (an analogue of the stability result proved standard Boson Sampling [82]), which is used in the tomography scheme of FLO unitaries. Finally, in Appendix D we prove #P-Hardness of probabilities in shallow depth active FLO circuits.

Acknowledgements

We would like to thank Ramis Movassagh for explanations regarding his work. MO and ND acknowledge support by the Foundation for Polish Science through the IRAP project cofinanced by the EU within the Smart Growth Operational Programme (contract no. 2018/MAB/5) and through the TEAM-NET project (contract no. POIR.04.04.00-00-17C1/18-00). ZZ was supported by the NKFIH through the Quantum Technology National Excellence Program (project no. 2017-1.2.1-NKP-2017-00001), the grants K124152, K124176, KH129601, K120569 and the Quantum Information National Laboratory of Hungary.

II. NOTATION AND BASIC CONCEPTS

In this section we describe main concepts and notation needed in the paper. Specifically, we will introduce the language of second quantization, vital for describing fermionic systems. We will define passive and active fermionic linear optical circuits. Finally, we survey Jordan-Wigner transformation which allows to implement fermionic systems and associated unitaries acting on them in terms of spin systems and standard quantum circuits. All these ingredients allow us to formally define our scheme for attaining quantum computational advantage with FLO circuits.

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. Normalized vectors in this space will be denoted by $|\Psi\rangle, |\Phi\rangle$ etc. Such normalized vectors give rise to pure states, i.e., rank 1 nonnegative operators on $\mathcal{H}$. For the sake of brevity we will use the notation $\Psi = |\Psi\rangle\langle\Psi|\,, \Phi = |\Phi\rangle\langle\Phi|$ etc. We will use the symbol $\mathcal{D}(\mathcal{H})$ for the set of all (possibly mixed) quantum states on $\mathcal{H}$. Finally, by $\mathrm{U}(\mathcal{H})$ we denote group of unitary operators on $\mathcal{H}$. We will be consider a system of fermions with single-particle Hilbert space being $\mathbb{C}^d$. The Hilbert space associated to this system is a d mode Fock space

$$\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d) = \bigoplus_{n=0}^{d} \bigwedge^{n}(\mathbb{C}^d)\ , \tag{1}$$

where $\bigwedge^n(\mathbb{C}^d)$, is the totally anti-symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$ describing states consisting of exactly n fermions, and $\bigwedge^0(\mathbb{C}^d) = \mathrm{span}_{\mathbb{C}}(|0_F\rangle)$, where $|0_F\rangle$ is the Fock vacuum. Any basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ of single-particle Hilbert space defines a family of creation and annihilation operators acting on $\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)$: $f_j^\dagger$ and f_j, respectively, where $j = 1, 2, \ldots, d$. These operators satisfy canonical anti-commutation relations $\{f_j, f_k^\dagger\} \equiv f_j f_k^\dagger + f_k^\dagger f_j = \delta_{j,k}$ and $\{f_j, f_k\} = \{f_j^\dagger, f_k^\dagger\} = 0$, with $\delta_{j,k}$ being the Kronecker symbol.

Given this set of creation and annihilation operators, it is natural to introduce the so-called Fock basis states, which forms a basis of $\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)$, as

$$|\mathbf{x}\rangle := (f_1^\dagger)^{x_1}(f_2^\dagger)^{x_2}\cdots(f_d^\dagger)^{x_d}|0_F\rangle \tag{2}$$

for any $\mathbf{x} \in \{0,1\}^d$, where we used the notation $(f_1^\dagger)^0 = \mathbb{I}$. Throughout the paper, we will denote the set $\{1, \ldots, d\}$ as $[d]$. Given an arbitrary subset $\mathcal{X} \subset [d]$, it will also be useful to introduce the notation $|\mathcal{X}\rangle$ for the Fock basis state $|\mathbf{x}\rangle$ with $x_j = 1$ if $j \in \mathcal{X}$ and $x_j = 0$ otherwise. We will also use $\binom{\mathcal{X}}{k}$ to denote the collection of subsets of finite set $\mathcal{X}$ of size k (we shall assume the convention $\binom{\mathcal{X}}{k} = \emptyset$ if $|\mathcal{X}| < k$.

Considering the direct sum decomposition of the Fock space into fixed particle number subspaces in Eq. (1), a specific Fock basis state $|\mathcal{X}\rangle$ (with $|\mathcal{X}| = n$) is an element of the n-particle subspace $\bigwedge^n(\mathbb{C}^d)$. Note that since $\bigwedge^n(\mathbb{C}^d)$ can be regarded as a subspace of $(\mathbb{C}^d)^{\otimes n}$, it is natural to consider such a Fock basis state $|\mathcal{X}\rangle$ (where $\mathcal{X} = \{a_1, \ldots a_n\}$ with $a_i < a_j$ if $i < j$) as an element in $(\mathbb{C}^d)^{\otimes n}$ which is given by the formula

$$|\mathcal{X}\rangle = |a_1\rangle \wedge |a_2\rangle \wedge \ldots \wedge |a_n\rangle = \frac{1}{\sqrt{n!}} \sum_{i_1,\ldots i_n=1}^{n} \epsilon_{i_1,i_2,\ldots,i_n} |a_{i_1}\rangle \otimes |a_{i_2}\rangle \otimes \cdots |a_{i_n}\rangle. \tag{3}$$

Here and throughout the paper we will use the generalized Levi-Civita symbol, i.e., for any string of positive integers $(k_1, k_2, \ldots, k_n)$ with $k_i \neq k_j$ if $i \neq j$ we define $\epsilon_{k_1,k_2,\ldots,k_n} = (-1)^p$, where p is the parity of the permutation π for which $k_{\pi(i)} < k_{\pi(j)}$ if $i < j$ and p is its parity, while $\epsilon_{k_1,k_2,\ldots,k_n} = 0$ if some of the entries in $(k_1, k_2, \ldots, k_n)$ coincide.

A *passive fermionic linear optical transformation* on the n-particle subspace $\bigwedge^n(\mathbb{C}^d) \subset (\mathbb{C}^d)^{\otimes n}$ is given as a transformation $U^{\otimes n}$ restricted from being $(\mathbb{C}^d)^{\otimes n} \to (\mathbb{C}^d)^{\otimes n}$ function to being a $\bigwedge^n(\mathbb{C}^d) \to \bigwedge^n(\mathbb{C}^d)$ map. Passive FLO can be understood abstractly as the irreducible representation of the low-dimensional symmetry group $\mathrm{U}(d)$ in the Hilbert space $\bigwedge^n(\mathbb{C}^d)$

$$\Pi_{\mathrm{pas}} : \mathrm{U}(d) \longrightarrow \mathrm{U}\left(\bigwedge^n(\mathbb{C}^d)\right), \tag{4}$$

$$U \longmapsto U^{\otimes n}\big|_{\bigwedge^n(\mathbb{C}^d)} . \tag{5}$$

That is, we get a representation of $\mathrm{U}(d)$ on a fixed particle fermionic subspace. A useful equivalent definition is that for any $U = e^{iK} \in \mathrm{SU}(d)$, Π_{pas} is the restriction of the Fock state unitary $e^{i/2\sum_{n,m} K_{nm} f_n^\dagger f_m}$ to the subspace $\bigwedge^n(\mathbb{C}^d)$.

An important concept when discussing passive FLO transformations are Slater determinant states. These are states of the form $|\Psi\rangle = |\xi_1\rangle| \wedge \xi_2\rangle \wedge \ldots \wedge |\xi_n\rangle$, where $\{|\xi_i\rangle\}_{i=1}^n \subset \mathbb{C}^d$ is a set of orthonormal vectors of the one-particle Hilbert space $\mathbb{C}^d$. By definition, Fock basis states are special cases of Slater determinant states. And passive FLO transformations act transitively on the set of Slater determinant states. The overlap between any two Slater determinant states, $|\Psi\rangle = |\xi_1\rangle| \wedge |\xi_2\rangle \wedge \ldots \wedge |\xi_n\rangle$ and $|\Phi\rangle = |\phi_1\rangle \wedge |\phi_2\rangle \wedge \ldots \wedge |\phi_n\rangle$, can be expressed by the simple determinant formula

$$\langle \Psi | \Phi \rangle = \det C\,, \quad C_{i,j} = \langle \xi_i | \phi_j \rangle. \tag{6}$$

A standard way to measure fermionic systems is to perform particle number measurement i.e a projective measurement in the Fock basis basis $|\mathbf{x}\rangle$ defined previously. Upon obtaining measurement result labelled by $\mathcal{X}$, numbers x_i have the interpretation of number of particles in mode i.

Let us next introduce the self-adjoint Majorana mode operators

$$m_{2j-1} = f_j + f_j^\dagger\,, \qquad m_{2j} = -i\,(f_j - f_j^\dagger), \tag{7}$$

with anti-commutation relations $\{m_j, m_k\} = 2\,\mathbb{I}\delta_{j,k}$. These operators define parity operator $Q = i^d \prod_{i=1}^{2d} m_i$ in $\mathcal{H}_{\mathrm{Fock}}(C^d)$. The subspace of $\mathcal{H}_{\mathrm{Fock}}(C^d)$ that corresponds to eigenvalue of $+1$ of Q is spanned by Fock states $|\mathbf{n}\rangle$ having even number of particles. In what follows we shall refer it to this vector space as positive parity subspace and denote it by $\mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d)$. Majorana operators allow also to active fermionic linear optical transformations. We say that a fermionic unitary U is *free*, *Gaussian*, or *linear-optical*, if it can be written as an exponential of a quadratic Hamiltonian, i.e., $U = \mathrm{e}^{iH}$, where

$$H = \frac{i}{4}\sum_{j,k=1}^{2d} A_{j,k}\, m_j\, m_k, \tag{8}$$

and $A = -A^T \in \mathbb{R}^{2d\times 2d}$. Active FLO transformation form a group which can be conveniently understood in terms of (projective) representation of the $\mathrm{SO}(2d)$ group[2]:

$$\Pi_{\mathrm{act}} : \mathrm{SO}(2d) \longrightarrow \mathrm{U}(\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)) \tag{9}$$

$$O \longmapsto \exp\left(\frac{1}{4}\sum_{i,j=1}^{2d} [\log(O)]_{ij}\, m_i m_j\right), \tag{10}$$

Often the restriction of Π_{act} to the positive parity subspace $\mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d)$ is considered, we will not use a new symbol for this restricted representation rather simply refer to it by writing $\Pi_{\mathrm{act}} : \mathrm{SO}(2d) \to \mathrm{U}(\mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d))$. Pure positive-parity Gaussian states are defined as pure states the form $\Psi = \Pi(O)\,|0_F\rangle\langle O_F|\,\Pi(O)^\dagger$, for $O \in SO(2d)$. In other words pure positive-parity Gaussian fermionic states are states that can be generated from the vacuum by active FLO transformations. Similarly, it is possible to define negative-parity pure

---

[2] The FLO operators themselves form a group isomorphic to the universal cover of $\mathrm{SO}(2d)$, called $\mathrm{Spin}(2d)$.

fermionic Gaussian states as states generated by active FLO from, say, a Fock state with a single excitation.

If we look at the action on the operators, we get an actual (i.e., non-projective) representation. In particular, a single Majorana operator evolves under an active FLO transformation as follows

$$U^\dagger\, m_j\, U = \sum_{k=1}^{2d} O_{jk}\, m_k, \tag{11}$$

where $U = \mathrm{e}^{-iHt}$ with $H = \frac{i}{4}\sum_{j,k=1}^{2d} A_{j,k} m_j m_k$ and and $O = e^{-A} \in \mathrm{SO}(2d)$.

We will also use the notation $\mathcal{G}_{\mathrm{pas}}$ and $\mathcal{G}_{\mathrm{act}}$ to denote respectively passive and active fermionic linear optical gates. The name comes from the fact that these gates transform single creation/majorana operators to linear combination of creation/majorana operators, respectively.

An important ingredient when discussing how to implement FLO transformations on qubit systems is the Jordan-Wigner transformation, that provides an equivalence between fermion and qubit systems through the unitary mapping $\mathcal{V}_{\mathrm{JW}} : \mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d) \to (\mathbb{C}^2)^{\otimes d}$ given as the following mapping between

$$\mathcal{V}_{\mathrm{JW}}\left((f_1^\dagger)^{x_1}(f_2^\dagger)^{x_2}\cdots(f_d^\dagger)^{x_d}|0_F\rangle\right) = |x_1\rangle\otimes|x_2\rangle\otimes\cdots\otimes|x_d\rangle\,, \quad \forall \mathbf{x} = (x_1, x_2, \ldots, x_d) \in \{0,1\}^d, \tag{12}$$

which in turn induces an isomorphic mapping between majorana and spin operators

$$m_{2p-1} \mapsto \mathcal{V}_{\mathrm{JW}}\, m_{2p-1}\, \mathcal{V}_{\mathrm{JW}}^\dagger \quad = Z_1\cdots Z_{p-1}X_p, \qquad p = 1,\ldots d, \tag{13}$$

$$m_{2p} \mapsto \mathcal{V}_{\mathrm{JW}}\, m_{2p}\, \mathcal{V}_{\mathrm{JW}}^\dagger \quad = Z_1\cdots Z_{p-1}Y_p, \qquad p = 1,\ldots d. \tag{14}$$

To make the connection between fermions and qubit systems even more transparent, one often introduces the *occupation number notation* for vectors in $\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)$ as $|\mathbf{x}\rangle := (f_1^\dagger)^{x_1}(f_2^\dagger)^{x_2}\cdots f_d^\dagger)^{x_d}|0_F\rangle$ for any $\mathbf{x}\in\{0,1\}^d$. As the $|\mathbf{x}\rangle$ vectors are mapped via the Jordan-Wigner transformation to the computational basis states of , they are also called the *fermionic computational basis states* in $\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)$.

Since groups $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$ are compact groups (for comprehensive introduction to the theory of Lie groups and their representations, see [83, 84]), each possesses a unique normalized integration measure invariant under any group translation called Haar measure. We will donate this measure by μ_G for the G one of the symmetry groups above. Invariance of μ_G means that any measurable subset $A \subset G$ and any $h \in G$, we have that

$$\mu(hA) = \mu(Ah) = \mu(A)\ . \tag{15}$$

The above condition to the level of expectation values (averages) reads

$$\int_G d\mu(g) f(gh) = \int_G d\mu(g) f(hg) = \int_G d\mu(g) f(g)\ . \tag{16}$$

where f is any integrable function on G and $h \in G$. We will denote by ν_{pas} the distribution of the unitaries $V = \Pi_{\mathrm{pas}}(U)$, where U $\sim \mu_{\mathrm{U}(d)}$ and by ν_{act} distribution of the unitaries $\Pi_{\mathrm{act}}(O)$, where $O \sim \mu_{\mathrm{SO}(2d)}$. In order to keep the notation compact we will suppress the dependance of these measures on d and n (values of these parameters will be implied from the context).

Finally, we use the following notation to denote growth of functions: Let f and g be two positive-valued functions. We write $f = O(g)$ iff $\lim_{x\to\infty} f(x)/g(x) < \infty$ and $f = o(g)$ iff $\lim_{x\to\infty} f(x)/g(x) = 0$.

III. MAIN RESULTS

In this part we formally define our scheme for demonstration of quantum computational advantage and present informally main results of this work. In the end we comment on the practical feasibility of our quantum advantage scheme.

Having reviewed the basic concepts needed, we are now ready to formally introduce our quantum advantage proposal, which is illustrated in Fig. 1. We have a system of $d = 4N$ fermionic modes. The input state of the scheme is an N-fold tensor product the non-Gaussian magic state $|\Psi_4\rangle = (|1100\rangle + |0011\rangle)/\sqrt{2}$, i.e.,

$$|\Psi_{\text{in}}\rangle = |\Psi_4\rangle^{\otimes N} . \tag{17}$$

Note that states equivalent to this has been used in FLO computation schemes in [62, 64, 65]. After the initialization, a generic FLO operation is applied either respecting the particle-number conservation (passive scheme) or not (active scheme). Any FLO unitary can be decomposed into two-qubit FLO gates of linear depth either in diamond, triangle or brickwall layouts, see Figs. 1 and 3. The choice of the FLO operation V is done via the probability distributions ν_{pas} and ν_{act} induced from the Haar measures on $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$, respectively (see Section. II).

For a type of particular type of FLO circuit the computational task we address is ability is to sample from the output distribution

$$p_{\mathbf{x}}(V, \Psi_{\text{in}}) = |\langle \mathbf{x}|V|\Psi_{\text{in}}\rangle|^2 \ , \tag{18}$$

where output bitstring satisfy $|\mathbf{x}| = 2N$ and $|\mathbf{x}|$-even for passive FLO and active FLO respectively. This computational task will be referred to as *Fermion Sampling*. We prove four main technical results that underpin the hardness of Fermion Sampling.

The first result is anticoncentration for FLO circuits. Informally speaking it states that for the considered familly of circuits and fixed output $\mathbf{x}$ values $|\langle \mathbf{x}|V|\Psi_{\text{in}}\rangle|^2$ are typically not much smaller compared to they average average value.

Result 1 (Anticoncentration for generic FLO circuits)**.** *Let $\nu = \nu_{\text{pas}}$ or $\nu = \nu_{\text{act}}$ be uniform distribution over passive and respectively active FLO circuit acting on $4N$ fermion modes. Let Ψ_{in} be the input state to our quantum advantage proposal. Then, there exist a positive constant C such that for every outcome $\mathbf{x}$ and for every $\alpha \in [0, 1]$*

$$\Pr_{V \sim \nu}\left(p_{\mathbf{x}}(V, \Psi_{\text{in}}) > \frac{\alpha}{|\mathcal{H}|} \right) > (1 - \alpha)^2 C \ , \tag{19}$$

where $\mathcal{H} = \bigwedge^{2N}(\mathbb{C}^{4N})$ for passive FLO and $\mathcal{H} = \mathcal{H}^{+}_{\text{Fock}}(\mathbb{C}^{4N})$.

The formal version of this result is given in Theorem 1. It is important to emphasize that in the course of the proof of the this results we do not use the property of gate sets of interest forming an (approximate) $2-$design [37]. In fact, it can be proved that measures $\nu_{\text{pas}}, \nu_{\text{act}}$ do not form a projective $2-$design. We perform the proof of anticoncentration by heavily using group-theoretical techniques and particular properties of fermionic representations of symmetry groups $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$.

In line with standard methodology based on Stockmayer algorithm [60]), anticoncentration, and hiding property we reduce approximate sampling from $\{p_{\mathbf{x}}(V, \Psi_{\text{in}})\}$ to approximate computation of particular probability $p_{\mathbf{x}_0}(V, \Psi_{\text{in}})$ (see Theorem 2). This allows us to prove hardness of approximate Fermion Sampling in Theorem 3 by conjecturing non collapse of the polynomial hierarchy (cf. Conjecture 2) and average-case hardness of computation approximate computation of $p_{\mathbf{x}_0}(V, \Psi_{\text{in}})$ in relative error (cf. Conjecture 1).

Remark 1. *It is important to stress that in the passive FLO case our anticoncentration results* do not *follow from anticoncentration results for the determinant proved in [25]. The reason is that our probability amplitudes can be only expressed via determinants of submatrices of $U \in \mathrm{U}(d)$ (cf. Section VIII). Also, these submatrices cannot be approximated via Gaussian matrices (we work in the regime in which number of modes d is comparable to the total number of particles n.*

To give evidence for Conjecture 1 we prove two worst-to-average-case reductions that allow us to prove weaker versions of approximate hardness result

Result 2 (Worst-case to average reduction for exact computation of probabilities)**.** *Let $\nu = \nu_{\text{pas}}$ or $\nu = \nu_{\text{act}}$ be uniform distribution over passive and respectively active FLO circuit acting on $4N$ fermion modes. Let Ψ_{in} be the input state to our quantum advantage proposal. Let V_0 be a FLO gate (either active or passive)*

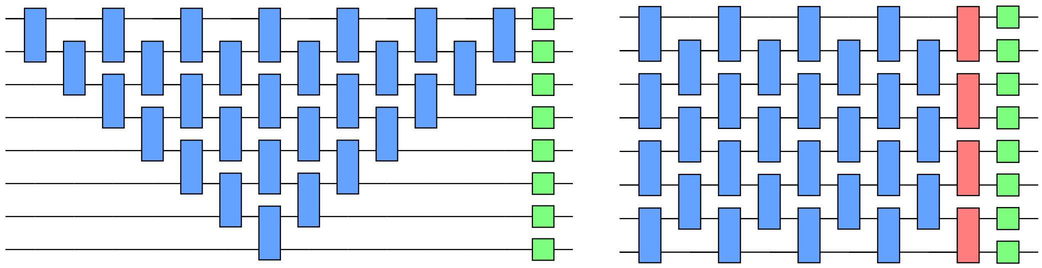

FIG. 3. Circuit layouts implementing arbitrary passive and active FLO transformations. These layouts are based on the decomposition of arbitrary elements of the U(d) and SO($2d$) groups into a sequence of nearest-neighbor Givens rotations and a diagonal matrix. The depicted two-qubit gates in the passive FLO case are of the type $D_{\mathrm{pas}}(\alpha_1, \alpha_2)$ (see Eq. (20)), while the single-qubit gates are Z-rotations. The two-qubit gates in the active FLO case are of the type $D_{\mathrm{act}}(\{\beta_i\})$ (see Eq. (21)) and the single-qubit gates are Pauli unitaries. The extra layer of red colored two-qubit gates are only needed in the active case. The decomposition of the two-qubit gates $D_{\mathrm{pas}}(\alpha_1, \alpha_2)$ and $D_{\mathrm{act}}(\{\beta_i\})$ into native gates of superconducting qubit architectures are provided in Fig. 4.

such that $p_{\mathbf{x}_0}(V_0), \Psi_{\mathrm{in}})$ *is* #P*-hard to compute (see Remark 10). It is then* #P*-hard to compute values of* $p_{\mathbf{x}_0}(V, \Psi_{\mathrm{in}})$ *with probability greater than* $\frac{3}{4} + \frac{1}{\mathrm{poly}(N)}$ *over the choice of* $V \sim \nu$*.*

Result 3 (Worst-case to average reduction for approximate computation of probabilities)**.** *Under the notation given in Result 2 we have that it is* #P*-hard to approximate probability* $p_{\mathbf{x}_0}(V, \Psi_{\mathrm{in}})$ *to within accuracy* $\epsilon = \exp(-\Theta(N^6))$ *with probability greater than* $1 - o(N^{-2})$ *over the choice of* $V \sim \nu$*.*

Formal versions of above two results can be found in Theorems 5 and 7. To obtain the above result we generalize the method developed recently by Movassagh [1] in the context of random quantum circuits. The key technical ingredient a Cayley path, which gives rational interpolation between quantum circuits. We realize that, for the purpose of the two reductions given above, it is possible to apply it directly on one the level of the Lie group underlying a particular class of FLO transformations (U(d) and SO($2d$) for passive and active FLO respectively). We then use the fact that fermionic representations can be realized low degree of polynomials in entries of matrices of appropriate symmetry groups. This observation allows us to adapt the the reduction method of Movassagh with relative ease.

Remark 2. *In the course of the proof of the above result we have realised an inadequate usage of the oracle in the reduction by Movassagh [1] (the author assumed that the oracle works as in* (156) *but without the necessary dependence on* Δ *. Correction of the proof seams to give in that case worse then claimed tolerance for error* $\epsilon = \exp(-\theta(N^{4.5})$ *(for the Google layout), which is still better then the one claimed here.*

Finally, the experimental feasibility of our proposal is further increased by the fact that due to the structure of FLO circuits, they can be efficiently certified using resources scaling polynomially with the system size.

Result 4 (Efficient tomography of FLO circuits)**.** *Let* V *be an unknown active FLO circuit on a system of* d *qubits that encodes* d *fermionic modes. Assume we have access to computational basis measurements and single qubit gates. Then* V *can be estimated up to accuracy* ϵ *in the diamond norm by repeating* $r \approx \frac{d^3}{\epsilon^2}$ *rounds of experiments, each involving* $O(d^2)$ *independent single qubit state preparations and single Pauli measurements at the end of the circuit.*

The rigorous formulation of the above, together with the explicit protocol for carrying out tomography, is provided in Section X. Importantly, our method avoids exponential scaling inherent to the general multiqubit tomography protocols. Moreover, it can can be also viewed as a fermionic analogue of the certification methods developed previously in the context of photonics and bosonic linear optics [85–87].

Implementation of the scheme

It is important to stress that our proposal has a strong potential for experimental realization, e.g., on quantum processors with superconducting qubit architectures. The actual implementation should be feasible already on near-term quantum devices, as the construction of parametric programmable passive linear optical circuits,

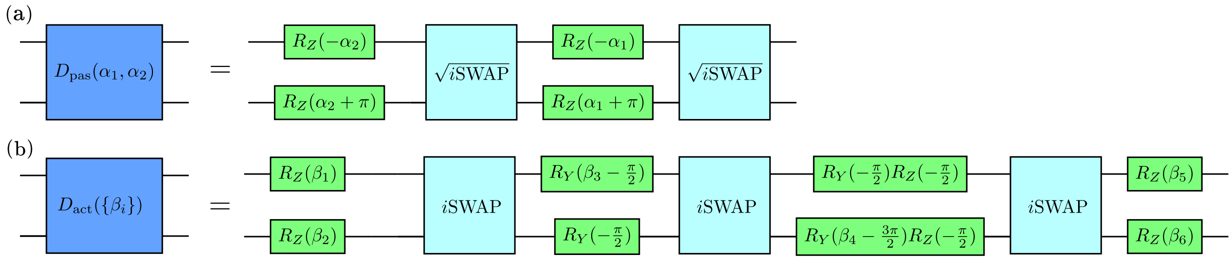

FIG. 4. Decomposition of (a) the Givens rotation in the passive FLO setting, $D_{\rm pas}(\alpha_1,\alpha_2)$, in terms of $\sqrt{i\rm SWAP}$ gates and (b) the merged Givens rotations in the active FLO setting, $D_{\rm act}(\{\beta_i\})$, in terms of iSWAP gates. $R_W(\alpha)$ (with $W\in\{X,Y,Z\}$) denotes the one-qubit rotation gate $\mathrm{e}^{i\alpha W}$.

due to their relevance in Quantum Chemistry, has been already experimentally demonstrated on Google's Sycamore quantum processor [21].

The preparation of the input fermionic magic state $|\Psi_4\rangle^{\otimes N}$, vital to our proposal, can be performed by applying on the computational basis state $|0\rangle^{\otimes 4N}$ a simple constant depth circuit consisting of 3 CNOTs and 3 one-qubit gates per quadruple blocks of qubits as shown in Fig. 1. One can implement an arbitrary passive FLO (or *basis rotation* in the Quantum Chemistry lingo) in linear depth using only nearest neighbor gates and assuming a minimal linearly connected architecture [46, 47]. Two such layouts are depicted in Fig. 3. In terms of two-qubit gates, the triangle layout has a depth of $d-1$, while the depth of the brickwall layout is only $d/2$. These circuits are analogous to the layouts of Boson Sampling circuits [50, 51] and are based on decomposing a unitary $U\in\mathrm{U}(d)$ into individual Givens rotations, which we describe in Appendix A. In the passive FLO case the the two qubit gates have the form:

$$D_{\rm pas}(\alpha_1,\alpha_2)=(\mathrm{e}^{-i\alpha_1 Z/2}\otimes \mathrm{e}^{i\alpha_1 Z/2})\,\mathrm{e}^{i\alpha_2(X\otimes X+Y\otimes Y)/2}, \tag{20}$$

and the final one qubit gates are Z rotations. The triangle and the brickwall layout can also be used to decompose an arbitrary active FLO operation [47, 48], however, in this case the two-qubit gates will have a more complicated structure (as they arise from merging several Givens rotations):

$$D_{\rm act}(\{\beta_i\})=(\mathrm{e}^{i\beta_5 Z/2}\otimes \mathrm{e}^{i\beta_6 Z/2})\,\mathrm{e}^{i(\beta_3 X\otimes X+\beta_4 Y\otimes Y)/2}\,(\mathrm{e}^{i\beta_1 Z/2}\otimes \mathrm{e}^{i\beta_2 Z/2}), \tag{21}$$

and the one-qubit unitaries at the end of the circuit are either Pauli matrices or identities. The derivation of these statements are given in Appendix A, they are based on the decomposition of arbitrary elements of the $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$ groups into a sequence of nearest-neighbor Givens rotations and a diagonal matrix. The passive FLO representation of the Givens rotations and of the diagonal matrix are then translated to two-qubit gates of the type $D_{\rm pas}(\alpha_1,\alpha_2)$ and a series single-qubit Z rotations in a layout the depicted Fig. 3. In the active FLO case several represented Givens rotations are merged into two-qubit gates of type $D_{\rm act}(\{\beta_i\})$ and the single-qubit unitaries at the end of the circuit are Pauli gates.

In the experimental demonstration of programmable passive FLO transformations by the Google team [21], the native gates of the Sycamore processors, the $\sqrt{i\rm SWAP}$ gates and single-qubit Z rotations, were used. The iSWAP and $\sqrt{i\rm SWAP}$ gates, defined as

$$i\mathrm{SWAP}=\begin{pmatrix}1&0&0&0\\0&0&-i&0\\0&-i&0&0\\0&0&0&1\end{pmatrix},\qquad \sqrt{i\mathrm{SWAP}}=\begin{pmatrix}1&0&0&0\\0&\frac{1}{\sqrt{2}}&\frac{-i}{\sqrt{2}}&0\\0&\frac{-i}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&0&0&1\end{pmatrix}, \tag{22}$$

were exactly introduced in quantum computing as standard gates because they are native in superconducting qubit architectures [88]. It is important to note that these gates are actually FLO gates. This lucky coincidence supports the feasibility of our proposal, since the Givens rotations for passive FLO, i.e., the two-qubit gates $D_{\rm pas}(\alpha_1,\alpha_2)$ in the layouts of Figs. 3, can be decomposed into two $\sqrt{i\rm SWAP}$ gates and four single qubit Z-rotations as depicted in part (a) of Fig. 4. The two-qubit gates used in the active FLO setup,

$D_{\mathrm{act}}(\{\beta_i\})$, can be decomposed into 3 iSWAP gates shown in part (b) of Fig. 4.

IV. DISCUSSION AND OPEN PROBLEMS

We believe that our results and techniques used to establish them will be of relevance also for problems not directly related to Fermion Sampling.

The first group of potential applications is related to the structure of our quantum advantage scheme. As discussed in the introduction, quantum advantage proposals are typically not constructed because of their practical usefulness. However, recently several proposals for applications of Boson Sampling [25] and Gaussian Boson Sampling [33, 34] have been suggested. These include combinatorial optimization problems [89, 90], calculation of Franck–Condon profiles for vibronic spectra [91, 92], molecular docking [93] and machine learning using graph kernels [94]. All of those application are based on the fact that this type of sampling, unlike the generic Random Circuit Sampling, have a very structured nature. In particular, most of the mentioned applications use the fact that one can sample with probabilities proportional to the permanents and Hafnians of certain matrices constructed from the circuit description. These polynomial functions of matrix entries encode interesting properties, e.g., for adjacency matrices of graphs they provide the number of cycle covers and perfect matchings of the graph, respectively. In our proposal similar polynomials appear when describing the sampling probabilities: the mixed discriminant [63] and their generalizations (e.g., mixed Pfaffian [95]), which also encode important graph properties. Thus, we have good reasons to believe that our proposal, beside providing a robust computational advantage setup, also can be used for other algorithms with interesting applications.

We also want to emphasize the universality of our techniques for establishing anticoncentration and worst-to-average-case reduction for structured random circuits. Our anticoncentration result exploits group-theoretic properties of fermionic circuits and can be likely generalized to other scenarios where low-dimensional group structure appears. Moreover, our generalization of the worst-to-average-case reduction of Movassagh [1] can be applied to any sampling problem provided outcome probabilities can be interpreted as polynomials on low-dimensional groups (Cayley transformation that underlines the reduction can be defined on arbitrary Lie groups). For example, one can view Boson Sampling in the first quantization picture where the group of linear optical networks acts on the totally symmetric subspace of N qudits, where d is the number of modes (or other representation when bosons are partially distinguishable [96]), as opposed to the totally antisymmetric representation for fermions.

We conclude this part with stating a number of interesting problems that require further study.

- *Role of non-Gaussianity for hardness and anticoncentration*: In practice magic states are not perfect and a high level of noise can bring these states into the convex hull of Gaussian states [64, 76, 77], which we know are efficiently simulable classically under FLO evolutions and Gaussian measurements. How much noise does our hardness result tolerate? The same question applies to anticoncentration of output probabilities, in which case we do not yet have a proof that FLO circuits with Gaussian inputs do not anticoncentrate, but we have numerical evidence that proofs based on the Paley-Zygmund inequality do not work (see Remark 5).

- *Fermion Sampling with less magic*: In our scheme, all the input qubit lines are injected with magic states. In contrast, [81] shows that FLO circuits with $O(1)$ magic input states remain weakly simulable classically even with adaptive measurements. Do the hardness result and anticoncentration hold if we use only, say, $O(\log m)$ magic states?

- *Algorithms for classical simulation*: Devising algorithms to approximately simulate FLO circuits with magic input states on average would not only lead to useful applications (for example in the context of quantum chemistry), but is also vital to understand the complexity landscape of random FLO circuits. For RCS scheme employed in Google's experiment with qubits placed on a 2D grid, advances in classical simulation techniques imposed a limit on the robustness of the average-case hardness that can be achieved with the current worst-to-average-case reduction that is agnostic to the circuit architecture and depth [97].

- *Tomography and certification of FLO circuits and Fermion Samping*: In this work, we only gave an efficient method to estimate an unknown FLO circuit (A related benchmarking of FLO circuits was recently proposed in [98].). It is interesting to extend our scheme beyond unitary circuits and to devise a method for which sample complexity and number of experimental settings exhibit an optimal scaling with the system size. Additionally, with further assumption on how the quantum device operates (e.g. the noise model), is there a simple diagnostic tool for Fermion Sampling similar to cross-entropy benchmarking for RCS [28]?

V. ANTICONCENTRATION OF FLO CIRCUITS

In this section we prove that outcome probabilities in fermionic circuits initialized in the state Ψ_{in} anticoncentrate for Haar random fermionic linear optical circuits. We prove anticoncentration for both passive and active fermionic linear optics. Our proof is based on interpretation of these circuits in terms of representation of group $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$, where d is the number of fermionic modes used.

Let $\mathcal{H}$ be a Hilbert space and let $\{|\mathbf{x}\rangle\}$ be a fixed (computational) basis of $\mathcal{H}$. For $V \in \mathrm{U}(\mathcal{H})$ and a pure state $|\Psi\rangle$. In what follows we will denote by $p_{\mathbf{x}}(V, \Psi)$ the probability of obtaining outcome $\mathbf{x}$ on some input state $|\Psi\rangle$ on which unitary V was applied. Born rule implies:

$$p_{\mathbf{x}}(V, \Psi) = |\langle \mathbf{x}|V|\Psi\rangle|^2 \ . \tag{23}$$

In what follows we restrict our attention to $\mathcal{H} = \bigwedge^{2N}(\mathbb{C}^{4N})$ (for passive FLO) and $\mathcal{H} = \mathcal{H}_{\mathrm{Fock}}^{+}(\mathbb{C}^{4N})$ (for active FLO. Moreover for $\mathbf{x} \in \{0,1\}^{4N}$ vectors $|\mathbf{x}\rangle$ will denote standard Fock states (cf. Section II). In both of the cases considered the set of allowed $\mathbf{x}$ is different (See Theorem 1 for more details).

Definition 1 (Anticoncentration of ensemble of unitary matrices)**.** *Let ν be an ensemble (probability distribution) of unitary matrices $\mathrm{U}(\mathcal{H})$. We say that that ν exhibits anticoncentration on input state $|\Psi\rangle$ if and only if for every outcome $\mathbf{x}$ of computational basis measurement*

$$\Pr_{V\sim\nu}\left(p_{\mathbf{x}}(V, \Psi) > \frac{\alpha}{|\mathcal{H}|}\right) > \beta \ , \tag{24}$$

where α, β are positive constants.

Remark 3. *In this work we will be concerned with families of probability distributions that are defined on Hilbert spaces of increasing dimension, parametrized by the total number of fermionic modes d. In this context, motivated by structure of the proof of hardness of sampling (see Theorem 3) we will be interested in cases when $\alpha, \beta = \Theta(1)$ i.e are independent on $|\mathcal{H}|$.*

Below we state our main result regarding anticoncentration of fermionic linear circuits initialized in the tensor product of Fermionic magic states

$$|\Psi_{\mathrm{in}}\rangle = |\Psi_4\rangle^{\otimes N}, \tag{25}$$

where $|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$. Note that $|\Psi_{\mathrm{in}}\rangle \in \bigwedge^{2N}(\mathbb{C}^{4N})$.

