The Power of Noisy Fermionic Quantum Computation

Fernando de Melo[1], Piotr Ćwikliński[2], Barbara M. Terhal[2]

[1]Centrum Wiskunde & Informatica,
Science Park 123, 1098 XG Amsterdam, The Netherlands
[2]Institute for Quantum Information, RWTH Aachen University,
52056 Aachen, Germany

E-mail: `melo@cwi.nl`, `cwiklinski@physik.rwth-aachen.de`,
`terhal@physik.rwth-aachen.de`

Abstract. We consider the realization of universal quantum computation through braiding of Majorana fermions supplemented by unprotected preparation of noisy ancillae. It has been shown by Bravyi [*Phys. Rev. A* **73**, 042313 (2006)] that under the assumption of perfect braiding operations, universal quantum computation is possible if the noise rate on a particular 4-fermion ancilla is below 40%. We show that beyond a noise rate of 89% on this ancilla the quantum computation can be efficiently simulated classically: we explicitly show that the noisy ancilla is a convex mixture of Gaussian fermionic states in this region, while for noise rates below 53% we prove that the state is not a mixture of Gaussian states. These results are obtained by generalizing concepts in entanglement theory to the setting of Gaussian states and their convex mixtures. In particular we develop a set of criteria, namely the existence of a Gaussian-symmetric extension, which determine whether a state is a convex mixture of Gaussian states.

1. Introduction

One interesting route towards universal quantum computation is through the realization of Majorana fermion qubits. Such Majorana fermion qubits, encoded in pairs of nonlocal fermionic zero-energy modes, are believed to be present in various quantum systems such as a $\nu = 5/2$ fractional Quantum Hall system, $p_x + \mathrm{i}p_y$ superconductors, and recently proposed topological insulator/superconductor and semiconducting nanowires/superconductor structures (see [1] for a review). Braiding operations on such Majorana fermion qubits can implement certain topologically-protected gates, namely single-qubit Clifford gates [2, 3]. A system of Majorana fermions initially prepared in a fermionic Gaussian state (see definition below) and undergoing braiding operations (which are a subset of non-interacting fermion operations ‡) can be classically efficiently simulated if it is not supplemented by additional resources.

‡ Non-interacting fermionic operations are unitary transformations generated by quadratic Hamiltonians on the creation and annihilation operators of fermionic modes. Such Hamiltonians can always be block-diagonalized, and in this new basis the different fermionic modes do not interact.

Universal quantum computation can be achieved if this supplement consists, for example, of either (i) gates which use quartic interaction between Majorana fermions [4] or (ii) a quartic parity measurement [5] or (iii) two ancillae in certain special states $|a_4\rangle$ and $|a_8\rangle$, involving respectively 4 and 8 Majorana fermions [2]. The advantage of the last realization is that even when these ancillae are noisy, one can purify them using braiding operations. This distillation of clean ancillae states, which are then used to implement the required gates for universality, is similar to the magic-state-distillation scheme by which Clifford group operations are used to distill almost noise-free single qubit $\pi/8$ ancillae from noisy ones [6]. For the model of computation based on braiding of Majorana fermions, distilled $|a_4\rangle$ states give the ability to perform single quibt $\pi/8$ gates, while distilled $|a_8\rangle$ states allow for the implementation of $CNOT$ gates [2]. The noise threshold for such distillation schemes, which assume that the distilling gates and operations are noise-free, is of the order of tens of percents which makes them attractive. But one can also ask the converse question: how noisy are these ancillae allowed to be before one can efficiently classically simulate the entire quantum computation? This question has been addressed in the case of noisy single-qubit magic states and noisy single-qubit gates [7, 8, 9].

In this paper we consider a similar question for computation using Majorana fermions. It is not hard to show (see Section 5) that if the noisy ancillae are convex mixtures of Gaussian fermionic states and the computation involves only non-interacting fermionic operations, one can still classically efficiently simulate such quantum computation. Hence we set out to develop a criterion that determines whether a state is a convex mixture of Gaussian fermionic states in Section 3. We find such a criterion in the form of a hierarchy of semidefinite programs, similar as for separable states [10]. Unfortunately, the computational effort for implementing this general criterion is too large to give decisive information for our problem of interest and we have recourse to an analytical approach for the noisy $|a_8\rangle$ ancilla in Section 4. Even though our general criterion is not immediately useful for the problem at hand, its generality and similarity with separability criteria makes it interesting in itself.

Our work is different from previous work on criteria which determine whether a fermionic state with a fixed number of fermions has a single Slater determinant, or whether a fermionic state can be written as a convex combination of states with single Slater determinant [11, 12]. The important distinction is that we fix only the parity of the fermionic state and not the number of fermions. Our goal is to extend the class of Gaussian fermionic states in a natural way, by considering states which can be written as convex combinations of Gaussian states. We call such states convex-Gaussian or 'having a Gaussian decomposition'. Even though physical states have a fixed number of fermions, Gaussian fermionic states are important approximations to physically non-trivial states, such as the superconducting BCS state. Our criterion thus intends to separate Gaussian states and convex combinations thereof, from fermionic states with a richer structure which cannot be simply viewed as states in which fermions are paired

§. Note that the question of having a Gaussian decomposition is also different from the question of *pairing* which is analyzed in [14]: Gaussian fermionic states can be paired while single Slater determinant states cannot. We hope that our results in separating convex-Gaussian states from fermionic states with a richer structure may lead to tools for understanding ground states of interacting fermion systems beyond mean-field theory.

2. Preliminaries: Fermionic Gaussian states

We consider a system of m fermionic modes, with corresponding creation $(a_k^\dagger)$ and annihilation (a_k) operators $(k = 1, \ldots, m)$, respecting the Fermi-Dirac anti-commutation rules, $\{a_j, a_k\} = 0$ and $\{a_j, a_k^\dagger\} = \delta_{jk}I$. For systems in which fermionic parity is conserved, it is more convenient to use the $2m$ Majorana fermion operators defined as $c_{2k-1} = a_k + a_k^\dagger$ and $c_{2k} = -i(a_k^\dagger - a_k)$. The operators $\{c_i\}_{i=1}^{2m}$ are Hermitian, traceless and form a Clifford algebra $\mathcal{C}_{2m}$ with $\{c_j, c_k\} = 2\delta_{jk}I$ ‖.

Any Hermitian operator $X \in \mathcal{C}_{2m}$ that can be written as the linear combination of products of an even number of Majorana operators is called an *even* operator, i.e.

$$X = \alpha_0 I + \sum_{k=1}^{m} i^k \sum_{1 \leq a_1 < a_2 < \ldots < a_{2k} \leq 2m} \alpha_{a_1, a_2, \ldots, a_{2k}} c_{a_1} c_{a_2} \ldots c_{a_{2k}}, \tag{1}$$

where the coefficients α_0 and $\alpha_{a_1, a_2, \ldots, a_{2k}}$ are real, for $(c_{a_1} c_{a_2} \ldots c_{a_{2k}})^\dagger = (-1)^k c_{a_1} c_{a_2} \ldots c_{a_{2k}}$. The parity of the number of fermions is conserved by the action of an even operator X as X commutes with the fermionic number-parity operator $C_{\text{all}} = i^m c_1 c_2 \ldots c_{2m} = \prod_{i=1}^{m}(I - 2a_i^\dagger a_i)$. Thus the projector onto a pure state $|\psi\rangle$ with *fixed* parity is an even fermionic operator, while $|\psi\rangle$ has eigenvalues $C_{\text{all}} = \pm 1$ depending on whether the parity of the number of fermions in $|\psi\rangle$ is odd or even.

Given an even state $\varrho \in \mathcal{C}_{2m}$, the correlation matrix M is a $2m \times 2m$ real, anti-symmetric matrix with elements

$$M_{ab} := \frac{i}{2}\text{Tr}(\varrho[c_a, c_b]), \quad \text{with} \quad a, b = 1, \ldots, 2m. \tag{2}$$

Real, anti-symmetric matrices such as M can be brought to block-diagonal form by a real orthogonal transformation $R \in SO(2m)$, i.e.

$$M = R \bigoplus_{j=1}^{m} \begin{pmatrix} 0 & \lambda_j \\ -\lambda_j & 0 \end{pmatrix} R^T. \tag{3}$$

Let us now define fermionic Gaussian states. Fermionic Gaussian states ϱ are even states of the form $\varrho = K \exp(-i\sum_{i \neq j} \beta_{ij} c_i c_j)$ with real anti-symmetric matrix β_{ij} and normalization K. Hence Gaussian fermionic states are ground-states and thermal

---

§ Any Gaussian fermionic state with an even number of fermions can be brought, by fermion-number preserving quadratic interactions, to a normal form which is a superposition of states with fixed pairs of fermions created from the vacuum, see e.g. [13].

