arXiv:2504.15356v1 [quant-ph] 21 Apr 2025

Efficiently learning fermionic unitaries with few non-Gaussian gates

Sharoon Austin,[1,2] Mauro E.S. Morales,[1] and Alexey Gorshkov[1,2]

[1]*Joint Center for Quantum Information and Computer Science, NIST/University of Maryland, College Park, MD, 20742, USA*

[2]*Joint Quantum Institute, NIST/University of Maryland, College Park, MD, 20742, USA*

(Dated: April 23, 2025)

Fermionic Gaussian unitaries are known to be efficiently learnable and simulatable. In this paper, we present a learning algorithm that learns an n-mode circuit containing t parity-preserving non-Gaussian gates. While circuits with $t = \text{poly}(n)$ are unlikely to be efficiently learnable, for constant t, we present a polynomial-time algorithm for learning the description of the unknown fermionic circuit within a small diamond-distance error. Building on work that studies the state-learning version of this problem, our approach relies on learning approximate Gaussian unitaries that transform the circuit into one that acts non-trivially only on a constant number of Majorana operators. Our result also holds for the case where we have a qubit implementation of the fermionic unitary.

I. INTRODUCTION

The task of learning unknown quantum unitaries is fundamental to quantum information science [1–3]. This task is important for the development of quantum algorithms and the characterization of quantum devices. However, learning unitaries of arbitrary gate complexity is exponentially hard [4, 5], making it crucial to identify classes of unitaries that can be learned efficiently. Moreover, practical quantum computation requires verification and validation of quantum circuits with bounded gate complexity. From an experimental standpoint, benchmarking and calibrating quantum devices can be thought of as a learning problem. Previous works have focused on providing learning algorithms in various scenarios, including circuits with Clifford unitaries together with a constant number of T gates [6], unitaries with a constant number of two-qubit gates [7], and quantum circuits of constant depth [8].

This work focuses on learning fermionic unitaries [9, 10]. We consider two cases. The first case, which we refer to as the *fermionic implementation*, is where the unknown unitary is implemented on fermionic modes. To define our learning problem, it is important to distinguish Gaussian and non-Gaussian unitaries. In the fermionic implementation, we will restrict Gaussian unitaries to be parity-preserving, which corresponds to time evolution under quadratic fermionic Hamiltonians, allowing for both hopping and pairing terms [10, 11]. The learning algorithm in this case must use input states that can be efficiently prepared on a fermionic quantum computer using parity-preserving gates. The second case, which we refer to as the *qubit implementation*, is where the unknown unitary is implemented on a chain of qubits (which can be related to a chain of fermionic modes via the Jordan-Wigner transformation). In this qubit implementation, the allowed Gaussian unitaries are not required to preserve parity. They are generated by nearest-neighbor matchgates (which are parity-preserving and map to fermionic Gaussian gates under the Jordan-Wigner transformation) and X_1, the Pauli X matrix on the first qubit [12, 13].

It is well-established that Gaussian unitaries in both implementations can be learned efficiently [14, 15]. Throughout this work, we refer to quantum circuits on qubits defined using the Jordan-Wigner mapping as fermionic circuits. We will also refer to unitaries defined by Majorana operators acting on fermions as fermionic circuits. Augmenting fermionic Gaussian circuits with non-Gaussian gates enables universal quantum computation. In the qubit implementation, adding SWAP, controlled-Z, or controlled-phase gates enables universal quantum computation [16]. In the fermionic implementation, adding $\exp(i\pi\gamma_1\gamma_2\gamma_3\gamma_4/4)$ enables universal quantum computation [11].

This raises the question whether, in both implementatons, unitaries composed of fermionic Gaussian unitaries and a constant number of non-Gaussian gates are efficiently learnable. In Ref. [17], it was shown that quantum states produced by such unitaries are efficiently learnable, leaving open whether the unitaries themselves are efficiently learnable. In this work, we solve this problem by providing an efficient algorithm to learn such unitaries in both fermionic and qubit implementations. Our result may have applications in fermionic quantum devices, such as those proposed in Refs. [18–20] and also complements the classical simulation algorithm for this class of circuits [21–23]. Moreover, previous work has shown that there is an efficient algorithm to learn fermionic unitaries in any finite level of the matchgate hierarchy [15]. However, we show that fermionic unitaries composed of just two non-Gaussian gates and a Gaussian gate, where the non-Gaussian gates belong to the third level and the Gaussian gate belongs to the second level [24], do not belong to any finite level of the matchgate hierarchy.