Theorem 1 (Anticoncentration for fermionic linear optical circuits initialized in product of magic states)**.** *Let $\mathcal{H}_{\mathrm{pas}} = \bigwedge^{2N}(\mathbb{C}^{4N})$ and let $\mathcal{H}_{\mathrm{act}} = \mathcal{H}_{\mathrm{Fock}}^{+}(\mathbb{C}^{4N})$ be Hilbert spaces describing $2N$ Fermions in $4N$ modes and positive parity Fermions in $4N$ modes. Let $\mathcal{G}_{\mathrm{pas}}$ and $\mathcal{G}_{\mathrm{act}}$ be respectively passive and active FLO transformations acting on the respective Hilbert spaces and distributed according to the uniform measures ν_{pas} and ν_{act} (see Section II). Let $|\Psi_{\mathrm{in}}\rangle$ be the initial state to which both families of circuits are applied. Then, for every $\mathbf{x}$ of Hamming weight $|\mathbf{x}| = 2N$ we have*

$$\Pr_{V\sim\nu_{\mathrm{pas}}}\left(p_{\mathbf{x}}(V, \Psi_{\mathrm{in}}) > \frac{\alpha}{|\mathcal{H}_{\mathrm{pas}}|}\right) > (1-\alpha)^2 C_{\mathrm{pas}} \ , \tag{26}$$

where $C_{\rm pas} = 5.7$ *and* $|\mathcal{H}_{\rm pas}| = \binom{4N}{2N}$*. Moreover, for every* $\mathbf{x}$ *with even Hamming weight we have*

$$\Pr_{V\sim\nu_{\rm act}}\left(p_{\mathbf{x}}(V,\Psi_{\rm in}) > \frac{\alpha}{|\mathcal{H}_{\rm act}|}\right) > (1-\alpha)^2 C_{\rm act}\ , \tag{27}$$

where $C_{\rm act} = 9$ *and* $|\mathcal{H}_{\rm act}| = 2^{4N}/2$*.*

Proof. In order to prove Eq. (26) and Eq. (26) we start with a standard tool used when proving anticoncentration - the Paley-Zygmund inequality. It states that for arbitrary nonnegative bounded random variable X and for $0<\alpha<1$, we have

$$\Pr_X(X > \alpha\mathbb{E}X) \geq (1-\alpha)^2\frac{\mathbb{E}X^2}{(\mathbb{E}X)^2}\ . \tag{28}$$

We use this bound for $X = |\langle\mathbf{x}|V|\Psi_{\rm in}\rangle|^2$, where $V\sim\nu_{\rm pas}$ or $V\sim\nu_{\rm pas}$. Recall that, as explained in the Section II, linear circuits $\mathcal{G}_{\rm pas}$ and $\mathcal{G}_{\rm act}$ can be understood in terms of representations of symmetry groups $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$. Haar measures on these symmetry groups induce uniform distributions on the $\mathcal{G}_{\rm pas}$ and $\mathcal{G}_{\rm act}$. Therefore for $k=1,2$ we have

$$\mathop{\mathbb{E}}_{V\sim\nu}\left[p_{\mathbf{x}}(V,\Psi_{\rm in})^k\right] = \int_G d\mu(g)\left[\mathrm{tr}(|\mathbf{x}\rangle\langle\mathbf{x}|\,\Pi(g)\Psi_{\rm in}\Pi(g)^\dagger)\right]^k\ , \tag{29}$$

where μ is the Haar measure on a Lie group G, and Π is a unitary representation of G in a suitable Hilbert space $\mathcal{H}$. The case of passive FLO corresponds to $G=\mathrm{U}(4N)$ and $\Pi=\Pi_{\rm pas}$ while for active FLO we have $G=\mathrm{SO}(8N)$ and $\Pi=\Pi_{\rm act}$ (c.f. Eq.(4) and Eq. (9)). Both groups are irreducibly represented in Hilbert spaces $\mathcal{H}_{\rm act}$ and $\mathcal{H}_{\rm pas}$ by virtue of Schur lemma unitaries $\Pi(g)$ forming a 1-design. Consequently

$$\mathop{\mathbb{E}}_{V\sim\nu}\left[p_{\mathbf{x}}(V,\Psi_{\rm in})\right] = \int_G d\mu(g)\left[\mathrm{tr}(|\mathbf{x}\rangle\langle\mathbf{x}|\,\Pi(g)\Psi_{\rm in}\Pi(g)^\dagger)\right] = \mathrm{tr}(|\mathbf{x}\rangle\langle\mathbf{x}|\int_G d\mu(g)\left[\Pi(g)\Psi_{\rm in}\Pi(g)^\dagger\right]) = \frac{1}{|\mathcal{H}|}\ , \tag{30}$$

where in the last equality we used the 1-design property and the fact that $|\mathbf{x}\rangle\in\mathcal{H}$ is a normalized vector. Computation of the second moment can be greatly simplified by the usage of group theory. Let us first rewrite $\mathop{\mathbb{E}}_{V\sim\nu}\left[p_{\mathbf{x}}(V,\Psi_{\rm in})^2\right]$ in the form convenient for computation:

$$\mathop{\mathbb{E}}_{V\sim\nu}\left[p_{\mathbf{x}}(V,\Psi_{\rm in})^2\right] = \int_G d\mu(g)\left[\mathrm{tr}(|\mathbf{x}\rangle\langle\mathbf{x}|^{\otimes 2}\,\Pi(g)^{\otimes 2}\Psi_{\rm in}^{\otimes 2}(\Pi(g)^\dagger)^{\otimes 2}\right] = \mathrm{tr}(A_{\Pi,G}\Psi_{\rm in}\otimes\Psi_{\rm in})\ , \tag{31}$$

where, due to unitarity of representation Π, and invariance of Haar measure under transformation $g\mapsto g^{-1}$

$$A_{\Pi,G} = \int_G d\mu(g)\left[\Pi(g)^{\otimes 2}\,|\mathbf{x}\rangle\langle\mathbf{x}|^{\otimes 2}\,(\Pi(g)^\dagger)^{\otimes 2}\right]\ . \tag{32}$$

Operator $A_{\Pi,G}$ acts on two copies of the original Hilbert space, $\mathcal{H}\otimes\mathcal{H}$ and is a manifestly G invariant in the sense that for all g we have $[A_{G,\Pi},\Pi(g)^{\otimes 2}]=0$. The integration in (32) can be carried out explicitly because objects in question have very specific properties that are rooted in the fact that Fock states constitute generalized coherent states of the considered representations of $\mathrm{U}(4N)$ and $\mathrm{SO}(8N)$ (cf. Remark 4 for more details). Let $|\Psi\rangle$ be a fixed pure state in $\mathcal{H}$ and let $|\mathbf{x}\rangle$ be a fixed fermionic Fock state belonging to appropriate Hilbert space $\mathcal{H}$

$$\text{There exist } g\in G \text{ s.t. } \Psi = \Pi(g)\,|\mathbf{x}\rangle\langle\mathbf{x}|\,\Pi(g)^\dagger \iff |\Psi\rangle^{\otimes 2}\in\tilde{\mathcal{H}}\ , \tag{33}$$

where $\tilde{\mathcal{H}}\subset\mathcal{H}\otimes\mathcal{H}$ is the carrier space of certain unique irreducible representation of G. In other words, it appears as one of the irreducible representations in the decomposition of the space $\mathcal{H}\otimes\mathcal{H}$, where G is represented via $g\mapsto\Pi(g)^{\otimes 2}$. Let $\tilde{\mathbb{P}}$ be the orthonormal projector onto $\tilde{\mathcal{H}}\subset\mathcal{H}\otimes\mathcal{H}$. Due to property (33) we get that $\mathrm{supp}(A_{\Pi,G})\subset\tilde{\mathcal{H}}$. Combining this with G-invariance of $A_{\Pi,G}$ we get, using Schur lemma, that $A_{\Pi,G}$ must be proportional to $\tilde{\mathbb{P}}$. The proportionality constant follows easily from normalization of $A_{\Pi,G}$.

Putting this all together we obtain

$$A_{\Pi,G} = \frac{1}{|\tilde{\mathcal{H}}|}\tilde{\mathbb{P}} \ . \tag{34}$$

Inserting the expressions for the first and second moments to Payley-Zygmund inequality we get

$$\Pr_{V\sim\nu}\left(p_{\mathbf{x}}(V,\Psi_{\mathrm{in}}) > \frac{\alpha}{|\mathcal{H}|}\right) \geq (1-\alpha)^2 \frac{|\tilde{\mathcal{H}}|}{|\mathcal{H}|^2}\frac{1}{\mathrm{tr}(\tilde{\mathbb{P}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}})} \ . \tag{35}$$

From the above expression it is clear that anticoncentration is controlled by: (i) the ratio of $\frac{|\tilde{\mathcal{H}}|}{|\mathcal{H}|^2}$ and (ii) expectation value $\mathrm{tr}(\tilde{\mathbb{P}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}})$. We will give explicit forms of the projectors $\tilde{\mathbb{P}}$, as well-as the dimensions $|\tilde{\mathcal{H}}|$ for both passive and active FLO in Lemmas 12 and 14 in the Appendix. From the expressions given there we obtain [3]

$$\frac{|\tilde{\mathcal{H}}_{\mathrm{pas}}|}{|\mathcal{H}_{\mathrm{pas}}|^2} \geq \frac{1}{N}\ , \ \frac{|\tilde{\mathcal{H}}_{\mathrm{act}}|}{|\mathcal{H}_{\mathrm{act}}|^2} \geq \frac{1}{\sqrt{\pi N}} \ . \tag{36}$$

For passive FLO this gives (recall that $|\mathbf{x}| = 2N$ and $\mathcal{H}_{\mathrm{pas}} = \bigwedge^{2N}(\mathbb{C}^{4N})$)

$$\Pr_{V\sim\nu_{\mathrm{pas}}}\left(p_{\mathbf{x}}(V,\Psi_{\mathrm{in}}) > \frac{\alpha}{\binom{4N}{2N}}\right) \geq (1-\alpha)^2 \frac{1}{N}\frac{1}{\mathrm{tr}(\mathbb{P}_{\mathrm{pas}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}})} \ . \tag{37}$$

Similarly, for active FLO we obtain (recall that $|\mathbf{x}|$ is even and $\mathcal{H}_{\mathrm{act}} = \mathcal{H}^{+}_{\mathrm{Fock}}(\mathbb{C}^{4N})$) we have

$$\Pr_{V\sim\nu_{\mathrm{act}}}\left(p_{\mathbf{x}}(V,\Psi_{\mathrm{in}}) > \frac{\alpha}{2^{4N-1}}\right) \geq (1-\alpha)^2 \frac{1}{\sqrt{\pi N}}\frac{1}{\mathrm{tr}(\mathbb{P}_{\mathrm{act}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}})} \ . \tag{38}$$

In order to complete the proof we need the following inequalities

$$\mathrm{tr}(\mathbb{P}_{\mathrm{pas}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}}) \leq \frac{C_{\mathrm{pas}}}{N} \quad , \quad \mathrm{tr}(\mathbb{P}_{\mathrm{act}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}}) \leq \frac{C_{\mathrm{act}}}{\sqrt{N}} \ . \tag{39}$$

Prove of the above relies on the explicit form of the projectors as well as some combinatorial considerations. The details are given in the appendix (see specifically Lemma 13 for of passive FLO and Lemma 15 for active FLO). ☐

Remark 4. *The existence of projector $\tilde{\mathbb{P}}$ such that equivalence in Eq.* (33) *holds follows form the the group-theoretical characterizations of of Slater determinants as well as pure fermionic Gaussian states with positive parity. Namely, these classes of states constitute examples the so-called* generalized coherent states *of simple, compact and connected Lie groups (*$\mathrm{SU}(d)$ *and* $\mathrm{Spin}(2d)$*) that are irreducibly represented in the appropriate Hilbert space (*$\bigwedge^n(\mathbb{C}^d)$ *and* $\mathcal{H}^{+}_{\mathrm{Fock}}(\mathbb{C}^d)$ *respectively). The fact that such classes of states can be characterized via the quadratic condition* $A|\Psi\rangle^{\otimes 2} = 0$ *is as known result in algebraic geometry [99]. This was translated to the quantum information language in [100], later rephrased as* (33) *and used to characterize correlations in systems consisting of indistinguishable particles [101, 102] (see also Chapter 3 of [103]). An equivalent characterization of pure fermionic gaussian states was also independently discovered by Bravyi in the context of fermionic quantum information [69] (see also [76]).*

Remark 5. *A curious reader may wonder whether anticoncentration holds also if FLO circuits that are initialized in free Gaussian states* Ψ_{gauss} *(with fixed number of particles for passive FLO). For such states* $\mathrm{tr}(\tilde{\mathbb{P}}\,\Psi_{\mathrm{gauss}}\otimes\Psi_{\mathrm{gauss}}) = 1$ *and therefore for such we cannot get strong anticoncentration inequalities using Eq.* (35)*. We have also tried to use higher moments in conjugation with Payley-Zygmund inequality but this*

---

[3] To simplify expressions for active FLO, we use the bound $\binom{4N}{2N} \leq \frac{2^{8N}}{\sqrt{\pi 4N}}$.

did not . We leave the question whether FLO circuits anticoncentrate when acting on Gaussian states as an open problem.

VI. HARDNESS OF SAMPLING

In this part we use anticoncentration of FLO circuits and standard complexity-theoretic conjectures to prove classical hardness for sampling from FLO circuits initialized by magic states. We adopt to the fermionic setting standard techniques [27, 31, 32, 59] that use the anticoncentration property to prove hardness of sampling based on conjectures about hardness of approximation of probability amplitudes $p_{\mathbf{x}}(V, \Psi_{\mathrm{in}})$ to within relative error.

We start with a formal definition of a sampling problem defined by FLO circuits initialized in magic input states.

Definition 2 (ϵ-Fermion Sampling task)**.** *Let $\mathcal{H}_{\mathrm{pas}} = \bigwedge^{2N}(\mathbb{C}^{4N})$ and let $\mathcal{H}_{\mathrm{act}} = \mathcal{H}^{+}_{\mathrm{Fock}}(\mathbb{C}^{4N})$ be Hilbert spaces describing $2N$ Fermions in $4N$ modes and positive parity Fermions in $4N$ modes. Let $\mathcal{G}_{\mathrm{pas}}$ and $\mathcal{G}_{\mathrm{act}}$ be passive and active FLO transformation. Let V be an FLO circuit on the Hilbert space $\mathcal{H}_{\mathrm{pas}}$ or $\mathcal{H}_{\mathrm{act}}$ and let $p(V)$ denote probability distribution $p_{\mathbf{x}}(V, \Psi_{\mathrm{in}})$. Given a description of V, sample from a probability distribution $q(V)$ that is ϵ-close to $p(V, \Psi_{\mathrm{in}})$ in l_1-norm (twice the total variation distance)*

$$\|p(V) - q(V)\|_1 = \sum_{\mathbf{x}} |p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| \leq \epsilon, \tag{40}$$

in time $\mathrm{poly}(N)$.

Remark 6. *It is more convenient to use l_1-norm in place of the TVD as it appears more directly in the proof of Theorem 2.*

It was realized in [25, 27] that, by virtue of Stockmeyer's theorem, the hardness of classically sampling from $p_{\mathbf{x}}(V, \Psi)$ up to an additive error is connected to the hardness of computing $p_{\mathbf{x}}(V, \Psi)$ for most instances of $\mathbf{x}$ and U. In particular, the existence of a classical machine that performs the sampling task implies average-case approximation in a low level of the complexity class called the polynomial hierarchy. To prove this fact, we start by defining the notion of approximating in the average-case.

Definition 3. *An algorithm $\mathcal{O}$ is said to give an (η, δ)-multiplicative approximate of $q_{\mathbf{z}}$ on average over the probability distribution $\mathcal{P}$ of inputs $\mathbf{z}$ iff $\mathcal{O}$ outputs $\mathcal{O}_{\mathbf{z}}$ such that*

$$\Pr_{\mathbf{z} \sim \mathcal{P}} [|\mathcal{O}_{\mathbf{z}} - q_{\mathbf{z}}| \leq \eta q_{\mathbf{z}}] \geq 1 - \delta \tag{41}$$

Remark 7. *For applications to hardness of sampling, $\mathbf{z}$ will generally be a tuple of inputs $(V, \mathbf{x})$, an FLO circuit and a measurement outcome. Correspondingly, $\mathcal{P}$ will be the joint probability distribution $V \sim \nu_{\mathrm{pas}}$ and $\mathbf{x} \sim \mathrm{unif}(\mathcal{H}_{\mathrm{pas}})$ in the case of passive FLO (resp. $V \sim \nu_{\mathrm{act}}$ and $\mathbf{x} \sim \mathrm{unif}(\mathcal{H}_{\mathrm{act}})$ in the case of active FLO), where $\mathbf{x} \sim \mathrm{unif}(\mathcal{H})$ is the uniform distribution of outcomes restricted to the Hilbert space $\mathcal{H}$.*

We now prove the hiding property [25, 27, 29], of FLO circuits. This will would allow us to focus on hardness of particular outcome probability.

Lemma 1 (Hiding property for FLO)**.** *Consider a fixed state $|\mathbf{x}_0\rangle \in \mathcal{H}_{\mathrm{pas}}$ ($\mathcal{H}_{\mathrm{act}}$ resp.) then for any V passive FLO (active FLO resp.) and $|\mathbf{x}\rangle \in \mathcal{H}_{\mathrm{pas}}$ ($\mathcal{H}_{\mathrm{act}}$ resp.) there is a passive (active) FLO $V_{\mathbf{x}}$ such that $|\langle \mathbf{x}|V|\Psi_{\mathrm{in}}\rangle|^2 = |\langle \mathbf{x}_0|V_{\mathbf{x}}|\Psi_{\mathrm{in}}\rangle|^2$*

Proof. It is enough to show that given $\mathbf{x}$ there is $V_{\mathbf{x}}$ passive (active) FLO s.t. $V_{\mathbf{x}}|\mathbf{x}_0\rangle = |\mathbf{x}\rangle$ up to a global phase. In the passive case this is achieved with gates implementing fermionic swaps $U^{[i,j]}$ such that $U^{[i,j]} f_i^\dagger U^{[i,j]\dagger} = f_j^\dagger$ and $U^{[i,j]} f_j^\dagger U^{[i,j]\dagger} = f_i^\dagger$, the order in which they are applied is defined by $|\mathbf{x}\rangle$. The same can be accomplished in active FLO case with operators $-\mathrm{i} m_{2i} m_{2i+1}$ changing the number of fermions (but not parity) and quasi braiding operators $U^{(p,q)}$ to exchange the majorana operators to the corresponding places. The quasi braidings act on majorana operators as $U^{(p,q)}m_p(U^{(p,q)})^\dagger = m_q$, $U^{(p,q)}m_q(U^{(p,q)})^\dagger = m_p$ and $U^{(p,q)}m_x(U^{(p,q)})^\dagger = m_x$ when $x \neq p, q$.

□

An additional ingredient required for a quantum sampling advantage is anti-concentration which states that most output probabilities of a random circuit are sufficiently big so that the approximation error to computing the probabilities is small relative to the probabilities being computed. Both average-case hardness and anti-concentration provide robustness of the sampling task to noise.

Theorem 2 (From approximate sampling to approximately computing probabilities)**.** *Let $\mathcal{H}_{\text{pas}} = \bigwedge^{2N}(\mathbb{C}^{4N})$ and let $\mathcal{H}_{\text{act}} = \mathcal{H}^+_{\text{Fock}}(\mathbb{C}^{4N})$ be Hilbert spaces describing $2N$ Fermions in $4N$ modes and positive parity Fermions in $4N$ modes. Consider in parallel passive FLO circuits and active FLO circuits acting on the input state $|\Psi_{\text{in}}\rangle$. If there is a classical algorithm $\mathcal{C}$ that performs Fermion Sampling as described in Definition 2 with the l_1-error $C/64$, where C is the constant $C_{\text{pas}} = 5.7$ (resp. $C_{\text{act}} = 9$) appearing in the anticoncentration condition for passive FLO circuits (resp. active FLO circuits) in Theorem 1.*

Then there is an algorithm in BPP^{NP} that approximates the probability $p_{\mathbf{x}_0}(V, \Psi_{\text{in}})$ for an arbitrary but fixed fiducial outcome $\mathbf{x}_0$ up to multiplicative error $1/4 + o(1)$ on $C/8$ fraction of FLO circuits drawn from the distribution $\nu = \nu_{\text{pas}}$ for passive FLO circuits (resp. ν_{act} for active FLO circuits.)

Proof. With the fixed input $|\Psi_{\text{in}}\rangle = |\Psi_4\rangle^{\otimes N}$, let us write $p_{\mathbf{x}}(V) = |\langle \mathbf{x}|V|\Psi_{\text{in}}\rangle|^2$ for the probability of outcome $\mathbf{x}$, and $p(V)$ for the output probability distribution of a circuit V. Suppose that there exists a classical sampler $\mathcal{C}$ that performs Fermion Sampling for a fixed but arbitrary FLO circuit V, and denote by $q(V)$ the distribution from which $\mathcal{C}$ samples. Then for a given $\mathbf{x}$, by Stockmeyer's approximate counting algorithm [60], a BPP^{NP} machine with an oracle access to $\mathcal{C}$ can produce a multiplicative estimates $\tilde{q}_{\mathbf{x}}(V)$ of $q_{\mathbf{x}}(V)$ such that

$$|q_{\mathbf{x}}(V) - \tilde{q}_{\mathbf{x}}(V)| \leq \frac{q_{\mathbf{x}}}{\text{poly}(N)} \tag{42}$$

for every $\mathbf{x}$. We will show that $\tilde{q}_{\mathbf{x}}(V)$ is also close to $p_{\mathbf{x}}(V)$ for most $\mathbf{x}$ and V that anti-concentrate. Judiciously applying the triangle inequality, we have that

$$\begin{aligned} |p_{\mathbf{x}}(V) - \tilde{q}_{\mathbf{x}}(V)| &\leq |p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| + |q_{\mathbf{x}}(V) - \tilde{q}_{\mathbf{x}}(V)| && (43)\\ &\leq |p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| + \frac{q_{\mathbf{x}}(V)}{\text{poly}(N)} && (44)\\ &\leq |p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| + \frac{|p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| + p_{\mathbf{x}}(V)}{\text{poly}(N)} && (45)\\ &= \frac{p_{\mathbf{x}}(V)}{\text{poly}(N)} + |p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| \left(1 + \frac{1}{\text{poly}(N)}\right) && (46) \end{aligned}$$

Given that the distributions $p(V)$ and $q(V)$ are ϵ-close in the l_1 norm, particular probabilities $p_{\mathbf{x}}(V)$ and $q_{\mathbf{x}}(V)$ must be exponentially close for most $\mathbf{x}$. This statement is made precise using Markov's inequality: for a nonnegative random variable X and $a > 0$,

$$\Pr(X \geq a) \leq \frac{\mathbb{E}X}{a}. \tag{47}$$

Setting $X = |p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)|$ and $a = \epsilon/(|\mathcal{H}|\delta)$, (the probability is over the outcomes $\mathbf{x}$ which is distributed uniformly over $\mathcal{H}$ as described in Remark 7)

$$\Pr_{\mathbf{x}\sim\text{unif}(\mathcal{H})}\left(|p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)| \geq \frac{\epsilon}{|\mathcal{H}|\delta}\right) \leq \frac{\mathbb{E}_{\mathbf{x}\sim\text{unif}(\mathcal{H})}(|p_{\mathbf{x}}(V) - q_{\mathbf{x}}(V)|)|\mathcal{H}|\delta}{\epsilon} \leq \delta. \tag{48}$$

Combining the probability bound with the inequality (46), we have that

$$\Pr_{\mathbf{x}\sim\mathrm{unif}(\mathcal{H})}\left[|p_{\mathbf{x}}(V)-\tilde{q}_{\mathbf{x}}(V)|<\frac{p_{\mathbf{x}}(V)}{\mathrm{poly}(N)}+\frac{\epsilon}{|\mathcal{H}|\delta}\left(1+\frac{1}{\mathrm{poly}(N)}\right)\right]>1-\delta. \tag{49}$$

To turn the additive estimate to a multiplicative estimate, we use the anticoncentration condition (Theorem 1), which let us replace $1/|\mathcal{H}|$ by an upper bound $p_{\mathbf{x}}(V)/\alpha$ with probability $(1-\alpha)^2C$.

In order to do so, we must consider the joint probability of $(V,\mathbf{x})$ as described in Remark 7. Let A be the event that $p_{\mathbf{x}}(V)$ and $q_{\mathbf{x}}(V)$ for a fixed V are exponential close due to Markov's inequality, and B be the event that the distribution $p(V)$ anticoncentrates. The probability of both "good events" happening is lower bounded by $\Pr(A\cap B)\geq\max\{0,\Pr(A)+\Pr(B)-1\}$. That is, we have

$$\Pr_{V\sim\nu_{\mathrm{pas}},\mathbf{x}\sim\mathrm{unif}(\mathcal{H}_{\mathrm{pas}})}\left\{|p_{\mathbf{x}}(V)-\tilde{q}_{\mathbf{x}}(V)|<p_{\mathbf{x}}(V)\left[\frac{1}{\mathrm{poly}(N)}+\frac{\epsilon}{\alpha\delta}\left(1+\frac{1}{\mathrm{poly}(N)}\right)\right]\right\}>(1-\alpha)^2C_{\mathrm{pas}}-\delta, \tag{50}$$

$$\Pr_{V\sim\nu_{\mathrm{act}},\mathbf{x}\sim\mathrm{unif}(\mathcal{H}_{\mathrm{act}})}\left\{|p_{\mathbf{x}}(V)-\tilde{q}_{\mathbf{x}}(V)|<p_{x}(V)\left[\frac{1}{\mathrm{poly}(N)}+\frac{\epsilon}{\alpha\delta}\left(1+\frac{1}{\mathrm{poly}(N)}\right)\right]\right\}>(1-\alpha)^2C_{\mathrm{act}}-\delta. \tag{51}$$

We can simplify the above by using the hiding property described in Lemma 1. It implies that $p_x(V)=p_{\mathbf{x}_0}(V_{\mathbf{x}})$ and $\tilde{q}_{\mathbf{x}}(V)=\tilde{q}_{\mathbf{x}_0}(V_{\mathbf{x}})$. If we denote the by $\mathcal{A}_{\mathbf{x}}(V,\mathbf{x})$ an event in the left-hand side of (54) we obtain

$$\Pr_{V\sim\nu_{\mathrm{pas}},\mathbf{x}\sim\mathrm{unif}(\mathcal{H}_{\mathrm{pas}})}[\mathcal{A}(V,\mathbf{x})]=\mathbb{E}_{\mathbf{x}\sim\mathrm{unif}(\mathcal{H}_{\mathrm{pas}})}\left(\Pr_{V\sim\nu_{\mathrm{pas}}}[\mathcal{A}(V_{\mathbf{x}},\mathbf{x}_0)]\right) \tag{52}$$

Moreover from the invariance of the Haar measure it follows that for every $|\mathbf{x}\rangle\in\mathcal{H}_{\mathrm{pas}}$, $V_{\mathbf{x}}$ is distributed in the same way as V. Consequently,

$$\mathbb{E}_{\mathbf{x}\sim\mathrm{unif}(\mathcal{H}_{\mathrm{pas}})}\left(\Pr_{V\sim\nu_{\mathrm{pas}}}[\mathcal{A}(V_{\mathbf{x}},\mathbf{x}_0)]\right)=\mathbb{E}_{\mathbf{x}\sim\mathrm{unif}(\mathcal{H}_{\mathrm{pas}})}\left(\Pr_{V\sim\nu_{\mathrm{pas}}}[\mathcal{A}(V,\mathbf{x}_0)]\right)=\Pr_{V\sim\nu_{\mathrm{pas}}}[\mathcal{A}(V,\mathbf{x}_0)] \tag{53}$$

Repeating the same steps for active FLO we finally obtain that for every $\mathbf{x}_0$

$$\Pr_{V\sim\nu_{\mathrm{pas}}}\left\{|p_{\mathbf{x}_o}(V)-\tilde{q}_{\mathbf{x}_o}(V)|<p_{\mathbf{x}_o}(V)\left[\frac{1}{\mathrm{poly}(N)}+\frac{\epsilon}{\alpha\delta}\left(1+\frac{1}{\mathrm{poly}(N)}\right)\right]\right\}>(1-\alpha)^2C_{\mathrm{pas}}-\delta, \tag{54}$$

$$\Pr_{V\sim\nu_{\mathrm{act}}}\left\{|p_{\mathbf{x}_o}(V)-\tilde{q}_{\mathbf{x}_o}(V)|<p_{\mathbf{x}_0}(V)\left[\frac{1}{\mathrm{poly}(N)}+\frac{\epsilon}{\alpha\delta}\left(1+\frac{1}{\mathrm{poly}(N)}\right)\right]\right\}>(1-\alpha)^2C_{\mathrm{act}}-\delta. \tag{55}$$

Following [26] and requiring a constant ϵ and relative error $\epsilon/(\alpha\delta)$ (See Remark 8) we may set, for instance,

$$\alpha=\frac{1}{2},\qquad\qquad \delta=\frac{(1-\alpha)^2C}{2}=\frac{C}{8},\qquad\qquad \epsilon=\frac{\alpha\delta}{4}=\frac{C}{64}, \tag{56}$$

Stockmeyer's algorithm is able to output $(1/4+o(1),C/8)$)-multiplicative approximates of the output probabilities for $C/8$ fraction of the (passive or active, with constant C_{pas} or C_{act} respectively) FLO circuits V if there is a classical machine that approximately sample from $p_{\mathbf{x}}(V)$ for any FLO circuit V within the l_1 distance $C/64$.

□

Remark 8. *Of the three parameters $\epsilon,\delta,$ and α, the l_1-distance ϵ and the relative error $\epsilon/(\alpha\delta)$ are typically assumed to be constant ($1/4+o(1)$ for the latter) in quantum advantage proposals [27, 32, 57, 58]. In which case δ is also a constant, and then one optimizes for the constant α. However, one may allow ϵ to decay inverse polynomially in the size of the system while retaining a sensible notion of simulation by the sampling task [25, 59]. Doing so allows a more plausible (weaker) average-case hardness assumption but the sampling task becomes more demanding.*

Remark 9. *The proof given here follows the standard proof for circuits, for example in [27, 59]. Alternatively, one could arrive at a similar result in two steps: first showing that a classical approximate sampler implies approximations up to an additive error $\epsilon/|\mathcal{H}|$, where ϵ is the TV distance achieved in the sampling task in the polynomial hierarchy, then showing that anticoncentration improves the approximations to multiplicative ones [29]. The alternative proof may be beneficial when anticoncentration does not hold or is undesirable, for example, when anticoncentration renders (black box) certification of quantum advantage infeasible [104].*

Armed with Theorem 2, we now state the other conjectures needed before proving the hardness of sampling.

Conjecture 1 (Average-case of approximating probabilities on FLO circuits initialized in $|\Psi_{\rm in}\rangle$)**.** *Computing a $(1/4+o(1), C/8)$-multiplicative approximate to $p_{\mathbf{x}_0}(V,\Psi_{\rm in})$ for $C/8$ fraction of V sampled from the Haar distribution ν is #P-hard. ($C = C_{\rm pas}, \nu = \nu_{\rm pas}$ for passive FLO circuits and $C = C_{\rm act}, \nu = \nu_{\rm act}$ for active FLO circuits)*

Conjecture 2. *The polynomial hierarchy does not collapse.*

Remark 10. *The motivation for Conjecture 1 comes from the fact that computing exactly the probabilities is #P-hard, this can be seen by writing the output as a polynomial as in Lemma 5, it has been shown that computing a permanent exactly reduces to computing this polynomial and it is know that computing the permanent exactly is #P-hard.*

Theorem 3 (Hardness of sampling from FLO circuits initialized in $|\Psi_{\rm in}\rangle$)**.** *If Conjectures 1 and 2 are true, then there is no efficient classical algorithm that can approximately sample with l_1-error $C_{\rm pas}/64$ (resp. $C_{\rm act}/64$) from output probability distributions induced by passive (resp. active) FLO circuits with the input given by $|\Psi_{\rm in}\rangle$.*

Proof. By Theorem 2, if there were an approximate sampler with respect to passive (resp. active) FLO circuits with input $|\Psi_{\rm in}\rangle$, then there would exist a algorithm $\mathrm{BPP}^{\mathrm{NP}}$ that $(1/4+o(1), C/8)$-multiplicative approximates $p_{\mathbf{x}_0}(V,\Psi_{\rm in})$ in for $C/8$ fraction of passive (resp. active) FLO circuits. Where $C = C_{\rm pas}$ in the passive case and $C = C_{\rm act}$ in the active. By Conjecture 1 this is a #P-hard problem. It is known [105] that BPP is inside the third level of the polynomial hierarchy, i.e., $\mathrm{BPP}^{\mathrm{NP}} \subseteq \Sigma_3$. By a well known result of Toda [106] $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$ and thus $\mathrm{PH} \subseteq \Sigma_3$. ☐

VII. CAYLEY PATH FOR UNITARY AND ORTHOGONAL GROUPS

In this section, following [1], we introduce a rational interpolation between elements of the low-dimensional symmetry groups underlying FLO transformations. In what follows by G we will denote either of the Lie group $\mathrm{U}(d)$ ore $\mathrm{SO}(2d)$. The rational interpolation is constructed from the Cayley transform, which is a rational mapping form the Lie algebra $\mathfrak{g}$ into the corresponding group G. For both groups we give upper bounds for the total variation distance (TVD) between the Haar measure μ_G on G and and its *deformations* μ_G^θ obtained via Cayley path. These bounds imply TVD bounds between distributions of the corresponding FLO circuits. This and other technical results established bellow will be called upon in the proof of the worst-to-average-case reduction in Section IX.

The Lie algebras $\mathfrak{u}(d)$ and $\mathfrak{so}(2d)$ of $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$ are defined to be

$$\mathfrak{u}(d) = \{X \in \mathbb{C}^{d\times d} | X^\dagger = -X\}, \tag{57}$$

$$\mathfrak{so}(2d) = \{X \in \mathbb{R}^{2d\times 2d} | X^T = -X\}, \tag{58}$$

where X^T denotes the transpose of the matrix X.

Remark 11. *We do not use the physicists' convention which requires that elements of Lie algebra X satisfy $\exp(i\theta X) \in G$. Therefore, In particular, here $\mathfrak{u}(d)$ (resp. $\mathfrak{so}(d)$) consists of skew-Hermitian (resp. antistmmetric) matrices.*

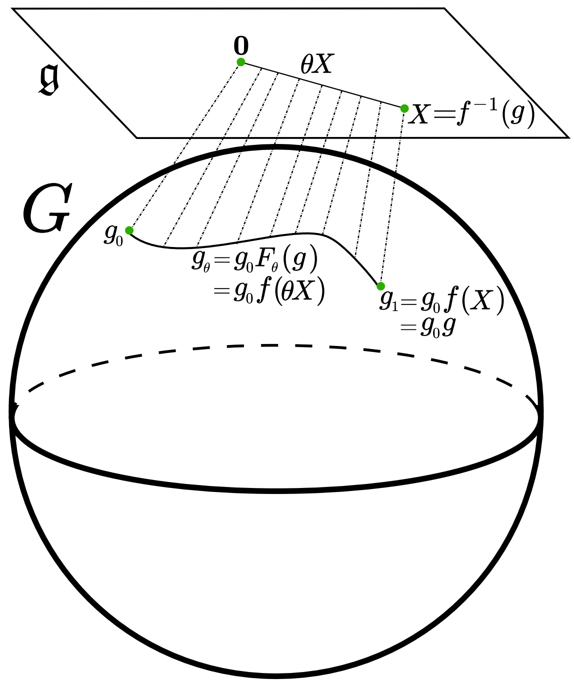

FIG. 5. Path deformation defined by the Cayley map in Eq. (59). A path is induced between element $g_0 \in G$ and $g_0 g$ by taking $X = f^{-1}(g) \in \mathfrak{g}$ and considering the perturbation $g_\theta = g_0 f(\theta X)$.

Every element $X \in \mathfrak{g}$ defines a one-parameter path in G: $\{\exp(\theta X)\}_{\theta\in\mathbb{R}}$, via the exponential map, $\exp : \mathfrak{g} \to G$. Both orthogonal and unitary groups are compact and connected, Therefore exponential map is surjective and can be used to parametrize G, and provides an interpolation between any two group elements. However, the interpolation is not polynomial in nature, and while it is possible to truncate the power series of exp to obtain a polynomial interpolation [29], the resulting interpolation represents circuits that are not unitary cf.[1]).