‖ A system of m qubits is isomorphic with a system with m fermions and the unitary Jordan-Wigner transformation maps each Majorana fermion operator onto a nonlocal product of Pauli operators acting on m qubits.

states of non-interacting fermion systems. One can block-diagonalize β and re-express ϱ in *standard form* as

$$\varrho = \frac{1}{2^m} \prod_{k=1}^{m} \chi_k, \quad \text{where} \quad \chi_k = I + \mathrm{i}\lambda_k \tilde{c}_{2k-1}\tilde{c}_{2k}, \tag{4}$$

where $\tilde{c} = R^T c$ with R block-diagonalizing the matrix β_{ij}. The coefficients λ_j (which can be expressed in terms of the eigenvalues of β_{ij}) will lie in the interval $[-1, 1]$. For Gaussian pure states, $\lambda_j \in \{-1, 1\}$ so that $M^T M = I$, while for Gaussian mixed states $M^T M < I$. In the theory of Gaussian fermionic states, a special role is played by those unitary transformations which map Gaussian states onto Gaussian states. These are the transformations generated by Hamiltonians of non-interacting fermionic systems, i.e. Hamiltonians which are quadratic in Majorana fermion operators. In this paper we will refer to these unitary transformations as fermionic linear optics (FLO) transformations, as they, similarly as for bosonic linear optics transformations, have the property that

$$U c_i U^\dagger = \sum_j R_{ij} c_j, \tag{5}$$

where U is a FLO transformation and $R \in SO(2m)$. Hence the transformations which block-diagonalize M (or β) are FLO transformations. Note that C_{all} is invariant under any unitary FLO transformation U, as $U C_{\mathrm{all}} = C_{\mathrm{all}} U$.

It is clear from the standard form, Eq.(4), that a fermionic state is fully determined by its correlation matrix M. The expectation of higher order correlators for a Gaussian fermionic state are efficiently obtained by virtue of Wick's theorem

$$\mathrm{Tr}(\varrho\, c_{a_1} c_{a_2} \dots c_{a_{2k}}) = \mathrm{i}^{-k} \mathrm{Pf}(M|_{a_1,\dots,a_{2k}}), \tag{6}$$

where $M|_{a_1,\dots,a_{2p}}$ is the sub-matrix of M which contains only the elements M_{jk} with $j, k = a_1, \dots, a_{2p}$ and $\mathrm{Pf}(.)$ is the Pfaffian ¶.

Their efficient description (2) combined with the possibility to efficiently evaluate the expectation value of observables (6) makes fermionic Gaussian states a valuable tool for *approximating* ground-states, thermal states or dynamically-generated states using (generalized) Hartree-Fock methods of interacting fermion systems, see e.g. [15, 16, 13, 17]. Their concise representation together with Eq.(5) also allows for an efficient classical simulation of quantum computations that employ only FLO operations and are initialized with Gaussian states [18, 19, 20, 21].

3. Beyond Gaussian states: Gaussian decompositions

Given all the applications of Gaussian states, it is natural to try to enlarge this set of states to form a convex set, in analogy with extending product states to separable states. A first observation in this direction is that mixed Gaussian states

¶ Let $A = (a_{i,j})$ be a $2m \times 2m$ anti-symmetric matrix, then $\mathrm{Pf}(A) = \frac{1}{2^m m!} \sum_{\pi \in S_{2m}} \mathrm{sgn}(\pi) \prod_{i=1}^{m} a_{\pi(2i-1),\pi(2i)}$, where S_{2m} is the set of all permutations of $2m$ symbols. The Pfaffian is non-zero only for anti-symmetric matrix of even dimension.

are straightforward convex mixtures of pure Gaussian states. This is easily seen using the standard form (4), i.e., any Gaussian state can be written as $\varrho = \prod_{k=1}^{m} \chi_k / 2^m$ with $\chi_k = I + \mathrm{i}(2p_k - 1)c_{2k-1}c_{2k} = p_k(I + \mathrm{i}c_{2k-1}c_{2k}) + (1 - p_k)(I - \mathrm{i}c_{2k-1}c_{2k})$ where $0 \leq p_k \leq 1$ (by setting $p_k = 1/2$ we obtain the state $I/2^m$). However, the convex mixture of two Gaussian states is in general not a Gaussian state [22, 23]. This motivates the following definition

Definition 1 (Convex-Gaussian). *An even density matrix $\varrho \in \mathcal{C}_{2m}$ is convex-Gaussian iff it can be written as a convex combination of pure Gaussian states in $\mathcal{C}_{2m}$, i.e. $\varrho = \sum_i p_i \sigma_i$ where σ_i are pure Gaussian states, $p_i \geq 0$ and $\sum_i p_i = 1$.*

Remark 1: Since every even state in $\mathcal{C}_{2m}$ is defined by $2^{2m} - 1$ real coefficients, as is clear from Eq. (1) fixing the normalization $\alpha_0 = 1/2^m$, Carathéodory's theorem guarantees us that for any convex-Gaussian state there exists a Gaussian decomposition with at most 2^{2m} pure Gaussian states.

Remark 2: There is both similarity and difference between the set of separable states and the set of convex-Gaussian states. For example, for separable states local unitary transformations captured by $O(m)$ parameters relate the extreme points of the set, whereas for convex-Gaussian states the extreme points are the pure Gaussian states which are related by FLO transformations, captured by $O(m^2)$ parameters. Note that the pure states σ_i in decomposition of a convex-Gaussian state will typically have a correlation matrix $M(\sigma_i)$ which is block-diagonal in a different $\{c_i\}$ basis. If we were to restrict ourselves to convex combinations of Gaussian states which are in standard form using one and the same set $\{c_i\}$, we would obtain a convex set isomorphic to the set of separable states diagonal in the classical bit-string basis.

We will now prove that for systems of $1, 2$ or 3 fermionic modes, all pure even states are Gaussian (a different proof of this result can be found in [24]). From this observation it is then immediate that any even state $\varrho \in \mathcal{C}_{2m}$, with $m = 1, 2, 3$, is convex-Gaussian. In order to prove this result we start with a useful known Lemma, reproduced here for completeness, which shows that any fermionic even density matrix has a correlation matrix with eigenvalues in the complex $[-\mathrm{i}, \mathrm{i}]$ interval.

Lemma 1. *The antisymmetric correlation matrix M of any even density matrix $\varrho \in \mathcal{C}_{2m}$ has eigenvalues $\pm \mathrm{i}\lambda_k$ with $\lambda_k \in [-1, 1]$ and $k \in \{1, ..., m\}$. We have $M^T M \leq I$ with equality if and only if ϱ is a Gaussian pure state.*

Proof. We present two proofs. The correlation matrix of an even density matrix is an antisymmetric matrix, and hence it can be block-diagonalized as in Eq.(3). Its eigenvalues are thus $\pm \mathrm{i}\lambda_k$ and $\lambda_k \in [-1, 1]$, as from Eq.(2) λ_k is the expectation of the Hermitian operator $\mathrm{i}\tilde{c}_{2k-1}\tilde{c}_{2k}$ which has ± 1 eigenvalues. We can also prove the Lemma by using a dephasing approach introduced in [25]. We provide this alternative proof as it clearly shows that $M^T M = I$ iff ϱ is a pure Gaussian state, and because we later use elements of this proof in Proposition 1. Let $\varrho \in \mathcal{C}_{2m}$ be any density matrix and let

$\{c_i\}_{i=1}^{2m}$ be the set of Majorana fermions in which M is block-diagonal (if the choice for $\{c_i\}$ is not unique, pick one). Define the FLO transformation U_k, $k = 1, \ldots, m$ as

$$U_k c_{2k} U_k^\dagger = -c_{2k}, \; U_k c_{2k-1} U_k^\dagger = -c_{2k-1}, \; U_k c_i U_k^\dagger = c_i \; \forall i \neq 2k, 2k-1. \quad (7)$$

Note that the FLO transformation U_k induces an orthogonal transformation R_k that leaves the correlation matrix M of ϱ invariant. Let $\varrho_k = \frac{1}{2}(\varrho_{k-1} + U_k \varrho_{k-1} U_k^\dagger)$, with $\varrho_0 = \varrho$. The iteration in k has the effect of dephasing ϱ in the eigenbasis of each $\mathrm{i}c_{2k-1}c_{2k}$. Thus ϱ_m is a density matrix which contains only the mutually commuting operators $\mathrm{i}c_{2k-1}c_{2k}$, and hence its eigendecomposition involves the eigenstates of these operators which are Gaussian pure states. Note that ϱ_m is not necessarily a Gaussian state, but its eigenstates are Gaussian pure states, each of which has correlation matrix block-diagonal in the same basis. This implies that the correlation matrix M is that of a Gaussian mixed state. Note that the dephasing procedure can only increase the entropy of ϱ. Therefore, if $M^T M = I$ at the end of this procedure, then the state at the end of the procedure, ϱ_m, must be a pure Gaussian state. By the same token, ϱ at the beginning of the procedure (with the same $M^T M = I$) must be pure Gaussian. Thus $M^T M = I$ iff ϱ is a pure Gaussian state. □

Proposition 1. *Any even pure state $|\psi\rangle\langle\psi| \in \mathcal{C}_{2m}$ for $m = 1, 2, 3$ is Gaussian.*