To remedy this [1] employs an algebraic Cayley transformation between $\mathfrak{u}(d)$ and $\mathrm{U}(d)$. This transformation can be however defined more generally as a mapping between Lie algebra ans the corresponding Lie group [107]. For our needs it is enough to consider the case of unitary and special orthogonal groups.

Definition 4 (Cayley transform for unitary and orthogonal group)**.** *Let G be $\mathrm{U}(d)$ or $\mathrm{SO}(2d)$, and let $\mathfrak{g}$ denotes its Lie algebra. The Cayley transform is a mapping $f : \mathfrak{g} \to G$ defined via*

$$f(X) = (\mathbb{I} - X)(\mathbb{I} + X)^{-1} \ . \tag{59}$$

It is easy to see that the image of $f(\mathfrak{g})$ equals a dense subset $\tilde{G} = \{g \in G \mid \{-1\} \notin \mathrm{sp}(g)\}$ consisting of elements of G (i.e unitary or orthogonal matrices) that do not have -1 in their spectrum. On $\tilde{G}$ the inverse of f is well-defined. Specifically, $f^{-1} : \tilde{G} \to \mathfrak{g}$ is given by

$$f^{-1}(g) = (\mathbb{I} - g)(\mathbb{I} + g)^{-1} \ , \tag{60}$$

where $g \in \tilde{G}$. This explicit form of the inverse map can be verified directly from the definition of f. Cayley map defines a path deformation between $g_0 \in G$ and $g_0 f(X)$ as follows (see Fig. VII)

Cayley map can be used to define a rational interpolation between arbitrary group elements. To this end consider first the map $F_\theta : \tilde{G} \to G$, given by

$$F_\theta(g) = f(\theta f^{-1}(g)), \ \theta \in [0, 1] \ . \tag{61}$$

The above mapping can be evaluated explicitly (note that elements of the considered Lie groups are normal matrices and therefore functional calculus can be performed effectively in the same way as if we were dealing with functions of a real variable):

$$F_\theta(g) = \frac{(1-\theta)\mathbb{I} + (1+\theta)g}{(1+\theta)\mathbb{I} + (1-\theta)g} \ , \ \theta \in [0,1] \ . \tag{62}$$

For both orthogonal and unitary operators we have $\|g\| = 1$. Therefore for $\theta \in (0,1]$ the denominator of (62) does not vanish and therefore we can use (62) to define F_θ to be a function defined on whole G, while for any $g \in G$ we get that $\lim_{\theta\to 0} F_\theta(g) = \mathbb{I}$. Therefore for $\theta \in [0,1]$ the denominator of (62) does not vanish and therefore we can use (62) to define F_θ to a be a function defined on whole G. Importantly, for the fixed input as θ goes from 0 to 1 we move on a rational path form the identity $\mathbb{I}$ to g. Consequently the path

$$g_\theta = g_0 F_\theta(g), \ \theta \in [0,1] \ . \tag{63}$$

a rational interpolation between a fixed group element g_0 (which can correspond, for example, to a worst-case #P-hard FLO circuit) and a completely generic group element $g_0 g$.

It is important to note that both $f(\theta X)$ and X be simultaneously brought into a block diagonal form by conjugation by elements of the group: $M \mapsto gMg^{-1}$. It follows from the fact that $f(\theta X)$ is simply a function of X and than the transformation properties of elements of $\mathfrak{g}$ under the conjugation by elements of G. For the case of $X \in \mathfrak{u}(d)$ we have an elementary fact from linear algebra that there exist a unitary $U \in \mathrm{U}(d)$ such that

$$UXU^\dagger = \sum_{j=1}^{d} \phi_j X_j \ , \tag{64}$$

where $X_j = i\,|j\rangle\langle j|$. Similarly, for any $X \in \mathfrak{so}(2d)$ there exist $O \in \mathrm{SO}(2d)$ sush that

$$OXO^T = \sum_{j=1}^{d} \phi_j \tilde{X}_j \tag{65}$$

where $\tilde{X}_j = |2j\rangle\langle 2j-1| - |2j-1\rangle\langle 2j|$ is the generator for the jth block. These statements have analogues on the level of elements of the group. Every unitary U can be transformed into a diagonal form

$$\mathrm{diag}(e^{i\phi_1}, e^{i\phi_2}, \ldots, e^{i\phi_d}) = \exp\left(\sum_{j=1}^{d} \phi_j X_j\right) \ . \tag{66}$$

For elements $\mathrm{SO}(2d)$, the block diagonalization amounts to the geometric fact that any $2d$-dimensional rotation can be decomposed into d independent planar rotations.

$$\mathrm{diag}\left(\begin{pmatrix} \cos\phi_1 & -\sin\phi_1 \\ \sin\phi_1 & \cos\phi_1 \end{pmatrix}, \begin{pmatrix} \cos\phi_2 & -\sin\phi_2 \\ \sin\phi_2 & \cos\phi_2 \end{pmatrix}, \ldots, \begin{pmatrix} \cos\phi_d & -\sin\phi_d \\ \sin\phi_d & \cos\phi_d \end{pmatrix}\right) = \exp\left(\sum_{j=1}^{d} \phi_j \tilde{X}_j\right) \ . \tag{67}$$

We now prove that for $1-\theta \leq o(\frac{1}{d^2})$ the distribution of elements of the group g, and $g_\theta = g_0 F_\theta(g)$, where $g \sim \mu_G$, are close in total variation distance.

Lemma 2 (TV distance between the Haar measure in G and its θ-deformation)**.** *Let G be equal to* $\mathrm{U}(d)$ *or* $SO(2d)$*. Let $g_0 \in G$ be a fixed element in G. Let $g \sim \mu_G$ an let $g_\theta = g_0 F_\theta(g)$, for $\theta \in [0,1]$ and $F_\theta : G \to G$ defined in* (62)*. Let now μ_G^θ denotes the induced measure according to which g_θ? is distributed. Assume furthermore that $\theta \leq 1-\Delta$, for $\Delta > 0$. We then have*

$$\left\|\mu_{\mathrm{U}(d)} - \mu^\theta_{\mathrm{U}(d)}\right\|_{\mathrm{TVD}} \leq d^2\Delta/2 \ , \ \left\|\mu_{\mathrm{SO}(2d)} - \mu^\theta_{\mathrm{SO}(2d)}\right\|_{\mathrm{TVD}} \leq d^2\Delta/2 \ . \tag{68}$$

Remark 12. *A similar analysis was carried out in [1] for the case of unitary group* $\mathrm{U}(d)$*. There however considerations were carried out for* $d = O(1)$*. This was justified because gates in question were only single and two qubit gates. The above Lemma can be viewed as an extension of the analysis given there in the sense of allowing arbitrary relation between* d *and* Δ*.*

Proof. By the block diagonalization previously discussed in this section, the only nontrivial contribution to the TVD comes from the maximal torus $\mathbb{T}$ of G:

$$\left\|\mu_G - \mu_G^\theta\right\|_{\mathrm{TVD}} = \frac{1}{2}\int_{\mathbb{T}} d\boldsymbol{\varphi} \left|\mu_G(\boldsymbol{\varphi}) - \mu_G^\theta(\boldsymbol{\varphi})\right|. \tag{69}$$

μ_G is the distribution for generic $g \in G$ of the "generalized eigenvalues" $\boldsymbol{\phi} \coloneqq (\phi_1, \ldots, \phi_d)$, quantities that are invariant under conjugation by any element of G, and it is given by the celebrated Weyl's integration formulas:

Fact 1 (Weyl's integration formula for $\mathrm{U}(d)$ and $\mathrm{SO}(d)$)**.**

$$\mu_{\mathrm{U}(d)}(\boldsymbol{\phi}) = \frac{1}{d!(2\pi)^d} \prod_{1\le j,k\le d} \left|e^{i\phi_k} - e^{i\phi_j}\right|^2 \tag{70}$$

$$\mu_{\mathrm{SO}(2d)}(\boldsymbol{\phi}) = \frac{2}{d!(2\pi)^d} \prod_{1\le j,k\le d} 4(\cos(\phi_k) - \cos(\phi_j))^2 \tag{71}$$

To upper bound the TVD, we use the fact that the Haar measure $\mu_G(\boldsymbol{\phi})$ is induced from $\mu_G^\theta(\boldsymbol{\varphi})$ by the inverse map F_θ^{-1} to compute $\mu_G(\boldsymbol{\varphi})$ by Fact 2 below. In particular, we will show that the two measures μ_G and μ_G^θ expressed in the same coordinates $\boldsymbol{\varphi}$ are proportional to each other and bound the proportionality constant.

Fact 2 (Transport of measure)**.** *Let* M *and* N *be* d*-dimensional smooth manifolds with local coordinates* $\boldsymbol{\phi} = (\phi_1, \phi_2, \ldots, \phi_d)$ *and* $\boldsymbol{\varphi} = (\varphi_1, \varphi_2, \ldots)$*,* μ *a measure on* M*, and* $F : M \to N$ *a smooth map. Then*

$$\tilde{\mu} = \mu \circ F^{-1} \tag{72}$$

is a measure on N *transported under* F*, where* F^{-1} *denotes the pre-image of* F*. In particular, for any measurable set* $A \subset N$*,*

$$\tilde{\mu}(A) = \mu(F^{-1}(A)) \coloneqq \int_{F^{-1}(A)} \mu(\boldsymbol{\phi}) d\boldsymbol{\phi}. \tag{73}$$

Explicitly, since the manifolds are locally Euclidean, $\tilde{\mu}(A)$ *has an expression in terms of the Jacobian:*

$$\tilde{\mu}(A) = \int_A \mu(F^{-1}(d\boldsymbol{\varphi})) \left|DF^{-1}(\boldsymbol{\varphi})\right|, \tag{74}$$

where $\left|DF^{-1}(\boldsymbol{\varphi})\right|$ *is the Jacobian, which by the inverse function theorem*

$$\left|DF^{-1}(\boldsymbol{\varphi})\right| = \left|DF(F^{-1}(\boldsymbol{\varphi}))\right|^{-1}. \tag{75}$$

Remark 13. *Since* $F^{-1}(\boldsymbol{\varphi}) = \boldsymbol{\phi}$*, the formula can be interpreted as a change of variable from* $\boldsymbol{\varphi}$ *to* $\boldsymbol{\phi}$*. In our case,* $F_\theta^{-1} : \mathbb{T}(\boldsymbol{\phi}) \to \mathbb{T}(\boldsymbol{\varphi})$ *plays the role of* F*. (78) is precisely the change of variable induced by* F_θ^{-1}*.*

As an intermediate step, let us derive the explicitly change-of-variable formula from $\boldsymbol{\varphi}$ to $\boldsymbol{\phi}$. By applying to

$$\exp(\varphi_j \tilde{X}_j) = F_\theta \ (\exp(\phi_j \tilde{X}_j)). \tag{76}$$

(recalling that $\tilde{X}$ are generators of the maximal torus (66) for $\mathrm{U}(d)$ or (67) for $\mathrm{SO}(2d)$) the identity

$$f^{-1}(\exp(\phi_j \tilde{X}_j)) = -\tan(\phi_j/2)\tilde{X}_j, \tag{77}$$

which can be verified by explicitly computing the Cayley transform (59) of at most a 2×2 matrix, we obtain the change-of-variable formula:

$$\varphi = 2\tan^{-1}[\theta\tan(\phi/2)]. \tag{78}$$

Now we compute and bound (74)

$$\mu_G(A) = \int_A \mu_G(d\boldsymbol{\phi} = F_\theta(d\boldsymbol{\varphi})) \left| DF_\theta^{-1}(\boldsymbol{\phi} = F_\theta(\boldsymbol{\varphi}))\right|^{-1}. \tag{79}$$

Throughout the proof, we set $\theta = 1-\Delta$ and notice that the final upper bound on the TVD would still hold for $\theta \le 1-\Delta$. The change-of-variable formula (78) directly gives the element of the (diagonal) Jacobian

$$\begin{aligned}
|\partial_\phi \varphi|^{-1} &= \frac{\cos^2(\phi/2) + (1-\Delta)^2\sin^2(\phi/2)}{1-\Delta} & (80)\\
&= \frac{1-\Delta(2-\Delta)\sin^2(\phi/2)}{1-\Delta}, & (81)
\end{aligned}$$

which attains the minimum when $\sin^2(\phi/2) = 1$ and the maximum when $\sin^2(\phi/2) = 0$. Thus, we have the following bound on the Jacobian for both the passive and active cases

$$\begin{aligned}
1-\Delta \le |\partial_\phi \varphi|^{-1} &\le \frac{1}{1-\Delta}, & (82)\\
(1-\Delta)^d \le \left|DF_\theta^{-1}(\boldsymbol{\phi} = F_\theta(\boldsymbol{\varphi}))\right|^{-1} &\le \frac{1}{(1-\Delta)^d}. & (83)
\end{aligned}$$

At last, to bound the TVD, we express the measures μ_G and μ_G^θ in the same coordinates $\boldsymbol{\varphi}$. For the case of passive FLO, this can be done by directly applying the inverse of the deformation map (61) to each group element $e^{i\phi_j}$, $j \in [d]$

$$F_{1-\Delta}^{-1}(e^{i\varphi_j}) = \frac{\Delta + (\Delta-2)e^{i\varphi_j}}{\Delta(e^{i\varphi_j}+1) - 2}. \tag{84}$$

As a result,

$$\begin{aligned}
\left|e^{i\phi_k} - e^{i\phi_j}\right| &= \left|F_{1-\Delta}^{-1}(e^{i\varphi_k}) - F_{1-\Delta}^{-1}(e^{i\varphi_j})\right| & (85)\\
&= \frac{1-\Delta}{\left|1-\frac{\Delta}{2}(e^{i\varphi_j}+1)\right|\left|1-\frac{\Delta}{2}(e^{i\varphi_k}+1)\right|}\left|e^{i\varphi_k} - e^{i\varphi_j}\right| =: \Gamma_{\mathrm{pas}}\left|e^{i\varphi_k} - e^{i\varphi_j}\right|, & (86)
\end{aligned}$$

which implies, via the Weyl's formula (70) that the two measures are proportional:

$$\mu_{\mathrm{U}(d)}(\boldsymbol{\varphi}) = \Gamma_{\mathrm{pas}}^{d(d-1)/2}\mu_{\mathrm{U}(d)}^\theta(\boldsymbol{\varphi}). \tag{87}$$

The proportionality constant Γ_{pas} attains the maximum value when $e^{i\varphi_j} = e^{i\varphi_k} = 1$ and the minimum value when $e^{i\varphi_j} = e^{i\varphi_k} = -1$, giving the following bound

$$(1-\Delta)^2 \le \Gamma_{\mathrm{pas}} \le \frac{1}{(1-\Delta)^2}, \tag{88}$$

which leads to the bound of the TVD stated in the lemma:

$$\left\|\mu_{\mathrm{U}(d)} - \mu^{\theta}_{\mathrm{U}(d)}\right\|_{\mathrm{TVD}} \le \frac{1}{2}\left|1-(1-\Delta)^{d^2}\right| \int_{\mathbb{T}} d\boldsymbol{\varphi} \left|\mu^{\theta}_{\mathrm{U}(d)}(\boldsymbol{\varphi})\right| \tag{89}$$

$$= \frac{1}{2}\left|1-(1-\Delta)^{d^2}\right| \tag{90}$$

$$\le \frac{d^2\Delta}{2}; \tag{91}$$

the inequality in the last line can be proved by induction on $d^2 \ge 1$.

Turning to the case of active FLO, the change-of-variable formula (78) implies that for any $j, k \in [d]$,

$$\cos\phi_k - \cos\phi_j = \frac{(1-\Delta)^2 - \tan^2(\varphi_k/2)}{(1-\Delta)^2 + \tan^2(\varphi_k/2)} - \frac{(1-\Delta)^2 - \tan^2(\varphi_j/2)}{(1-\Delta)^2 + \tan^2(\varphi_j/2)} \tag{92}$$

$$= \frac{(1-\Delta)^2}{\left(1-\Delta(1-\frac{\Delta}{2})(1+\cos\varphi_j)\right)\left(1-\Delta(1-\frac{\Delta}{2})(1+\cos\varphi_k)\right)}(\cos\varphi_k - \cos\varphi_j) \tag{93}$$

$$=: \Gamma_{\mathrm{act}}(\cos\varphi_k - \cos\varphi_j), \tag{94}$$

where we have used $\cos(2\theta) = (1-\tan^2\theta)(1+\tan^2\theta)^{-1}$ in the first line and $\tan^2\theta = (1-\cos(2\theta))(1+\cos(2\theta))^{-1}$ in the second line. Thus we have from the Weyl's formula (71) that

$$\mu_{\mathrm{SO}(2d)}(\boldsymbol{\varphi}) = \Gamma_{\mathrm{act}}^{d(d-1)/2}\mu^{\theta}_{\mathrm{SO}(2d)}(\boldsymbol{\varphi}). \tag{95}$$

The proportionality constant Γ_{act} attains the maximum value when $\cos\varphi_j = 1$ and the minimum value when $\cos\varphi_j = -1$, giving the bound

$$(1-\Delta)^2 \le \Gamma_{\mathrm{act}} \le \frac{1}{(1-\Delta)^2}. \tag{96}$$

Therefore, the TVD is bounded in a similar manner to the passive case.

$$\left\|\mu_{\mathrm{SO}(2d)} - \mu^{\theta}_{\mathrm{SO}(2d)}\right\|_{\mathrm{TVD}} \le \frac{1}{2}\left|1-(1-\Delta)^{d^2}\right| \int_{\mathbb{T}} d\boldsymbol{\varphi} \left|\mu^{\theta}_{\mathrm{SO}(2d)}(\boldsymbol{\varphi})\right| \tag{97}$$

$$= \le \frac{1}{2}\left|1-(1-\Delta)^{d^2}\right| \tag{98}$$

$$\le \frac{d^2\Delta}{2}. \tag{99}$$

□

The robustness of the quantum supremacy claim will be tied directly to the degree of the rational functions that interpolate between quantum circuits (Section VIII). Here we give the explicit rational functions and their degrees in the Cayley-path interpolation $g_\theta = F_\theta(g)$ at the group level (62) in U(d) and SO($2d$). (A similar result for U(d) was derived in [1].)

In the case of U(d), since g can always be diagonalized by some element h: $hgh^{-1} = \sum_{j=1}^{d} e^{i\phi_j}\,|j\rangle\langle j|$, we have that

$$g_\theta = \sum_{j=1}^{d} \frac{(1-\theta)+(1+\theta)e^{i\phi_j}}{(1+\theta)+(1-\theta)e^{i\phi_j}} g_0 h^{-1} |j\rangle\langle j| h \tag{100}$$

$$= \sum_{j=1}^{d} \frac{1+i\theta\tan\phi_j}{1-i\theta\tan\phi_j} g_0 h^{-1} |j\rangle\langle j| h \tag{101}$$

$$= \frac{1}{\mathcal{Q}_g(\theta)} \sum_{j=1}^{d} P_j(\theta) g_0 h^{-1} |j\rangle\langle j| h =: \frac{\mathcal{P}_{g_0,g}(\theta)}{\mathcal{Q}_g(\theta)}, \tag{102}$$

where

$$\mathcal{Q}_g(\theta) = \prod_{j=1}^{d} (1 - i\theta\tan\phi_j), \tag{103}$$

$$P_j(\theta) = (1+i\theta\tan\phi_j) \prod_{\substack{1\le k\le d\\ k\neq j}} (1-i\theta\tan\phi_k) \tag{104}$$

are both polynomials of degree d in θ, and $\mathcal{P}_{g_0,g}(\theta)$ is a formal polynomial that depends on the matrices g and g_0.

The same calculation applies to the case SO($2d$), except that now each eigenspace is two-dimensional and spanned by $\mathbb{I}_j = |2j-1\rangle\langle 2j-1| + |2j\rangle\langle 2j|$ and $\tilde{X}_j = |2j\rangle\langle 2j-1| - |2j-1\rangle\langle 2j|$. Again, let $hgh^{-1} = \sum_{j=1}^{d}(\cos\phi_j \mathbb{I}_j + \sin\phi_j \tilde{X}_j)$, and one has

$$g_\theta = g_0 \sum_{j=1}^{d} \frac{\left[1+\cos\phi_j - \theta^2(1-\cos\phi_j)\right]\mathbb{I}_j + 2\theta\sin\phi_j h^{-1}\tilde{X}_j h}{1+\cos\phi_j + \theta^2(1-\cos\phi_j)} \tag{105}$$

$$= g_0 \sum_{j=1}^{d} \frac{[1-\theta^2\tan^2(\phi_j/2)]\mathbb{I}_j + 2\theta\tan(\phi/2)h^{-1}\tilde{X}_j h}{1+\theta^2\tan^2(\phi_j/2)} \tag{106}$$

$$= \frac{1}{\mathcal{Q}_g(\theta)} \sum_{j=1}^{d} \left(P_j^{\mathrm{diag}}(\theta) g_0 \mathbb{I}_j + P_j^{\mathrm{off}}(\theta) g_0 h^{-1}\tilde{X}_j h\right) =: \frac{\mathcal{P}_{g_0,g}(\theta)}{\mathcal{Q}_g(\theta)}\ , \tag{107}$$

where in (106) we divided both the numerator and the denominator by $1+\cos\phi_j$ and

$$\mathcal{Q}_g(\theta) = \prod_{j=1}^{d} (1+\theta^2\tan^2(\phi_j/2)), \tag{108}$$

$$P_j^{\mathrm{diag}}(\theta) = (1+\theta^2\tan^2(\phi_j/2))^2) \prod_{\substack{1\le k\le d\\ k\neq j}} (1+\theta^2\tan^2(\phi_j/2))^2), \tag{109}$$

$$P_j^{\mathrm{off}}(\theta) = 2\theta\tan(\phi_j/2) \prod_{\substack{1\le k\le d\\ k\neq j}} (1+\theta^2\tan^2(\phi_j/2))^2) \tag{110}$$

are polynomials in θ of degree $2d$, $2d$, and $2d-1$ respectively, and $\mathcal{P}_{g_0,g}(\theta)$ is a formal polynomial that depends on the matrices g and g_0.

Below we give a lower bound for $\mathcal{Q}_g(\theta)$ to assure that the rational function does not blow up, and an upper bound for generic $g \in G$, which will be crucial for a robust reduction in Section IX. Note that the coefficients of the polynomial $\mathcal{Q}_g(\theta)$ depends only on generalized eigenvalues of g ($e^{i\phi_j}$ in the unitary case and $\cos\phi_j$, $\sin\phi_j$ in the orthogonal case) and hence $Q(\theta)$ can be pre-computed in time polynomial in d by diagonalizing g, computing each $\tan(\phi_j/2)$ which is just an algebraic function of $e^{i\phi_j}$, and computing the final result.

Lemma 3. *Let $\mathcal{Q}_g(\theta)$ be the polynomial in defined in (103) for $G = \mathrm{U}(d)$ and in (108) for $G = \mathrm{SO}(2d)$. Let now $\tilde{\Delta} > 0$. Then we have the following inequalities*

$$\Pr_{g\sim\mu_{\mathrm{U}(d)}}\left(|\mathcal{Q}_g(\theta)|^2 \leq \left[1 + \left(\frac{\theta\pi}{\tilde{\Delta}}\right)^2\right]^d\right) \geq 1 - d\frac{\tilde{\Delta}}{\pi}\ , \tag{111}$$

$$\Pr_{g\sim\mu_{\mathrm{SO}(2d)}}\left(|\mathcal{Q}_g(\theta)|^2 \leq \left[1 + \left(\frac{\theta\pi}{\tilde{\Delta}}\right)^2\right]^{2d}\right) \geq 1 - d\frac{\tilde{\Delta}}{\pi}\ . \tag{112}$$

In addition, for all g $|Q_g(\theta)|^2 \geq 1$ for both $U(d)$ and $\mathrm{SO}(2d)$.

Proof. Since $g \in G$ is Haar distributed, every generalised eigenphase ϕ_j is distributed uniformly on the interval $[-\pi, \pi]$ [108]. Therefore, for every j we have

$$\Pr_{g\sim\mu_G}\left(\phi_j \in [\pi - \tilde{\Delta}, \pi] \cup [-\pi, -\pi + \tilde{\Delta}]\right) = \frac{\tilde{\Delta}}{\pi}. \tag{113}$$

It is easy to verify that for $\phi_j \in [-\pi + \tilde{\Delta}, \pi - \tilde{\Delta}]$ we have $|\tan(\phi_j/2)| \leq \pi/\tilde{\Delta}$. Using the union bound over different ϕ_j, $j \in [d]$ we obtain that with probability at least $1 - d\frac{\tilde{\Delta}}{\pi}$,

$$|\tan(\phi_j/2)| \leq \pi/\tilde{\Delta} \text{ for all } j \in [d]\ . \tag{114}$$

Using the definition of polynomials $\mathcal{Q}_g(\theta)$ from Eq. (103) and Eq. (108), we obtain the claimed inequalities (111) and (112). ☐

Remark 14. *We believe that the inequalities stated in Lemma 3 can be greatly improved by the usage of more sophisticated techniques from random matrix theory. However, for our purposes these crude estimates are sufficient (see proof of Theorem 7).*

VIII. POLYNOMIALS ASSOCIATED TO PROBABILITIES IN FLO CIRCUITS

In this section, we give the degrees of matrix polynomials associated to fermionic representations of $G = \mathrm{U}(d)$ and $G = \mathrm{SO}(2d)$. These polynomials, when evaluated on the Cayley path g_θ in the appropriate group (see Eq. (62)), give rise polynomials and rational functions θ for the outcome probabilities $p_{\mathbf{x}}(\Pi(g_\theta), \Psi_{\mathrm{in}}) = |\langle\mathbf{x}|\Pi(g)|\Psi_{\mathrm{in}}\rangle|^2$ in our quantum advantage schemes. The explicit form of these polynomials will be used in Section IX when discussing worst-to-average-case reductions.

We start with discussing the passive FLO case and then the active FLO case.

It will be useful to introduce the following notation. Given a $d \times d$ matrix M and two subsets of indices $\mathcal{X}, \mathcal{Y} \subset [d]$ with cardinality n, where $\mathcal{X} = \{a_1, a_2, \ldots a_n\}$ ($a_i < a_j$ if $i < j$) and $\mathcal{Y} = \{b_1, b_2, \ldots, b_n\}$ ($b_i < b_j$ if $i < j$), we define $M_{\mathcal{X},\mathcal{Y}}$ as the $n \times n$ matrix with entries

$$(M_{\mathcal{X},\mathcal{Y}})_{k,\ell} = M_{a_k, b_\ell}\ , \quad k, \ell = 1, \ldots n. \tag{115}$$

Lemma 4. *Given two Fock basis states $|\mathcal{X}\rangle, |\mathcal{Y}\rangle \in \bigwedge^n(\mathbb{C}^d)$ and a $U \in \mathrm{U}(d)$, the the amplitude between $|\mathcal{X}\rangle$ and $\Pi_{\mathrm{pas}}(U)|\mathcal{Y}\rangle$ is provided by the expression*

$$\langle\mathcal{X}|\Pi_{\mathrm{pas}}(U)|\mathcal{Y}\rangle = \det(U_{\mathcal{X},\mathcal{Y}}). \tag{116}$$

Proof. Let $\mathcal{X} = \{a_1, a_2, \ldots a_n\}$ ($a_i < a_j$ if $i < j$) and $\mathcal{Y} = \{b_1, b_2, \ldots, b_n\}$ ($b_i < b_j$ if $i < j$). By definition we have that

$$\Pi_{\mathrm{pas}}(U)|\mathcal{Y}\rangle = U^{\otimes n}|b_1\rangle \wedge |b_2\rangle \wedge \cdots \wedge |b_n\rangle = |\xi_1\rangle \wedge |\xi_2\rangle \wedge \cdots \wedge |\xi_n\rangle \tag{117}$$

where

$$|\xi_\ell\rangle = U|b_\ell\rangle = \sum_{j=1}^{d} U_{j,b_\ell}|j\rangle\,, \quad \ell = 1,\dots,n. \tag{118}$$

Using the last two equations and Eq. (6), we can deduce that

$$\langle\mathcal{X}|\Pi_{\mathrm{pas}}(U)|\mathcal{Y}\rangle = \det(C)\,, \quad C_{k,\ell} = \langle a_k|\xi_\ell\rangle = \langle a_k|\sum_{j=1}^{d} U_{j,b_\ell}|j\rangle = U_{a_k,b_\ell} = (U_{\mathcal{X},\mathcal{Y}})_{k,\ell} \tag{119}$$

which proves the statement. □

This lemma allows us to directly obtain the following result:

Proposition 1 (Degrees of polynomials describing probabilities associated to passive FLO circuits.)**.** *Consider a state $|\Psi\rangle \in \bigwedge^n(\mathbb{C}^d)$. For an arbitrary $U \in \mathrm{U}(d)$ the outcome probability $p_{\mathbf{x}}(\Pi_{\mathrm{pas}}(U),\Psi) = |\langle\mathbf{x}|\Pi_{\mathrm{pas}}(U)|\Psi\rangle|^2$ is a degree $2n$ homogeneous polynomial in the entries of U and $U^\dagger$.*

Proof. One can expand the vector $|\Psi\rangle$ in terms of the Fock basis states belonging to $\bigwedge^n(\mathbb{C}^d)$ as

$$|\Psi\rangle = \sum_{\substack{\mathcal{Y}\subset[d]\\|\mathcal{Y}|=n}} c_{\mathcal{Y}}|\mathcal{Y}\rangle. \tag{120}$$

Let $\mathcal{X}\subset[d]$ denote the set of indices corresponding to $\mathbf{x}$ as an indicator function (i.e., $|\mathbf{x}\rangle = |\mathcal{X}\rangle$). Using Lemma 4, we can write the relevant amplitude as

$$\langle\mathbf{x}|\Pi_{\mathrm{pas}}(U)|\Psi\rangle = \sum_{\substack{\mathcal{Y}\subset[d]\\|\mathcal{Y}|=n}} c_{\mathcal{Y}}\langle\mathcal{X}|\Pi_{\mathrm{pas}}(U)|\mathcal{Y}\rangle = \sum_{\substack{\mathcal{Y}\subset[d]\\|\mathcal{Y}|=n}} c_{\mathcal{Y}}\det(U_{\mathcal{X},\mathcal{Y}}). \tag{121}$$

As each term in the sum is a determinant of a $n\times n$ submatrix of U, this expression gives a homogeneous polynomial of the entries of U of order n. This in turn directly implies that $p_{\mathbf{x}}(\Pi_{\mathrm{pas}}(U),\Psi) = |\langle\mathbf{x}|\Pi_{\mathrm{pas}}(U)|\Psi\rangle|^2$ is a degree $2n$ polynomial in the entries of U and $U^\dagger$. □

Lemma 5 (Polynomial for output amplitude of passive FLO [62])**.** *Consider the input state $|\Psi_{\mathrm{in}}\rangle = |\Psi_4\rangle^{\otimes N} \in \bigwedge^{2N}(\mathbb{C}^{4N})$. For an arbitrary $U \in \mathrm{U}(4N)$ the outcome amplitude is given by*

$$\langle\mathbf{x}|\Pi_{\mathrm{pas}}(U)|\Psi\rangle = \frac{1}{\sqrt{2^N}}\sum_{(y_1,\cdots,y_N)\in\{0,1\}^N} \det(U^T_{\{2y_1+1,2y_1+2,\cdots,2y_N+4N-3,2y_N+4N-2\},\mathcal{X}})\,, \tag{122}$$

where $U^T_{\{2y_1+1,2y_1+2,\cdots,2y_N+4N-3,2y_N+4N-2\},\mathcal{X}}$ indicates the transpose of U with the rows not indexed by $\{2y_1+1,2y_1+2,\cdots,2y_N+4N-3,2y_N+4N-2\}$ and columns not indexed by $\mathcal{X}$. Note that this is a degree N polynomial in the entries of U.

Proof. To derive this polynomial, we rewrite the input fermionic magic state $|\Psi_{\mathrm{in}}\rangle$ as in Eq. (B18).

$$|\Psi_{\mathrm{in}}\rangle = \frac{1}{\sqrt{2^N}}\sum_{\mathcal{Y}\in\mathcal{C}_{\mathrm{in}}}|\mathcal{Y}\rangle \tag{123}$$

$$= \frac{1}{\sqrt{2^N}}\sum_{\mathbf{y}\in\{0,1\}^N}|\mathcal{Y}_{\mathbf{y}}\rangle, \tag{124}$$

where $\mathcal{C}_{\rm in}$ consists of subsets labelled by bitstrings (for more detail, see paragraph after Eq. (B18)). Using the expression for the output amplitude in Proposition 1 we write

$$\langle \mathbf{x}|\Pi_{\rm pas}(U)|\Psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{\mathbf{y}\in\{0,1\}^N} \det(U_{\mathcal{X},\mathcal{Y}_{\mathbf{y}}}) \tag{125}$$

$$= \frac{1}{\sqrt{2^N}} \sum_{(y_1,\cdots,y_N)\in\{0,1\}^N} \det(U^T_{\{2y_1+1,2y_1+2,\cdots,2y_N+4N-3,2y_N+4N-2\},\mathcal{X}}) \,, \tag{126}$$

where in the last line we have replaced the definition of $\mathcal{Y}_y$ and also used the fact that the determinant is invariant under the transpose. □

For the case of $|\Psi_{\rm in}\rangle = |\Psi_4\rangle^{\otimes N}$, the expression in Eq. (126) can be rewritten as a mixed discriminant

$$D_{2,2}(v_1,\ldots,v_{4N}) = \frac{1}{\sqrt{2^N}} \sum_{\substack{i_k=0,1,\\ k=1,\ldots,N}} \det \begin{bmatrix} v_{2i_1+1} \\ v_{2i_1+2} \\ v_{2i_2+5} \\ v_{2i_2+6} \\ \vdots \\ v_{2i_N+4N-3} \\ v_{2i_N+4N-2} \end{bmatrix} \,, \tag{127}$$

here v_k correspond to the rows of the matrix U^T in Eq. (126) with the columns not indexed by $\mathbf{x}$ removed. This polynomial over entries of matrices of size $2N \times N$ was found to be #P-hard in the general case [62]. This was proven by reducing the computation of the permanent of a weighted adjacency matrix to these polynomials of a transformed adjacency matrix with polynomial overhead.

Next we turn to studying the output probabilities after an active FLO evolution. It will be useful to introduce the following notation: given a set of (majorana) indices $\mathcal{A} = \{a_1, a_2, \ldots a_k\} \subset [2d]$ (with $a_i < a_j$ if $i < j$), we define

$$m_{\mathcal{A}} = m_{a_1} m_{a_2} \cdots m_{a_k}. \tag{128}$$

These majorana monomials define an orthogonal (but not orthonormal) basis in the space of operators with respect to the Hilbert-Schmidt scalar product

$$\operatorname{tr}(m_{\mathcal{A}} m_{\mathcal{B}}^\dagger) = (-1)^{f(|\mathcal{B}|)} \operatorname{tr}(m_{\mathcal{A}} m_{\mathcal{B}}) = \delta_{\mathcal{A},\mathcal{B}} \frac{1}{2^d}, \tag{129}$$

where $f(n) = 1$ if $(n \mod 4) \in \{2, 3\}$ and $f(n) = 0$ otherwise.

Consider a subset $\mathcal{A} = a_1, a_2 \ldots a_k \subset [2d]$ (with $a_i < a_j$ if $i < j$), then from Eq. (11) and the majorana anticommutation relations it follows for $O \in \mathrm{SO}(2d)$ that

$$\Pi_{\rm act}(O) m_{\mathcal{A}} \Pi_{\rm act}(O)^\dagger = \sum_{b_1,\ldots b_k=1}^{d} \epsilon_{b_1,b_2,\ldots,b_k} O_{a_1,b_1} O_{a_2,b_2} \cdots O_{a_k,b_k} m_{\{b_1,\ldots b_k\}}. \tag{130}$$

Proposition 2 (Degrees of polynomials describing probabilities associated to active FLO circuits.)**.** *Consider a state $|\Psi\rangle \in$. For an arbitrary $O \in \mathrm{SO}(2d)$ the outcome probability $p_{\mathbf{x}}(\Pi_{\rm act}(O), \Psi) = |\langle \mathbf{x}|\Pi_{\rm act}(O)|\Psi\rangle|^2$ is a degree d polynomial in the entries of O.*

Proof. Let us consider the expansion of $|\mathbf{x}\rangle\langle\mathbf{x}|$ and Ψ in terms of majorana monomials

$$|\mathbf{x}\rangle\langle\mathbf{x}| = \sum_{\mathcal{A}\subset[d]} (a_{\mathcal{A}}\, m_{\mathcal{A}} + b_{\mathcal{A}}\, Q m_{\mathcal{A}}) \,, \quad \Psi = \sum_{\mathcal{B}\subset[d]} (c_{\mathcal{B}}\, m_{\mathcal{B}} + d_{\mathcal{B}}\, Q m_{\mathcal{B}}). \tag{131}$$

Using this and Eqs. (129) and (130) can now write the outcome probability as

$$\begin{aligned} p_{\mathbf{x}}(\Pi_{\mathrm{act}}(O),\Psi) &= \mathrm{tr}\left(|\mathbf{x}\rangle\langle\mathbf{x}|\,\Pi_{\mathrm{act}}(O)\Psi\Pi_{\mathrm{act}}(O)^\dagger\right) \\ &= \sum_{\mathcal{A},\mathcal{B}\subset[d]} \left(a_{\mathcal{A}}c_{\mathcal{B}}\,\mathrm{tr}\left(m_{\mathcal{A}}\Pi_{\mathrm{act}}(O)m_{\mathcal{B}}\Pi_{\mathrm{act}}(O)^\dagger\right) + b_{\mathcal{A}}d_{\mathcal{B}}\,\mathrm{tr}\left(Qm_{\mathcal{A}}\Pi_{\mathrm{act}}(O)Qm_{\mathcal{B}}\Pi_{\mathrm{act}}(O)^\dagger\right)\right) \\ &= \sum_{k=0}^{d} \sum_{\substack{\mathcal{A},\mathcal{B}\subset[d] \\ |\mathcal{A}|=|\mathcal{B}|=k}} w_{\mathcal{A},\mathcal{B}} \sum_{\ell_1,\ldots\ell_k=1}^{d} \epsilon_{\ell_1,\ell_2,\ldots,\ell_k}\delta_{\mathcal{A},\{\ell_1,\ldots,\ell_k\}}O_{b_1,\ell_1}O_{b_2,\ell_2}\cdots O_{b_k,\ell_k}, \end{aligned} \tag{132}$$

where $w_{\mathcal{A},\mathcal{B}} = \frac{(-1)^{f(|\mathcal{A}|)}}{2^d}(a_{\mathcal{A}}c_{\mathcal{B}} + (-1)^k b_{\mathcal{A}}d_{\mathcal{B}})$. Since each term in the sum is a degree d or less polynomial in the entries of O the theorem is proved. □

Definition 5 (Degree of rational functions)**.** *Let $P(\theta), Q(\theta)$ be polynomials of degree d_1 and d_2 respectively. Let $R(\theta) = \frac{P(\theta)}{Q(\theta)}$ be the corresponding rational function. Assume that that P and Q do not have non-constant polynomial divisors. Then, we define rational degree of R as the pair $\deg(R) = (d_1, d_2)$*

The following results states that FLO circuit representations of elements of the appropriate symmetry group G, when evaluated on Cayley paths, give rise to outcome probabilities that are rational functions of low degree (in number of modes d and number of particles n).

Lemma 6 (Degrees of rational functions describing probabilities associated to interpolation of FLO circuits)**.** *Let G be equal to $\mathrm{U}(d)$ or $\mathrm{SO}(2d)$. Let $g_0, g \in G$ be a fixed elements of the group G. Consider a rational path in the group defined by interpolation via Cayley path*

$$g_\theta = g_0 F_\theta(g)\ ,\ \theta\in[0,1]\ . \tag{133}$$

Let now $\Pi : G \to \mathrm{U}(\mathcal{H})$ be the appropriate representation of G describing appropriate class of FLO circuits ($G = \mathrm{U}(d)$, $\Pi = \Pi_{\mathrm{pas}}$, $\mathcal{H} = \bigwedge^n(\mathbb{C}^d)$ for passive FLO and $G = \mathrm{SO}(2d)$, $\Pi = \Pi_{\mathrm{act}}$, $\mathcal{H} = \mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d)$ for active FLO). Let us fix $|\Psi\rangle \in \mathcal{H}$ and a Fock state $|\mathbf{x}\rangle \in \mathcal{H}$. Then the outcome probability

$$R_{g_0,g}(\theta) = \mathrm{tr}(|\mathbf{x}\rangle\langle\mathbf{x}|\Pi(g_\theta)\rho\Pi(g_\theta)^\dagger) \tag{134}$$

viewed as a function of parameter θ is a rational function of degrees

$$\textit{Passive FLO:}\quad \deg(R_{g_0,g}) = (2dn, 2dn)\quad ,\quad \textit{Active FLO:}\quad \deg(R_{g_0,g}) = (2d^2, 2d^2) \tag{135}$$

Moreover the denominator of the rational functions are given by

$$\textit{Passive FLO:}\quad Q_g(\theta) = \prod_{j=1}^{d}(1+\theta^2\tan^2(\phi_j/2))^n\ ,\quad \textit{Active FLO:}\ \ Q_g(\theta) = \prod_{j=1}^{d}(1+\theta^2\tan^2(\phi_j/2))^d\ , \tag{136}$$

where ϕ_j , $j \in [d]$ are phases of generalized eigenvalues of matrix g belonging to the suitable group G and thus $Q_g(\theta)$ can be efficiently computed (see Section VII).

Proof. We begin by proving the passive FLO case. Recall from Eq. (102) that g_θ was expressed as a matrix with entries of degree (d, d) on θ. By virtue of Proposition 1, we know that $p_{\mathbf{x}}(\Pi_{\mathrm{pas}}(g_\theta), \Psi) = R_{g_0,g}(\theta)$ is a polynomial of degree $2n$ on the entries of g_θ which immediately implies the degree on θ is $\deg(R_{g_0,g}) = (2dn, 2dn)$. The denominator of the rational functions in g_θ is given by Eq. (103), from the expression for the amplitude in Proposition 1, we know that the denominator in $R_{g_0,g}$ must be of the form $|\mathcal{Q}_g(\theta)^n|^2$ which gives the result form $\prod_{j=1}^{d}(1+\theta^2\tan^2(\phi_j/2))^n$.

For the active case, we obtain from Eq. (107) that g_θ is a matrix with entries that are polynomials of degree $(2d, 2d)$. Then by Proposition 2, $p_{\mathbf{x}}(\Pi_{\mathrm{act}}(g_\theta), \Psi)$ is of degree d on the entries of g_θ implying $\deg(R_{g_0,g}) = (2d^2, 2d^2)$. The denominator $Q_g(\theta)$ is obtained by noting that the expression in Eq. (108) for $\mathcal{Q}_g(\theta)$ appears as the denominator in each entry of g_θ and by Proposition 2 the degree on this denominator is d, thus proving the result. □

IX. ROBUST AVERAGE-CASE HARDNESS OF OUTPUT PROBABILITIES OF FERMIONIC CIRCUITS

In this part we give strong evidence for the Conjecture 1 used to show classical hardness of sampling from fermionic linear circuits initialized in $|\Psi_{\rm in}\rangle$ (cf. Theorem 3). There we conjectured that it is #P-hard to approximate probabilities $p_{\mathbf{x}}(V,\Psi_{\rm in}) = |\langle \mathbf{x}|V|\Psi_{\rm in}\rangle|^2$ of *generic* FLO circuits initialized in $|\Psi_{\rm in}\rangle$ to relative error. To support the conjecture we prove weaker theorems showing average-case #P hardness of exact computation of $p_{\mathbf{x}}(V,\Psi_{\rm in})$ (Theorem 5) and extend it further to average-case #P-hardness of approximating $p(\mathbf{x}|V,\Psi_{\rm in})$ up to error $\epsilon=\exp(-\Theta(N^6))$ (Theorem 7), where N is the number of states $|\Psi_4\rangle$ used.

To establish this we combine previously known worst-case hardness results (see discussion in Section VI) and adopt to our setting rational interpolation method based on Cayley transform introduced recently by Movassagh [1]. We also use the fact that both passive FLO circuits ($\mathcal{G}_{\rm pas}$) as well active FLO ($\mathcal{G}_{\rm act}$) are representations of low-dimensional symmetry group G (equal to $\mathrm{U}(d)$ or $\mathrm{SO}(2d)$). As shown in the previous section, this implies that, when evaluated on the Cayley path g_θ, the circuit rise to outcome probabilities being rational functions of low degree (cf. Lemma 6). This low-degree structure allows to perform worst-to-average-case reductions for the family of circuits considered. Specifically, we reduce the problem of computation of the worst-case probability $p(\mathbf{x}|V_0,\Psi_{\rm in})$ to computing $p(\mathbf{x}|V,\Psi_{\rm in})$, for V being typical passive or active FLO circuit.

We will need the following result that guarantees that it is possible to recover an unknown rational function $F(\theta)$ from a set of its values at different points, even if some of the evaluation are erroneous.

Theorem 4 (Berlekamp-Welch for rational functions [1])**.** *Let $R(\theta)$ be a rational function of degree $\deg(R)=(d_1,d_2)$. A set of points $\mathcal{S}=\{(\theta_1,r_1),(\theta_2,r_2),\dots,(\theta_L,r_L)\}$ specifies $R(\theta)$ uniquely provided $L>d_1+d_2+2t$, where*

$$|\{\, i\in[L] \mid R(\theta_i)\neq r_i\}|\leq t\ . \tag{137}$$

Moreover, $F(\theta)$ can be recovered in polynomial time in L and $\deg(R)$, when $\mathcal{S}$ is given.

Recall that in our quantum advantage scheme we have $d=4N$, $|\Psi_{\rm in}\rangle = |\Psi_4\rangle^{\otimes N}$, for $|\Psi_4\rangle = (|0011\rangle + |1100\rangle)/\sqrt{2}$ (therefore for the case of passive FLO $n=2N$). Let now $g_0\in G$ be an element of the symmetry group such that $p_{\mathbf{x}_0}(V_0,\Psi_{\rm in})$ is #P-hard to compute, where $V_0=\Pi(g_0)$ and $\mathbf{x}_0$ is the specific output state. We use a Cayley path interpolation between g_0 and Haar-random elements from G

$$g_\theta = g_0 F_\theta(g)\ ,\ g\sim\mu_G\ . \tag{138}$$

Let μ_G^θ be the distribution of g_θ obtained in this way. In Lemma 2 we proved bounds for the TV distances $\|\mu_G-\mu_G^\theta\|_{\rm TVD}$. These bounds can be directly translated on the level of the corresponding circuits. Indeed, let $V_\theta=\Pi(g_\theta)$ and let ν_G^θ denote the distribution of the corresponding quantum circuits obtained by appropriate representation Π of G. Since distribution of the Haar random FLO circuits $\nu_{\rm pas},\nu_{\rm pas}$ are obtained in exactly the same way we get from the monotonicity of TV distance (cf. Section II).

$$\left\|\nu_{\rm pas}-\nu_{\rm pas}^\theta\right\|_{\rm TVD}\leq 8N^2\Delta\ ,\ \left\|\nu_{\rm act}-\nu_{\rm act}^\theta\right\|_{\rm TVD}\leq 8N^2\Delta\ , \tag{139}$$

where $\theta\in[1-\Delta,1]$. Finally, from Lemma 6 we know that probabilities $R(\theta)=\mathrm{tr}(|\mathbf{x}_0\rangle\langle\mathbf{x}_0|\Pi(g_\theta)\rho\Pi(g_\theta)^\dagger)$ are rational functions of the deformation parameter θ of degrees

$$\text{Passive FLO:}\quad \deg(R)=(16N^2,16N^2)\ \ ,\ \ \text{Active FLO:}\quad \deg(R)=(32N^2,32N^2)\ . \tag{140}$$

and act that passive and active Fermionic linear circuits gives an average to worst-case reduction for outcome probabilities generated by fermionic circuits.

Theorem 5 (Average-case #P-hardness of computation of outcome probabilities of FLO circuits)**.** *Let V_0 be a FLO circuit such that computing $p_{\mathbf{x}_0}(V_0,\Psi_{\rm in})=|\langle\mathbf{x}_0|V_0|\Psi_{\rm in}\rangle|^2$ is #P-Hard, where V_0 is element of either passive or active FLO circuits and the output Fock state $|\mathbf{x}_0\rangle$ belongs to the suitable Hilbert space $\mathcal{H}_{\rm pas}=\bigwedge^{2N}(\mathbb{C}^{4N})$ for passive FLO and $\mathcal{H}_{\rm act}=\mathcal{H}_{\rm Fock}^{+}(\mathbb{C}^{4N})$, respectively.*

Then it is #P*-Hard to compute* $p_{\mathbf{x}_0}(V,\Psi_{\rm in}) = |\langle \mathbf{x}_0|V|\Psi_{\rm in}\rangle|^2$ *with probability* $\alpha > \frac{3}{4}+\delta$, $\delta = \frac{1}{\mathrm{poly}(N)}$, *over the the uniform distribution of circuits:* $V\sim\nu_{\rm pas}$ *for passive FLO and* $V\sim\nu_{\rm act}$ *for active FLO.*

Remark 15. *Due to hiding property (see Lemma 1 both active and passive FLO gates can permute between possible output Fock states* $|\mathbf{x}\rangle$ *in* $\mathcal{H}_{\rm pas} = \bigwedge^{2N}(\mathbb{C}^{4N})$ *and* $\mathcal{H}_{\rm act} = \mathcal{H}^{+}_{\rm Fock}(\mathbb{C}^{4N})$*, respectively. Therefore, using the invariance of the Haar measure on* G*, we can transform* $\mathbf{x}_0$ *above into any other output* $\mathbf{x}$ *satisfying* $|\mathbf{x}| = 2N$ *(for passive FLO) and* $|\mathbf{x}|$ *even (for active FLO).*

Proof. We first fix the symmetry group G describing a class of FLO circuits. The proof is virtually identical for both $G = \mathrm{U}(4N)$ and $G = \mathrm{SO}(8N)$. Suppose that $\mathcal{O}$ is an oracle that given a description of $\Pi(g)$ computes $|\langle \mathbf{x}_0|\Pi(g)|\Psi_{\rm in}\rangle|^2$ with high probability, i.e.,

$$\Pr_{g\sim\mu_G}\left[\mathcal{O}(\Pi(g)) = |\langle \mathbf{x}_0|\Pi(g)|\Psi_{\rm in}\rangle|^2\right] > \alpha\ . \tag{141}$$

The uniform distribution of FLO circuits ν_G is obtained by setting $V = \Pi(g)$, where $g\sim\mu_G$ (recall that $\nu_G = \nu_{\rm pas}$ for $G = \mathrm{U}(4N)$ and $\nu_G = \nu_{\rm act}$ for $G = \mathrm{SO}(8N)$). Therefore Eq. (141) is equivalent to

$$\Pr_{V\sim\nu_G}\left[\mathcal{O}(V) = |\langle \mathbf{x}_0|V|\Psi_{\rm in}\rangle|^2\right] > \alpha\ . \tag{142}$$

In what follows we argue that oracle $\mathcal{O}$ can be used to compute the #P-hard probability in polynomial time. The argument presented bellow follows steps from worst-to-average-case reduction for permanents of Gaussian matrices from [25], and its modification that involving rational interpolation from [1]. We consider a rational path interpolation $g_\theta = g_0 F_\theta(g)$ between worst-case g_0 and $=g' = g_0 g$, where g is chosen according to Haar measure on G. We will call $\mathcal{O}$ on L distinct FLO circuits $\Pi(g_{\theta_1}), \Pi(g_{\theta_2}),\ldots,\Pi(g_{\theta_L})$, where $\theta_i\in[1-\Delta,1]$, and the parameter Δ will be chosen later. We use evaluations $\{\mathcal{O}(\Pi(g_{\theta_i}))\}_{i=1}^{L}$ to efficiently reconstruct the rational function using Berlekamp-Welch algorithm for rational functions $R(\theta) = |\langle \mathbf{x}_0|\Pi(g_\theta)|\Psi_{\rm in}\rangle|^2$ (cf. Theorem 4). If the reconstruction is successful, evaluation of $R(\theta)$ at $\theta = 0$ gives us the #P-hard probability $R(0) = |\langle \mathbf{x}_0|V_0|\Psi_{\rm in}\rangle|^2$ (we used here $V_0 = \Pi(g_0)$).

To assess the success probability with which the above scheme evaluates $|\langle \mathbf{x}_0|V_0|\Psi_{\rm in}\rangle|^2$ correctly we first bound the success probability with which oracle $\mathcal{O}$ computes the value of $p_{\mathbf{x}_0}(\Pi(g_\theta),\Psi_{\rm in})$ correctly. Using variational characterization of TV distance and bounds from Eq.(139) we obtain

$$\Pr_{V\sim\nu_G}\left[\mathcal{O}(V) = |\langle \mathbf{x}_0|V|\Psi_{\rm in}\rangle|^2\right] - \Pr_{V\sim\nu_G^\theta}\left[\mathcal{O}(V) = |\langle \mathbf{x}_0|V|\Psi_{\rm in}\rangle|^2\right] \le CN^2\Delta\ . \tag{143}$$

Combining the above with (142) we get

$$\Pr_{V\sim\nu_G^\theta}\left[\mathcal{O}(V) = |\langle \mathbf{x}_0|V|\Psi_{\rm in}\rangle|^2\right] \ge \alpha - CN^2\Delta\ . \tag{144}$$

Or equivalently

$$\Pr_{g\sim\mu_G}\left[\mathcal{O}(\Pi(g_\theta)) = |\langle \mathbf{x}_0|\Pi(g_\theta)|\Psi_{\rm in}\rangle|^2\right] \ge \alpha - CN^2\Delta\ . \tag{145}$$

According to rational Berlekamp-Welch algorithm the number of evaluations L of a rational function $R(\theta)$ that allows to reconstruct it despite heaving at most t incorrect evaluations has to satisfy $L > d_1 + d_2 + 2t$. Note that in the considered case $d_1 + d_2 = \Theta(N^2)$ (cf. (140)). The probability of having number of errors that exceeds the bound allowing for reconstruction of $R(\theta)$ can be estimated using Markov inequality applied for the random variable counting the number of invalid evaluations of the oracle

$$t(g) = \left|\left\{\theta_i \mid \mathcal{O}(\Pi(g_{\theta_i})) \ne |\langle \mathbf{x}_0|\Pi(g_{\theta_i})|\Psi_{\rm in}\rangle|^2\ ,\ i\in[L]\right\}\right|\ . \tag{146}$$

From the definition of t and the inequality (145) it follows that $\mathbb{E}_{g\sim\mu_G} t(g) \le [1-\alpha+CN^2\Delta]L$. Using this estimate in Markov inequality (recall that by assumption $\alpha > \frac{3}{4} + \delta$, for $\delta = \frac{1}{\mathrm{poly}(N)}$) we get

$$\Pr_{g\sim\mu_G}\left[t(g) > \frac{L-d_1-d_2}{2}\right] \leq \frac{[1-\alpha+CN^2\Delta]L}{\frac{L-d_1-d_2}{2}} \leq \frac{\frac{1}{4}-\delta+CN^2\Delta}{\frac{1}{2}-\frac{d_1+d_2}{2L}} \ . \tag{147}$$

By choosing Δ and L such that $CN^2\Delta \leq \frac{\delta}{2}$ and $\frac{d_1+d_2}{2L} \leq \frac{\delta}{4}$ (this can be done with $\Delta = \frac{1}{\mathrm{poly}(N)}$ and $L = \mathrm{poly}(N)$ because $d_1 + d_2 = \Theta(N^2)$), we obtain

$$\Pr_{g\sim\mu_G}\left[t(g) > \frac{L-d_1-d_2}{2}\right] \leq \frac{\frac{1}{4}-\frac{\delta}{2}}{\frac{1}{2}-\frac{\delta}{4}} \leq \frac{1}{2} - \frac{\delta}{4} \ . \tag{148}$$

The leftmost part of the above inequality is the probability of failure of our protocol. Therefore, since $\delta = \frac{1}{\mathrm{poly}(N)}$, we can repeat the procedure polynomially many number of times, for different choices of $\Pi(g)$, compute $R\Pi(g)(0)$ each time, and output the majority vote. The probability of successfully computing the right result (i.e., $|\langle \mathbf{x}_0|V_0|\Psi_{\mathrm{in}}\rangle|^2$) can be made exponentially close to 1 in this way. $\square$

We proceed with proving the robust version of the above result. To this end we shift to polynomial interpolation because much more is known about its robustness to errors. To phrase our problem using polynomials we first note that the rational function $R_{g_0,g} = |\langle \mathbf{x}_0|\Pi(g_\theta)|\Psi_{\mathrm{in}}\rangle|^2$, where $g_\theta = g_0 F_\theta(g)$ can be written as

$$R_{g_0,g}(\theta) = \frac{D_{g_0,g}(\theta)}{Q_g(\theta)} \ , \tag{149}$$

where for both groups $D_{g_0,g}, Q_g$ are real polynomials of degrees $D_{g_0,g} = d_1 = \Theta(N^2)$, $Q_g = d_2 = \Theta(N^2)$ (cf Lemma 6). Moreover, the denominator $Q_g(\theta)$ can be computed efficiently in N (see Eq. (136)) given a classical description of g. Hence, we have

Lemma 7. *Let $R_{g_0,g}(\theta)$ be defined as in (149) (for fixed $g_0, g \in G$, where $G = \mathrm{U}(4N)$ or $G = \mathrm{SO}(8N)$). Then complexity of computation of $R_{g_0,g}(\theta)$ and $D_{g_0,g}(\theta)$ is equivalent up to $\Theta(N^2)$ overhead.*

The above allows us to use, following [1, 29], techniques of polynomial interpolation in order to estimate the hard probability $R_{g_0,g}(0)$. We will now state two results form this domain that will be used later in the robust version of the worst-to-average-case reduction given above.

Lemma 8 (Paturi lemma [109])**.** *Let $P(\theta)$ be a polynomial of degree k and suppose that for $|P(\theta)| \leq \epsilon$ for $\theta \in [1-\Delta, 1]$, $\Delta \in (0,1]$. Then*

$$P(0) \leq \epsilon \exp(4k(1+\Delta^{-1})) \ . \tag{150}$$

Remark 16. *The above lemma is usually presented in a slightly different form in which the assumption $|P(\theta)| \leq \epsilon$ for $\theta \in [-\Delta, \Delta]$ ($\Delta > 0$) is used to establish $P(0) \leq \epsilon \exp(2k(1+\Delta^{-1}))$. Our result can be deduced from the former via simple affine change of variables $\theta \mapsto \theta' = -\frac{2}{2-\Delta}\theta + 1$.*

Theorem 6 (Values of polynomials bounded at equally spaced points [110])**.** *Let θ_i, $i = 1, \ldots, L$ be a collection of L equally spaced points in the interval $[1-\Delta, 1]$, $\Delta \in (0,1)$. Let $P(\theta)$ be a polynomial of degree k. Assume that for every i, $|P(\theta_i)| \leq \epsilon$. Then there exist absolute constants $a, b > 0$ such that*

$$\max_{\theta\in[1-\Delta,1]} |P(\theta)| \leq \epsilon \exp\left(b\frac{k^2}{L} + a\right) \ . \tag{151}$$

Remark 17. *The problem of bounding values of polynomials that are bounded on uniformly spaced interval has a long history and there were more recent developments in this topic (see for example [111]). However for our purposes the above result by Coppersmith and Rivlin is sufficient.*

Before we formulate our result and prove our main theorem we need one more technical ingredient. Informally speaking, since $Q_g(\theta)$ appears in the denominator of (149) we need ensure that values of $Q_g(\theta)$ are not too large for typical values of g. This is achieved by combining Lemma 3 and explicit formulas for $Q_g(\theta)$ given in (136) we obtain

Corollary 1. *Let $g \in G$ and let $Q_g(\theta)$ be the polynomial in defined in (136) for $G = \mathrm{U}(d)$ in $G = \mathrm{SO}(2d)$. Assume that $n = 2N$, $d = 4N$. Let now $\tilde{\Delta} > 0$. We then have the following inequalities*

$$\Pr_{g\sim\mu_{\mathrm{U}(d)}}\left(Q_g(\theta) \leq \left[1 + \left(\frac{\theta\pi}{\tilde{\Delta}}\right)^2\right]^{16N^2}\right) \geq 1 - 4N\frac{\tilde{\Delta}}{\pi} \ , \tag{152}$$

$$\Pr_{g\sim\mu_{\mathrm{SO}(2d)}}\left(Q_g(\theta) \leq \left[1 + \left(\frac{\theta\pi}{\tilde{\Delta}}\right)^2\right]^{32N^2}\right) \geq 1 - 4N\frac{\tilde{\Delta}}{\pi} \ . \tag{153}$$

Combining all technical ingredients stated above we are in the position to prove our main result.

Theorem 7 (Average-case #P-hardness of approximation outcome probabilities of FLO circuits)**.** *Let V_0 be a FLO circuit such that computing $p_{\mathbf{x}_0}(V_0, \Psi_{\mathrm{in}}) = |\langle\mathbf{x}_0|V_0|\Psi_{\mathrm{in}}\rangle|^2$ is #P-Hard, where V_0 is element of either passive or active FLO circuits and the output Fock state $|\mathbf{x}_0\rangle$ belongs to the suitable Hilbert space $\mathcal{H}_{\mathrm{pas}} = \bigwedge^{2N}(\mathbb{C}^{4N})$ for passive FLO and $\mathcal{H}_{\mathrm{act}} = \mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^{4N})$, respectively.*

Let $\epsilon = \exp(-\Theta(N^6))$. Then it is #P-Hard to compute $p_{\mathbf{x}_0}(V, \Psi_{\mathrm{in}}) = |\langle\mathbf{x}_0|V|\Psi_{\mathrm{in}}\rangle|^2$ to accuracy ϵ with probability $\alpha > 1 - \delta$, $\delta = o(N^{-2})$, over the the uniform distribution of circuits: $V \sim \nu_{\mathrm{pas}}$ for passive FLO and $V \sim \nu_{\mathrm{act}}$ for active FLO.

Remark 18. *Using the same arguments as in remark below Theorem 5 we can transform $\mathbf{x}_0$ above into any other output $\mathbf{x}$ satisfying $|\mathbf{x}| = 2N$ (for passive FLO) and $|\mathbf{x}|$ even (for active FLO).*

Proof. We first fix the symmetry group G describing a class of FLO circuits. The uniform distribution of FLO circuits ν_G is obtained by by setting $V = \Pi(g)$, where $g \sim \mu_G$ (recall that $\nu_G = \nu_{\mathrm{pas}}$ for $G = \mathrm{U}(4N)$ and $\nu_G = \nu_{\mathrm{act}}$ for $G = \mathrm{SO}(8N)$). The general idea of the proof is similar to the reasoning used to prove Theorem 5. We start with an oracle $\mathcal{O}$ that given a classical description of $V = \Pi(g)$, is able to approximately compute $p_{\mathbf{x}_0}(V, \Psi_{\mathrm{in}}) = |\langle\mathbf{x}_0|\Pi(g)|\Psi_{\mathrm{in}}\rangle|^2$,

$$\Pr_{g\sim\mu_G}\left[\left|\mathcal{O}(\Pi(g)) - |\langle\mathbf{x}_0|\Pi(g)|\Psi_{\mathrm{in}}\rangle|^2\right| \leq \epsilon\right] > 1 - \delta \ . \tag{154}$$

Equivalently we have

$$\Pr_{V\sim\nu_G}\left[\left|\mathcal{O}(V) - |\langle\mathbf{x}_0|V|\Psi_{\mathrm{in}}\rangle|^2\right| \leq \epsilon\right] > 1 - \delta \ . \tag{155}$$

For a generic Haar random $g \in G$ we again consider a rational path $g_\theta = g_0 F_\theta(g)$ between $g_0 g$ and g_0, where g_0 is an element of the group corresponding to the worst-case circuit. Recall that by μ_G^θ we denoted the distribution of g_θ for $g \sim \mu_G$. We will now query oracle $\mathcal{O}$ multiple times on g_{θ_i}, where θ_i are L equally distributed points in the interval $[1-\Delta, 1]$, for $\Delta > 0$ to be set latter. As done previously in the proof of Theorem 5 by using variational characterization of TV distance and Eq. (139), we obtain that for every $\theta_i \in [1-\Delta, 1]$

$$\Pr_{g\sim\mu_G}\left[\left|\mathcal{O}(\Pi(g_{\theta_i})) - |\langle\mathbf{x}_0|\Pi(g_{\theta_i})|\Psi_{\mathrm{in}}\rangle|^2\right| \leq \epsilon\right] > 1 - \delta - C\Delta N^2 \ , \tag{156}$$

where C is a constant depending on G. Let now $D_{g_0,g}(\theta)$ be a polynomial of degree $\deg(D_{g_0,g}) = \Theta(N^2)$ that we defined (149). Recall that the denominator of $R_{g_0,g}(\theta)$, $Q_g(\theta)$ can be computed efficiently (cf. Lemma 7). Therefore we can use $\mathcal{O}$ to construct an oracle $\tilde{\mathcal{O}}$ that computes approximations of values of polynomial $D_{g_0,g}$ at point θ_i with potentially high probability over the choice of g

$$\Pr_{g\sim\mu_G}\left[\left|\tilde{\mathcal{O}}(\Pi(g_{\theta_i})) - D_{g_0,g}(\theta_i)\right| \leq \epsilon Q_g(\theta_i)\right] > 1 - \delta - C\Delta N^2 \ , \tag{157}$$

We now use Corollary 1 to bound $Q_g(\theta)$ in the above expression:

$$\Pr_{g\sim\mu_G}\left[Q_g(\theta) \leq \exp\left(\frac{A}{\tilde{\Delta}}N^2\right)\right] \geq 1 - 4N\frac{\tilde{\Delta}}{\pi} \ , \tag{158}$$

where $\tilde{\Delta} > 0$ and A a positive numerical constant mildly depending on the group G. Using the bound $\Pr(A \cap B) \geq \Pr(A) + \Pr(B) - 1$ we obtain

$$\Pr_{g\sim\mu_G}\left[\left|\tilde{\mathcal{O}}(\Pi(g_{\theta_i})) - D_{g_0,g}(\theta_i)|\right| \leq \epsilon \exp\left(\frac{A}{\tilde{\Delta}}N^2\right)\right] > 1 - \delta - C\Delta N^2 \ - 4N\frac{\tilde{\Delta}}{\pi}, \tag{159}$$

We finally use union bound lower to bound the probability that $\tilde{\mathcal{O}}$ is successful *for all* L equally spaced θ_i in $[1-\Delta, 1]$:

$$\Pr_{g\sim\mu_G}\left[\forall\theta_i \ \left|\tilde{\mathcal{O}}(\Pi(g_{\theta_i})) - D_{g_0,g}(\theta_i)|\right| \leq \epsilon \exp\left(\frac{A}{\tilde{\Delta}}N^2\right)\right] > 1 - L(\delta + C\Delta N^2 \ + 4N\frac{\tilde{\Delta}}{\pi}), \tag{160}$$

If $L \approx \deg(D_{g_0,g}) = \Theta(N^2)$ the above evaluations of $\tilde{\mathcal{O}}$ can be used to recover polynomial $\tilde{P}_{g_0,g}$ passing through points $(\theta_i, \tilde{\mathcal{O}}(\Pi(g_{\theta_i})))$ and having identical degree to $D_{g_0,g}$. By (159) and results of Coppersmith and Rivlin stated in [110] we know that (note that we set $L \approx \deg(D_{g_0,g}) = \Theta(N^2)$)

$$\max_{\theta\in[1-\Delta,1}\left|\tilde{P}_{g_0,g}(\theta) - D_{g_0,g}(\theta)\right| \leq \epsilon \exp\left(\frac{A}{\tilde{\Delta}}N^2\right)\exp(\Theta(N^2)) = \epsilon \exp\left(\frac{\Theta(N^2)}{\tilde{\Delta}}\right) \ . \tag{161}$$

Recall that by assumption and definition of Cayley path $D_{g_0,g}(0)$ encodes a (rescaled) #P-hard probability amplitude. Using Paturi lemma for the polynomial $\tilde{D}_{g_0,g}(\theta) - D_{g_0,g}(\theta)$ we finally obtain

$$\left|\tilde{D}_{g_0,g}(0) - D_{g_0,g}(0)\right| \leq \epsilon \exp\left(\frac{\Theta(N^2)}{\tilde{\Delta}} + \Theta(N^2)(1+\Delta^{-1})\right) \tag{162}$$

To sum up, the initially assumed oracle $\mathcal{O}$ allows us to construct an efficient algorithm $\mathcal{A}$ that approximately computes #P-hard quantity $D_{g_0,g}(0) = Q_g(\theta)\left|\langle \mathbf{x}_0|\Pi(g_0)|\Psi_{\text{in}}\rangle\right|^2$:

$$\Pr_{g\sim\mu_G}\left[|\mathcal{A}(\Pi(g)) - D_{g_0,g}(0)|| \leq \tilde{\epsilon}\right] > 1 - BN^2(\delta + C\Delta N^2 \ + 4N\frac{\tilde{\Delta}}{\pi}), \tag{163}$$

where $\tilde{\epsilon} = \epsilon \exp\left(\frac{\Theta(N^2)}{\tilde{\Delta}} + \Theta(N^2)(1+\Delta^{-1})\right)$, and $B > 0$ is a numerical constant. Success probability of the protocol to exceeds $\frac{1}{2}$ with the following scaling

$$\Delta = \Theta(N^{-4}) \ , \tilde{\Delta} = \Theta(N^{-3}) \ . \tag{164}$$

From the result of [112] we have #P hardness guarantees up to constant multiplicative error. Since for #P-hard quantity this such error implies additive error of magnitude at most $2^{-\Theta(N)}$. Therefore by setting $\tilde{\epsilon} \leq 2^{-\Theta(N)}$ which, by the virtue of Eq.(164) corresponds to scaling of the original error $\epsilon = \exp(-\Theta(N^6))$ allows to to extrapolate to the hardness neighbored.

□

Remark 19. *In the course of the proof of the above result we have realised an inadequate usage of the oracle in the reduction by Movassagh [1] (the author assumed that the oracle works as in* (156) *but without the neccesary dependence on* Δ *. Correction of the proof seams to give in that case worse then claimed tolerance for error* $\epsilon = \exp(-\theta(N^{4.5})$ *(for the Google layout), which is still better then the one claimed here.*

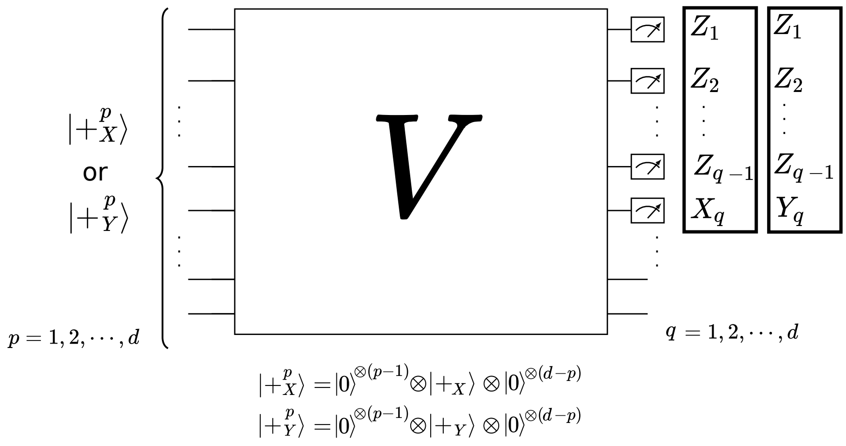

FIG. 6. A graphical presentation of the tomography protocol of an active FLO circuit V. A single step of the protocol consists of (i) preparation of $2d$ input states $|+^p_X\rangle$ and $|+^p_Y\rangle$ ($p = 1, \ldots, d$), (ii) transformation of the states via the circuit V and (iii) for each of the $2d$ states measuring the operators $Z_1 Z_2 \cdots Z_{q-1} X_q$ and $Z_1 Z_2 \cdots Z_{q-1} Y_q$ ($q = 1, \ldots, d$). These operations are then repeated multiple times in order to gather sufficient statistics necessary to reconstruct the orthogonal matrix $O \in \mathrm{SO}(2d)$ that defines the unitary channel Φ_V associated to $V = \Pi_{\mathrm{act}}(O)$.

X. EFFICIENT TOMOGRAPHY OF FERMIONIC LINEAR OPTICS

The tomography and certification of gates, i.e., the task of ensuring that the correct unitary was implemented, is vital for near-term quantum devices. However, it is often an inherently challenging problem due to exponential scaling of the number of parameters describing a general multiqubit quantum operation [113]. Here we show that the structure of FLO unitaries allows us to perform their tomography efficiently using resources scaling only polynomially with the system size. As passive fermionic gates form a subset of active FLO circuits, we focus only on the tomography of the latter ones, since from this also the tomography of passive circuit follows.