Proof. The statement is trivial for $m = 1$. Consider $m = 2$ and observe that when we block-diagonalize its correlation matrix, any even pure state can written as some linear combination of I, quadratic terms $\mathrm{i}c_{2k-1}c_{2k}$ and C_{all}. The dephasing procedure in the proof of Lemma 1 leaves any such even density matrix invariant – remember that the operator C_{all} is invariant under FLO transformations. As the output is always convex-Gaussian, the input state was a pure Gaussian state. The proof for $m = 3$ follows the same structure as for $m = 2$, but employs the additional observation that $C_{\mathrm{all}}|\psi\rangle\langle\psi| = \pm|\psi\rangle\langle\psi|$ for even pure states. Any pure state density matrix $|\psi\rangle\langle\psi| \in \mathcal{C}_6$, when written in the basis in which its correlation matrix is block-diagonal, can be expressed as $|\psi\rangle\langle\psi| = \alpha I + \beta C_{\mathrm{all}} + \mathrm{i}\sum_k \gamma_k c_{2k-1}c_{2k} + \sum_{i<j<k<l} \eta_{ijkl} c_i c_j c_k c_l$. The condition that $C_{\mathrm{all}}|\psi\rangle\langle\psi| = \pm|\psi\rangle\langle\psi|$ implies that the quartic terms only have paired correlators $c_{2k-1}c_{2k}$: this is because C_{all} interchanges the quartic and quadratic terms. Thus $|\psi\rangle\langle\psi|$ has quartic terms which only involve commuting operators $c_{2k-1}c_{2k}$. As argued in the proof of Lemma 1, $|\psi\rangle\langle\psi|$ is then a convex mixture of pure Gaussian states, and the result follows. □

As for separable states [26, 27, 28], the volume of convex-Gaussian states is non-zero for any m: any state $\varrho \in \mathcal{C}_{2m}$ is convex-Gaussian if it is "close enough" to the maximally mixed state $I/2^m$, which is Gaussian. The following Lemma proves this, using arguments similar as those in Ref. [27]:

Theorem 1. *For every even state $\varrho \in \mathcal{C}_{2m}$ there exists a sufficiently small $\epsilon > 0$ such that $\varrho_\epsilon = \epsilon\varrho + (1 - \epsilon)I/2^m$ is convex-Gaussian.*

Proof. Consider the set $\{\sigma(\vec{\lambda}, \pi)\}$ of pure Gaussian states, with each $\sigma(\vec{\lambda}, \pi) \in \mathcal{C}_{2m}$ defined as

$$\sigma(\vec{\lambda}, \pi) = \frac{1}{2^m} \prod_{k=1}^{m} (I + \mathrm{i}\lambda_k c_{\pi(2k-1)} c_{\pi(2k)}), \tag{8}$$

where $\vec{\lambda} \in \{-1, 1\}^m$ and $\pi \in S_{2m}^+$, with S_{2m}^+ the set of permutations with positive signature (these correspond to $SO(2m)$ rotations of the correlation matrix, i.e., FLO operations). There are $(2m)!/m!$ pure states in this set and we will show that they form an over-complete basis for $\mathcal{C}_{2m}$. We prove this by showing that *any* Hermitian ϱ can be written as

$$\varrho = \sum_{(\vec{\lambda}, pi)} w_{(\vec{\lambda}, \pi)} \sigma(\vec{\lambda}, \pi) - c\frac{I}{2^m}, \tag{9}$$

where $w_{(\vec{\lambda}, \pi)} \geq 0$ and $c \geq 0$. Furthermore, we can write

$$\frac{I}{2^m} = \frac{m!}{(2m)!} \sum_{\vec{\lambda}, \pi} \sigma(\vec{\lambda}, \pi).$$

If we find the decomposition in Eq. (9) with a certain c (which one could try to minimize in our construction of the decomposition), it then follows immediately that $\frac{1}{1+c}\varrho + \frac{c}{1+c}\frac{I}{2^m}$ is convex-Gaussian. Taking $\epsilon = \frac{1}{1+c}$ we obtain our result. One could in principle upper bound c as a function of m. Eq. (9) can be proved by considering how to express a single correlator $\alpha_{a_1, \ldots, a_{2k}} c_{a_1} c_{a_2} \ldots c_{a_{2k}}$ in terms of Gaussian states and I. Let us call the subset $\{a_1, \ldots, a_{2k}\} = S$ and the coefficient $\alpha_{a_1, \ldots, a_{2k}} = \alpha$. Let $C_S = c_{a_1} c_{a_2} \ldots c_{a_{2k}}$. We will use Gaussian mixed states $\xi(\vec{\lambda}, \pi) = \frac{1}{2^m} \prod_{k=1}^{m}(I + \mathrm{i}\lambda_k c_{\pi(2k-1)} c_{\pi(2k)})$ where $\lambda_i \in [-1, 1]$; such states can in turn be expressed as convex mixtures of pure states $\sigma(\vec{\lambda}, \pi)$ for $\lambda_i \in \{-1, 1\}$ as in Eq. (8). We have

$$\mathrm{i}^k \mathrm{Tr}\, C_S \xi(\vec{\lambda}, \pi) = \Pi_{k:\pi(2k-1), \pi(2k) \in S} \lambda_k. \tag{10}$$

By choosing $\lambda_k \in \{-1, 1, 0\}$ we can make sure that (i) $|\alpha|\xi(\vec{\lambda}, \pi) = w_{\vec{\lambda}, \pi}\xi(\vec{\lambda}, \pi)$ has the correct expectation α for the correlator C_S (note that the sign of λ_k can be chosen to fit the sign of α) and (ii) $\xi(\vec{\lambda}, \pi)$ has *no higher-order correlators* (by choosing some $\lambda_k = 0$). The state $\xi(\vec{\lambda}, \pi)$ will then also have *lower-order* non-zero correlators $C_{S'}$ for $S' \subseteq S$, including $S' = \emptyset$ corresponding to I. Thus we repeat the procedure with these various lower-order correlators, i.e. we represent them as a Gaussian mixed state $\xi(\vec{\lambda}, \pi)$ plus additional correlators corresponding to subsets of S'. Proceeding this way, we remove all correlators except for I and end up expressing $\alpha C_S = \sum_{\vec{\lambda}, \pi} w_{(\vec{\lambda}, \pi)} \xi(\vec{\lambda}, \pi) - \beta I$ for $\beta = 2^{-m} \sum_{\lambda, \pi} w_{\lambda, \pi}$. This procedure is probably far from optimal, i.e. gives rise to a large c. One can optimize this by applying the procedure to a density matrix ϱ from which we repeatedly take out Gaussian mixed states, i.e. $\varrho \to \varrho - w\xi$ which remove the current highest-order correlator and the Gaussian state ξ is chosen to be the one with minimum (but non-negative) weight $\mathrm{Tr}\, w\xi$. $\square$

Now that we have established the essential features of the set of convex-Gaussian states, the natural question that follows is how to determine whether a state has a decomposition in terms of Gaussian pure states. As for separability, there are two sides to this question. One is to find a Gaussian decomposition, a problem which is likely, as in the entanglement case, to be computationally hard in general. The reverse question is to find a criterion which establishes that a state is not convex-Gaussian. Note that the goal is to find a criterion which acts linearly on the pure Gaussian states, so that it can naturally be extended to convex mixtures thereof. The Hermitian operator $\Lambda = \sum_{i=1}^{2m} c_i \otimes c_i \in \mathcal{C}_{2m} \otimes \mathcal{C}_{2m}$, introduced in Ref. [19], will be useful in this context as it has been shown to lead to a necessary and sufficient criteria for a state to be Gaussian:

Lemma 2 (Bravyi [19]). *An even state $\varrho \in \mathcal{C}_{2m}$ is Gaussian iff $[\Lambda, \varrho \otimes \varrho] = 0$.*

The operator Λ has the important property of being invariant under $U \otimes U$ where U is any FLO transformation. The action of Λ on $\varrho \otimes \varrho$ can be appreciated by considering the trace norm $||.||_1$ of the positive operator $\Lambda(\varrho \otimes \varrho)\Lambda$:

$$
\begin{aligned}
||\Lambda(\varrho \otimes \varrho)\Lambda||_1 &= \sum_{a,b=1}^{2m} \mathrm{Tr}[(c_a \otimes c_a)(\varrho \otimes \varrho)(c_b \otimes c_b)] \\
&= 2m - \sum_{a \neq b} (\mathrm{Tr}\, ic_a c_b \varrho)^2 \\
&= 2m - \sum_{a,b} (M_{ab})^2 = 2m - \mathrm{Tr}\, M^T M,
\end{aligned}
\tag{11}
$$

where M is the correlation matrix of the state ϱ. For a pure Gaussian state $\varrho = \sigma$, we have $M^T M = I$ implying that $\Lambda(\sigma \otimes \sigma) = 0$. For a mixed Gaussian state or non-Gaussian state $M^T M < I$, see Lemma 1, and hence $||\Lambda(\varrho \otimes \varrho)\Lambda||_1 > 0$. These observations are collected in the following corollary.

Corollary 1. *For an even state $\varrho \in \mathcal{C}_{2m}$, $\Lambda(\varrho \otimes \varrho) = 0$ iff ϱ is a pure Gaussian state.*

Corollary 1 says that the state of two copies of pure Gaussian states is contained in the null-space of the operator Λ. In Lemma 4 in the Appendix A we will prove that the null-space of the operator Λ is contained in the symmetric subspace $\mathbf{Sym}^2(\mathbb{C}^{2^m})$ spanned by vectors $|\psi\rangle$ which are invariant under the SWAP operator P, i.e. $|\psi\rangle = P|\psi\rangle$. In particular, the null-space of Λ is spanned by states $|\psi, \psi\rangle$ where ψ is Gaussian, while the symmetric subspace is spanned by $|\phi, \phi\rangle$ for any ϕ. We will call the null-space of Λ the Gaussian-symmetric subspace. As Λ is a sum of mutually commuting Hermitian operators $c_i \otimes c_i$ with $\mu_i = \pm 1$ eigenvalues, the projectors on the eigenstates are $P_{\vec{\mu}} = \frac{1}{2^{2m}} \Pi_{i=1}^{2m}(I + \mu_i c_i \otimes c_i)$ with eigenvalue $\sum_{i=1}^{2m} \mu_i$ of Λ. Hence the Gaussian-symmetric subspace is spanned by $\binom{2m}{m}$ orthogonal eigenvectors $P_{\vec{\mu}}$ with the property that $\sum_i \mu_i = 0$. Clearly, the dimension of the Gaussian-symmetric subspace $\binom{2m}{m}$ is smaller than the dimension of the symmetric subspace $\mathbf{Sym}^2(\mathbb{C}^{2^m})$ which is $\binom{2^m+1}{2}$ for any $m \geq 1$.

In [10, 29] the authors established a series of tests for separability based on the existence of a symmetric extension of any separable state. The usefulness of these tests

relies on the fact that they correspond to semi-definite programs which for small numbers of extensions can be implemented numerically. Furthermore, these tests are complete, in the sense that an entangled state does not have a symmetric extension to an arbitrary number of parties in the extension. Here we formulate a similar series of extension tests which are all passed by convex-Gaussian states, but non-convex-Gaussian states fail in some of them. Our criterion is based on the following simple observation: Let a density matrix $\varrho \in \mathcal{C}_{2m}$ be convex-Gaussian, i.e. we can write $\varrho = \sum_i p_i \sigma_i$ with σ_i pure Gaussian states, then there exists a symmetric extension $\varrho_{ext} \in \mathcal{C}_{2m}^{\otimes n}$, namely $\varrho_{ext} = \sum_i p_i \sigma_i^{\otimes n}$, which is annihilated by Λ acting on any pair of tensor-factors, and $\mathrm{Tr}_{2,\dots,n-1} \varrho_{ext} = \varrho$. This immediately leads to the following feasibility semi-definite program:

Program 1. *Input:* $\varrho \in \mathcal{C}_{2m}$ *and an integer* $n \geq 2$
            Body: *Is there a* $\varrho_{\mathrm{ext}} \in \mathcal{C}_{2m}^{\otimes n}$
            s.t. $\mathrm{Tr}_{2,\dots,n} \varrho_{ext} = \varrho$
                  $\mathrm{Tr}\, \varrho_{\mathrm{ext}} = 1$
                  $\Lambda^{k,l} \varrho_{ext} = 0, \forall k \neq l$
                  $\varrho_{\mathrm{ext}} \geq 0$
        Output: `yes` *(provide* ϱ_{ext}*) or* `no`

As there exists an isomorphism between $\mathcal{C}_{2m}^{\otimes n}$ and $\mathcal{C}_{2mn}$ (see the explicit map in [19] for $\mathcal{C}_{2m} \otimes \mathcal{C}_{2m}$ and $\mathcal{C}_{4m}$), one could alternatively express program 1 as an extension of ϱ to a physical system with $2mn$ Majorana fermions (see [30]).

Note that in program 1 we do not need to enforce any permutation or Bose-symmetry on the extension [+] because of the following. By Lemma 4 in Appendix A, the null-space of $\Lambda_{k,l}$ is spanned by vectors $|\psi, \psi\rangle_{k,l}$ where $|\psi\rangle$ is any pure Gaussian state. Thus the intersection of null-spaces of all $\Lambda_{k,l}$ is spanned by vectors $|\psi^{\otimes n}\rangle$ where ψ is a pure Gaussian state, which are vectors in the symmetric subspace of n parties. As ϱ_{ext} lies in this null-space, it will thus be Bose-symmetric [31], i.e. $\pi \varrho_{ext} = \varrho_{ext}$ where π is any permutation in S_n.

It is easy to see that any state ϱ has a Bose-symmetric extension, hence the stronger constraint imposed by Λ is crucial. We say that a even state ϱ has a n-Gaussian-symmetric extension if Program 1 returns `yes` for inputs ϱ and n. An explicit construction of the SDP for the case $n = 2$ is given in Appendix B, and some numerical results are discussed in the following section. Clearly all convex-Gaussian states have n-Gaussian-symmetric extensions for all n. Here we will prove that if a state has a n-Gaussian-symmetric extension for all n, then its distance to the set of convex-Gaussian states converges to zero.

Theorem 2. *If an even state* $\varrho \in \mathcal{C}_{2m}$ *has a n-Gaussian-symmetric extension for all n, then there exists a sequence of convex-Gaussian states* $\omega_1, \omega_2, \dots \in \mathcal{C}_{2m}$ *such that* $\lim_{n \to \infty} ||\varrho - \omega_n||_1 = 0$.

Proof. To prove that we will invoke the quantum de Finetti theorem [31]. Let $\varrho_{\mathrm{ext}}^n \geq 0$

[+] Adding the permutation-symmetry would of course leave the program in SDP form.

be the extension of ϱ to $\mathcal{C}_{2m}^{\otimes n}$ such that $\Lambda^{k,l}\varrho_{\text{ext}}^n = 0$ and $\text{Tr}_{2,\ldots,n}\varrho_{\text{ext}}^n = \varrho$. Using Lemma 4 in the appendix this shows that ϱ_{ext}^n is Bose-symmetric. Let $\varrho_{1,2}^n$ be the reduced density matrix for the first two tensor factors, i.e. $\varrho_{1,2}^n = \text{Tr}_{3,\ldots,n}\varrho_{ext}^n$. Then Theorem II.8 in [31] tells us that there exists a probability distribution $\{\gamma_a(n)\}$ and states $\{\tau_a(n)\} \subset \mathcal{C}_{2m}$ such that

$$||\varrho_{1,2}^n - \sum_a \gamma_a(n)\tau_a(n) \otimes \tau_a(n)||_1 \leq \epsilon_m(n), \tag{12}$$

with $\epsilon_m(n) = \frac{4\cdot 2^m}{n}$. Since the trace-norm can not increase by taking the partial trace, then

$$||\varrho - \sum_a \gamma_a(n)\tau_a(n)||_1 \leq \epsilon_m(n). \tag{13}$$

Therefore, in the limit of $n \to \infty$ we have that $\sum_a \gamma_a(n)\tau_a(n)$ converges to ϱ.

On the other hand, we have

$$|| \Lambda \sum_a \gamma_a(n)\tau_a(n) \otimes \tau_a(n)\Lambda ||_1 = || \Lambda(\varrho_{1,2}^n - \sum_a \gamma_a(n)\tau_a(n) \otimes \tau_a(n))\Lambda ||_1$$

$$\leq ||\Lambda||_1^2 \epsilon_m(n) \equiv \tilde{\epsilon}_m(n), \tag{14}$$

with $||\Lambda||_1^2 = 4(m+1)^2\binom{2m}{m+1}^2$. For fixed m, in the limit $n \to \infty$ the upper-bound $\tilde{\epsilon}_m(n) \to 0$. Corollary 1 then implies that for each a either $\gamma_a(n) \to 0$ or $\tau_a(n)$ converges to a pure Gaussian state. That means that there exists a series of pure Gaussian states $\upsilon_a(1), \upsilon_a(2), \ldots \in \mathcal{C}_{2m}$ such that $\lim_{n\to\infty} ||\tau_a(n) - \upsilon_a(n)||_1 = 0$.

Defining the convex-Gaussian states $\omega_n = \sum_a \gamma_a(n)\upsilon_a(n)$, from Eq.(13) we have:

$$\epsilon_m(n) \geq ||\varrho - \omega_n + \omega_n - \sum_a \gamma_a(n)\tau_a(n)||_1 \tag{15}$$

$$\geq \left| \ ||\varrho - \omega_n||_1 - ||\omega_n - \sum_a \gamma_a(n)\tau_a(n)||_1 \ \right|. \tag{16}$$

Where we used the reversed triangle inequality. Therefore:

$$||\varrho - \omega_n||_1 \leq \epsilon_m(n) + ||\omega_n - \sum_a \gamma_a(n)\tau_a(n)||_1 \tag{17}$$

$$\leq \epsilon_m(n) + \sum_a \gamma_a(n)||\upsilon_a(n) - \tau_a(n)||_1. \tag{18}$$

The claimed result then follows by noting that both $\epsilon_m(n)$ and $||\upsilon_a(n) - \tau_a(n)||_1$ go to zero for $n \to \infty$. $\qquad\square$

Remark 3: A quantitative version of this result will be presented somewhere else [30].

Note that convex-Gaussian states always have a symmetric extension which is separable in relation to all tensor-factors. This property can be used to provide an alternative formulation of the necessary and sufficient criterion for a state to be convex-Gaussian:

Proposition 2. *A state $\varrho \in \mathcal{C}_{2m}$ is convex-Gaussian iff there exists an extension $\varrho_{\mathrm{ext}} \in \mathcal{C}_{2m} \otimes \mathcal{C}_{2m}$ that is a feasible solution to Program 1 —input ϱ and $n = 2$— with the additional constraint that ϱ_{ext} is separable between the tensor-factors.*

Proof. As before one direction is immediate. For the other direction, assume that there exists a state $\varrho_{\mathrm{ext}} \in \mathcal{C}_{2m} \otimes \mathcal{C}_{2m}$ which is separable, i.e. it is of the form $\varrho_{\mathrm{ext}} = \sum_i p_i \tau_i \otimes \varsigma_i$, with $\{\tau_i\}$ and $\{\varsigma_i\}$ sets of density matrices in $\mathcal{C}_{2m}$ and $\{p_i\}$ a probability distribution. From the constraint $\Lambda \varrho_{\mathrm{ext}} = 0$, it follows that

$$
\begin{aligned}
0 &= \mathrm{Tr}\Lambda \left(\sum_i p_i \tau_i \otimes \varsigma_i \right) \Lambda \\
&= 2m - \sum_i p_i \sum_{a \neq b} (\mathrm{Tr}\ \mathrm{i} c_a c_b \tau_i)(\mathrm{Tr}\ \mathrm{i} c_a c_b \varsigma_i) \\
&= 2m - \sum_i p_i \mathrm{Tr} M^T(\tau_i) M(\varsigma_i).
\end{aligned}
\tag{19}
$$

Where the notation $M(\varrho)$ represents the correlation matrix of the state ϱ.