We will use here again the Jordan-Wigner mapping between d qubit system and fermionic Fock space with d physical modes (see Section II), and define the following $2d$ pure states:

$$|+^p_X\rangle = \mathbb{I}^{\otimes(p-1)} \otimes H \otimes \mathbb{I}^{\otimes(d-p)} |0\rangle^{\otimes d} = |0\rangle^{\otimes(p-1)} \otimes |+_X\rangle \otimes |0\rangle^{\otimes(d-p)} \;, \tag{165}$$

$$|+^p_Y\rangle = \mathbb{I}^{\otimes(p-1)} \otimes \tilde{H} \otimes \mathbb{I}^{\otimes(d-p)} |0\rangle^{\otimes d} = |0\rangle^{\otimes(p-1)} \otimes |+_Y\rangle \otimes |0\rangle^{\otimes(d-p)} \;, \tag{166}$$

where $p = 1, \ldots, d$. In terms of majorana operators, one can write the density matrices of these states as

$$\rho_{2p-1} = |+^p_X\rangle\langle +^p_X| = \prod_{q=1}^{p-1} \left(\frac{\mathbb{I} + i m_{2q-1} m_{2q}}{2} \right) \left(\frac{\mathbb{I} + \prod_{q=1}^{p-1} (i m_{2q-1} m_{2q}) m_{2p-1}}{2} \right) \prod_{q=p+1}^{d} \left(\frac{\mathbb{I} + i m_{2q-1} m_{2q}}{2} \right) \;, \tag{167}$$

$$\rho_{2p} = |+^p_Y\rangle\langle +^p_Y| = \prod_{q=1}^{p-1} \left(\frac{\mathbb{I} + i m_{2q-1} m_{2q}}{2} \right) \left(\frac{\mathbb{I} + \prod_{q=1}^{p-1} (i m_{2q-1} m_{2q}) m_{2p}}{2} \right) \prod_{q=p+1}^{d} \left(\frac{\mathbb{I} + i m_{2q-1} m_{2q}}{2} \right) \;, \tag{168}$$

where, as before, $p = 1, \ldots, d$. Expanding these density matrices in terms of majorana monomials (given in Eq. (128)), we observe that for an arbitrary ρ_x ($x = 1, \ldots, 2d$) there is only one majorana monomial of degree 1 appearing, namely m_x. Thus, considering the FLO evolved states $V \rho_x V^\dagger$, the degree 1 majorana terms will be of the form (see Eq. (11)) $V m_x V^\dagger = \sum_{y=1}^{2d} O_{yx} m_y$, where $O \in \mathrm{SO}(2d)$ is the orthogonal matrix that encodes the FLO circuit V. In order to obtain arbitrary element of the orthogonal matrix O_{yx}, one needs only to insert the state ρ_x, evolve it with the FLO unitary V, and then measure the expectation value of m_y:

$$O_{yx} = \mathrm{tr}(m_y V \rho_y V^\dagger) \ . \tag{169}$$

Measuring the expectation value of m_{2q-1} and m_{2q} amounts to measuring $Z_1 \cdots Z_{q-1} X_q$ and $Z_1 \cdots Z_{q-1} Y_q$, respectively. These can all be done, after a single layer of local base change operations, through usual computational basis measurements. The graphical presentation of our tomography scheme is given in Fig. 6. The following theorem show that the construction outlined above allows to recover an unknown FLO circuit V efficiently in d, both in terms of the number of different setups needed for the implementation as well as in terms of sample complexity. Importantly, our results give rigorous recovery guarantees in the diamond norm, despite the presence of statistical fluctuations.

Theorem 8 (Efficient tomography of active FLO unitary channels)**.** *Let V be an unknown active FLO circuit acting on d qubits. Consider the following estimation protocol using the states ρ_x and observables m_y ($x, y \in [2d]$) and comprising of r independent experimental rounds. A single experimental round, say the k'th, consists of the following routines:*

- *For every pair $(x, y) \in [2d]^{\times 2}$: (i) prepare ρ_x as input state; (ii) evolve ρ_x via the circuit V; (iii) measure $V \rho_x V^\dagger$ using m_y obtaining outcome $m_{yx}^{(k)} \in \{-1, 1\}$.*

The outcomes of the k'th round are gathered in the $2d \times 2d$ matrix $M^{(k)}$ with entries $m_{yx}^{(k)}$. After r rounds, define $\hat{M}_r := \frac{1}{r} \sum_{k=1}^{r} M^{(k)}$ as the sample average of matrices $M^{(k)}$. Then, let $\hat{O}_r \in \mathrm{SO}(2d)$ be defined as the orthogonal matrix appearing in the polar decomposition of $\hat{M}_r$ (i.e., $\hat{M}_r = O_r P$, where P is a semidefinite real $2d \times 2d$ matrix). Finally, set $\hat{V} := \Pi_{\mathrm{act}}(\hat{O}_r)$ as the estimator of the circuit V after r rounds of the protocol.

Assume that all routines in the protocol are implemented perfectly. Furthermore, let $\delta \in (0, 1)$ be fixed and let Φ_V and $\Phi_{\hat{V}}$ be the unitary channels defined by the active FLO circuits V and $\hat{V}$, respectively. Then, for the number of rounds satisfying

$$r \geq \frac{7c^2 d^3}{\epsilon^2} \log\left(\frac{4d}{\delta}\right) \ , \tag{170}$$

the protocol outputs an FLO circuit $\hat{V}$ such that $\|\Phi_V - \Phi_{\hat{V}}\|_\diamond \leq \epsilon$ with probability at least $1 - \delta$.

Remark 20. *We believe that it possible to improve the sampling complexity and the number of quantum circuits needed for the tomography of an unknown FLO unitary V. Moreover, we expect that our proof technique can also be used for the quantum process tomography of general fermionic Gaussian channels.*

There are three key difficulties that need to be circumvented in order to establish the above result. The first one is related to the fact that, by the virtue of (169), the protocol estimates an orthogonal matrix $O \in \mathrm{SO}(2d)$ not the circuit V or the associated d-qubit channel Φ_V. The following Lemma, proved in Appendix C, allows us to connect operator-norm distance between elements of the orthogonal group with the diamond norm between the corresponding quantum channels (this result can be viewed as a fermionic version of the analogous stability result proved by Arkhipov for standard Boson Sampling [82]) .

Lemma 9 (Stability of the active FLO representation)**.** *Consider two elements of the orthogonal group, $O, O' \in \mathrm{SO}(2d)$, and let V and V' be the corresponding active FLO unitaries, i.e., $V = \Pi_{\mathrm{act}}(O)$ and $V' = \Pi_{\mathrm{act}}(O')$. Furthermore, let Φ_V and $\Phi_{V'}$ be the unitary channels defined by V and V', respectively. Then the following inequality is satisfied*

$$\|\Phi_V - \Phi_{V'}\|_\diamond \leq 2d \|O - O'\|. \tag{171}$$

The second technical issue arises because the sample-average matrices $\hat{M}_s$ appearing in the protocol are not necessarily orthogonal. For this reason we use the (real) polar decomposition in order to get an orthogonal matrix from $\hat{M}_s$. The Lemma below gives an upper bound for the possible operator-norm error that can result from this procedure.

Lemma 10 (Operator-norm stability of the real polar decomposition [114])**.** *Let O be orthogonal matrix $n \times n$. Let Δ be $n \times n$ real matrix such that $\|\Delta\| \leq 1$. Let O_Δ be the orthogonal transformation appearing in the polar decomposition of $O + \Delta A$ (i.e. $O + \Delta = O_{O+\Delta} P$ for a semidefinite real matrix P). We then have the following inequality*

$$\|O - O_\Delta\| \leq \|\Delta\| \ . \tag{172}$$

The above lemma follows as a direct corollary of Theorem 2.3 in [114].

The last technical ingredient needed for the proof of Theorem 8 is the following matrix concentration bound, which allows to control the magnitude of statistical fluctuations incurred in our scheme.

Lemma 11 (Matrix Bernstein inequality [115])**.** *Let $S^{(1)}, \ldots, S^{(r)}$ be independent, centered real $n \times n$ random matrices with uniformly bounded operator norm, i.e., for all $k \in [r]$*

$$\mathbb{E} S^{(k)} = 0 \ , \ \|S^{(k)}\| \leq L \ . \tag{173}$$

Assume furthermore that the entries of each $S^{(k)}$ are independently distributed with a variance upper bounded by a constant, $\mathrm{Var}(S^{(k)}_{ij}) \leq c$.

We then have the following concentration inequality valid for arbitrary $\tau > 0$

$$\Pr\left(\left\| \frac{1}{r} \sum_{k=1}^{r} S^{(k)} \right\| \geq \tau \right) \leq 2n \exp\left(-\frac{r\tau^2}{2(nc + \frac{L}{3}\tau)} \right) \ . \tag{174}$$

A more general version of the above inequality (that does not require independently distributed entries of matrices $S^{(k)}$) can be found in Theorem 1.6.2 from [115].

Proof of Theorem 8. Let us remark first that our tomography protocol was defined such that the matrices $M^{(k)}$ originating form different rounds k are independent from each other, and for fixed k also their entries $m^{(k)}_{yx}$ are independent. Furthermore, by virtue of Eq. (169), we have

$$\mathbb{E} m^{(k)}_{yx} = O_{yx} \ , \tag{175}$$

where $O \in \mathrm{SO}(2d)$ is an orthogonal matrix corresponding to the circuit V. We now apply Lemma 11 to the sequence of $2d \times 2d$ matrices $\Delta^{(k)} := M^{(k)} - O$. From definition matrix elements of $\Delta^{(k)}$ satisfy $|\Delta^{(k)}_{yx}| \leq 2$. From this and the fact that $m^{(k)}_{yx} \in \{-1, 1\}$ it easily follows that

$$\|\Delta^{(k)}\| \leq 4d \ , \ \mathrm{Var}(\Delta^{(k)}_{yx}) \leq 1 \ . \tag{176}$$

Inserting these estimates in Eq. (174) (and noting that $n = 2d$) gives

$$\Pr\left(\left\| \frac{1}{r} \sum_{k=1}^{r} \Delta^{(k)} \right\| \geq \tau \right) \leq 4d \exp\left(-\frac{r\tau^2}{4d(1 + \frac{2}{3}\tau)} \right) \ . \tag{177}$$

Recalling that $\hat{M}_r = \frac{1}{r} \sum_{k=1}^{r} M^{(k)}$, using the definition of $\Delta^{(k)}$, and assuming that $\tau < 1$ (in what follows we will see that we can indtroduce this constraint without the loss of generality) we obtain

$$\Pr\left(\left\| \hat{M}_r - O \right\| \leq \tau \right) \geq 1 - 4d \exp\left(-\frac{r\tau^2}{7d} \right) \ . \tag{178}$$

We therefore know that, provided r is high enough, the sample average $\hat{M}^{(k)}$ approximates matrix O in operator norm. Applying Lemma 10 to $\hat{O}_r$, i.e., to the orthogonal part of the polar decomposition of $\hat{M}_r$ (this corresponds to setting $\Delta = \hat{M}_r - O$ in (172)), we obtain

$$\Pr\left(\left\|\hat{O}_r - O\right\| \leq \tau\right) \geq 1 - 4d\exp\left(-\frac{r\tau^2}{7d}\right) . \tag{179}$$

Recalling that $\hat{V} = \Pi_{\mathrm{act}}(\hat{O})$ and $V = \Pi_{\mathrm{act}}(O)$ and invoking Lemma 9 we finally arrive to

$$\Pr\left(\left\|\Phi_{\hat{V}} - \Phi_V\right\|_\diamond \leq 2d\,\tau\right) \geq 1 - 4d\exp\left(-\frac{r\tau^2}{7d}\right) . \tag{180}$$

We conclude the proof by setting $\epsilon \coloneqq 2d\,\tau$ and noting that (170) follows from requiring that right-hand side of Eq. (180) is larger than $1-\delta$.

□

[1] R. Movassagh, arXiv e-prints , arXiv:1909.06210 (2019), arXiv:1909.06210 [quant-ph].

[2] C. Gidney and M. Ekerå, arXiv e-prints , arXiv:1905.09749 (2019), arXiv:1905.09749 [quant-ph].

[3] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. Girvin, L. Jiang, *et al.*, Nature **536**, 441 (2016).

[4] L. Egan, D. M. Debroy, C. Noel, A. Risinger, D. Zhu, D. Biswas, M. Newman, M. Li, K. R. Brown, M. Cetina, and C. Monroe, arXiv e-prints , arXiv:2009.11482 (2020), arXiv:2009.11482 [quant-ph].

[5] J. Preskill, Quantum **2**, 79 (2018).

[6] B. Bauer, S. Bravyi, M. Motta, and G. Kin-Lic Chan, Chemical Reviews **120**, 12685 (2020).

[7] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, Nature **549**, 242 (2017).

[8] S. Aaronson and L. Chen, in *Proceedings of the 32nd Computational Complexity Conference*, CCC '17 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, DEU, 2017).

[9] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, Nature Communications **5**, 4213 (2014).

[10] E. Farhi, J. Goldstone, and S. Gutmann, arXiv e-prints , arXiv:1411.4028 (2014), arXiv:1411.4028 [quant-ph].

[11] N. Moll, P. Barkoutsos, L. S. Bishop, J. M. Chow, A. Cross, D. J. Egger, S. Filipp, A. Fuhrer, J. M. Gambetta, M. Ganzhorn, A. Kandala, A. Mezzacapo, P. Müller, W. Riess, G. Salis, J. Smolin, I. Tavernelli, and K. Temme, Quantum Science and Technology **3**, 030503 (2018).

[12] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, *et al.*, arXiv preprint arXiv:2012.09265 (2020).

[13] S. Hadfield, Z. Wang, B. O'Gorman, E. Rieffel, D. Venturelli, and R. Biswas, Algorithms **12**, 34 (2019).

[14] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, Nature **549**, 195 (2017).

[15] V. Havlícek, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, Nature **567**, 209 (2019).

[16] C. Ciliberto, M. Herbster, A. D. Ialongo, M. Pontil, A. Rocchetto, S. Severini, and L. Wossnig, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **474**, 20170551 (2018).

[17] Y. Cao, J. Romero, J. P. Olson, M. Degroote, P. D. Johnson, M. Kieferová, I. D. Kivlichan, T. Menke, B. Peropadre, N. P. D. Sawaya, S. Sim, L. Veis, and A. Aspuru-Guzik, Chemical Reviews **119**, 10856 (2019).

[18] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'brien, Nature communications **5**, 4213 (2014).

[19] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, S. Boixo, M. Broughton, B. B. Buckley, D. A. Buell, B. Burkett, N. Bushnell, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, S. Demura, A. Dunsworth, D. Eppens, E. Farhi, A. Fowler, B. Foxen, C. Gidney, M. Giustina, R. Graff, S. Habegger, M. P. Harrigan, A. Ho, S. Hong, T. Huang, L. B. Ioffe, S. V. Isakov, E. Jeffrey, Z. Jiang, C. Jones, D. Kafri, K. Kechedzhi, J. Kelly, S. Kim, P. V. Klimov, A. N. Korotkov, F. Kostritsa, D. Landhuis, P. Laptev, M. Lindmark, M. Leib, E. Lucero, O. Martin, J. M. Martinis, J. R. McClean, M. McEwen, A. Megrant, X. Mi, M. Mohseni, W. Mruczkiewicz, J. Mutus, O. Naaman, M. Neeley, C. Neill, F. Neukart, H. Neven, M. Yuezhen Niu, T. E. O'Brien, B. O'Gorman, E. Ostby, A. Petukhov, H. Putterman, C. Quintana, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, A. Skolik, V. Smelyanskiy, D. Strain, M. Streif, K. J. Sung, M. Szalay,

A. Vainsencher, T. White, Z. J. Yao, P. Yeh, A. Zalcman, and L. Zhou, arXiv e-prints , arXiv:2004.04197 (2020), arXiv:2004.04197 [quant-ph].

[20] C. Hempel, C. Maier, J. Romero, J. McClean, T. Monz, H. Shen, P. Jurcevic, B. P. Lanyon, P. Love, R. Babbush, A. Aspuru-Guzik, R. Blatt, and C. F. Roos, Phys. Rev. X **8**, 031022 (2018).

[21] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, S. Boixo, M. Broughton, B. B. Buckley, D. A. Buell, B. Burkett, N. Bushnell, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, S. Demura, A. Dunsworth, E. Farhi, A. Fowler, B. Foxen, C. Gidney, M. Giustina, R. Graff, S. Habegger, M. P. Harrigan, A. Ho, S. Hong, T. Huang, W. J. Huggins, L. Ioffe, S. V. Isakov, E. Jeffrey, Z. Jiang, C. Jones, D. Kafri, K. Kechedzhi, J. Kelly, S. Kim, P. V. Klimov, A. Korotkov, F. Kostritsa, D. Landhuis, P. Laptev, M. Lindmark, E. Lucero, O. Martin, J. M. Martinis, J. R. McClean, M. McEwen, A. Megrant, X. Mi, M. Mohseni, W. Mruczkiewicz, J. Mutus, O. Naaman, M. Neeley, C. Neill, H. Neven, M. Y. Niu, T. E. O'Brien, E. Ostby, A. Petukhov, H. Putterman, C. Quintana, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, D. Strain, K. J. Sung, M. Szalay, T. Y. Takeshita, A. Vainsencher, T. White, N. Wiebe, Z. J. Yao, P. Yeh, and A. Zalcman, Science **369**, 1084 (2020), https://science.sciencemag.org/content/369/6507/1084.full.pdf.

[22] A. P. Lund, M. J. Bremner, and T. C. Ralph, npj Quantum Information **3**, 15 (2017).

[23] A. W. Harrow and A. Montanaro, Nature (London) **549**, 203 (2017), arXiv:1809.07442 [quant-ph].

[24] S. Bravyi, D. Gosset, and R. König, Science **362**, 308 (2018), https://science.sciencemag.org/content/362/6412/308.full.pdf.

[25] S. Aaronson and A. Arkhipov, Theory of Computing **4**, 143 (2013).

[26] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A **467**, 459 (2011).

[27] M. Bremner, A. Montanaro, and D. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).

[28] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Nature Physics **14**, 595–600 (2018), arXiv:1608.00263 [quant-ph].

[29] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Nature Physics **15**, 159 (2019).

[30] B. Fefferman and C. Umans, in *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 61, edited by A. Broadbent (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2016) pp. 1:1–1:19.

[31] T. Morimae, Phys. Rev. A **96**, 040302 (2017).

[32] J. Bermejo-Vega, D. Hangleiter, M. Schwarz, R. Raussendorf, and J. Eisert, Phys. Rev. X **8**, 021010 (2018), arXiv: 1703.00466.

[33] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Physical review letters **119**, 170501 (2017).

[34] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Physical review letters **113**, 100502 (2014).

[35] J. Haferkamp, D. Hangleiter, A. Bouland, B. Fefferman, J. Eisert, and J. Bermejo-Vega, arXiv e-prints , arXiv:1908.08069 (2019), arXiv:1908.08069 [quant-ph].

[36] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Land huis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Nature (London) **574**, 505 (2019).

[37] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Quantum **2**, 65 (2018).

[38] A. Harrow and S. Mehraban, arXiv e-prints , arXiv:1809.06957 (2018), arXiv:1809.06957 [quant-ph].

[39] D. J. Brod, E. F. Galvão, A. Crespi, R. Osellame, N. Spagnolo, and F. Sciarrino, Advanced Photonics **1**, 034001 (2019).

[40] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, Z. Wang, *et al.*, Physical review letters **123**, 250503 (2019).

[41] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Science **370**, 1460 (2020), https://science.sciencemag.org/content/370/6523/1460.full.pdf.

[42] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).

[43] E. Knill, arXiv e-prints , quant-ph/0108033 (2001), arXiv:quant-ph/0108033 [quant-ph].

[44] L. Valiant, SIAM J. Comput. **31**, 1229 (2002).

[45] E. Bocquillon, V. Freulon, F. D. Parmentier, J.-M. Berroir, B. Plaçais, C. Wahl, J. Rech, T. Jonckheere, T. Martin, C. Grenier, *et al.*, Annalen der Physik **526**, 1 (2014).

[46] I. D. Kivlichan, J. McClean, N. Wiebe, C. Gidney, A. Aspuru-Guzik, G. K.-L. Chan, and R. Babbush, Phys. Rev. Lett. **120**, 110501 (2018).

[47] Z. Jiang, K. J. Sung, K. Kechedzhi, V. N. Smelyanskiy, and S. Boixo, Phys. Rev. Applied **9**, 044036 (2018).
[48] P.-L. Dallaire-Demers, J. Romero, L. Veis, S. Sim, and A. Aspuru-Guzik, Quantum Science and Technology **4**, 045005 (2019).
[49] B. Foxen, C. Neill, A. Dunsworth, P. Roushan, B. Chiaro, A. Megrant, J. Kelly, Z. Chen, K. Satzinger, R. Barends, F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, S. Boixo, D. Buell, B. Burkett, Y. Chen, R. Collins, E. Farhi, A. Fowler, C. Gidney, M. Giustina, R. Graff, M. Harrigan, T. Huang, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, P. Klimov, A. Korotkov, F. Kostritsa, D. Landhuis, E. Lucero, J. McClean, M. McEwen, X. Mi, M. Mohseni, J. Y. Mutus, O. Naaman, M. Neeley, M. Niu, A. Petukhov, C. Quintana, N. Rubin, D. Sank, V. Smelyanskiy, A. Vainsencher, T. C. White, Z. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Phys. Rev. Lett. **125**, 120504 (2020).
[50] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, Optica **3**, 1460 (2016).
[51] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[52] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, 1st ed. (Cambridge University Press, USA, 2009).
[53] B. M. Terhal and D. P. DiVincenzo, Quantum Information & Computation **4**, 134 (2004).
[54] S. Fenner, F. Green, S. Homer, and R. Pruim, Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **455**, 3953 (1999).
[55] E. Farhi and A. W. Harrow, arXiv e-prints , arXiv:1602.07674 (2016), arXiv:1602.07674 [quant-ph].
[56] D. J. Brod, Phys. Rev. A **91**, 042316 (2015).
[57] A. Bouland, J. F. Fitzsimons, and D. E. Koh, in *33rd Computational Complexity Conference (CCC 2018)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 102, edited by R. A. Servedio (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2018) pp. 21:1–21:25, iSSN: 1868-8969.
[58] X. Gao, S.-T. Wang, and L.-M. Duan, Phys. Rev. Lett. **118**, 040502 (2017), publisher: American Physical Society.
[59] H. Pashayan, S. D. Bartlett, and D. Gross, Quantum **4**, 223 (2020).
[60] L. Stockmeyer, SIAM J. Comput. **14**, 849 (1985).
[61] S. B. Bravyi and A. Y. Kitaev, Annals of Physics **298**, 210 (2002).
[62] D. A. Ivanov, Phys. Rev. A **96**, 012322 (2017).
[63] D. A. Ivanov and L. Gurvits, Phys. Rev. A **101**, 012303 (2020).
[64] S. Bravyi, Phys. Rev. A **73**, 042313 (2006).
[65] M. Hebenstreit, R. Jozsa, B. Kraus, S. Strelchuk, and M. Yoganathan, Phys. Rev. Lett. **123**, 080503 (2019).
[66] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Phys. Rev. Lett. **119**, 170501 (2017).
[67] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, Phys. Rev. X **6**, 021039 (2016).
[68] M. Oszmaniec and Z. Zimborás, Phys. Rev. Lett. **119**, 220502 (2017), arXiv:1705.11188 [quant-ph].
[69] S. Bravyi, Quantum Info. Comput. **5**, 216–238 (2005).
[70] S. Bravyi and R. Koenig, arXiv e-prints , arXiv:1112.2184 (2011), arXiv:1112.2184 [quant-ph].
[71] R. Jozsa and A. Miyake, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **464**, 3089 (2008).
[72] D. J. Brod and E. F. Galvão, Phys. Rev. A **86**, 052307 (2012).
[73] D. J. Brod, Phys. Rev. A **93**, 062332 (2016).
[74] S. Bravyi and A. Kitaev, Physical Review A **71**, 022316 (2005).
[75] S. Bravyi, arXiv e-prints , quant-ph/0507282 (2005), arXiv:quant-ph/0507282 [quant-ph].
[76] F. d. Melo, P. Ćwikliński, and B. M. Terhal, New J. Phys. **15**, 013015 (2013).
[77] M. Oszmaniec, J. Gutt, and M. Kuś, Phys. Rev. A **90**, 020302 (2014).
[78] D. J. Brod and E. F. Galvão, Phys. Rev. A **84**, 022310 (2011).
[79] Z. Zimborás, R. Zeier, M. Keyl, and T. Schulte-Herbrüggen, EPJ Quantum Technology **1**, 11 (2014).
[80] C. Beenakker, D. DiVincenzo, C. Emary, and M. Kindermann, Physical review letters **93**, 020501 (2004).
[81] M. Hebenstreit, R. Jozsa, B. Kraus, and S. Strelchuk, arXiv e-prints , arXiv:2007.08231 (2020), arXiv:2007.08231 [quant-ph].
[82] A. Arkhipov, Physical Review A **92**, 062326 (2015).
[83] R. W. Goodman and N. R. Wallach, *Symmetry, Representations, and Invariants*, Graduate Texts in Mathematics (Springer, Dordrecht, 2009).
[84] B. C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction* (Springer, 2000).
[85] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky, Science **322**, 563 (2008), https://science.sciencemag.org/content/322/5901/563.full.pdf.
[86] S. Rahimi-Keshari, A. Scherer, A. Mann, A. T. Rezakhani, A. I. Lvovsky, and B. C. Sanders, New Journal of Physics **13**, 013006 (2011).
[87] S. Rahimi-Keshari, M. A. Broome, R. Fickler, A. Fedrizzi, T. C. Ralph, and A. G. White, Opt. Express **21**, 13450 (2013).

[88] N. Schuch and J. Siewert, Physical Review A **67**, 032301 (2003).
[89] J. M. Arrazola and T. R. Bromley, Physical review letters **121**, 030503 (2018).
[90] J. M. Arrazola, T. R. Bromley, and P. Rebentrost, Physical Review A **98**, 012322 (2018).
[91] J. Huh, G. G. Guerreschi, B. Peropadre, J. R. McClean, and A. Aspuru-Guzik, Nature Photonics **9**, 615 (2015).
[92] J. Huh and M.-H. Yung, Scientific reports **7**, 1 (2017).
[93] L. Banchi, M. Fingerhuth, T. Babej, C. Ing, and J. M. Arrazola, Science Advances **6**, eaax1950 (2020).
[94] M. Schuld, K. Brádler, R. Israel, D. Su, and B. Gupt, Physical Review A **101**, 032314 (2020).
[95] H. Ikai, Linear algebra and its applications **434**, 1094 (2011).
[96] A. E. Moylett and P. S. Turner, Physical Review A **97**, 062329 (2018).
[97] J. Napp, R. L. La Placa, A. M. Dalzell, F. G. S. L. Brandao, and A. W. Harrow, arXiv e-prints , arXiv:2001.00021 (2019), arXiv:2001.00021 [quant-ph].
[98] J. Helsen, S. Nezami, M. Reagor, and M. Walter, arXiv preprint arXiv:2011.13048 (2020).
[99] W. Lichtenstein, Proceedings of the American Mathematical Society **84**, 605 (1982).
[100] M. Kuś and I. Bengtsson, Phys. Rev. A **80**, 022319 (2009).
[101] M. Oszmaniec and M. Kuś, Phys. Rev. A **88**, 052328 (2013).
[102] M. Oszmaniec and M. Kuś, Phys. Rev. A **90**, 010302 (2014).
[103] M. Oszmaniec, arXiv e-prints , arXiv:1412.4657 (2014), arXiv:1412.4657 [quant-ph].
[104] D. Hangleiter, M. Kliesch, J. Eisert, and C. Gogolin, Physical review letters **122**, 210502 (2019).
[105] C. Lautemann, Information Processing Letters **17**, 215 (1983).
[106] S. Toda, SIAM Journal on Computing **20**, 865 (1991).
[107] R. Goodman and N. R. Wallach, *Symmetry, Representations, and Invariants* (Springer, 2009).
[108] G. Aubrun and S. J. Szarek, *Alice and Bob meet Banach: the interface of asymptotic geometric analysis and quantum information theory*, Mathematical surveys and monographs (American Mathematical Society, Providence, RI, 2017).
[109] R. Paturi, in *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '92 (Association for Computing Machinery, New York, NY, USA, 1992) p. 468–474.
[110] D. Coppersmith and T. J. Rivlin, SIAM Journal on Mathematical Analysis **23**, 970 (1992), https://doi.org/10.1137/0523054.
[111] E. A. Rakhmanov, Annals of Mathematics **165**, 55 (2007).
[112] M. E. Dyer, L. A. Goldberg, C. S. Greenhill, and M. Jerrum, in *Proceedings of the Third International Workshop on Approximation Algorithms for Combinatorial Optimization*, APPROX '00 (Springer-Verlag, Berlin, Heidelberg, 2000) p. 108–119.
[113] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nature Reviews Physics **2**, 382 (2020).
[114] R. Mathias, SIAM Journal on Matrix Analysis and Applications **14**, 588 (1993), https://doi.org/10.1137/0614041.
[115] J. A. Tropp, Found. Trends Mach. Learn. **8**, 1–230 (2015).
[116] E. M. Rains, IEEE Transactions on Information Theory **46**, 54 (2000).
[117] H. Elvang, P. Cvitanović, and A. D. Kennedy, Journal of Mathematical Physics **46**, 043501 (2005), https://doi.org/10.1063/1.1832753.
[118] A. J. Coleman and V. I. Yukalov, *Reduced density matrices: Coulson's challenge*, Vol. 72 (Springer Science & Business Media, 2000).
[119] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Pub. Co., 1983).
[120] M. Oszmaniec, A. Sawicki, and M. Horodecki, arXiv e-prints , arXiv:2007.10885 (2020), arXiv:2007.10885 [quant-ph].
[121] J. Fuchs and C. Schweigert, *Symmetries, Lie algebras and representations: A graduate course for physicists* (Cambridge University Press, 2003).

Appendix

We collect here technical results that are used in the main part of the paper. Some of the results stated here can be of independent interest for further works on quantum information processing with fermions.

Appendix A: Decomposition of passive and active FLO unitaries into two-qubit gates

Here we provide the derivation of the decomposition of arbitrary passive and active FLO gates into two-qubit gates with layouts depicted in Fig. 3, which was also studied in Refs. [46–48]. For passive bosonic linear optics the analogous decompositions were discussed in Refs. [50, 51]. The way to obtain these results is to consider the standard decomposition of $\mathrm{U}(d)$ and $\mathrm{SO}(2d)$ elements into so-called Givens rotations and then apply the appropriate FLO representations Π_{pas} and Π_{act} on this decomposition, as we will explain below. For simplicity, we will assume that d is even, which is also the relevant case for our paper.

The (nearest neighbor) Givens rotations $G^k(\alpha,\varphi)\in\mathrm{U}(d)$ $(k=1,\ldots,d{-}1)$ have the form

$$G^{(k)}(\alpha,\varphi)=\begin{bmatrix}1 & \cdots & 0 & 0 & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & & \vdots\\ 0 & \cdots & e^{i\varphi}\cos(\alpha) & -\sin(\alpha) & \cdots & 0\\ 0 & \cdots & e^{i\varphi}\sin(\alpha) & \cos(\alpha) & \cdots & 0\\ \vdots & & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & 1\end{bmatrix}, \tag{A1}$$

where only the 2×2 block consisting of the entries with row and column indices k and $k+1$ are non-trivial. A general element $U\in\mathrm{U}(d)$ can then be decomposed into Givens rotations in different ways, we will consider two of these (also discussed in [50]). In the first decomposition one applies alternatingly (d number of times) a series of Givens rotations $G^{(k)}$ with odd and even k indices, and finally a diagonal unitary $T=\mathrm{diag}(e^{i\kappa_1},e^{i\kappa_2},\ldots,e^{i\kappa_d})$, i.e.,

$$U=TB_{d/2}A_{d/2}\ldots B_2A_2B_1A_1\,, \tag{A2}$$

$$A_j=\prod_{\substack{k\in[d-1]\\ k\ \text{odd}}}G^{(k)}(\alpha_{(k,j)},\varphi_{(k,j)})\,,\quad B_j=\prod_{\substack{k\in[d-1]\\ k\ \text{even}}}G^{(k)}(\beta_{(k,j)},\nu_{(k,j)}),\quad j\in[d/2]. \tag{A3}$$

Also in the second decomposition one applies alternatingly a series of Givens rotations $G^{(k)}$ with odd and even k indices, however, this time there is $2d{-}1$ such layers and in the ℓth layer there are only Givens rotations up to index $(d{-}|\ell{-}d|)$, and finally there is again a diagonal unitary $T'=\mathrm{diag}(e^{i\kappa'_1},e^{i\kappa'_2},\ldots,e^{i\kappa'_d})$, i.e.,

$$U=T'A'_dB'_{d-1}\ldots B'_2A'_2B'_1A'_1\,, \tag{A4}$$

$$A'_j=\prod_{\substack{k=1\\ k\ \text{odd}}}^{d-|2j-d|}G^{(k)}(\gamma_{(k,j)},\tau_{(k,j)})\,,\quad B'_j=\prod_{\substack{k\in[d-1]\\ k\ \text{even}}}^{d-|2j-d|}G^{(k)}(\delta_{(k,j)},\sigma_{(k,j)}),\quad j\in[d/2]. \tag{A5}$$

Note that the both decompositions use the same number of elementary Givens rotations.

Now, given an arbitrary passive FLO transformation $V=\Pi_{\mathrm{pas}}(U)$, with $U\in\mathrm{U}(d)$, we can use the fact that Π_{pas} is a representation (and thus a homomorphism) and apply it to the decompositions of Eqs. (A2) and (A4). We obtain

$$V=\Pi_{\mathrm{pas}}(U)=\Pi_{\mathrm{pas}}(T)L_{d/2}K_{d/2}\ldots L_2K_2L_1K_1\,, \tag{A6}$$

$$K_j=\prod_{\substack{k\in[d-1]\\ k\ \text{odd}}}\Pi_{\mathrm{pas}}(G^{(k)}(\alpha_{(k,j)}),\varphi_{(k,j)})\,,\quad L_j=\prod_{\substack{k\in[d-1]\\ k\ \text{even}}}\Pi_{\mathrm{pas}}(G^{(k)}(\beta_{(k,j)},\nu_{(k,j)})),\quad j\in[d/2], \tag{A7}$$

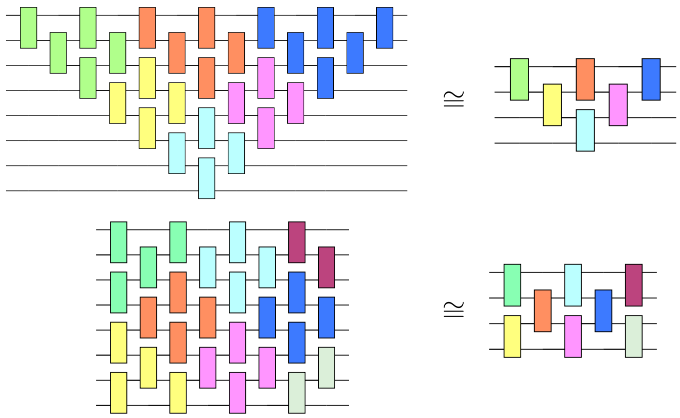

FIG. 7. Decomposition of an arbitrary $V = \Pi_{\mathrm{act}}(O)$ using majorana-line (left) and qubit-line (right) circuit pictures. The represented Givens rotations can be merged (identical colors depicting the merged rotations) giving rise to a layout of Fig. 3, with two-qubit gates of type $D_{\mathrm{act}}(\{\beta_i\})$.

and similarly

$$V = \Pi_{\mathrm{pas}}(U) = \Pi_{\mathrm{pas}}(T')K'_d L'_{d-1} \dots L'_2 K'_2 L'_1 K'_1 \,, \tag{A8}$$

$$K'_j = \prod_{\substack{k=1 \\ k \text{ odd}}}^{d-|2j-d|} \Pi_{\mathrm{pas}}(G^{(k)}(\gamma_{(k,j)}, \tau_{(k,j)}))\,, \quad L'_j = \prod_{\substack{k\in[d-1] \\ k \text{ even}}}^{d-|2j-d|} \Pi_{\mathrm{pas}}(G^{(k)}(\delta_{(k,j)}, \sigma_{(k,j)})), \quad j \in [d/2]. \tag{A9}$$

Using the definition of Π_{pas} and the Jordan-Wigner correspondence between fermions and qubits systems, we have that

$$\Pi_{\mathrm{pas}}(\mathrm{diag}(e^{i\alpha}, e^{i\alpha_2}, \dots, e^{i\alpha_d})) = \mathrm{e}^{i\alpha_1 Z} \otimes \mathrm{e}^{i\alpha_1 Z} \otimes \dots \otimes \mathrm{e}^{i\alpha_d Z}, \tag{A10}$$

$$\Pi_{\mathrm{pas}}(G^{(k)}(\alpha_1, \alpha_2)) = \mathbb{I}^{\otimes k-1} \otimes (\mathrm{e}^{-i\alpha_1 Z/2} \otimes \mathrm{e}^{i\alpha_1 Z/2})\, \mathrm{e}^{i\alpha_2 (X\otimes X + Y\otimes Y)/2} \otimes \mathbb{I}^{\otimes d-k-1} \tag{A11}$$

Thus, Eq. (A16) and Eq. (A18) provides exactly the brickwall and triangle decomposition of Fig. 3.

Let us now turn to the decomposition of an arbitrary active FLO gate $V = \Pi_{\mathrm{act}}(O)$ ($O \in \mathrm{SO}(2d)$). An orthogonal matrix O can be decomposed into a sequence of real Givens rotations $G^{(k)}(\alpha) := G^{(k)}(\alpha, 0) \in SO(2d)$ analogously to the decompositions of a unitary (Eqs. (A2) and (A4)). One can apply alternatingly (d number of times) a series of real Givens rotations $G^{(k)}$ with odd and even k indices, and finally a diagonal orthogonal matrix $S = \mathrm{diag}(s_1, s_2, \dots, s_d)$ (with $s_i \in \{1, -1\}$ and $\prod_{i=1}^{2d} = 1$), i.e.,

$$U = S D_{d/2} C_{d/2} \dots D_2 C_2 D_1 C_1 \,, \tag{A12}$$

$$C_j = \prod_{\substack{k\in[d-1] \\ k \text{ odd}}} G^{(k)}(\alpha_{(k,j)})\,, \quad D_j = \prod_{\substack{k\in[d-1] \\ k \text{ even}}} G^{(k)}(\beta_{(k,j)}), \quad j \in [d/2]. \tag{A13}$$

Alternatively, one can apply alternatingly a series of Givens rotations $G^{(k)}$ with odd and even k indices with $2d{-}1$ layers and in the ℓth layer there are only real Givens rotations up to index $(d{-}|\ell{-}d|)$, and finally there is again a diagonal matrix with signs $S' = \mathrm{diag}(s'_1, s'_2, \dots, s'_d)$, i.e.,

$$U = S' C'_d D'_{d-1} \dots D'_2 C'_2 D'_1 C'_1 \,, \tag{A14}$$

$$C'_j = \prod_{\substack{k=1 \\ k \text{ odd}}}^{d-|2j-d|} G^{(k)}(\gamma_{(k,j)})\,, \quad D'_j = \prod_{\substack{k\in[d-1] \\ k \text{ even}}}^{d-|2j-d|} G^{(k)}(\delta_{(k,j)}), \quad j \in [d/2]. \tag{A15}$$

Given an arbitrary active FLO transformation $V=\Pi_{\rm act}(O)$, with $O\in\mathrm{SO}(2d)$, we can use the fact that $\Pi_{\rm act}$ is a projective representation (and thus a projective homomorphism) and apply it to the decompositions of Eqs. (A12) and (A14), obtaining upto an irrelevant signs $\sigma,\sigma'\in\{1,-1\}$ that

$$V=\Pi_{\rm act}(O)=\sigma\Pi_{\rm act}(S)F_{d/2}E_{d/2}\dots F_2E_2F_1E_1\,, \tag{A16}$$
$$E_j=\prod_{\substack{k\in[d-1]\\ k\ \text{odd}}}\Pi_{\rm act}(G^{(k)}(\alpha_{(k,j)}))\,,\quad F_j=\prod_{\substack{k\in[d-1]\\ k\ \text{even}}}\Pi_{\rm act}(G^{(k)}(\beta_{(k,j)})),\quad j\in[d/2], \tag{A17}$$

and

$$V=\Pi_{\rm act}(O)=\sigma'\Pi_{\rm pas}(S')F'_dE'_{d-1}\dots F'_2E'_2F'_1E'_1\,, \tag{A18}$$
$$E'_j=\prod_{\substack{k=1\\ k\ \text{odd}}}^{d-|2j-d|}\Pi_{\rm act}(G^{(k)}(\gamma_{(k,j)}))\,,\quad L'_j=\prod_{\substack{k\in[d-1]\\ k\ \text{even}}}^{d-|2j-d|}\Pi_{\rm act}(G^{(k)}(\delta_{(k,j)})),\quad j\in[d/2]. \tag{A19}$$

Using the definition of $\Pi_{\rm pas}$ and the Jordan-Wigner correspondence between fermions and qubits systems, we have that

$$\Pi_{\rm act}(S)=\pm X^{s_1}Y^{s_2}\otimes X^{s_3}Y^{s_4}\otimes\ldots\otimes X^{s_{2d-1}}Y^{s_{2d}}, \tag{A20}$$

and

$$\Pi_{\rm pas}(G^{(k)}(\alpha))=\mathrm{e}^{-\alpha\, m_km_{k+1}}=\begin{cases}\mathbb{I}^{\otimes(\ell-1)}\otimes \mathrm{e}^{i\alpha Z_\ell}\otimes\mathbb{I}^{\otimes(d-\ell)} & \text{if } k=2\ell \text{ is even}\\ \mathbb{I}^{\otimes(\ell-1}\otimes \mathrm{e}^{i\alpha X_\ell X_{\ell+1}}\otimes\mathbb{I}^{\otimes(d-\ell-1)} & \text{if } k=2\ell+1 \text{ is odd}\end{cases} \tag{A21}$$

Thus, the circuits would resemble the brickwall and layouts, however with depths $2d$ and $(4d-1)$ on $2d$ majorana lines and not of depth d and $2d-1$ on d qubit lines, see Fig. 7. (In circuits with majorana lines the lines represent individual operators and gates between two majorana lines are unitaries that is composed only of the corresponding two majorana operators [61].) However, we can make some simplifications by merging gates as shown in Fig. 7: in the middle of the circuit we can merge 4 two-qubit gates (corresponding to 4 Givens rotations) of the form $\mathrm{e}^{i\alpha_1X\otimes X}\,(\mathrm{e}^{i\alpha_2Z}\otimes\mathrm{e}^{i\alpha_3Z})\,\mathrm{e}^{i\alpha_4X\otimes X}$ and these are equal to gates of the form $D_{\rm act}(\{\beta_i\})=(\mathrm{e}^{i\beta_5Z/2}\otimes\mathrm{e}^{i\beta_6Z/2})\,\mathrm{e}^{i(\beta_3X\otimes X+\beta_4Y\otimes Y)/2}\,(\mathrm{e}^{i\beta_1Z/2}\otimes\mathrm{e}^{i\beta_2Z/2})$, where the β_i's has to be chosen to satisfy

$$\cos(\alpha_1+\alpha_4)\cos(\alpha_2-\alpha_3)=\cos(\theta_2)\cos(\theta_1+\theta_3),\quad \sin(\alpha_1+\alpha_4)\cos(\alpha_2-\alpha_3)=\sin(\theta_2)\cos(\theta_1-\theta_3), \tag{A22}$$
$$\cos(\alpha_1-\alpha_4)\sin(\alpha_2-\alpha_3)=\cos(\theta_2)\sin(\theta_1+\theta_3),\quad \cos(\alpha_1-\alpha_4)\sin(\alpha_2+\alpha_3)=\cos(\theta_5)\sin(\theta_4+\theta_6), \tag{A23}$$
$$\cos(\alpha_1+\alpha_4)\cos(\alpha_2+\alpha_3)=\cos(\theta_5)\cos(\theta_4+\theta_6),\quad \sin(\alpha_1+\alpha_4)\cos(\alpha_2+\alpha_3)=\sin(\theta_5)\cos(\theta_4-\theta_6), \tag{A24}$$

where we used the notations $\theta_1=\beta_1-\beta_2$, $\theta_2=\beta_3-\beta_4$, $\theta_3=\beta_5-\beta_6$, $\theta_4=\beta_1+\beta_2$, $\theta_5=\beta_3+\beta_4$, $\theta_6=\beta_5+\beta_6$. At the edges of the the circuit we may just either have to join additional local Z-rotations to the merged gates, thus it can be again expressed as $D_{\rm act}(\{\beta_i\})$, or it is already of the form of $D_{\rm act}(\{\beta_i\})$. In this way, we obtain exactly the brickwall and triangle decomposition of Fig. 3 with two-qubit gates of the form of $D_{\rm act}(\{\beta_i\})$.

Appendix B: Details of computations for anticoncentration

1. Passive FLO

In this part we give detailed computations related to establishing upper bound in Eq. (39) for the case of passive FLO:

$$\mathrm{tr}(\mathbb{P}_{\rm pas}\Psi_{\rm in}\otimes\Psi_{\rm in})\leq\frac{C_{\rm pas}}{N}\ ,\ \text{for } C_{\rm pas}=5.7 \tag{B1}$$

The prove of the above inequality is split into three parts. First, in Lemma 12 we give an explicit form of $\mathbb{P}_{\text{pas}}$. Second, in Lemma 13 we find an upper bound on $\text{tr}(\mathbb{P}_{\text{pas}}\Psi_{\text{in}} \otimes \Psi_{\text{in}})$ via combinatorial expression that can be efficiently computed for any fixed value of N. Finally, in Lemma 17 given in Part B 3 of the Appendix we prove an upper bound to the said combinatorial expression which yields Eq. (B1).

Lemma 12 (Projector for passive fermionic linear optics). *Let $\bigwedge^n\left(\mathbb{C}^d\right)$ be a fermionic n-particle representation of $\mathrm{U}(d)$ $(d \geq n)$. Let $\mathbb{P}_{\text{pas}}$ be the projector onto a unique irreducible representation $\tilde{\mathcal{H}}_f \subset \bigwedge^n\left(\mathbb{C}^d\right) \otimes \bigwedge^n\left(\mathbb{C}^d\right)$ of $\mathrm{U}(d)$ such that $|\mathbf{n}\rangle \otimes |\mathbf{n}\rangle \in \tilde{\mathcal{H}}_f$, where $|\mathbf{n}\rangle$ is a n-particle Fock state. Then, for any $\rho \in \mathcal{D}\left(\bigwedge^n(\mathbb{C}^d)\right)$ we have*

$$\text{tr}(\mathbb{P}_{\text{pas}}\rho \otimes \rho) = \frac{1}{n+1}\sum_{k=0}^{n}\binom{n}{k}\text{tr}(\rho_k^2) \ , \tag{B2}$$

where $\rho_k = \text{tr}_{n-k}(\rho)$ is a k-particle reduction of ρ. Moreover, the dimension of $\tilde{\mathcal{H}}_f$ equals

$$|\tilde{\mathcal{H}}_f| = \binom{d}{n}^2 \frac{d+1}{(d-n+1)(n+1)} \ . \tag{B3}$$

Proof. We consider $\bigwedge^n(\mathbb{C}^d)$ as anti-symmetric subspace of the Hilbert space of n distinguishable partices: $\bigwedge^n(\mathbb{C}^d) \subset (\mathbb{C}^d)^{\otimes n}$ with d dimensional single particle Hilbert spaces. Therefore also $\bigwedge^n(\mathbb{C}^d) \otimes \bigwedge^n(\mathbb{C}^d)$ can be considered as a subspace of $2n$ distinguishable particles:

$$\bigwedge^n(\mathbb{C}^d) \otimes \bigwedge^n(\mathbb{C}^d) \subset (\mathbb{C}^d)^{\otimes n} \otimes (\mathbb{C}^d)^{\otimes n} \ . \tag{B4}$$

Let us now label particles entering the first factor of the latter tensor product by $1,\ldots,n$ and by $1',\ldots,n'$ particles entering the second factor. In [101] it was proven that

$$\mathbb{P}_{\text{pas}} = \frac{2^n}{n+1}\mathbb{P}_{\text{asym}}^{\{1,\ldots,n\}}\mathbb{P}_{\text{asym}}^{\{1',\ldots,n'\}}\left(\prod_{k=1}^{n}\mathbb{P}_{\text{sym}}^{k,k'}\right)\mathbb{P}_{\text{asym}}^{\{1,\ldots,n\}}\mathbb{P}_{\text{asym}}^{\{1',\ldots,n'\}} \ . \tag{B5}$$

In the above $\mathbb{P}_{\text{sym}}^{k,k'} = \frac{1}{2}(\mathbb{I}\otimes\mathbb{I} + \mathbb{S}^{k,k'})$ is the projector onto a subspace of $(\mathbb{C}^d)^{\otimes n} \otimes (\mathbb{C}^d)^{\otimes n}$ which is symmetric upon interchange of particles k and k' (by $\mathbb{S}^{k,k'}$ we denote the unitary operator that swaps particles k and k'). Moreover, $\mathbb{P}_{\text{asym}}^{\mathcal{A}}$ denotes the projector onto a subspace which is anti-symmetric under exchange of particles in a subset $\mathcal{A}$. Now for $\rho \in \mathcal{D}\left(\bigwedge^n(\mathbb{C}^d)\right)$ we have

$$\mathbb{P}_{\text{asym}}^{\{1,\ldots,n\}}\mathbb{P}_{\text{asym}}^{\{1',\ldots,n'\}}\rho\otimes\rho = \rho\otimes\rho \tag{B6}$$

and therefore

$$\text{tr}(\mathbb{P}_{\text{pas}}\rho\otimes\rho) = \frac{2^n}{n+1}\,\text{tr}\left[\left(\prod_{k=1}^{n}\mathbb{P}_{sym}^{k,k'}\right)\rho\otimes\rho\right] \ . \tag{B7}$$

Using the definition of $\mathbb{P}_{sym}^{k,k'}$ we get the expansion

$$\prod_{k=1}^{n}\mathbb{P}_{sym}^{k,k'} = \frac{1}{2^n}\sum_{\mathcal{X}\subset[d]}\prod_{i\in\mathcal{X}}\mathbb{S}^{i,i'} \ , \tag{B8}$$

where the summation is over subsets X of $[d] = \{1,\ldots,d\}$. Using a well-known connection between partial swaps and purites of reduced density matrices (see for example [116]):

$$\text{tr}\left(\prod_{i\in\mathcal{X}}\mathbb{S}^{i,i'}\rho\otimes\rho\right) = \text{tr}(\rho_X^2) \ , \tag{B9}$$

where $\rho_X = \mathrm{tr}_{[d]\setminus\mathcal{X}}(\rho)$ is the reduction of ρ to particles in X. From the symmetry of ρ we have $\mathrm{tr}(\rho_X^2) = \mathrm{tr}(\rho_k^2)$, where $k = |X|$ (size of the set X). Inserting this into (B8) and (B7) we finally obtain

$$\mathrm{tr}(\mathbb{P}_{\mathrm{pas}}\rho\otimes\rho) = \frac{1}{n+1}\sum_{k=0}^{n}\binom{n}{k}\mathrm{tr}(\rho_k^2)\ . \tag{B10}$$

The formula for the dimension (B3) follows from the fact that the Hilbert space $\tilde{\mathcal{H}}_f$ is a carrier space of an irreducible representation of $\mathrm{U}(d)$ labelled by a Young diagram having two columns each of which has n rows. Formulas for dimensions of such irreducible representations are known (see for example [117]) and were used previously in the context of detection of mixed states that cannot be decomposed as a convex combination of Slater determinants [102]. □

Note that for all n-particle pure states we have $\mathrm{tr}(\rho_k^2) = \mathrm{tr}(\rho_{n-k}^2)$. This observation gives us the following

Corollary 2. *Let $\Psi \in \mathcal{D}\left(\bigwedge^{2m}(\mathbb{C}^d)\right)$ be a pure state. Let $\mathbb{P}_{\mathrm{pas}}$ be defined as in Lemma 12. We then have*

$$\mathrm{tr}(\mathbb{P}_{\mathrm{pas}}\Psi\otimes\Psi) = \frac{1}{2m+1}\left[2\sum_{k=0}^{m-1}\binom{2m}{k}\mathrm{tr}(\rho_k^2) + \binom{2m}{m}\mathrm{tr}(\rho_m^2)\right]\ . \tag{B11}$$

We now proceed with some further technical results which will allow us to compute $\mathrm{tr}(\mathbb{P}_{\mathrm{pas}}\rho_{\mathrm{in}}\otimes\rho_{\mathrm{in}})$.
For a set of indices $\mathcal{X} = \{x_1, x_2, \ldots, x_n\} \subset [d]$ where $x_i < x_j$ if $i < j$, and a subset of it $\mathcal{S} = \{x_{\ell_1}, x_{\ell_2}, \ldots, x_{\ell_k}\} \subset \mathcal{X}$ it will be useful to introduce the following sign

$$(-1)^{J(\mathcal{X},\mathcal{S})}\ ,\ \text{where}\ \ J(\mathcal{X},\mathcal{S}) = \ell_1 + \ell_2 + \ldots + \ell_k + \frac{k(k-1)}{2}\,. \tag{B12}$$

This notation allows us to express in a compact way the following matrix element: for any two Fock basis states $|\mathcal{X}\rangle, |\mathcal{Y}\rangle \in \bigwedge^n \mathbb{C}^d$ belonging to the index sets $\mathcal{X}, \mathcal{Y} \subset [d]$, we have that

$$\langle\mathcal{X}|f_{s_1}^\dagger f_{s_2}^\dagger \cdots f_{s_k}^\dagger f_{q_k}\cdots f_{q_2}f_{q_1}|\mathcal{Y}\rangle = \begin{cases}\delta_{\mathcal{X}\setminus\mathcal{S},\mathcal{Y}\setminus\mathcal{Q}}\,\epsilon_{s_1,\ldots,s_k}\epsilon_{q_1,\ldots,q_k}(-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{Q})} & \text{if } \mathcal{S}\subset\mathcal{X} \text{ and } \mathcal{Q}\subset\mathcal{Y},\\ 0 \ \text{ else,}\end{cases} \tag{B13}$$

where $\mathcal{S} = \{s_1, s_2 \ldots s_k\}$ and $\mathcal{Q} = \{q_1, q_2, \ldots q_k\}$.

Proposition 3. *Let $|\mathcal{X}\rangle, |\mathcal{Y}\rangle \in \bigwedge^n(\mathbb{C}^d)$ be a fermionic n-particle Fock states corresponding to n-element subsets $\mathcal{X}, \mathcal{Y} \subset [d]$ (cf. notation introduced in Section II), then for any $k = 0, \ldots, n$ we have*

$$\mathrm{tr}_k(|\mathcal{X}\rangle\langle Y|) = \frac{1}{\binom{n}{k}}\sum_{\mathcal{S}\in\binom{\mathcal{X}\cap\mathcal{Y}}{k}}(-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{S})}\,|\mathcal{X}\setminus\mathcal{S}\rangle\langle\mathcal{Y}\setminus\mathcal{S}|\ . \tag{B14}$$

Note that the notation used in the above expression implies $\mathrm{tr}_k(|\mathcal{X}\rangle\langle\mathcal{Y}|) = 0$ if $|\mathcal{X}\cap\mathcal{Y}| < k$.

Proof. For any two states $|\Psi\rangle, |\Phi\rangle \in \bigwedge^n \mathbb{C}^d \subset (\mathbb{C}^d)^{\otimes n}$, the k-fold partial trace (wrt the tensor product structure) results in an operator $O = \mathrm{tr}_k(|\Psi\rangle\langle\Phi|) \in \mathcal{B}(\bigwedge^\ell \mathbb{C}^d) \subset \mathcal{B}((\mathbb{C}^d)^{\otimes\ell})$ (with $\ell = n-k$) that has the following matrix elements [118]:

$$\langle v_1|\otimes\langle v_2|\otimes\cdots\langle v_\ell|\,O\,|w_1\rangle\otimes|w_2\rangle\otimes\cdots\otimes|w_\ell\rangle = \frac{1}{\binom{n}{k}}\langle\Phi|(f_1^\dagger)^{v_1}(f_2^\dagger)^{v_2}\cdots(f_\ell^\dagger)^{v_\ell}(f_\ell)^{w_\ell}\cdots(f_2)^{w_2}(f_1)^{w_1}|\Psi\rangle\,. \tag{B15}$$

Inserting in this equation the $|\Psi\rangle = |\mathcal{X}\rangle$ and $|\Phi\rangle = |\mathcal{Y}\rangle$ and using Eq. (B13), we get that

$$\langle v_1| \otimes \langle v_2| \otimes \cdots \langle v_\ell| \, O \, |w_1\rangle \otimes |w_2\rangle \otimes \cdots \otimes |w_\ell\rangle = \begin{cases} \binom{n}{k}^{-1} \delta_{\mathcal{Y}\setminus\mathcal{A},\mathcal{X}\setminus\mathcal{B}} \, \epsilon_{v_1,\ldots,v_k} \epsilon_{w_1,\ldots,w_k} (-1)^{J(\mathcal{Y},\mathcal{A})+J(\mathcal{X},\mathcal{B})} & \text{if } \mathcal{A} \subset \mathcal{Y} \text{ and } \mathcal{B} \subset \mathcal{X}, \\ 0 & \text{else}, \end{cases} \tag{B16}$$

where $\mathbf{v} = (v_1, \ldots, v_\ell)$ and $\mathbf{w} = (w_1, \ldots, w_\ell)$ are the indicator bit strings of the sets $\mathcal{A}$ and $\mathcal{B}$, respectively. Now considering also the following matrix entries

$$\begin{aligned}
&\langle v_1| \otimes \langle v_2| \otimes \cdots \langle v_\ell| \Big(\frac{1}{\binom{n}{k}} \sum_{\mathcal{S} \in \binom{\mathcal{X}\cap\mathcal{Y}}{k}} (-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{S})} \, |\mathcal{X} \setminus \mathcal{S}\rangle\langle \mathcal{Y} \setminus \mathcal{S}| \Big) |w_1\rangle \otimes |w_2\rangle \otimes \cdots \otimes |w_\ell\rangle = \\
&\mathrm{tr} \Big(\frac{1}{\binom{n}{k}} \sum_{\mathcal{S} \in \binom{\mathcal{X}\cap\mathcal{Y}}{k}} (-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{S})} \, |\mathcal{X} \setminus \mathcal{S}\rangle\langle \mathcal{Y} \setminus \mathcal{S}| \, (f_1^\dagger)^{v_1} \cdots (f_\ell^\dagger)^{v_\ell} (f_\ell)^{w_\ell} \cdots (f_1)^{w_1} \Big) = \\
&\frac{1}{\binom{n}{k}} \sum_{\mathcal{S} \in \binom{\mathcal{X}\cap\mathcal{Y}}{k}} (-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{S})} \langle \mathcal{Y} \setminus \mathcal{S}| (f_1^\dagger)^{v_1} \cdots (f_\ell^\dagger)^{v_\ell} (f_\ell)^{w_\ell} \cdots (f_1)^{w_1} |\mathcal{X} \setminus \mathcal{S}\rangle = \\
&\frac{1}{\binom{n}{k}} \sum_{\mathcal{S} \in \binom{\mathcal{X}\cap\mathcal{Y}}{k}} (-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{S})} \, \delta_{\mathcal{Y}\setminus\mathcal{S},\mathcal{A}} \delta_{\mathcal{X}\setminus\mathcal{S},\mathcal{B}} \, \epsilon_{v_1,\ldots,v_k} \epsilon_{w_1,\ldots,w_k} = \\
&\frac{1}{\binom{n}{k}} \sum_{\mathcal{S} \in \binom{\mathcal{X}\cap\mathcal{Y}}{k}} (-1)^{J(\mathcal{X},\mathcal{S})+J(\mathcal{Y},\mathcal{S})} \, \delta_{\mathcal{Y}\setminus\mathcal{A},\mathcal{S}} \delta_{\mathcal{Y}\setminus\mathcal{B},\mathcal{S}} \, \epsilon_{v_1,\ldots,v_k} \epsilon_{w_1,\ldots,w_k} = \\
&\qquad \begin{cases} \binom{n}{k}^{-1} \delta_{\mathcal{Y}\setminus\mathcal{A},\mathcal{X}\setminus\mathcal{B}} \, \epsilon_{v_1,\ldots,v_k} \epsilon_{w_1,\ldots,w_k} (-1)^{J(\mathcal{Y},\mathcal{A})+J(\mathcal{X},\mathcal{B})} & \text{if } \mathcal{A} \subset \mathcal{Y} \text{ and } \mathcal{B} \subset \mathcal{X}, \\ 0, & \text{else}, \end{cases}
\end{aligned} \tag{B17}$$

where we have used that $(-1)^{J(\mathcal{Y},\mathcal{A})+J(\mathcal{X},\mathcal{B})} = (-1)^{J(\mathcal{Y},\mathcal{S})+J(\mathcal{X},\mathcal{S})}$, which follows from the fact that $(-1)^{J(\mathcal{X},\mathcal{S})} = (-1)^{J(\mathcal{X},\mathcal{X}\setminus\mathcal{S})+|\mathcal{X}|\cdot|\mathcal{S}|}$. Thus, the matrix elements of Eq. (B16) and Eq. (B17) coincide, which proves the propositions. □

We introduce the convenient notation for $|\Psi_{\mathrm{in}}\rangle$:

$$|\Psi_{\mathrm{in}}\rangle = \frac{1}{\sqrt{2^N}} \sum_{\mathcal{X} \in \mathcal{C}_{\mathrm{in}}} |\mathcal{X}\rangle \ , \tag{B18}$$

where $\mathcal{C}_{\mathrm{in}}$ is a collection of subsets of $[4N]$ that appear in the decomposition of $|\Psi_{\mathrm{in}}\rangle$. Note that from the definition of $|\Psi_{\mathrm{in}}\rangle$ it follows that subsets are labelled by bitstrings $\mathbf{x} = (x_1, \ldots, x_N)$, where $x_i \in \{0, 1\}$ labels which pair of the neighbouring physical modes are occupied in a given quadropule of modes. For $N = 2$ we have four possible subsets belonging to $\mathcal{C}_{\mathrm{in}}$

$$\mathcal{X}_{00} = \{1, 2, 5, 6\} \ , \ \mathcal{X}_{01} = \{1, 2, 7, 8\} \ , \ \mathcal{X}_{10} = \{3, 4, 5, 6\}, \ \mathcal{X}_{11} = \{3, 4, 7, 8\} \ . \tag{B19}$$

For general N the collection $\mathcal{C}_{\mathrm{in}}$ consists of the following subsets labelled by bitstrings $\mathbf{x}$

$$\mathcal{X}_{\mathbf{x}} = \{1+2x_1, 2+2x_1, 5+2x_2, 6+2x_2, \ldots, 4i-3+2x_i, 4i-2+2x_i, \ldots, 4N-3+2x_N, 4N-2+2x_N\} \ . \tag{B20}$$

The formula from Lemma 3 allows us to obtain bounds for the purities of reduced density matrices of Ψ_{in}.

Proposition 4 (Bounds on purites of reduced density matrices of ρ_{in})**.** *Consider the setting of this paper, i.e., $d = 4N$ and $n = 2N$, where N is the number of quadruples used in our quantum advantage proposal.*

Let $\Psi_{\text{in}} \in \mathcal{D}(\mathcal{H}_f)$ be the input state. Then, for $k = 0, \ldots, N$ we have

$$\operatorname{tr}\left[\operatorname{tr}_k(\Psi_{\text{in}})^2\right] \leq \frac{1}{\binom{2N}{k}^2} \sum_{l=0}^{\lfloor k/2 \rfloor} \frac{N!}{l!(k-2l)!(N-k+l)!} \tag{B21}$$

Proof. We use the decomposition of the state vector $|\Psi_{\text{in}}\rangle$ given in Eq. (B18) and obtain

$$\Psi_{\text{in}} = \frac{1}{2^N} \sum_{\mathcal{X},\mathcal{Y} \in \mathcal{C}_{\text{in}}} |\mathcal{X}\rangle\langle\mathcal{Y}| \ . \tag{B22}$$

Employing (B14) and denoting $J(\mathcal{X},\mathcal{S}) + J(\mathcal{Y},\mathcal{S}) = K(\mathcal{X},\mathcal{Y},\mathcal{S})$ we obtain (remember that $n = 2N$)

$$\operatorname{tr}_k(\Psi_{\text{in}}) = \frac{1}{2^N \binom{2N}{k}} \sum_{\mathcal{X},\mathcal{Y} \in \mathcal{C}_{\text{in}}} \sum_{\mathcal{S} \in \binom{\mathcal{X} \cap \mathcal{Y}}{k}} (-1)^{K(\mathcal{X},\mathcal{Y},\mathcal{S})} |\mathcal{X} \setminus \mathcal{S}\rangle\langle\mathcal{Y} \setminus \mathcal{S}| \ . \tag{B23}$$

By reordering the sum we obtain

$$\operatorname{tr}_k(\Psi_{\text{in}}) = \frac{1}{2^N \binom{2N}{k}} \sum_{\mathcal{X}',\mathcal{Y}' \in \binom{[4N]}{2N-k}} |\mathcal{X}'\rangle\langle\mathcal{Y}'| \sum_{\substack{\mathcal{S} \in \binom{[4N]}{k} \ , \ \mathcal{X},\mathcal{Y} \in \mathcal{C}_{\text{in}} \\ \text{s.t. } \mathcal{X} \setminus \mathcal{S} = \mathcal{X}', \mathcal{Y} \setminus \mathcal{S} = \mathcal{X}'}} (-1)^{K(\mathcal{X},\mathcal{Y},\mathcal{S})} \ , \tag{B24}$$

where the second sum is a combinatorial term that gives a coefficient which which particular operator $|\mathcal{X}'\rangle\langle\mathcal{Y}'|$ appears. Crucially, operators $|\mathcal{X}'\rangle\langle\mathcal{Y}'|$, $|\mathcal{X}'| = |\mathcal{Y}'| = 2N - k$ are orthonormal with respect to the Hilbert-Schmidt inner product in $\mathcal{B}(\bigwedge^{2N-k}(\mathbb{C}^{4N}))$. Therefore in order to bound purity of $\operatorname{tr}_k(\rho_{\text{in}})$ it suffices to count the number of terms in the second sum in (B24):

$$\operatorname{tr}\left[\operatorname{tr}_k(\Psi_{\text{in}})^2\right] \leq \frac{1}{2^{2N} \binom{2N}{k}^2} \sum_{\mathcal{X}',\mathcal{Y}' \in \binom{[4N]}{2N-k}} \mathcal{N}(\mathcal{X}',\mathcal{Y}')^2 \ , \tag{B25}$$

where

$$\mathcal{N}(\mathcal{X}',\mathcal{Y}') = \left| \left\{ (\mathcal{S},\mathcal{X},\mathcal{Y}) \mid \mathcal{S} \in \binom{[4N]}{k} \ , \ \mathcal{X},\mathcal{Y} \in \mathcal{C}_{\text{in}}, \ \mathcal{X} \setminus \mathcal{S} = \mathcal{X}', \ \mathcal{Y} \setminus \mathcal{S} = \mathcal{X}' \right\} \right| \ . \tag{B26}$$

In what follows, in order to make our considerations less abstract, we shall refer to lements of subsets involved as "particles". To compute $N(\mathcal{X}',\mathcal{Y}')$ we note that $\mathcal{X}',\mathcal{Y}'$ for which $\mathcal{N}(\mathcal{X}',\mathcal{Y}') \neq 0$ must arise from substracting from $\mathcal{X} \in \mathcal{C}_{\text{in}}$ particles occupying subset $\mathcal{S}$. Since particles corresponding to $\mathcal{X} \in \mathcal{C}_{\text{in}}$ occupy only two out of four possible modes in every quadropule of modes in a "binary fashion" (See Eq. (B19)), This imposes constraints on the possible configurations of particles from $\mathcal{X}'$ in every quadropole. Specifically, consider the quadropule of physical modes $\mathcal{A} = \{1,2,3,4\}$. Let $\mathcal{X}'_{\mathcal{A}} = \mathcal{X}' \cap \mathcal{A}$. We have seven possibilities for the set $\mathcal{X}'_{\mathcal{A}}$:

$$\mathcal{X}'^{\text{N1}}_{\mathcal{A}} = \{1,2\} \ , \ \mathcal{X}'^{\text{N2}}_{\mathcal{A}} = \{3,4\} \ , \ \mathcal{X}'^{\text{B}}_{\mathcal{A}} = \emptyset \ , \tag{B27}$$

$$\mathcal{X}'^{\text{F1}}_{\mathcal{A}} = \{1\} \ , \ \mathcal{X}'^{\text{F2}}_{\mathcal{A}} = \{2\} \ , \ \mathcal{X}'^{\text{F3}}_{\mathcal{A}} = \{3\} \ , \ \mathcal{X}'^{\text{F4}}_{\mathcal{A}} = \{4\} \ . \tag{B28}$$

All other forms of $\mathcal{X} \cap \mathcal{A}$ yield $\mathcal{N}(\mathcal{X}',\mathcal{Y}') = 0$. Under the condition that $\mathcal{X}'$ originates from $\mathcal{X} \in \mathcal{C}_{\text{in}}$ these configurations impose conditions on possible arrangement of lost particles in quadruple $\mathcal{A}$, denoted by $\mathcal{S}_{\mathcal{A}} = \mathcal{S} \cap \mathcal{A}$:

$$\mathcal{S}_{\mathcal{A}}(N1) = \mathcal{S}_{\mathcal{A}}(N2) = \emptyset \ , \ \mathcal{S}_{\mathcal{A}}(B) = \{1,2\} \text{ or } \mathcal{S}_{\mathcal{A}}(B) = \{3,4\} \ , \tag{B29}$$

$$\mathcal{S}_{\mathcal{A}}(F1) = \{2\} \ , \ \mathcal{S}_{\mathcal{A}}(F2) = \{1\} \ , \ \mathcal{S}_{\mathcal{A}}(F3) = \{4\} \ , \ \mathcal{S}_{\mathcal{A}}(F4) = \{3\} \ . \tag{B30}$$

This motivates us to introduce *type* of quadruples of $\mathcal{X}'$ whose names are motivated by types of constraints the impose on $\mathcal{S}\cap\mathcal{A}$:

$$T_{\mathcal{A}}(\mathcal{X}') = \begin{cases} \text{NULL} & \text{iff } \mathcal{X}'_{\mathcal{A}} = \{1,2\} \text{ or } \mathcal{X}'_{\mathcal{A}} = \{3,4\} \\ \text{BINARY} & \text{iff } \mathcal{X}'_{\mathcal{A}} = \emptyset \\ \text{FIXED} & \text{iff } \mathcal{X}'_{\mathcal{A}} \in \{\{1\},\{2\},\{3\},\{4\}\} \end{cases} . \tag{B31}$$

We repeat the same procedure for other quadruples $\{5,6,7,8\}$, $\{9,10,11,12\}$, etc. To a given $\mathcal{X}'$ we then associate "pattern of types":

$$\mathcal{X}' \longmapsto \mathcal{L}(\mathcal{X}') = (l_{\mathrm{N}}[\mathcal{X}']\ ,\ l_{\mathrm{B}}[\mathcal{X}']\ ,\ l_{\mathrm{F}}[\mathcal{X}'])\ , \tag{B32}$$

that lists the number of quadruples of different types in $\mathcal{X}'$. This pattern gives us the number of k-element subsets $\mathcal{S}\in\binom{[4N]}{k}$ contributing to $\mathcal{N}(\mathcal{X}',\mathcal{Y}')$ (cf. (B26)). From the considerations given previously $\mathcal{N}_{\mathcal{S}}(\mathcal{X}') = 2^{l_{\mathrm{B}}[\mathcal{X}']}$ different $\mathcal{S}$ that contribute. Let us chose $\mathcal{Y}'$ that is compatible with the pattern of lost particles in $\mathcal{X}'$ is the sense that $\mathcal{X}'\cap\mathcal{Y}'=\emptyset$ and $\mathcal{Y}'$ follows the general constrains of occupations in each quadruples described previously (like the ones stated in Eq.(B27) and Eq.(B28)). Since for fixed $\mathcal{X}',\mathcal{Y}'$ subset $\mathcal{S}$ uniquely specifies $\mathcal{X},\mathcal{Y}\in\mathcal{C}_{\mathrm{in}}$, we finally get

$$\mathcal{N}(\mathcal{X}',\mathcal{Y}') = 2^{l_{\mathrm{B}}[\mathcal{X}']}\ . \tag{B33}$$

It is now easy to see that, for $\mathcal{X}'$ characterized by particular $\mathcal{L}(\mathcal{X}')$, there are exactly

$$\mathcal{N}_{\mathrm{comp}}(\mathcal{X}') = 2^{l_{\mathrm{N}}[\mathcal{X}']} \tag{B34}$$

different compatible sets $\mathcal{Y}'$. In fact, compatible $\mathcal{Y}'$ necessarily satisfy $\mathcal{L}(\mathcal{Y}')=\mathcal{L}(\mathcal{X}')$. Finally, simple counting argument shows that there are

$$\mathcal{N}(\mathcal{L}) = 2^{2l_{\mathrm{F}}+l_{\mathrm{N}}}\frac{N!}{l_{\mathrm{N}}!l_{\mathrm{B}}!l_{\mathrm{F}}!} \tag{B35}$$

different subsets $\mathcal{X}'$ that have the "pattern type" $\mathcal{L}=(l_{\mathrm{N}},l_{\mathrm{B}},l_{\mathrm{F}})$. Hence the contribution in from subsets $\mathcal{X}',\mathcal{Y}'$ of "pattern type" $\mathcal{L}=(l_{\mathrm{N}},l_{\mathrm{B}},l_{\mathrm{F}})$ to the sum in Eq.(B25) is equals

$$\mathcal{N}(\mathcal{X}',\mathcal{Y}')^2\mathcal{N}_{\mathrm{comp}}(\mathcal{X}')\mathcal{N}(\mathcal{L}) = 4^{l_{\mathrm{N}}+l_{\mathrm{B}}+l_{\mathrm{F}}}\frac{N!}{l_{\mathrm{N}}!l_{\mathrm{B}}!l_{\mathrm{F}}!} = 2^{2N}\frac{N!}{l_{\mathrm{N}}!l_{\mathrm{B}}!l_{\mathrm{F}}!}\ . \tag{B36}$$

Parameters $l_{\mathrm{N}},l_{\mathrm{B}},l_{\mathrm{F}}$ are not independent because of identities: $N=l_{\mathrm{N}}+l_{\mathrm{B}}+l_{\mathrm{F}}$ (this one we already used implicitly) and $2l_{\mathrm{B}}+l_{\mathrm{F}}=2N-k$. Choosing l_{B} as an independent parameter applying the above considerations to (B25) we finally obtain

$$\mathrm{tr}\left[\mathrm{tr}_k(\Psi_{\mathrm{in}})^2\right] \leq \frac{1}{\binom{2N}{k}^2}\sum_{l_{\mathrm{B}}=0}^{\lfloor\frac{k}{2}\rfloor}\frac{N!}{(N-k+l_{\mathrm{B}})!(k-2l_{\mathrm{B}})!l_{\mathrm{B}}!}\ , \tag{B37}$$

where summation range for l_{B} comes from its definition as the number of quadropules in $\mathcal{X}'$ that are are left without particles. □

Combining Corollary 2 and Proposition 4 we obtain explicit upper bound for the expectation value of the projector $\mathbb{P}_{\mathrm{pas}}$

Lemma 13. *Consider the setting of our quantum advantage proposal, i.e.,* $d=4N$ *and* $n=2N$*. Let* $\Psi_{\mathrm{in}}\in\mathcal{D}\left(\bigwedge^{2N}(\mathbb{C}^{4N})\right)$*. Let* $\mathbb{P}_{\mathrm{pas}}$ *be defined as in Lemma 12. We then have*

$$\mathrm{tr}\left(\mathbb{P}_{\mathrm{pas}}\Psi_{\mathrm{in}}\otimes\Psi_{\mathrm{in}}\right) \leq \frac{1}{2N+1}\left[2\sum_{k=0}^{N-1}\binom{2N}{k}\mathrm{tr}(\rho_k^2)+\binom{2N}{N}\mathrm{tr}(\rho_N^2)\right]\ , \tag{B38}$$

where

$$\mathrm{tr}(\rho_k^2) = \frac{1}{\binom{2N}{k}^2} \sum_{l=0}^{\lfloor k/2 \rfloor} \frac{N!}{l!(k-2l)!(N-k+l)!} \ . \tag{B39}$$

2. Active FLO

We give hire computations related to establishing upper bound in Eq. (39) for the case of active FLO:

$$\mathrm{tr}(\mathbb{P}_{\mathrm{act}} \Psi_{\mathrm{in}} \otimes \Psi_{\mathrm{in}}) \leq \frac{C_{\mathrm{act}}}{\sqrt{N}} \ , \text{ for } C_{\mathrm{act}} = 9 \tag{B40}$$

Similarly to the case of passive FLO the proof divided into three parts. First, in Lemma 14 we give an explicit form of $\mathbb{P}_{\mathrm{act}}$. Second, in Lemma 15 we find an upper bound on $\mathrm{tr}(\mathbb{P}_{\mathrm{act}} \Psi_{\mathrm{in}} \otimes \Psi_{\mathrm{in}})$ via combinatorial expression that can be efficiently computed for any fixed value of N. Finally, in Lemma 18 given in Part B 3 of the Appendix we prove an upper bound to the said expression which yields Eq. (B40).