Using the triangle and Cauchy-Schwartz inequalities, we have

$$
\begin{aligned}
2m &= |\sum_i p_i \mathrm{Tr} M^T(\tau_i) M(\varsigma_i)| \\
&\leq \sum_i p_i \sqrt{\mathrm{Tr} M^T(\tau_i) M(\tau_i)} \sqrt{\mathrm{Tr} M^T(\varsigma_i) M(\varsigma_i)}.
\end{aligned}
\tag{20}
$$

From Lemma 1 it follows that $\mathrm{Tr} M^T M = 2 \sum_{i=1}^{m} |\lambda_i|^2 \leq 2m$ with equality iff M is the correlation matrix of a pure Gaussian state. In order for equality to hold in Eq. (20), each τ_i (and ς_i) must thus be a pure Gaussian state and therefore $\varrho = \sum_i p_i \tau_i$ is convex-Gaussian. □

Including this extra separability constraint in Program 1 breaks its SDP structure – checking separability can in itself be cast as an SDP [29], but this would give a nested SDP structure to the program deciding if a state is convex-Gaussian. A direct semi-definite relaxation of this criteria is obtained by employing the partial-transposition test for separability [32, 33], leading to the following SDP:

Program 2. *Input:* $\quad \varrho \in \mathcal{C}_{2m}$
$\qquad\qquad$ *Body:* $\quad$ *Is there $\varrho_{\mathrm{ext}} \in \mathcal{C}_{2m} \otimes \mathcal{C}_{2m}$*
$\qquad\qquad\qquad$ *s.t.* $\quad \mathrm{Tr}_2 \varrho_{ext} = \varrho$
$\qquad\qquad\qquad\qquad\quad \mathrm{Tr} \varrho_{\mathrm{ext}} = 1$
$\qquad\qquad\qquad\qquad\quad \Lambda \varrho_{ext} = 0$
$\qquad\qquad\qquad\qquad\quad \varrho_{\mathrm{ext}} \geq 0$
$\qquad\qquad\qquad\qquad\quad \varrho_{\mathrm{ext}}^{T_1} \geq 0$
$\qquad\qquad$ *Output:* $\quad$ yes *(provide ϱ_{ext})* or no

Here T_1 is the transposition map on the first tensor-factor. As for the previous program, a negative answer means that the state is not convex-Gaussian. For the converse, it is likely that the PPT criterion together with the constraint that the extension lives in the

Gaussian-symmetric subspace is not sufficient to enforce separability (e.g., there exists symmetric bound-entangled states [34]), hence a positive answer is non-decisive, but we leave this as an open question.

4. Applications: depolarized $|a_8\rangle$

As mentioned in the introduction, one way to turn $\nu = 5/2$ topological quantum computation into an universal quantum computation scheme, is to assume that one has access to the auxiliary states $|a_4\rangle \in \mathcal{C}_4$ and $|a_8\rangle \in \mathcal{C}_8$, as shown in [2]. In the present section we want to assess the amount of noise that can be added to these extra resources before they turn convex-Gaussian. From Proposition 1 we know that any pure state in $\mathcal{C}_4$ is Gaussian, and therefore any noisy version of $|a_4\rangle$ is convex-Gaussian. We thus concentrate on the state $|a_8\rangle$ when undergoing depolarization. We consider the state

$$\varrho_{a_8}(p) = (1 - p)|a_8\rangle\langle a_8| + pI/16, \tag{21}$$

with $0 \leq p \leq 1$ and

$$|a_8\rangle\langle a_8| = \frac{1}{16}(I + S_1)(I + S_2)(I + S_3)(I + Q), \tag{22}$$

with $S_1 = -c_1 c_2 c_5 c_6$, $S_2 = -c_2 c_3 c_6 c_7$, $S_3 = -c_1 c_2 c_3 c_4$ and $Q = c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8$. Ref. [2] has shown that $\varrho_{a_8}(p)$ can be distilled for $p < 40\%$ (corresponding to the parameter ϵ_8 defined in Ref. [2] equal to 0.38). We would like to determine the noise threshold p_* such that $\varrho_{a_8}(p \geq p_*)$ is convex-Gaussian. Note that ϱ_{a_8} is Gaussian only for $p = 1$. The results in this Section are summarized in Fig.1.
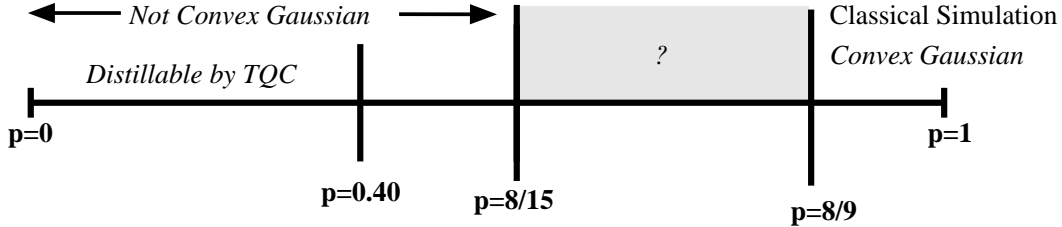

Figure 1. Properties of the state $\varrho_{a_8}(p) = (1 - p)|a_8\rangle\langle a_8| + pI/16$. Our results show that p_*, the noise threshold above which $\varrho_{a_8}(p)$ is convex-Gaussian is in the interval $[\frac{8}{15}, \frac{8}{9}]$, depicted in grey. In this interval we do not yet know whether ϱ_{a_8} is convex-Gaussian. For $p < 0.40$, Ref. [2] shows that ϱ_{a_8} can be distilled by noiseless braiding operations to enable topological quantum computation (TQC) with Clifford group elements (for quantum universality one also needs a sufficiently low-noise $|a_4\rangle$ ancilla). Our results from the SDP on the existence of a Gaussian-symmetric extension of $\varrho_{a_8}(p)$ for $p \geq 0.25$ do not provide additional information beyond these analytical results.

In order to give a lower-bound on p_* we implemented the SDP Program 1 for fixed $n = 2$ (see Appendix B) with the aid of the CVXOPT library for Sage [35]. The numerical results indicate that $p_* \geq 0.25$, as it is always possible to find a Gaussian-symmetric extension for $\varrho_{a_8}(p)$ with $n = 2$ for noise rates above this value. Our implementation of the feasibility SDP takes approximately one day for each value of p in a computer with

$2.3GHz$ processor, and takes about $30GB$ of RAM memory. The implementation of the SDP with an additional PPT condition on the extension is likely to provide stronger results, but it is more computationally intensive. Given these limitations, we provide an alternative analysis of the properties of $\varrho_{a_8}(p)$ using the notion of witnesses: Hermitian operators which have expectation values in a restricted range (e. g. non-negative for all Gaussian states) whereas expectation values on non-Gaussian states can extend beyond this range (e.g. be negative). The existence of such witness operators is guaranteed by the fact that they represent separating hyperplanes separating the convex-Gaussian states from all even Hermitian operators in $\mathcal{C}_{2m}$ (in addition, similar as in [29], witnesses could be constructed based on a negative output of feasibility SDP).

Clearly, such Hermitian witness operators, say W, should include terms which are quartic or higher-weight correlators, as the expectation value of quadratic Hamiltonians only depends on the correlation matrix of a state. For $\varrho_{a_8}(p)$ the obvious choice for such a witness operator is $W = |a_8\rangle\langle a_8|$, for which $\operatorname{Tr} W \varrho_{a_8}(p) = 1 - \frac{15p}{16}$. Let us understand how we can bound $\min_{\psi_g} \operatorname{Tr} W |\psi_g\rangle\langle\psi_g| = |\langle\psi_g|a_8\rangle|^2$ where ψ_g is any Gaussian pure state. We will use the fact that the correlation matrix of $|a_8\rangle$ is the null matrix, i.e. for all Majorana operators c_i, c_j, $\operatorname{Tr} c_i c_j |a_8\rangle\langle a_8| = 0$, which follows directly from Eq. (22). We will now prove that $|\langle\psi_g|a_8\rangle|^2 \leq \frac{1}{2}$ which shows that for $p < \frac{8}{15} \approx 0.53$, the state $\varrho_{a_8}(p)$ is not convex-Gaussian. The following proposition proves our claimed bound and can be intuitively understood by interpreting the state $|a_8\rangle$ as a maximally entangled state while Gaussian states are product states:

Proposition 3. *For all Gaussian pure states $|\psi_g\rangle$, we have $|\langle\psi_g|a_8\rangle|^2 \leq \frac{1}{2}$.*

Proof. Let c_1 and c_2, $c_1 c_2 = -c_2 c_1$, be two arbitrary Majorana fermion operators, from a complete set $\{c_{2k-1}, c_{2k}\}_{k=1}^4$ (note the $SO(8)$ freedom in choosing these). Let $|x\rangle$ denote an eigenvector of the mutually commuting operators $ic_1 c_2$, $ic_{2k-1} c_{2k}$ for $k = 2, \ldots 4$ where the bits (0 or 1) of x label the eigenvalues (resp. $+1$ and -1) of these operators. The Gaussian states $|x\rangle$ form a basis for the 4-fermion (or 4-qubit) space, hence we can write $|a_8\rangle = \sum_{x\in\{0,1\}^4} \alpha_x |x\rangle$ with $\sum_x |\alpha_x|^2 = 1$. Then

$$\operatorname{Tr} ic_1 c_2 |a_8\rangle\langle a_8| = \sum_{y\in\{0,1\}^3} |\alpha_{0y}|^2 - \sum_{y\in\{0,1\}^3} |\alpha_{1y}|^2 = 0. \tag{23}$$

This, together with normalization, implies that $\sum_y |\alpha_{0y}|^2 = \sum_y |\alpha_{1y}|^2 = \frac{1}{2}$, hence for all y, $|\alpha_{0y}|^2$ and $|\alpha_{1y}|^2$ are less than or equal to $1/2$. $\square$

A tighter bound than the one in Proposition 3 cannot be excluded if one uses further properties of the state $|a_8\rangle$ – such tighter bound would lead to a reduction of the grey area in Fig.1.

To give an upper-bound on p_* we construct explicit Gaussian decompositions of $\varrho_{a_8}(p)$ for large values of p. To do this we consider a subset of the convex-Gaussian states that share some key properties with $\varrho_{a_8}(p)$, namely: (i) zero correlation matrix, and (ii) only a small fraction of all possible correlators has non-zero coefficients.

To exploit these symmetries we define three types of states:

$$\varrho_i(\lambda) = \frac{1}{2} \left(\varrho_{M_i(\lambda)} + \varrho_{M_i(-\lambda)} \right), \tag{24}$$

where $\varrho_{M_i(\lambda)}$, for $i = 1, 2, 3$, is the Gaussian state generated by the correlation matrix $M_i(\lambda)$, with $\lambda \in [-1, 1]^4$, and $M_i(\lambda)$ assumes one of the three following forms:

$$M_1(\lambda) = \bigoplus_{i=1}^{4} \begin{pmatrix} 0 & \lambda_i \\ -\lambda_i & 0 \end{pmatrix},$$

$$M_2(\lambda) = \bigoplus_{i=1}^{2} \begin{pmatrix} 0 & 0 & \lambda_i & 0 \\ 0 & 0 & 0 & \lambda_{i+1} \\ -\lambda_i & 0 & 0 & 0 \\ 0 & -\lambda_{i+1} & 0 & 0 \end{pmatrix},$$

$$M_3(\lambda) = \bigoplus_{i=1}^{2} \begin{pmatrix} 0 & 0 & 0 & \lambda_i \\ 0 & 0 & \lambda_{i+1} & 0 \\ 0 & -\lambda_{i+1} & 0 & 0 \\ -\lambda_i & 0 & 0 & 0 \end{pmatrix}.$$

By construction, these states are convex-Gaussian, have null correlation matrix, and any convex combination of them has an expansion in terms of Majorana operators with non-vanishing coefficients only on the same correlators as $\varrho_{a_8}(p)$. The aim is to find for which p's it is possible to decompose $\varrho_{a_8}(p)$ as a convex sum of these type of convex-Gaussian states.

In order to describe the convex hull of these states, first note that M_2 and M_3 are related to M_1 by permutations (different choices of pairings):

$$M_2(\lambda) = (P_{12} \oplus P_{12}) M_1(\lambda) (P_{12} \oplus P_{12})^T,$$
$$M_3(\lambda) = (P_{13} \oplus P_{13}) M_1(\lambda) (P_{13} \oplus P_{13})^T,$$

where

$$P_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, P_{13} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{25}$$

Given that the transformation connecting the correlation matrices is formed by the direct sum of identical permutations, this transformation is in $SO(8)$ – one always gets the signature of the permutation squared, and therefore the corresponding determinant is always 1. Rotations in SO of the correlation matrix induce unitary transformations on the level of the states [19]: $P_{12} \mapsto U_2$, $P_{13} \mapsto U_3$. Bearing in mind this connection among the three classes of states above, we now determine the extreme points of the set of type 1 states.

Lemma 3 (Extreme points for type 1 states). *Let $\overline{\mathcal{S}}_1 = \mathrm{conv}\{\varrho_1(\lambda)|\lambda \in [-1, 1]^4\}$. Then the extreme points of $\overline{\mathcal{S}}_1$ are given by*

$$\phi_1(x) \doteq \frac{1}{2} \left(|x\rangle\langle x| + |\neg x\rangle\langle\neg x| \right),$$

with $x \in \{0,1\}^4$ and $\neg x$ is the bitwise negation of x.

Proof. It follows immediately from the expansion of the state $\varrho_1(\lambda)$:

$$\varrho_1(\lambda) = \frac{1}{2^5} \sum_{x \in \{0,1\}^4} \left[\prod_{k=1}^4 (1 - (-1)^{x_k} \lambda_k) + \prod_{k=1}^4 (1 - (-1)^{x_k}(-\lambda_k)) \right] |x\rangle\langle x|$$

$$= \frac{1}{2^5} \sum_{x \in \{0,1\}^4} \prod_{k=1}^4 (1 - (-1)^{x_k} \lambda_k) \left(|x\rangle\langle x| + |\neg x\rangle\langle \neg x| \right) \qquad (26)$$

$$= \frac{1}{2^4} \sum_{x \in \{0,1\}^4} \prod_{k=1}^4 (1 - (-1)^{x_k} \lambda_k) \, \phi_1(x).$$

$\square$

Defining in a similar fashion $\overline{\mathcal{S}}_2$, $\overline{\mathcal{S}}_3$, $\phi_2(x)$ and $\phi_3(x)$, we can then define the convex hull of any convex combination of the three types of states as $\overline{\mathcal{S}} = \mathrm{conv}\{\overline{\mathcal{S}}_1, \overline{\mathcal{S}}_2, \overline{\mathcal{S}}_3\}$. More explicitly:

$$\overline{\mathcal{S}} = \left\{ \sum_{i=1}^3 \sum_{x=0}^7 \gamma_i(x) \phi_i(x) \, \middle| \, \gamma_i(x) \geq 0, \sum_{i=1}^3 \sum_{x=0}^7 \gamma_i(x) = 1 \right\}, \qquad (27)$$

where the summation in x is to be carried out over its binary expansion in three bits.

The problem now reduces to determine for which values of $p \in [0,1]$ the linear system $\varrho_{a_8}(p) = \sum_{i=1}^3 \sum_{x=0}^7 \gamma_i(x) \phi_i(x)$, with $\{\gamma_i\}$ a probability distribution, has a solution. Simple inspection shows that such Gaussian decomposition is always possible whenever $p \geq 8/9 \approx 0.89$, which is then an upper-bound on p_*.

5. Discussion: Classical simulation of fermionic quantum computation

Contrary to bosonic linear optics, quantum computations based on fermionic linear optics (FLO) can be efficiently simulated by a classical computer even when augmented by measurements of fermionic number operators [18, 20, 19]. The simulation relies on the following facts:

(i) efficient encoding of Gaussian states – a Gaussian state of $2m$ Majorana fermions is fully described by its correlation matrix M, with $O(m^2)$ elements.

(ii) FLO transformations map Gaussian states onto Gaussian states, with efficient update rule – every FLO transformation $V \in \mathcal{C}_{2m}$ induces a rotation $R \in SO(2m)$ on the Majorana operators space, $V c_i V^\dagger = \sum_{j=1}^{2m} R_{ij} c_j$. This, in turn, induces the map $M \mapsto RMR^T$ on the $2m \times 2m$ correlation matrix, and this update can be evaluated in $O(m^3)$ steps.

(iii) efficient read-out of measurement probability distributions – via Wick's theorem (6) the probability of measuring the population in fermionic modes can be done efficiently, as the Pfaffian of a $2m \times 2m$ matrix can be evaluated in $O(m^3)$. Furthermore, number operator measurements project Gaussian states onto Gaussian states.

With these three ingredients, the evolution of any initial Gaussian state can be efficiently followed by a classical computer at any time in the computation, and the output distribution can be exactly evaluated. In references [19, 21] the allowed transformations in (ii) were extended to noisy *Gaussian maps*. These are completely-positive channels, not necessarily FLO unitaries, that map Gaussian states onto Gaussian states, and as such still admit efficient classical simulation.

Our results imply that if $p \geq 8/9$, $\varrho_{a_8}(p)$ is convex-Gaussian and this allows for the classical simulation of the computation as follows. Given a noise strength $p \geq 8/9$, one finds the decomposition of $\varrho_{a_8}(p)$ in $\overline{\mathcal{S}}$, by solving the linear system $\varrho_{a_8}(p) = \sum_{i=1}^{3} \sum_{x=0}^{7} \gamma_i(x)\phi_i(x)$ – this has to be done only once for a fixed p. As each $\phi_i(x)$ is in itself a convex sum of two pure Gaussian states, this leads to a decomposition of $\varrho_{a_8}(p)$ in terms of at most 48 pure Gaussian states. Let p_i be the probability associated with the i-th pure Gaussian state in such decomposition. Then, whenever a state $\varrho_{a_8}(p)$ is requested in the computation, one samples from $\{p_i\}$ and chooses the corresponding pure Gaussian state. From this point onwards, the simulation follows the scheme summarized in (i), (ii) and (iii) above.