Recall that by m_i, $i = 1, \ldots, 2d$ we denoted the standard majorana operators in the d mode Fermionic Fock space $\mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)$ (cf. Section II). The fermionic parity operator is given by $Q = i^d \prod_{i=1}^{2d} m_i$.

Lemma 14 (Projector for active fermionic linear optics)**.** *Let $\mathcal{H}_{\mathrm{act}} = \mathcal{H}^+_{\mathrm{Fock}}\left(\mathbb{C}^d\right)$ be the positive parity subspace of Fock space corresponding to d fermionic modes. Let $\mathbb{P}_{\mathrm{act}}$ be the projector onto a unique irreducible representation $\tilde{\mathcal{H}}_{\mathrm{act}} \subset \mathcal{H}_{\mathrm{act}} \otimes \mathcal{H}_{\mathrm{act}}$ of $\mathrm{SO}(2d)$ such that $|\Phi\rangle \otimes |\Phi\rangle \in \tilde{\mathcal{H}}_{\mathrm{act}}$, where Φ are arbitrary pure positive parity Gaussian states. We then have*

$$\mathbb{P}_{\mathrm{act}} = \mathbb{P}_+ \otimes \mathbb{P}_+ \mathbb{P}_0 \mathbb{P}_+ \otimes \mathbb{P}_+ \ , \tag{B41}$$

where $\mathbb{P}_+ = \frac{1}{2}(\mathbb{I} + Q)$ is the orthogonal projector onto $\mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d) \subset \mathcal{H}_{\mathrm{Fock}}(\mathbb{C}^d)$ and

$$\mathbb{P}_0 = \frac{1}{2^{2d}} \sum_{p=0}^{d} C_p \sum_{\mathcal{X} \in \binom{[2d]}{2p}} \prod_{i \in \mathcal{X}} m_i \otimes m_i \ . \tag{B42}$$

The numbers C_p satisfy $C_p = (-1)^d C_{d-p}$ and for $p \leq \lfloor d/2 \rfloor$ we have

$$C_p = (-1)^p \frac{(2p)!(2d-2p)!}{(d!)^2} \binom{d}{p} \tag{B43}$$

Moreover, the dimension $\tilde{\mathcal{H}}_{\mathrm{act}}$ equals

$$|\tilde{\mathcal{H}}_{\mathrm{act}}| = \frac{1}{2} \binom{2d}{d} \ . \tag{B44}$$

Proof. The result follows from the characterization of pure fermionic Gaussian states given in Corollary 1 in: [76] which states that a pure state Ψ is a pure Fermionic Gaussian state if and only if $\Lambda |\Psi\rangle \otimes |\Psi\rangle = 0$, where Λ is the operator acting on $\mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d) \otimes \mathcal{H}^+_{\mathrm{Fock}}(\mathbb{C}^d)$ introduced previously by Bravyi in [69]

$$\Lambda = \sum_{i=1}^{2d} m_i \otimes m_i \ . \tag{B45}$$

Equivalently, Ψ is pure Fermionic Gaussian state iff $\mathbb{P}_0^\Lambda |\Psi\rangle \otimes |\Psi\rangle = 0$, where $\mathbb{P}_0^\Lambda$ is the projector onto zero eigenspace of Λ. Since we are interested in Gaussian states having positive parity ($Q|\Psi\rangle = |\Psi\rangle$), and operators $Q \otimes \mathbb{I}$, $\mathbb{I} \otimes Q$ commute with Λ, we get the following equivalence

$$\Psi \text{ is pure positive parity fermionic Gaussian state} \Longleftrightarrow \mathbb{P}_+ \otimes \mathbb{P}_+ \mathbb{P}_0^\Lambda \mathbb{P}_+ \otimes \mathbb{P}_+ |\Psi\rangle \otimes |\Psi\rangle = 0 \ . \tag{B46}$$

We now show that $\mathbb{P}_0^\Lambda = \mathbb{P}_0$. The operator Λ from (B45) is a sum of $2d$ commuting hermitian operators $m_i \otimes m_i$ which satisfy $(m_i \otimes m_i)^2 = \mathbb{I} \otimes \mathbb{I}$. A one dimensional projector onto a joint eigenspace of M_i corresponding to eigenvalues μ_i, $i \in [2d]$ reads is given by

$$\mathbb{P}_{\boldsymbol{\mu}} = \frac{1}{2^{2d}} \prod_{i=1}^{2d} \left(\mathbb{I} \otimes \mathbb{I} + \mu_i m_i \otimes m_i \right) \ , \tag{B47}$$

where $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_{2d}) \in \{-1,1\}^{2d}$. Any arrangement of eigenvalues $\boldsymbol{\mu}$ corresponds to eigenvalue $\lambda = \sum_{i=1}^{2d} \mu_i$. Consequent, projector onto eigenspace zero of Λ reads

$$\mathbb{P}_0^\Lambda = \sum_{\substack{\boldsymbol{\mu} \in \{-1,1\}^{2d} \\ \sum_{i=1}^{2d} \mu_i = 0}} \mathbb{P}_{\boldsymbol{\mu}} \ . \tag{B48}$$

Expanding each of the projectors $\mathbb{P}_{\boldsymbol{\mu}}$ into sum of products of Majorana monomials gives

$$\mathbb{P}_{\boldsymbol{\mu}} = \frac{1}{2^{2d}} \sum_{k=0}^{2d} \sum_{\mathcal{X} \in \binom{[2d]}{k}} \boldsymbol{\mu}^{\mathcal{X}} \prod_{i \in \mathcal{X}} m_i \otimes m_i \ , \tag{B49}$$

where we have defined $\boldsymbol{\mu}^{\mathcal{X}} = \prod_{i \in \mathcal{X}} \mu_i$. Inserting this expression to (B48) gives

$$\mathbb{P}_0^\Lambda = \frac{1}{2^{2d}} \sum_{k=0}^{2d} \sum_{\mathcal{X} \in \binom{[2d]}{k}} A_{\mathcal{X}} \prod_{i \in \mathcal{X}} m_i \otimes m_i \ , \tag{B50}$$

with

$$A_{\mathcal{X}} = \sum_{\substack{\boldsymbol{\mu} \in \{-1,1\}^{2d} \\ \sum_{i=1}^{2d} \mu_i = 0}} \boldsymbol{\mu}^{\mathcal{X}} \ . \tag{B51}$$

Every $\boldsymbol{\mu} \in \{-1,1\}^{2d}$ can be identified with a subset $\mathcal{Y}_{\boldsymbol{\mu}} \subset [2d]$ defined by $\mathcal{Y}_{\boldsymbol{\mu}} = \{ i \mid \mu_i = -1 \}$. Under this identification $\boldsymbol{\mu}^{\mathcal{X}} = (-1)^{|\mathcal{X} \cap \mathcal{Y}_{\boldsymbol{\mu}}|}$. Consequently we obtain

$$A_{\mathcal{X}} = \sum_{\mathcal{Y} \in \binom{[2d]}{d}} (-1)^{|\mathcal{X} \cap \mathcal{Y}|} \ . \tag{B52}$$

Let us first observe that because $(-1)^{|\mathcal{X} \cap \mathcal{Y}|} = (-1)^d (-1)^{|\bar{\mathcal{X}} \cap \mathcal{Y}|}$, for $\bar{\mathcal{X}} = [2d] \setminus \mathcal{X}$ and $|Y| = d$, we have $C_{\mathcal{X}} = (-1)^d C_{\bar{\mathcal{X}}}$. Assuming $|X| = k \leq d$ we get

$$A_{\mathcal{X}} = \sum_{l=0}^{k} (-1)^l \sum_{\substack{\mathcal{Y} \in \binom{[2d]}{d} \\ |\mathcal{X} \cap \mathcal{Y}| = l}} = \sum_{l=0}^{k} (-l)^l \binom{k}{l} \binom{2d-k}{d-l} \ , \tag{B53}$$

where in to get the second equality we counted the number of sets $\mathcal{Y} \in \binom{[2d]}{d}$ satisfying $|\mathcal{X} \cap \mathcal{Y}| = l$, where $|X| = k \leq d$. Since we $A_{\mathcal{X}}$ depends only on $|\mathcal{X}|$ we will sue the notation denoting $A_{\mathcal{X}} = A_{|\mathcal{X}|}$. USing simple algebra we obtain

$$A_k = \sum_{l=0}^{k} (-1)^l \binom{k}{l} \binom{2d-k}{d-l} = \frac{k!(2d-k)!}{(d!)^2} \sum_{l=0}^{k} (-1)^l \binom{d}{l} \binom{d}{k-l} \ . \tag{B54}$$

This can be further simplified using the identity

$$\sum_{l=0}^{k}(-1)^l\binom{d}{l}\binom{d}{k-l} = \begin{cases}(-1)^{k/2}\binom{d}{k/2} & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd}\end{cases} . \tag{B55}$$

Denoting $A_{2p} = C_p$ and using $C_{\mathcal{X}} = (-1)^d C_{\bar{\mathcal{X}}}$ we observe that $C_{d-k} = C_k$. Inserting the expression for $A_{\mathcal{X}}$ to (B50) we finally obtain the desired result:

$$\mathbb{P}_0^{\Lambda} = \frac{1}{2^{2d}}\sum_{p=0}^{d} C_p \sum_{\mathcal{X}\in\binom{[2d]}{2p}} \prod_{i\in\mathcal{X}} m_i \otimes m_i \ . \tag{B56}$$

where C_p satisfy $C_p = (-1)^d C_{d-p}$ and for $p \leq \lfloor d/2 \rfloor$

$$C_p = (-1)^p \frac{(2p)!(2d-2p)!}{(d!)^2}\binom{d}{p} \ . \tag{B57}$$

We thus established $\mathbb{P}_{\text{act}} = \mathbb{P}_+ \otimes \mathbb{P}_+ \mathbb{P}_0 \mathbb{P}_+ \otimes \mathbb{P}_+$. The dimension of the subspace on which $\mathbb{P}_{\text{act}}$ projects, $|\tilde{\mathcal{H}}_{\text{act}}|$, can be now computed as $\text{tr}(\mathbb{P}_{\text{pas}})$ by using standard algebraic properties of Majorana operators.

□

In order to proof the following lemma we use explicit form of $\mathbb{P}_{\text{pas}}$ to compute $\text{tr}(\mathbb{P}_{\text{pas}}\Psi_{\text{in}} \otimes \Psi_{\text{in}})$.

Lemma 15. *Consider the setting of our quantum advantage proposal, i.e., $d = 4N$ and $n = 2N$. Let $\Psi_{\text{in}} \in \mathcal{D}\left(\mathcal{H}^+_{\text{Fock}}(\mathbb{C}^{4N})\right)$. Let $\mathbb{P}_{\text{act}}$ be a projector specified in Lemma 14. We then have*

$$\text{tr}(\mathbb{P}_{\text{act}}\Psi_{\text{in}} \otimes \Psi_{\text{in}}) = \frac{1}{2^{8N}}\left[2\sum_{q}^{N-1} C_{2q}\sum_{l=0}^{\lfloor\frac{q}{2}\rfloor}\frac{N!}{l!(q-2l)!(N-q+l)!}14^{q-2l} + C_{2N}\sum_{l=0}^{N}\frac{N!}{(l!)^2(4N-2l)!}14^{N-2l}\right] . \tag{B58}$$

where

$$C_{2q} = \frac{(4q)!(8N-4q)!}{((4N)!)^2}\binom{4N}{2q} \ . \tag{B59}$$

Proof. We start be observing that due to FLO invariance of $\mathbb{P}_{\text{act}}$ we have $\text{tr}(\mathbb{P}_{\text{act}}\Psi_{\text{in}}\otimes\Psi_{\text{in}}) = \text{tr}(\mathbb{P}_{\text{act}}\Psi'_{\text{in}}\otimes\Psi'_{\text{in}})$, where $\Psi'_{\text{in}} = V\Psi_{\text{in}}V^\dagger$, for $V \in \mathcal{G}_{\text{act}}$. Note that by applying $V = \prod_{1=1}^{N} m_{3i-1}m_{4i-i}$ we can transform $|\Psi_{\text{in}}\rangle = |\Psi_4\rangle^{\otimes N}$ (recall that $|\Psi_4\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$ into $|\Psi'_{\text{in}}\rangle = |a_8\rangle^{\otimes N}$, where $|a_8\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ is the state that was used considered previously by Bravyi in the context of magic state injection for model of computation based on Ising anyons [64] (see also [76, 77]). The state $\left|a_8^{\mathcal{B}}\right\rangle\!\left\langle a_8^{\mathcal{B}}\right|$ on octet of normally-ordered Majorana modes denoted by $\mathcal{B} \subset [2d]$ can be decomposed using Majorana monomials

$$\left|a_8^{\mathcal{B}}\right\rangle\!\left\langle a_8^{\mathcal{B}}\right| = \frac{1}{2^4}\left(\mathbb{I} + Q^{\mathcal{B}} + A_1^{\mathcal{B}} + A_2^{\mathcal{B}} + \ldots + A_{14}^{\mathcal{B}}\right) \ , \tag{B60}$$

where $Q^{\mathcal{B}} = \prod_{i\in B} m_i$ and operators $A_i^{\mathcal{B}}$, $i = 1, \ldots, 14$ are quartic (i.e. fourth other) Majorana monomials supported on modes belonging to $\mathcal{B}$ ant satisfying $(A_i^{\mathcal{B}})^2 = \mathbb{I}$. We will not need explicit form of $|a_8\rangle\langle a_8|$ but it can be found in the works cited above). The algebraic framework of Majorana fermion operators allows us to write the equivalent input state $|\Psi'_{\text{in}}\rangle\langle\Psi'_{\text{in}}|$ as a product (in a standard operator sense) of states $|a_8\rangle\langle a_8|$ supported on disjoint octets of modes

$$|\Psi'_{\text{in}}\rangle\langle\Psi'_{\text{in}}| = \prod_{i=1}^{N}\left|a_8^{\mathcal{B}_i}\right\rangle\!\left\langle a_8^{\mathcal{B}_i}\right| \ , \tag{B61}$$

where $\mathcal{B}_1 = \{1, 2, \ldots, 8\}$, $\mathcal{B}_1 = \{1, 2, \ldots, 8\}$,$\mathcal{B}_2 = \{9, 10, \ldots, 16\}$, etc. We proceed similarly as in the proof of Proposition 4 and expand the above expressions into product of majorana monomials and obtain

$$|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}| = \frac{1}{2^{4N}} \sum_{\mathcal{X}\in\mathcal{C}_{\rm A8}} (-1)^{F(\mathcal{X})} \prod_{i\in\mathcal{X}} m_i \ , \tag{B62}$$

where $\mathcal{C}_{\rm A8}$ is a collection of subsets of $8N$ Majorana modes modes that appear in the product expansion of $|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|$ and $(-1)^{F(\mathcal{X})}$ a sign possibly depending on a subset $\mathcal{X}$. Because $|\Psi'_{\rm in}\rangle \in \mathcal{H}^{+}_{\rm Fock}(\mathbb{C}^d)$ and the form projector $\mathbb{P}_{\rm act}$ (cf. Eq. (B41)) we have $\mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_{\rm act}\right) = \mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right)$, where $\mathbb{P}_0$ is given in (B42). Combining (B62) with (B42) gives

$$\mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right) = \frac{1}{2^{16N}} \sum_{p=0}^{4N} C_p \sum_{\mathcal{Z}\in\binom{[8N]}{2p}} \sum_{\mathcal{X},\mathcal{Y}\in\mathcal{C}_{\rm A8}} (-1)^{F(\mathcal{X})+F(\mathcal{Y})}\,\mathrm{tr}\left[\prod_{i\in\mathcal{X}} m_j \otimes \prod_{k\in\mathcal{Y}} m_i \prod_{k\in\mathcal{Z}} m_k \otimes m_k\right] . \tag{B63}$$

Using

$$(-1)^{F(\mathcal{X})+F(\mathcal{Y})}\,\mathrm{tr}\left[\prod_{i\in\mathcal{X}} m_j \otimes \prod_{k\in\mathcal{Y}} m_i \prod_{k\in\mathcal{Z}} m_k \otimes m_k\right] = 2^{8N}\delta_{\mathcal{X},\mathcal{Y}}\delta_{\mathcal{Z},\mathcal{X}} \tag{B64}$$

we obtain

$$\mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right) = \frac{1}{2^{8N}} \sum_{p=0}^{4N} C_p \sum_{\mathcal{X}\in\binom{[8N]}{2p}\cap\mathcal{C}_{\rm A8}} . \tag{B65}$$

Recall that from the definition of $\mathcal{C}_{\rm A8}$, this collection of subsets of $[8N]$ consists only on subsets that are have cardinality divisible by 4. Therefore the above can be described equivalently by

$$\mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right) = \frac{1}{2^{8N}} \sum_{q=0}^{2N} C_{2q} \sum_{\mathcal{X}\in\binom{[8N]}{4q}\cap\mathcal{C}_{\rm A8}} . \tag{B66}$$

Moreover, form $Q\,|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}| = |\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|$ we get $\bar{\mathcal{X}}\in\mathcal{C}_{\rm A8}$ if and only if $\mathcal{X}\in\mathcal{C}_{\rm A8}$ and consequently

$$\sum_{\mathcal{X}\in\binom{[8N]}{4q}\cap\mathcal{C}_{\rm A8}} = \sum_{\mathcal{X}\in\binom{[8N]}{8N-4q}\cap\mathcal{C}_{\rm A8}} . \tag{B67}$$

Using this and the property $C_{2q} = C_{8N-2q}$ we finally get

$$\mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right) = \frac{1}{2^{8N}} \sum_{q=0}^{N-1} 2\left(C_{2q} \sum_{\mathcal{X}\in\binom{[8N]}{4q}\cap\mathcal{C}_{\rm A8}}\right) + \left(C_{2N}\frac{1}{2^{8N}} \sum_{\mathcal{X}\in\binom{[8N]}{4N}\cap\mathcal{C}_{\rm A8}}\right) . \tag{B68}$$

Therefore, we have reduced the problem of computing $\mathrm{tr}\left(|\Psi'_{\rm in}\rangle\langle\Psi'_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right)$ (equal to $\mathrm{tr}\left(|\Psi_{\rm in}\rangle\langle\Psi_{\rm in}|^{\otimes 2}\,\mathbb{P}_0\right)$) to the problem of counting different sets of cardinality $4q$ ($q = 0, 1, \ldots, N$) one can find in $\mathcal{C}_{\rm A8}$. This problem can be tackled using similar technique to the one used in the proof of Proposition 4 i.e. by introducing *pattern of types* of subsets in $\mathcal{C}_{\rm A8}$. We have $8N$ Majorana modes in total. In what follows we shall refer to "standard octets" as N disjoint octets on which states $|a_8^{\mathcal{B}_i}\rangle$ are supported in Eq. (B61). A subset $\mathcal{X}\in\mathcal{C}_{\rm A8}$ satisfying $|\mathcal{X}| = 4q$ ($q \leq N$) can be characterized, in analogy to (B32), by pattern of types, i.e. a triple

$$\mathcal{X} \longmapsto \mathcal{L}(\mathcal{X}) = (l_{\rm oct}[\mathcal{X}]\ ,\ l_{\rm empty}[\mathcal{X}]\ ,\ l_{\rm quad}[\mathcal{X}])\ , \tag{B69}$$

where $l_{\rm oct}[\mathcal{X}]$ counts the number of standard octets contained in $\mathcal{X}$, $l_{\rm empty}[\mathcal{X}]$ counts how many standard octets are not populated by elements of $\mathcal{X}$, and finally $l_{\text{quad}}[\mathcal{X}]$ is the number of octets in which $\mathcal{X}$ intersects only in four elements (note that from the construction of $\mathcal{C}_{\text{A8}}$ and due to specific form of the state $|a_8^{\mathcal{B}}\rangle\langle a_8^{\mathcal{B}}|$ in Eq. (B60) these are the only possibilities). With these concepts counting of sets $\mathcal{X} \in \mathcal{C}_{\text{A8}}$ of carnality $4q$ can be done analogously as in Proposition 4 i.e by counting how many sets of different "pattern of types" $\mathcal{L}(\mathcal{X})$ of given carnality are there. The final results reads

$$\left|\left\{ \mathcal{X} \mid \mathcal{X} \in \binom{[8N]}{4q} \ , \ \mathcal{X} \in \mathcal{C}_{\text{A8}} \right\}\right| = \sum_{l=0}^{\lfloor \frac{q}{2} \rfloor} \frac{N!}{l!(q-2l)!(N-q+l)!} 14^{q-2l} \ , \tag{B70}$$

where l labels the number of possible "fully occupied" standard octets in $\mathcal{X}$ of carnality $4q$. The term 14^{q-2l} appears because for the said value of fully occupied octets there are necessarily $q-2l$ octets of quartic type, and every such octet there is exactly 14 possibilities. We conclude the proof by using the above identity in Eq. (B68) and employing the explicit formula for C_{2q} from (B43).

□

3. Computation of the sums

In this part we prove the bounds on the combinatorial sums appearing in Lemma 13, Lemma 15. This ultimately proves anticoncentration bounds for passive and active FLO circuits initialized in magic input states Ψ_{in} in Theorem 1.

Our general strategy for the analytical part will be based on the following tight inequalities satisfied by binomial and trinomial coefficients.

Lemma 16 (Bounds for binomial and trinomial coefficients)**.** *Let n, k be a natural numbers such that $k \in \{1, \ldots, n-1\}$. Let $x = \frac{k}{n}$. Then we have*

$$c \cdot \sqrt{\frac{n}{k(n-k)}} \exp\left(n\, h(x)\right) \leq \binom{n}{k} \leq C \cdot \sqrt{\frac{n}{k(n-k)}} \exp\left(n\, h(x)\right) \ , \tag{B71}$$

where $c = \frac{1}{2\sqrt{2}}$, $C = \frac{1}{\sqrt{2\pi}}$, and $h(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy.

Moreover, let k, l, m be nonzero natural numbers such that $k + l + m = n$. Let $x = \frac{k}{n}, y = \frac{l}{n}, z = \frac{m}{n}$. Then we have

$$a \sqrt{\frac{n}{k \cdot l \cdot m}} \exp\left(n\, h(x,y,z)\right) \leq \binom{n}{k, l, m} \leq A \sqrt{\frac{n}{k \cdot l \cdot m}} \exp\left(n\, h(x,y,z)\right) \ , \tag{B72}$$

where $a = \frac{1}{8}$, $A = \frac{1}{2\pi}$ and $h(x,y,z) = -x\log(x) - y\log(y) - z\log(z)$ is the entropy of three-outcome probability distribution.

The inequality (B71) can be found in Lemma 7 in Chapter 10 of [119] while (B72) follows from it due to identity $\binom{n}{k,l,m} = \binom{n}{k}\binom{l+m}{m}$.

We first consider the case of passive FLO. We observe that from Eq. (B38) it follows that

$$\operatorname{tr}\left(\mathbb{P}_{\text{pas}} \Psi_{\text{in}} \otimes \Psi_{\text{in}}\right) \leq \frac{2}{2N+1} \sum_{k=0}^{N} \sum_{l=0}^{\lfloor k/2 \rfloor} \frac{\binom{N}{l, k-2l, N-k+l}}{\binom{2N}{k}} \ . \tag{B73}$$

Lemma 17. *Consider the setting of our quantum advantage proposal, i.e., $d = 4N$ and $n = 2N$. Let*

$\Psi_{\rm in} \in \mathcal{D}\left(\bigwedge^{2N}(\mathbb{C}^{4N})\right)$. *Let $\mathbb{P}_{\rm pas}$ be defined as in Lemma 12. We then have*

$$\mathrm{tr}\left(\mathbb{P}_{\rm pas}\Psi_{\rm in}\otimes\Psi_{\rm in}\right) \leq \frac{C_{\rm pas}}{N},\ \textit{for}\ C_{\rm pas} = 5.7\ . \tag{B74}$$

Proof. Let us denote

$$f_N(k,l) := \frac{\binom{N}{l,k-2l,N-k+l}}{\binom{2N}{k}}\ . \tag{B75}$$

From (B73) it follows that

$$\mathrm{tr}\left(\mathbb{P}_{\rm pas}\Psi_{\rm in}\otimes\Psi_{\rm in}\right) \leq \frac{2}{2N+1}\sum_{k=0}^{N}\sum_{l=0}^{\lfloor k/2\rfloor} f_N(k,l) \leq \frac{1}{N}\left(\mathcal{A}_{k=0}+\mathcal{A}_{l=0}+\mathcal{A}_{k=2l}+\mathcal{A}_{gen}\right)\ , \tag{B76}$$

where

$$\mathcal{A}_{k=0} = f_N(0,0) = 1\ , \tag{B77}$$

$$\mathcal{A}_{l=0} = \sum_{k=1}^{N}\frac{\binom{N}{k}}{\binom{2N}{k}}\ , \tag{B78}$$

$$\mathcal{A}_{k=2l} = \sum_{\substack{k>1\\ k\ \text{even}}}^{N}\frac{\binom{N}{k/2}}{\binom{2N}{k}}\ , \tag{B79}$$

$$\mathcal{A}_{gen} = \sum_{k=1}^{N}\sum_{l=1}^{l<k/2} f_N(k,l)\ . \tag{B80}$$

We upper bound each term above separately (except for the trivial case of $\mathcal{A}_{k=0}$). The following analytical proof for the bound requires $N \geq 130$. In particular, the bound for (B85) $\mathcal{A}_{l=0}$ is valid for $N \geq 40$, and the bound (B101) for $\mathcal{A}_{gen}$ is valid for $N \geq 130$. At the end of the proof, we show in Fig. 9 that the bound also holds for all smaller values of N.

Upper bound on $\mathcal{A}_{l=0}$. In this case, we derive a bound valid for $N > 40$. The bounds from Lemma 16 gives

$$\mathcal{A}_{l=0} \leq \frac{1}{\binom{2N}{N}} + \frac{C}{c}\sum_{k=1}^{N-1}\sqrt{\frac{2N-k}{2(N-k)}}\exp\left[N\left\{h(k/N)-2h(k/2N)\right\}\right]\ . \tag{B81}$$

We use now the inequality $h(x) - 2h(x/2) \leq -\frac{2}{3}x$, valid for $x \in [0,1]$ to obtain

$$\mathcal{A}_{l=0} \leq \frac{1}{\binom{2N}{N}} + \frac{C}{c}\sum_{k=1}^{N-1}\sqrt{\frac{2N-k}{2(N-k)}}\exp\left(-\frac{2k}{3}\right)\ . \tag{B82}$$

We then apply the bound $\binom{2N}{N} \geq c2^{2N}\sqrt{2/N}$ and divide the sum over k into two parts

$$\mathcal{A}_{l=0} \leq \frac{\sqrt{N}}{\sqrt{2}c}2^{-2N} + \frac{C}{c}\left(\sum_{k=1}^{k\leq 1/2N}\sqrt{\frac{2N-k}{2(N-k)}}\exp\left(-\frac{2k}{3}\right) + \sum_{k>1/2N}^{N-1}\sqrt{\frac{2N-k}{2(N-k)}}\exp\left(-\frac{2k}{3}\right)\right) \tag{B83}$$

For $k \leq N/2$ we have $\sqrt{\frac{2N-k}{2(N-k)}} \leq \sqrt{3/2}$ and therefore

$$\mathcal{A}_{l=0} \leq \frac{\sqrt{N}}{\sqrt{2}c} 2^{-2N} + \frac{C}{c}\left(\sqrt{\frac{3}{2}}\frac{1}{e^{2/3}-1} + \frac{N^{3/2}}{2}\exp\left(-\frac{N}{3}\right)\right) , \tag{B84}$$

where we have utilized the expression for the sum of geometric progression and the upper bound $\sqrt{\frac{2N-k}{2(N-k)}} \leq \sqrt{N}$, valid for $k \leq N-1$. Using expression (B84) it is easy to verify that for $N > 40$ we have

$$\mathcal{A}_{l=0} \leq \frac{3}{2} . \tag{B85}$$

Upper bound on $\mathcal{A}_{k=2l}$. Estimates for binomials from Lemma 16 yield

$$\mathcal{A}_{k=2l} \leq \frac{C\sqrt{2}}{c} \sum_{\substack{k>1 \\ k \text{ even}}}^{N} \exp\left[-Nh(k/2N)\right] . \tag{B86}$$

Concavity of binary entropy $h(\cdot)$ implies that for $x \in [0,1]$ we have $\frac{\log(2)}{2}x \leq h(x/2)$ and consequently

$$\mathcal{A}_{k=2l} \leq \frac{C\sqrt{2}}{c} \sum_{\substack{k>1 \\ k \text{ even}}}^{N} \exp\left(-\frac{k\log(2)}{2}\right) = \frac{C\sqrt{2}}{c} \sum_{p=1}^{\lfloor N/2 \rfloor} 2^{-p} . \tag{B87}$$

The sum of the geometric series in the above expression is upper bounded by 1 and therefore

$$\mathcal{A}_{k=2l} \leq \frac{C\sqrt{2}}{c} \leq \frac{8}{5} . \tag{B88}$$

Upper bound on $\mathcal{A}_{gen}$. In the following proof, we require that $N \geq 130$. For the generic points in the sum (B73) inequalities from Lemma 16 give

$$\mathcal{A}_{gen} \leq \frac{A}{\sqrt{2}c} \sum_{k=1}^{N} \sum_{l=1}^{l<k/2} \sqrt{\frac{k(2N-k)}{l(k-2l)(N-k+l)}} \exp\left(N\left\{h\left[x_l, y_k - 2x_l, 1 - y_k + x_l\right] - 2h\left[y_k/2\right]\right\}\right) , \tag{B89}$$

where $x_l = l/N$, $y_k = k/N$. Note that $k = 1$ and $k = 2$ are implicitly excluded from the above sum because of the constraints on l and hence

$$\mathcal{A}_{gen} \leq \frac{A}{\sqrt{2}c} \sum_{k=3}^{N} \sum_{l=1}^{l<k/2} \sqrt{\frac{k(2N-k)}{l(k-2l)(N-k+l)}} \exp\left(N\left\{h\left[x_l, y_k - 2x_l, 1 - y_k + x_l\right] - 2h\left[y_k/2\right]\right\}\right) . \tag{B90}$$

In order to upper bound the expression we maximize the function

$$F(x,y) = h\left(x, y-2x, 1-y+x\right) - 2h\left(y/2\right) \tag{B91}$$

over $x \in [0, y/2]$, for fixed value of $y \in [0,1]$. Looking for critical points reduces the problem to solving quadratic equation which gives a unique solution in the interval $[0, y/2]$:

$$x_{opt}(y) = \frac{1}{6}\left(1 + 3y - \sqrt{1 + 6y - 3y^2}\right) . \tag{B92}$$

Crucially, the function $F_{opt}(y) \coloneqq F(x_{opt}(y), y)$ is a continuous function of parameter y, which is also analytic

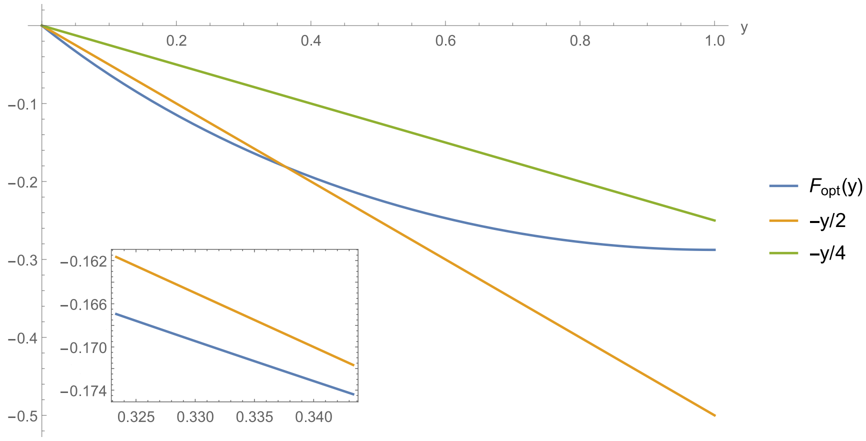

FIG. 8. Function $F_{opt}(y) \coloneqq F(x_{opt}(y), y)$ where F is defined in Eq. (B91) and $x_{opt}(y)$ is given in Eq. (B92). The function is bounded by $-y/3$ in the interval $[0, 1/3]$ and by $-y/4$ in the interval $[1/3, 1]$. The inset plot shows that the inequality is also valid near $y = 1/3$.

in the interior the interval $(0, 1)$. Moreover, $F_{opt}(y)$ satisfies (see Fig. 8):

$$F_{opt}(y) \leq -\frac{1}{2}y \quad \text{for } y \in [0, 1/3] \;\; , \;\; F_{opt}(y) \leq -\frac{1}{4}y \quad \text{for } y \in [0, 1] \;\; . \tag{B93}$$

It follows that

$$N\left(h\left[x_l, y_k - 2x_l, 1 - y_k + x_l\right] - 2h\left[y_k/2\right]\right) \leq -\frac{1}{2}k \;\; \text{for} \;\; 1 \leq k \leq N/3 \; , \tag{B94}$$

$$N\left(h\left[x_l, y_k - 2x_l, 1 - y_k + x_l\right] - 2h\left[y_k/2\right]\right) \leq -\frac{1}{4}k \;\; \text{for} \;\; 1 \leq k \leq N. \tag{B95}$$

Moreover, for integer l satisfying $1 \leq l < k/2$ we have $l(k-2l) \geq (k-2)/2$ and consequently for $k \geq 3$ we have $\frac{k}{l(k-2l)} \leq \frac{2k}{k-2} \leq 6$. As a result we have

$$\sum_{l=1}^{l<k/2} \sqrt{\frac{k(2N-k)}{l(k-2l)(N-k+l)}} \leq \frac{\sqrt{6}k}{2} \sqrt{\frac{2N-k}{N-k+1}} \; . \tag{B96}$$

Inserting (B94) and (B96) into Eq. (B90) gives

$$\mathcal{A}_{gen} \leq \frac{\sqrt{3}A}{2c} \left(\sum_{k=3}^{k \leq N/3} \sqrt{\frac{2N-k}{N-k+1}} k \exp\left(-\frac{k}{2}\right) + \sum_{k > N/3}^{N} \sqrt{\frac{2N-k}{N-k+1}} k \exp\left(-\frac{k}{4}\right) \right) \tag{B97}$$

Observing that for $k \leq N/3$ we have $\sqrt{\frac{2N-k}{N-k+1}} \leq \sqrt{\frac{5}{2}}$, while and for general $k \leq N$ $\sqrt{\frac{2N-k}{N-k+1}} \leq \sqrt{N}$, we obtain

$$\mathcal{A}_{gen} \leq \frac{\sqrt{3}A}{2c} \left(\sqrt{\frac{5}{2}} \sum_{k=3}^{k \leq N/3} k \exp\left(-\frac{k}{2}\right) + \frac{2N^{\frac{3}{2}}}{3} \exp\left(-\frac{N}{12}\right) \right) \; . \tag{B98}$$

We bound the first summand as follows

$$\sum_{k=3}^{k \leq N/3} k \exp\left(-\frac{k}{2}\right) \leq \sum_{k=3}^{\infty} k \exp\left(-\frac{k}{2}\right) = \frac{3\sqrt{e} - 2}{(\sqrt{e} - 1)^2 e} \; . \tag{B99}$$

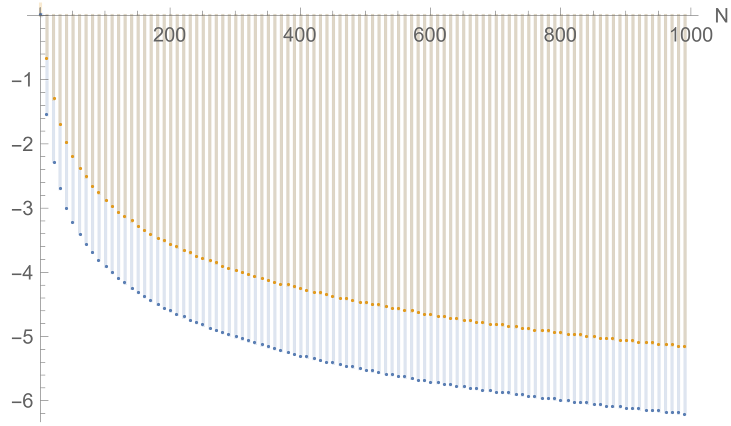

FIG. 9. Plots of the logarithm of the expression (B73) (blue) and $\log(C_{\text{pas}}/N) = \log(5.7/N)$ (orange), which constitutes a valid upper bound for all $N \leq 1000$.