The results in Fig. 1 leave some gaps in our understanding, in particular about the precise value of p_*. In order to improve the lower bounds on p_* one could consider distillation processes beyond the restricted set of braiding operations, but that still map Gaussian states onto Gaussian states, leaving thus the set of convex-Gaussian states unchanged. The distillation protocol of depolarized GHZ_4 states, which are isomorphic to $\varrho_{a_8}(p)$, proposed by Dür and Cirac at first sight suggests that our classical simulation threshold is tight, as it can distill a perfect GHZ_4 provided that $p < 8/9$. Nevertheless, their protocol uses non-FLO operations, as it assumes that one can locally create the GHZ_4 and uses distilled 2-qubits maximally entangled pairs for distribution. The protocol devised by Murao *et al.* in [36], directly distills GHZ_4 from depolarized copies of it for $p < 0.7328$. Despite the fact that this direct approach seems more related to our question, it employs gates that are not immediately translated into braiding operations or even to FLO transformations. Although the choice to distill via braiding operations is physically motivated – due to their topological protection–, a different distillation threshold from FLO operations would suggest that either Bravyi's distillation protocol can be improved to higher depolarizing noise rates, or that there exists a 'transition zone' in which the computation by braiding of Majorana fermions is neither quantumly-universal nor can be efficiently simulated classically.

Acknowledgements

Appendix A. Symmetric versus Gaussian-symmetric Subspace

Inspired by [37], we define a 'FLO twirl' as the map $\mathcal{S}(\varrho) = \frac{1}{\text{Vol}(U)} \int_{FLO} dU U \otimes U \varrho U^\dagger \otimes U^\dagger$ where $\int_{FLO} dU$ is defined by taking the Haar measure over the real orthogonal matrices R induced by U. The map $\mathcal{S}(\varrho)$ is normalized such that it is trace-preserving.

Lemma 4. *The projector onto the null-space of* $\Lambda = \sum_i c_i \otimes c_i$ *is* $\Pi_{\Lambda=0} = \binom{2m}{m} \mathcal{S}(|0,0\rangle\langle0,0|)$ *where* $|0\rangle$ *is a (Gaussian) vacuum state with respect to some set of annihilation operators* a_i. *Thus the states* $|\psi,\psi\rangle$ *where* ψ *is a pure fermionic Gaussian state span the null-space of* Λ *which implies that the null-space of* Λ *is a subspace of the symmetric subspace.*

Proof. In order to prove that $\Pi_{\Lambda=0} = \binom{2m}{m} \mathcal{S}(|0,0\rangle\langle0,0|)$, we note that both the l.h.s. and the r.h.s. are $U \otimes U$-invariant where U is any FLO transformation. Thus instead of considering whether $\text{Tr}X\Pi_{\Lambda=0} = \text{Tr}(X\binom{2m}{m}\mathcal{S}(|0,0\rangle\langle0,0|))$ for any X, we can just consider the trace with respect to invariant objects $\mathcal{S}(X)$. It can be shown that Λ^i for $i = 0,1,2,\ldots,2m$ (and linear combinations thereof) are the only invariants under the group $U \otimes U$ where U is FLO transformation [38]. Clearly, $\text{Tr}\Lambda^i\binom{2m}{m}\mathcal{S}(|0,0\rangle\langle0,0|) = 0 = \text{Tr}\Lambda^i\Pi_{\Lambda=0}$ for all $i \neq 0$ while $\text{Tr}\Pi_{\Lambda=0} = \binom{2m}{m}$ fixes the overall prefactor. Having established the form of the projector, it follows directly that the states $|\psi,\psi\rangle$ for any Gaussian ψ span the null-space (Assume this is false and hence a state in the null-space $|\chi\rangle = |\chi_{in}\rangle + |\chi_{out}\rangle$ where $|\chi_{in}\rangle$ is in the span of $|\psi,\psi\rangle$ while $|\chi_{out}\rangle$ is w.l.o.g. orthogonal to any $|\psi,\psi\rangle$. We have $\Pi_{\Lambda=0}|\chi\rangle = |\chi\rangle$ while $\binom{2m}{m}\mathcal{S}(|0,0\rangle\langle0,0|)|\chi\rangle = |\chi_{in}\rangle$ arriving at a contradiction.) As $|\psi,\psi\rangle$ for Gaussian pure states ψ span the null-space, and $P|\psi,\psi\rangle = |\psi,\psi\rangle$ with P the SWAP operator, the null-space is a subspace of the symmetric subspace. $\square$

Appendix B. SDP to detect non-convex-Gaussian states

Recall the series of tests constructed to detect that if a state $\varrho \in \mathcal{C}_{2m}$ is not convex-Gaussian:

> Input: $\varrho \in \mathcal{C}_{2m}$ and an integer $n \geq 2$
> Body: Is there $\varrho_{\text{ext}} \in \mathcal{C}_{2m}^{\otimes n}$
>   s.t. $\pi \varrho_{\text{ext}} \pi^\dagger = \varrho_{\text{ext}}, \forall \pi \in S_n$
> $\text{Tr}_{2,\ldots,n}\varrho_{ext} = \varrho$
> $\text{Tr}\varrho_{\text{ext}} = 1$
> $\Lambda^{k,l}\varrho_{ext} = 0, \forall k \neq l$
> $\varrho_{\text{ext}} \geq 0$
> Output: yes (provide ϱ_{ext}) or `no`

Note that we have explicitly kept the permutation-symmetry constraint in this program.

In this Appendix we convert this problem into a feasibility semi-definite programming problem. To do that we must show that the above problem can be cast as the standard form of SDP's, namely:

$$\begin{aligned}
\text{minimize} \quad & \mathbf{c}^T\mathbf{x} \\
\text{subject to} \quad & F_0 + \textstyle\sum_i x_i F_i \geq 0 \\
& A\mathbf{x} = \mathbf{b}
\end{aligned}$$

where $\mathbf{x} \in \mathbb{R}^d$ is the unknown vector to be optimized over, $\mathbf{c}$ is a given vector in $\mathbb{R}^d$, and $\{F_i\}_{i=0,\ldots,d}$ are given symmetric matrices. For the equality constraint, $A \in \mathbb{R}^{p \times d}$ is a given matrix, with $\text{rank}(A) = p$, and $\mathbf{b} \in \mathbb{R}^p$. The restriction on the rank of A demands that the linear system has at least one solution, and all the rows are linearly independent.

The first step is to associate an Hermitian operator M_j with each term $i^k c_{a_1} c_{a_2} \ldots c_{a_{2k}}$ in the expression (1). The set $\{M_j\}_{0 \leq j \leq 2^{2m-1}-1}$ spans all the even Hermitian operators of $\mathcal{C}_{2m}$. Then any state $\varrho \in \mathcal{C}_{2m}$ can be written as:

$$\varrho = \sum_{k=0}^{2^{2m-1}-1} \alpha_k M_k, \tag{B.1}$$

and we choose $M_0 = I$.

For definiteness, in what follows we restrict to the case $n = 2$. Extensions to larger n's follow the same structure and can be immediately constructed. That said, a general extension on $\mathcal{C}_{2m} \otimes \mathcal{C}_{2m}$ can be written as:

$$\varrho_{\text{ext}} = \sum_{i,j=0}^{2^{2m-1}-1} \beta_{ij} M_i \otimes M_j, \tag{B.2}$$

with the coefficients $\beta_{ij} \in \mathbb{R}$ to be fixed by the constraints of our problem. The symmetry constraint can be taken directly into the parametrization of ϱ_{ext} by imposing:

$$\varrho_{\text{ext}} = \sum_{i=0}^{2^{2m-1}-1} \beta_{ii} M_i \otimes M_i + \sum_{0 \leq i < j \leq 2^{2m-1}-1} \beta_{ij}(M_i \otimes M_j + M_j \otimes M_i). \tag{B.3}$$

At this point, the initially 2^{4m-2} coefficients of ϱ_{ext} are reduced to $2^{2m-2}(1 + 2^{2m-1})$.

The imposition that $\text{Tr}_1(\varrho_{\text{ext}}) = \varrho$ further demands:

$$2^m \sum_{j=0}^{2^{2m-1}-1} \beta_{0,j} M_j = \sum_{j=0}^{2^{2m-1}-1} \alpha_j M_j. \tag{B.4}$$

Therefore, $\beta_{0,j} = \alpha_j/2^m$. In this way, further 2^{2m-1} coefficients are determined, and thus remain $2^{2m-3}(2^{2m} - 2)$ free parameters. Note that the normalization of ϱ_{ext} is already guaranteed as long as $\text{Tr}(\varrho) = \alpha_0 = 1$.