This finally gives us

$$\mathcal{A}_{gen} \leq \frac{\sqrt{15}A}{2\sqrt{2}c} \frac{3\sqrt{e}-2}{(\sqrt{e}-1)^2 e} + \frac{A}{\sqrt{3}c} N^{\frac{3}{2}} \exp\left(-\frac{N}{12}\right) . \tag{B100}$$

Using the above expression we get that for $N \geq 130$ we have

$$\mathcal{A}_{gen} \leq \frac{8}{5} . \tag{B101}$$

Finally, combining bounds (B85), (B88) and (B101) together with $\mathcal{A}_{k=0} = 1$ we see that for $N \geq 130$,

$$\mathcal{A}_{k=0} + \mathcal{A}_{l=0} + \mathcal{A}_{k=2l} + \mathcal{A}_{gen} \leq 5.7 . \tag{B102}$$

Inserting this into the bound (B76) proves the lemma for $N \geq 130$. For $N \leq 130$, the validity of the bound can be verified numerically as shown in Fig. 9, which completes the proof.

□

Analogously for the active FLO case, Eq. (B58) implies that

$$\operatorname{tr}(\mathbb{P}_{\text{act}} \Psi_{\text{in}} \otimes \Psi_{\text{in}}) \leq \frac{\binom{8N}{4N}}{2^{8N-1}} \sum_{q=0}^{N} \sum_{l=0}^{\lfloor \frac{q}{2} \rfloor} \frac{\binom{4N}{2q}\binom{N}{l, q-2l, N-q+l}}{\binom{8N}{4q}} 14^{q-2l}. \tag{B103}$$

Lemma 18. *Consider the setting of our quantum advantage proposal, i.e., $d = 4N$ and $n = 2N$. Let $\Psi_{\text{in}} \in \mathcal{D}\left(\bigwedge^{2N}(\mathbb{C}^{4N})\right)$. Let $\mathbb{P}_{\text{act}}$ be defined as in Lemma 14. We then have*

$$\operatorname{tr}\left(\mathbb{P}_{\text{act}} \Psi_{\text{in}} \otimes \Psi_{\text{in}}\right) \leq \frac{C_{\text{act}}}{\sqrt{N}}, \ \textit{for } C_{\text{act}} = 9 . \tag{B104}$$

Proof. Our proof strategy is analogous to the one used in the case of passive FLO. Let us denote

$$g_N(q,l) := \frac{\binom{4N}{2q}\binom{N}{l, q-2l, N-q+l}}{\binom{8N}{4q}} 14^{q-2l} . \tag{B105}$$

It follows from (B103) and the entropic bound for binomial coefficients in Lemma 16,

$$\frac{\binom{8N}{4N}}{2^{8N-1}} \leq \frac{1}{\sqrt{\pi N}} \ , \tag{B106}$$

that

$$\mathrm{tr}(\mathbb{P}_{\mathrm{act}}\Psi_{\mathrm{in}} \otimes \Psi_{\mathrm{in}}) \leq \frac{1}{\sqrt{\pi N}} \sum_{q=0}^{N} \sum_{l=0}^{\lfloor \frac{q}{2} \rfloor} g_N(q,l) \leq \frac{1}{\sqrt{\pi N}} (\mathcal{B}_{q=0} + \mathcal{B}_{l=0} + \mathcal{B}_{q=2l} + \mathcal{B}_{gen}) \ , \tag{B107}$$

where

$$\mathcal{B}_{q=0} = g_N(0,0) = 1, \tag{B108}$$

$$\mathcal{B}_{l=0} = \sum_{q=1}^{N} \frac{\binom{4N}{2q}\binom{N}{q}}{\binom{8N}{4q}} 14^q, \tag{B109}$$

$$\mathcal{B}_{q=2l} = \sum_{\substack{q>1 \\ q \text{ even}}}^{N} \frac{\binom{4N}{2q}\binom{N}{q/2}}{\binom{8N}{4q}}, \tag{B110}$$

$$\mathcal{B}_{gen} = \sum_{q=1}^{N} \sum_{l=1}^{l<q/2} g_N(q,l) \ . \tag{B111}$$

We upper bound each term above separately (except for the trivial case of $\mathcal{B}_{q=0}$). The following analytical proof for the bound requires $N \geq 7000$. In particular, the bound for (B85) $\mathcal{B}_{l=0}$ is valid for $N \geq 1000$, and the bound (B101) for $\mathcal{B}_{gen}$ is valid for $N \geq 7000$. At the end of the proof, we show in Fig. 12 that the bound (B104) also holds for all smaller values of $N \leq 7000$ by numerically evaluating right-hand side of (B103).

Upper bound on $\mathcal{B}_{l=0}$. For this term, we require that $N \geq 1000$. The entropic bound in Lemma 16 implies that

$$\mathcal{B}_{l=0} \leq \frac{\binom{4N}{2N}}{\binom{8N}{4N}} + \frac{C^2\sqrt{2}}{c} \sum_{q=1}^{N-1} \sqrt{\frac{N}{q(N-q)}} \exp[N\{h(q/N) - 4h(q/2N) + \log(14)q/N\}] \ . \tag{B112}$$

To upper bound the sum, we split the sum into two sums: one from $k=1$ to $k \leq N/5$ and another from $k > N/5$ to $k = N-1$, and upper bound the function

$$H(x) \coloneqq h(x) - 4h(x/2) + x\log(14), \tag{B113}$$

$x \in [0,1]$ in the intervals $[0,1/5]$ and $(1/5,1]$ separately. In particular, we have that (See also Fig. 10)

$$H(x) \leq -\frac{4}{3}x \ \text{ for } x \in [0,2/5], \qquad\qquad H(x) \leq -\frac{1}{18}x \ \text{ for } x \in [0,1] \tag{B114}$$

Together with the bound $\binom{4N}{2N}/\binom{8N}{4N} \leq \frac{C\sqrt{2}}{c}2^{-4N}$ and $\sqrt{N/(q(N-q))} \leq \sqrt{2}$ valid for $N \geq 2$ (this is because $\sqrt{\frac{N}{q(N-q)}}$ is convex for $q \in [1, N-1]$ and thus the expression takes the maximum values at the end points), we obtain

$$\mathcal{B}_{l=0} \leq \frac{C\sqrt{2}}{c}2^{-4N} + \frac{2C^2}{c}\left(\sum_{q=1}^{q\leq N/5} \exp(-4q/3) + \sum_{q>N/5}^{N-1} \exp(-q/18)\right) \tag{B115}$$

$$\leq \frac{C\sqrt{2}}{c}2^{-4N} + \frac{2C^2}{c}\left(\frac{1}{e^{4/3}-1} + \frac{4N}{5}\exp\left[-\frac{N}{18\cdot 5}\right]\right), \tag{B116}$$

where we have used the sum of the geometric series to arrive at the final expression. Using the expression

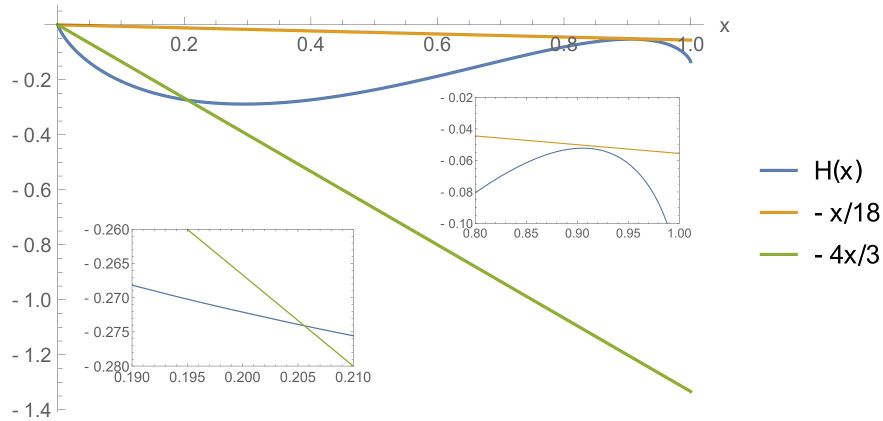

FIG. 10. Function $H(x)$ defined in (B114). The function is bounded above by $-4x/3$ in the interval $[0, 1/5]$ and by $-x/18$ in the interval $[0, 1]$. The inset plot shows the validity of the upper bound in each interval.

(B116), it can be verified that

$$\mathcal{B}_{l=0} \leq \frac{1}{3} \tag{B117}$$

holds for $N \geq 1000$.

Upper bound on $\mathcal{B}_{q=2l}$. From Lemma 16 we see that

$$\mathcal{B}_{q=2l} \leq \frac{C^2\sqrt{2}}{c} \sum_{\substack{q>1 \\ q \text{ even}}}^{N} \sqrt{\frac{N}{\frac{q}{2}(N-\frac{q}{2})}} \exp[-3Nh(q/2N)] \tag{B118}$$

Now by concavity of $h(x)$ for $x \in [0, \frac{1}{2}]$ we have $\log(2)x/2 \leq h(x/2)$ for $x \in [0, 1]$. Then

$$\mathcal{B}_{q=2l} \leq \frac{C^2\sqrt{2}}{c} \sum_{\substack{q>1 \\ q \text{ even}}}^{N} \sqrt{\frac{N}{\frac{q}{2}(N-\frac{q}{2})}} \exp[-3q\log(2)/2] \tag{B119}$$

$$= \frac{C^2\sqrt{2}}{c} \sum_{p=1}^{\lfloor N/2 \rfloor} \sqrt{\frac{N}{p(N-p)}} 2^{-3p} \tag{B120}$$

We can bound $\sqrt{\frac{N}{p(N-p)}} \leq \sqrt{2}$ the same way as in the passive case. Then we obtain

$$\mathcal{B}_{q=2l} \leq \frac{2C^2}{7c} \leq 0.13 \tag{B121}$$

where we used that the geometric sum of 2^{-3p} is bounded by $1/7$.

Upper bound on $\mathcal{B}_{gen}$. Following bounds form Lemma 16 and defining $x_l = \frac{l}{N}$ and $y_q = \frac{q}{N}$ we obtain

$$\mathcal{B}_{gen} \leq \frac{\sqrt{2}CA}{c} \sum_{q=1}^{N} \sum_{l=1}^{l<q/2} \sqrt{\frac{N}{l(q-2l)(N-q+l)}} \exp[NG(x_l, y_q)] \;, \tag{B122}$$

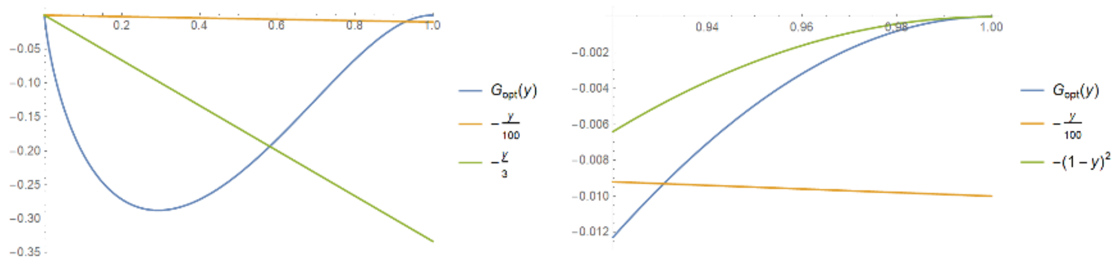

FIG. 11. Function $G_{opt}(y) = G(x_{opt}(y), y)$ where G is defined in Eq. (B123) and $x_{opt}(y)$ is defined in Eq. (B124). The function is presented alongside simple analitical lower bounds are valid in specific intervals formulated in Eq. (B125).

where, following the analogous construction in Lemma 17, we introduced

$$G(x, y) := -4h(y/2) + h(x, y - 2x, 1 - y + x) + (y - 2x)\log(14) \ . \tag{B123}$$

As in the case of passive FLO, our strategy is to upper bound $G(x, y)$ by a function that allows for analytical treatment. To this end, we first optimize $G(x, y)$ over $x \in [0, y/2]$ for fixed $y \in [0, 1]$. Solving for the critical points gives the following optimal solution $x_{opt} \in [0, y/2]$ (at the extremal points of this interval function $G(x, y)$, treated as a function of x for fixed y, takes smaller values)

$$x_{opt}(y) = \frac{1}{96}\left(-49 + 48y + 7\sqrt{40 - 96y + 48y^2}\right) \ . \tag{B124}$$

The maximum of $G(x, y)$ over $x \in [0, y/2]$, $G_{opt}(y) := G(x_{opt}(y), y)$ is a continuous function of $y \in [0, 1]$ and also analytic for $y \in (0, 1)$. We can bound $G_{opt}(y)$ in the following way (see Fig. 11)

$$G_{opt}(y) \leq -y/3 \ \text{for}\ y \in [0, 1/2] \ , \ G_{opt}(y) \leq -y/100 \ \text{for}\ y \in [1/5, 0.925] \ , \ G_{opt}(y) \leq -(1-y)^2 \ \text{for}\ y \in [0.925, 1] \ . \tag{B125}$$

We shall need much more refined information about $G(x, y)$ than in the case of analogous considerations for passive FLO. Namely, we will need to control how fast $G(x, y)$ decays as a function of $x - x_{opt}(y)$, for fixed y. To this end we compute for $x \in (0, y/2)$, $y \in (0, 1)$

$$\partial_x^2 G(x, y) = -\left(\frac{1}{x} + \frac{1}{1 - y + x} + \frac{4}{y - 2x}\right) \ . \tag{B126}$$

From the above expression we get[4]

$$\partial_x^2 G(x, y) \leq -16 \ \text{for}\ x \in (0, y/2) \ \ \text{and}\ \ \partial_x^2 G(x, y) \leq -\frac{2}{3x_{opt}(y)} \ \text{for}\ x \in \left[\frac{x_{opt}(y)}{2}, \frac{3x_{opt}(y)}{2}\right] \ . \tag{B127}$$

Using the analyticity of $G(x, y)$ as a function of x inside the interval $(0, y/2)$, we can Taylor expand it around $x_{opt}(y)$ (for fixed value of y):

$$G(x, y) = G_{opt}(y) + (\partial_x G(x_{opt}(y), y))(x - x_{opt}(y)) + \int_{x_{opt}(y)}^{x} d\tau \partial_\tau G(\tau, y) \ . \tag{B128}$$

Using the fact that $x_{opt}(y)$ is a critical point and bounds, identity

$$\partial_\tau G(\tau, y) = \int_{x_{opt}(y)}^{\tau} dx \partial_x^2 G(x, y) \tag{B129}$$

[4] It is easy to check that $3/2x_{opt}(y) \leq y/2$.

and bounds from Eq. (B127) we get finally get

$$G(x,y) \le G_{opt}(y) - 8(x - x_{opt}(y))^2 \qquad \text{for } x \in [0, y/2]\ ,\ y \in [0,1]\ , \tag{B130}$$

$$G(x,y) \le G_{opt}(y) - \frac{1}{3x_{opt}(y)}(x - x_{opt}(y))^2 \qquad \text{for } x \in \left[\frac{x_{opt}(y)}{2}, \frac{3x_{opt}(y)}{2}\right]\ ,\ y \in [0,1]\ . \tag{B131}$$

Coming back to the bound on $\mathcal{B}_{gen}$ from (B122), similarly to the case of passive FLO, due to constrains on l, the sum appearing in (B122) effectively starts from $q = 3$. Moreover, we also note that $l(q-2l) \ge (q-2)/2$ and therefore

$$\sqrt{\frac{N}{l(q-2l)(N-q+l)}} \le \sqrt{\frac{2N}{(q-2)(N-q+l)}} \le \sqrt{\frac{2N}{N-2}}\ , \tag{B132}$$

where in the second inequality we used the fact that $q \in [3, N]$ and $l \ge 1$. Using the above and expanding the expression in (B122) in the different intervals defined in (B125) we obtain

$$\mathcal{B}_{gen} \le \frac{2CA}{c}\sqrt{\frac{N}{N-2}}\left(\sum_{q=3}^{q\le N/2}\sum_{l=1}^{l<q/2}\exp[-q/2] + \sum_{q>N/2}^{q<0.925N}\sum_{l=1}^{l<q/2}\exp[-q/100]\right) \tag{B133}$$

$$+\frac{\sqrt{2}CA}{c}\sum_{q>0.925N}^{N}\sum_{l=1}^{l<q/2}\sqrt{\frac{N}{l(q-2l)(N-q+l)}}\exp[NG(x_l,y_q)]\ . \tag{B134}$$

Two sums from Eq. (B133) can be handled analogously as in the case of passive FLO:

$$\frac{2CA}{c}\sqrt{\frac{N}{N-2}}\left(\sum_{q=3}^{q\le N/5}\sum_{l=1}^{l<q/2}\exp[-q/3] + \sum_{q>N/2}^{q<0.925N}\sum_{l=1}^{l<q/2}\exp[-q/100]\right) \tag{B135}$$

$$\le \frac{2CA}{c}\sqrt{\frac{N}{N-2}}\left(\sum_{q=3}^{\infty}(q/2)\exp(-q/3) + +(N^{3/2}/2)\exp[-\frac{N}{200}]\right). \tag{B136}$$

$$= \frac{2CA}{c}\sqrt{\frac{N}{N-2}}\left(\frac{3e^{1/3}-2}{2e^{2/3}(e^{1/3}-1)} + (N^{3/2}/4)\exp[-\frac{N}{200}]\right) \le 2\ , \tag{B137}$$

where the last inequality is valid for $N \ge 1800$. The sum in (B134) will be analyzed using inequalities (B130) and (B131). For fixed y_q (Which corresponds to $q = y_q N$) we set $l_{opt}(y_q) = x_{opt}(y_q)N$ and divide the range of summation over l in (B134) into two parts that corresponds to intervals in bounds (B130) and (B131) respectively :

$$\mathcal{L}_q^{\max} = \left\{ l \;\middle|\; \frac{1}{2}l_{opt}(y_q) \le l \le \frac{3}{2}l_{opt}(y_q) \right\}\ , \tag{B138}$$

$$\mathcal{L}_q^{\text{gen}} = \left\{ l \;\middle|\; 1 \le l < \frac{1}{2}l_{opt}(y_q) \text{ or } \frac{3}{2}l_{opt}(y_q) < l < q/2 \right\}\ . \tag{B139}$$

(B140)

It is now straightforward to verify that:

$$\sqrt{\frac{N}{l(q-2l)(N-q+l)}} \le \sqrt{\frac{4N}{l_{opt}(q-3l_{opt})l_{op}}} \text{ for } l \in \mathcal{L}_q^{\max}\ , \tag{B141}$$

where for clarity we surpassed the dependence of l_{opt} on q. Moreover from (B130) and (B131) we get

$$NG(x_l, y_q) \leq NG_{opt}(y_q) - \frac{(l-l_{opt})^2}{3l_{opt}} \text{ for } l \in \mathcal{L}_q^{\max} \ , \tag{B142}$$

$$NG(x_l, y_q) \leq NG_{opt}(y_q) - 2x_{opt}^2 N \text{ for } l \in \mathcal{L}_q^{\text{gen}} \ . \tag{B143}$$

Finally, we arrive at the following bound

$$\frac{\sqrt{2}CA}{c} \sum_{q>0.925N}^{N} \sum_{l=1}^{l<q/2} \sqrt{\frac{N}{l(q-2l)(N-q+l)}} \exp[NG(x_l, y_q)] \tag{B144}$$

$$\leq \frac{\sqrt{2}CA}{c} \sum_{q>0.925N}^{N} \exp[NG_{opt}(y_q)] \sqrt{\frac{4N}{l_{opt}(q-3l_{opt})l_{opt}}} \sum_{l\in\mathcal{L}_q^{\max}} \exp\left(-\frac{(l-l_{opt})^2}{3l_{opt}}\right) \tag{B145}$$

$$+ \sqrt{\frac{N}{N-2}} \frac{CA}{c} \sum_{q>0.925N}^{N} q\exp[NG_{opt}(y_q)]\exp\left(-2x_{opt}^2 N\right) \ , \tag{B146}$$

where we used (B132) to get (B146). We first analyze the second sum. We using (B125) we obtain

$$\sum_{q>0.925N}^{N} q\exp[NG_{opt}(y_q)] \leq N \sum_{q>0.925N}^{N} \exp[\frac{(N-q)^2}{N}] \ \leq N(1+\frac{\sqrt{\pi N}}{2}) \leq N^{\frac{3}{2}} \ . \tag{B147}$$

where we used

$$\sum_{x=0}^{\infty} \exp(-\frac{x^2}{a}) \leq 1 + \int_0^{\infty} dx \exp(-\frac{x^2}{a}) = 1 + \frac{\sqrt{\pi a}}{2} \ , \tag{B148}$$

valid for all $a > 0$, and $N \geq 100$. Importantly, for $q > 0.925N$ (which corresponds to $y \geq 0.925$), we have $x_{opt} \geq 0.03$. Using this and assuming $N \geq 7000$, we finally obtain

$$\sqrt{\frac{N}{N-2}} \frac{CA}{c} \sum_{q>0.925N}^{N} q\exp[NG_{opt}(y_q)]\exp\left(-2x_{opt}^2 N\right) \leq \sqrt{\frac{N}{N-2}} \frac{CA}{c} N^{\frac{3}{2}} \exp(-\frac{9}{5000}N) \leq 1 \ . \tag{B149}$$

We use similar methods to bound (B145). First, we upper bound the exponential sum

$$\sum_{l\in\mathcal{L}_q^{\max}} \exp\left(-\frac{(l-l_{opt})^2}{3l_{opt}}\right) \leq 1 + \sqrt{\pi 3 l_{opt}} \leq \frac{10}{3}\sqrt{l_{opt}} \ , \tag{B150}$$

which allows estimate

$$\sqrt{\frac{4N}{l_{opt}(q-3l_{opt})l_{opt}}} \sum_{l\in\mathcal{L}_q^{\max}} \exp\left(-\frac{(l-l_{opt})^2}{3l_{opt}}\right) \leq \frac{10}{3}\sqrt{\frac{4N}{l_{opt}(q-3l_{opt})}} \leq \frac{10}{3}\sqrt{\frac{4}{(0.03)(0.7N)}} = \frac{20}{3}\sqrt{\frac{1000}{21N}} \ , \tag{B151}$$

where in the second inequality we used that for $q \geq 0.925N$ we have $l_{opt}(y_q) \geq 0.03N$ and $q - 3l_{opt}(y_q) \geq 0.7N$. Inserting thin inequality to (B145) and again using (B147) gives that for $N \geq 7000$

$$\frac{\sqrt{2}CA}{c} \sum_{q>0.925N}^{N} \sum_{l=1}^{l<q/2} \sqrt{\frac{N}{l(q-2l)(N-q+l)}} \exp[NG(x_l, y_q)] \leq 1 + \frac{\sqrt{2}CA}{c}\sqrt{\frac{1000}{21}} \leq 12.7 \ . \tag{B152}$$

Combining this estimate with the bound (B137) and using (B133), we finally obtain that for $N \geq 7000$

$$\mathcal{B}_{gen} \leq 14.7 \ . \tag{B153}$$

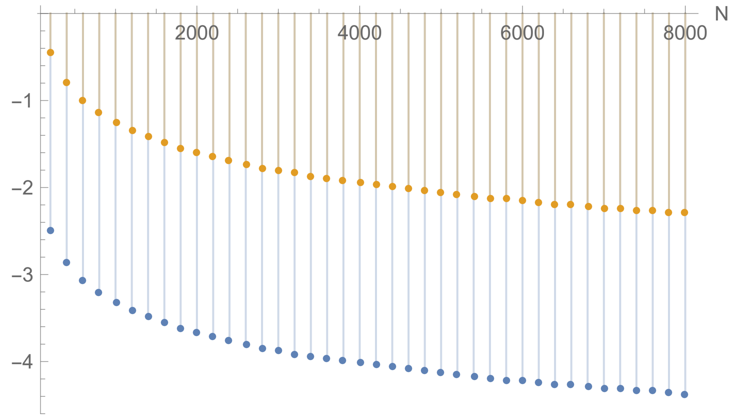

FIG. 12. Plots of the logarithm of the the expression (B103) (blue) and $\log(C_{\mathrm{act}}/\sqrt{N}) = \log(9/\sqrt{N})$ (orange), which is a valid upper bound for all $N \leq 7000$.

Finally, combining bounds (B117), (B121) and (B153) together with $\mathcal{B}_{k=0} = 1$ in inequality (B107) we see that for $N \geq 7000$,

$$\mathrm{tr}(\mathbb{P}_{\mathrm{act}} \Psi_{\mathrm{in}} \otimes \Psi_{\mathrm{in}}) \leq \frac{1}{\sqrt{\pi N}} (\mathcal{B}_{q=0} + \mathcal{B}_{l=0} + \mathcal{B}_{q=2l} + \mathcal{B}_{gen}) \leq \frac{9}{\sqrt{N}} \ . \tag{B154}$$

For $N \leq 7000$, the validity of the bound can be verified numerically as shown in Fig. 12, which completes the proof.

□

Appendix C: Efficient tomography of FLO unitaries

Here we prove Lemma 9, which establishes a bound concerning the stability of the active FLO representation which is needed in the efficient tomographic scheme of Section X.

Lemma (Stability of active FLO representation) *Consider two elements of the orthogonal group, $O, O' \in \mathrm{SO}(2d)$, and let V and V' be the corresponding active FLO unitaries, i.e., $V = \Pi_{\mathrm{act}}(O)$ and $V' = \Pi_{\mathrm{act}}(O')$. Let Φ_V and $\Phi_{V'}$ be the unitary channels defined by V and V' respectively. Then, the following inequality is satisfied*

$$\|\Phi_V - \Phi_{V'}\|_\diamond \leq 2d \|O - O'\|. \tag{C1}$$

Proof. The proof will rely on representation theoretic methods, however, as we have noted, Π_{act} is a projective representation of $\mathrm{SO}(2d)$ and not a proper representation. Instead, we will use $\Pi_{\mathrm{act}} \otimes \Pi_{\mathrm{act}}$, which is already a proper representation of $\mathrm{SO}(2d)$. Thus, we will bound the diamond norm difference between the unitary channels $\phi_{V \otimes V}$ and $\phi_{V' \otimes V'}$ corresponding to the unitaries $V \otimes V = \Pi_{\mathrm{act}} \otimes \Pi_{\mathrm{act}}(O)$ and $V' \otimes V' = \Pi_{\mathrm{act}} \otimes \Pi_{\mathrm{act}}(O')$, respectively, and then use the inequalities

$$\|\Phi_V - \Phi_{V'}\|_\diamond \leq \|\Phi_{V\otimes V} - \Phi_{V' \otimes V'}\|_\diamond \leq 2 \|V \otimes V - V' \otimes V'\|. \tag{C2}$$

Here the first inequality follows directly from the definition of the diamond norm, while the second is a standard inequality relating the diamond norm distance of unitary channels to the operator norm distance of unitaries (see, e.g., [120]).

Thus, our proof strategy will be to upper bound $\|V \otimes V - V' \otimes V'\| = \|\Pi_{\mathrm{act}} \otimes \Pi_{\mathrm{act}}(O) - \Pi_{\mathrm{act}} \otimes \Pi_{\mathrm{act}}(O')\|$.

For this we use the decomposition of the $\Pi_{\text{act}} \otimes \Pi_{\text{act}}$ into subrepresentations in the following way [121]:

$$\Pi_{\text{act}} \otimes \Pi_{\text{act}} \cong \bigoplus_{s=0}^{d-1} \left(\bigwedge^{s} \Pi \right)^{\oplus 2} \oplus \bigwedge^{d} \Pi, \tag{C3}$$

where Π denotes the defining representation of $\mathrm{SO}(2d)$ and its ℓth antisymmetric tensor power $\bigwedge^{\ell} \Pi$ is given by

$$\bigwedge^{\ell} \Pi : \mathrm{SO}(2d) \longrightarrow \mathrm{U}\Big(\bigwedge^{\ell} (\mathbb{C}^{2d}) \Big), \tag{C4}$$

$$O \longmapsto O^{\otimes n}\big|_{\bigwedge^{\ell}(\mathbb{C}^{d})} . \tag{C5}$$

This decomposition immediately implies that

$$\|V \otimes V - V' \otimes V'\| = \|\Pi_{\text{act}} \otimes \Pi_{\text{act}}(O) - \Pi_{\text{act}} \otimes \Pi_{\text{act}}(O')\| \leq \max_{\ell \in [d]} \| \bigwedge^{\ell} \Pi(O) - \bigwedge^{\ell} \Pi(O') \| \leq \max_{\ell \in [d]} \|O^{\otimes \ell} - O'^{\otimes \ell}\|. \tag{C6}$$

Inserting the above inequality into Eq. (C2) and using that $\|O^{\otimes \ell} - O'^{\ell}\| \leq \ell \|O - O'\|$ (and $\ell \leq d$), we obtain

$$\|\Phi_V - \Phi_{V'}\|_{\diamond} \leq 2d \|O - O'\|. \tag{C7}$$

□

Appendix D: #P-Hardness of probabilities in shallow depth active FLO circuits

We argued in section VI that amplitudes of active FLO circuits are #P-hard to compute. Here we show that similarly strong simulation (i.e., computing output probabilities) of constant-depth active FLO circuits is hard. It has been proven in previous work [26] that under certain conditions, non-universal circuit families of shallow depth are hard to simulate under plausible conjectures which in addition implies that the output probabilities are #P-hard. In concrete, it is required that the postselected version of the circuit family is universal for quantum computation. This method is not robust as it only shows that exactly computing the output probabilities are hard, nonetheless it may be of interest that such hardness results can be obtained for constant-depth active FLO circuits. The required theorem is as follows

Theorem 9. *Let $\mathcal{F}$ be a restricted family of quantum circuits. If circuits from $\mathcal{F}$ with the added power of postselection can simulate the output probability distributions of universal quantum circuits with postselection (i.e., $\mathcal{F}$ is universal with postselection) then computing the output probabilities (strong simulation) of circuits in $\mathcal{F}$ is #P-hard.*

Proof. Similar results have been proven in [25, 26] and later in other works related to active FLO [81]. Let C be some circuit with gates from a universal gate set and let $P_C(\mathbf{y})$ be the output probability of result $\mathbf{y}$. By hypothesis, with the power of postselection we can use a circuit F from $\mathcal{F}$ to simulate C and thus $P_C(\mathbf{y}) = P_F(\mathbf{y}_* | 00 \cdots 0) = \frac{P_F(\mathbf{y}_* 00 \cdots 0)}{P_F(00 \cdots 0)}$, where $\mathbf{y}_*$ is potentially a bitstring encoding $\mathbf{y}$ (which will be our case below). This directly implies that if we could compute the output probabilities of F then this would allow for computing the output probabilities of C. Since universal circuits are known to include #P-hard instances, the result follows. □

In what follows, we will always assume that the active FLO circuits are supplied with auxiliary states $|\Psi_4\rangle$. Throughout this section we will consider the encoding $|0_L\rangle = |00\rangle$ and $|1_L\rangle = |11\rangle$. To prove that computing the probabilities of shallow depth active FLO circuits is #P-hard, we prove now Lemma 19.

Lemma 19. *Constant-depth active FLO circuits supplied with auxiliary states $|\Psi_4\rangle$ with the added power of postselection are universal.*

To prove this, we follow Ref. [56], which showed similar results in the context of Boson Sampling. The starting point is the brickwork graph state which allows for universal computation on the measurement based quantum computation (MBQC) scheme. We can write the preparation of the brickwork graph state plus measurements on the state as a single circuit with adaptive measurements. If we are given the power to postselect measurements, then the preparation of the graph state requires a constant depth circuit with single qubit gates and CZ gates. If we can simulate these gates with constant-depth active FLO circuits and postselection, then this would imply Lemma 19. Using the encoding defined above, we show Theorem 10 which directly implies Lemma 19.

Theorem 10. *Active FLO acting on an initial state consisting of tensor products of* $|\Psi_4\rangle$ *with the added power of postselection can simulate single qubit gates and* CZ *with constant-depth circuits. These simulations are at the logical level using the encoding above.*

Proof. As explained before, the circuit induced by the brickwork state with post selection is universal and of constant depth, consisting of single qubit gates and CZ gates. Using the encoding above we can simulate single qubit gates and CZ gates in constant depth, then we can simulate the whole universal constant-depth circuit with a circuit from $\mathcal{C}_{act}$ and postselection.

That single qubit gates at the logical level can be implemented with this encoding is already known [61]. Implementing CZ at the logical level will require the use of post selection and the auxiliary states $|\Psi_4\rangle$. First, we note that the state $|\Psi_4\rangle$ can be transformed into the state $|a_8\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ using only active FLO operations. This was shown previously in the proof of Lemma 15. Second, in Lemma 1 of [64] it is shown that using a single copy of $|a_8\rangle$ and particle number measurements it is possible to implement a CZ at the logical level using the same encoding we use here. This two facts together imply that CZ can be implemented with active FLO circuits supplied by $|\Psi_4\rangle$ states and postselection. The auxiliary states can be swapped to the desired position when implementing a gate without incurring on extra negative signs with our encoding since the auxiliary states used are fermionic as for example argued in [65]. □