The question whether there exists an assignment of the remaining free coefficients respecting the last two constraints can be immediately posed as a feasibility SDP:

$$\begin{aligned}
\text{minimize} \quad & 0 \\
\text{subject to} \quad & \varrho_{\text{ext}} \geq 0 \\
& \Lambda \varrho_{\text{ext}} = 0.
\end{aligned}$$

Forgetting for the moment that the correlators are in general complex, a direct correspondence with the SDP standard form can be done as follows:

$$F_0 \to \beta_{0,0} M_0 \otimes M_0 + \sum_{j=1}^{2^{2m-1}-1} \beta_{0,j} (M_0 \otimes M_j + M_j \otimes M_0) \tag{B.5}$$

$$F_i \to \begin{cases} M_j \otimes M_j, \ 1 \le j \le 2^{2m-1} - 1 \\ M_j \otimes M_k + M_k \otimes M_j, \ 1 \le j < k \le 2^{2m-1} - 1 \end{cases}, \tag{B.6}$$

with $\mathbf{x} = (\{\beta_{j,j}\}_{1 \le j \le 2^{2m-1}-1}, \{\beta_{j,k}\}_{1 \le j < k \le 2^{2m-1}-1})^T$.

The equality constraint then reads:

$$\sum_{i=1}^{2^{2m-3}(2^{2m}-2)} x_i \Lambda F_i = -\Lambda F_0. \tag{B.7}$$

This can be cast in the form $A\mathbf{x} = \mathbf{b}$, by writing $A = ([\Lambda F_i]_{1 \le i \le 2^{2m-3}(2^{2m}-2)})$, and $\mathbf{b} = -[\Lambda F_0]$. The notation $[G]$ means a column matrix constructed by stacking each column of G below each other.

To finish the construction we must take into account that we are possibly dealing with complex values. To do that we employ the following well-known result.

Lemma 5. *Let* $Z = Z^\dagger \in \mathbb{C}^{d \times d}$. *Then* $Z \ge 0$ *iff* $\mathcal{T}(Z) = \begin{pmatrix} Re(Z) & -Im(Z) \\ Im(Z) & Re(Z) \end{pmatrix}$.

Proof. ($\Rightarrow$) Let $\mathbf{z} = \mathbf{x} + i\mathbf{y}$ be an eigenvector of Z with eigenvalue λ. Then it is easy to see that $(\mathbf{x}, \mathbf{y})^T$ is an eigenvector of $\mathcal{T}(Z)$ with eigenvalue λ.

($\Leftarrow$) By the same token, let $(\mathbf{x}, \mathbf{y})$ be an eigenvector of $\mathcal{T}(Z)$ with eigenvalue λ. Then $\mathbf{z} = \mathbf{x} + i\mathbf{y}$ is an eigenvector of Z with eigenvalue λ. $\quad\square$

The final dimension of each F_i is then $2^{2m+1} \times 2^{2m+1}$, and there are $2^{2m-3}(2^{2m} - 2)$ of such matrices. For the equality constraint we write

$$\begin{pmatrix} Re(A) \\ Im(A) \end{pmatrix} \mathbf{x} = \begin{pmatrix} Re(\mathbf{b}) \\ Im(\mathbf{b}) \end{pmatrix}. \tag{B.8}$$

The final matrix $(Re(A), Im(A))^T$ has dimension $2^{4m+1} \times 2^{2m-3}(2^{2m} - 2)$. Most likely the rank of this matrix is not equal to the number of rows. Therefore, before plugging it into the SDP one must evaluate its reduced-row form (echelon form), and remove the all-zero lines.

If one wishes to include the PPT test, as in Program 2, this can be done by rewriting the two positivity constraints, $\varrho_{\text{ext}} \ge 0$ and $\varrho_{\text{ext}}^{T_1} \ge 0$, as a single one, $\varrho_{\text{ext}} \oplus \varrho_{\text{ext}}^{T_1} \ge 0$. One thus need to map each complex F_i in the positivity constraint to $F_i' = F_i \oplus F_i^{T_1}$. The final dimension of each real F_i' is then $2^{2m+2} \times 2^{2m+2}$. The equality constraint remains the same.

References

[1] J. Alicea. New directions in the pursuit of Majorana fermions in solid state systems. *Rep. Prog. Phys.*, 75(7):076501, 2012.

[2] S. Bravyi. Universal quantum computation with the $\nu=5/2$ fractional quantum Hall state. *Phys. Rev. A*, 73:042313, 2006.

[3] A. Ahlbrecht, L. Georgiev, and R. F. Werner. Implementation of clifford gates in the ising-anyon topological quantum computer. *Phys. Rev. A*, 79:032311, Mar 2009.

[4] S. B. Bravyi and A. Y. Kitaev. Fermionic quantum computation. *Annals of Physics*, 298(1):210 – 226, 2002.

[5] C. W. J. Beenakker, D. P. DiVincenzo, C. Emary, and M. Kindermann. Charge detection enables free-electron quantum computation. *Phys. Rev. Lett.*, 93:020501, Jul 2004.

[6] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, 2005.

[7] B. W. Reichardt. Improved magic states distillation for quantum universality. *Quantum Inf. Process.*, 4:251, 2005.

[8] H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver, and F. Unger. New limits on fault-tolerant quantum computation. In *Foundations of Computer Science, 2006. FOCS'06. 47th Annual IEEE Symposium on*, pages 411–419. IEEE, 2006.

[9] W. van Dam and M. Howard. Tight Noise Thresholds for Quantum Computation with Perfect Stabilizer Operations. *Phys. Rev. Lett.*, 103:170504, 2009.

[10] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing Separable and Entangled States. *Phys. Rev. Lett.*, 88(18):187904, May 2002.

[11] J. Schliemann, D. Loss, and A. H. MacDonald. Double-occupancy errors, adiabaticity, and entanglement of spin qubits in quantum dots. *Phys. Rev. B*, 63(8):085311, 2001.

[12] K. Eckert, J. Schliemann, D. Bruß, and M. Lewenstein. Quantum Correlations in Systems of Indistinguishable Particles. *Ann. Phys.*, 299:88–127, 2002.

[13] C. Kraus. *A Quantum Information Perspective of Fermionic Quantum Many-Body Systems*. PhD thesis, TU Muenchen, 2009.

[14] C. V. Kraus, M. M. Wolf, J. I. Cirac, and G. Giedke. Pairing in fermionic systems: A quantum-information perspective. *Phys. Rev. A*, 79(1):012306, January 2009.

[15] V. Bach, E. Lieb, and J. Solovej. Generalized Hartree-Fock theory and the Hubbard model. *Journal of Statistical Physics*, 76:3–89, 1994. 10.1007/BF02188656.

[16] C. V. Kraus and J. I. Cirac. Generalized Hartree-Fock theory for interacting fermions in lattices: numerical methods. *New Journal of Physics*, 12(11):113004, 2010.

[17] C. Kittel. *Quantum Theory of Solids*. Wiley, New York, 1963.

[18] B. M. Terhal and D. P. DiVincenzo. Classical simulation of noninteracting-fermion quantum circuits. *Phys. Rev. A*, 65:032325, Mar 2002.

[19] S. Bravyi. Lagrangian representation for fermionic linear optics. *Quant. Inf. Comp.*, 5:216–238, 2005.

[20] R. Jozsa and A. Miyake. Matchgates and classical simulation of quantum circuits. *Proc. R. Soc. A*, 464:3089 – 3106, 2008.

[21] S. Bravyi and R. König. Classical simulation of dissipative fermionic linear optics. *Quant. Info. Comp.*, 12:0925–0943, 2012.

[22] J. C. Wolfe. Free states and automorphisms of the Clifford algebra. *Commun. Math. Phys.*, 45:53, 1975.

[23] M. Fannes and R. Alicki. *Quantum Dynamical Systems*. Oxford University Press, 2001.

[24] S. Bravyi. Classical capacity of fermionic product channels. *eprint arXiv:quant-ph/0507282*, 2005.

[25] S. Wehner and A. Winter. Higher entropic uncertainty relations for anti-commuting observables. *J. Math. Phys.*, 49(6):062105, June 2008.

[26] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable

states. *Phys. Rev. A*, 58:883–892, Aug 1998.

[27] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of Very Noisy Mixed States and Implications for NMR Quantum Computing. *Phys. Rev. Lett.*, 83:1054–1057, August 1999.

[28] L. Gurvits and H. Barnum. Better bound on the exponent of the radius of the multipartite separable ball. *Phys. Rev. A*, 72(3):032322, September 2005.

[29] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Complete family of separability criteria. *Phys. Rev. A*, 69(2):022308, February 2004.

[30] F. de Melo, B. M. Terhal, and A. Vershynina. To be published.

[31] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-Half Quantum de Finetti Theorems. *Comm. Math. Phys.*, 273:473–498, 2007.

[32] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, Aug 1996.

[33] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1 – 8, 1996.

[34] G. Tóth and O. Gühne. Entanglement and permutational symmetry. *Phys. Rev. Lett.*, 102:170503, May 2009.

[35] W. A. Stein et al. *Sage Mathematics Software (Version 5.0)*. The Sage Development Team, 2012. http://www.sagemath.org.

[36] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight. Multiparticle entanglement purification protocols. *Phys. Rev. A*, 57:R4075–R4078, Jun 1998.

[37] K. G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *Phys. Rev. A*, 64:062307, 2001.

[38] Volkher Scholz, 2012. Private Communication. Similar as in [37], one has to find the commutant algebra of the group UU for an FLO transformation U using group-representation theory, see e.g.[39, 40]. A more direct proof will be presented in [30].

[39] R. Goodman and R. N. Wallach. *Symmetry, Representations, and Invariants*. Springer, 2009.

[40] H. Wenzl. On Centralizer Algebras for Spin Representations. *Comm. Math. Phys.*, 314:243–263, 2012.