Our learning algorithm is based on the decomposition result in Ref. [17] that shows that the unknown unitary acts like a Gaussian unitary on all but a constant number of Majorana operators. We show that such Majorana operators can be efficiently learned by measuring expectation values of constant-weight fermionic observables on states prepared using the unknown unitary (e.g., using shadow tomography [25, 26]). This information can be used to form a circuit that acts trivially on a large number of Majorana operators. Finally, we construct and learn a circuit that acts on a constant number of modes or qubits either through brute force [1] or by estimating the expectation values of Pauli observables on states prepared by the circuit using shadow tomography [27, 28].

The remainder of the paper is organized as follows. In Sec. II, we define fermionic unitaries, their relation to matchgates, and the computational complexity of such circuits. In Sec. III, we define the learning problem and present the main result. In Sec. IV, we present the technical lemmas on which the learning algorithm is based. In Sec. V, we study how the fermionic unitaries in this work relate to unitaries in the matchgate hierarchy and show that, generally, fermionic unitaries with just two non-Gaussian unitaries do not belong to any finite level of the matchgate hierarchy. In the Appendices, we present details omitted from the main text.

II. REVIEW: FERMIONIC UNITARIES AND MATCHGATES

In this section, we present a review of fermionic unitaries, matchgates, and known results regarding their computational complexity. For a fermionic system, the modes labeled $1,\dots,n$ are defined by the creation and annihilation operators a_i and $a_i^\dagger$, respectively, acting on the Fock-space state $|z_1,\cdots,z_n\rangle$ as follows [11]:

$$\begin{aligned} &a_j\,|z_1,\dots,z_{j-1},1,z_{j+1},\dots,z_n\rangle \\ &=(-1)^{\sum_{k=1}^{j-1} z_k}\,|z_1,\dots,z_{j-1},0,z_{j+1},\dots,z_n\rangle\,, \qquad (1)\\ &a_j\,|z_1,\dots,z_{j-1},0,z_{j+1},\dots,z_n\rangle = 0, \qquad (2)\end{aligned}$$

where $z_i=0,1$. These operators satisfy the anticommutation relations $\{a_i,a_j\}=0$ and $\{a_i,a_j^\dagger\}=\delta_{ij}I$ for all i,j. We can define $2n$ Majorana operators γ_i as follows:

$$\gamma_{2i-1} = a_i + a_i^\dagger, \qquad (3)$$

$$\gamma_{2i} = -i(a_i - a_i^\dagger), \qquad (4)$$

where $i\in[n]$. Here γ_i obey the anticommutation relation $\{\gamma_i,\gamma_j\}=0$ for $i\neq j$, and $\gamma_i^2=I$. The n-mode Fock space can be associated with the n-qubit Hilbert Space [11]. Moreover, the system of n qubits can be mapped to $2n$ Majorana operators γ_i ($i=1,\dots,2n$) via the Jordan-Wigner transformation defined as

$$\gamma_{2k-1} = \left(\prod_{i=1}^{k-1} Z_i\right) X_k, \qquad (5)$$

$$\gamma_{2k} = \left(\prod_{i=1}^{k-1} Z_i\right) Y_k, \qquad (6)$$

Here X_k, Y_k, and Z_k are Pauli matrices acting on qubit k, and this mapping ensures that the Majorana operators satisfy the correct anticommutation relations. In this mapping, the Fock-space state

$$|z_1 z_2 \dots z_n\rangle \qquad (7)$$

of n fermionic modes is exactly identified with the computational basis state on n qubits, where an empty fermionic mode ($z_i=0$) corresponds to a qubit in computational basis state $|z_i=0\rangle$, while a filled fermionic mode ($z_i=1$) corresponds to a qubit in computational basis state $|z_i=1\rangle$ [11].

We define a fermionic Gaussian unitary G from its action on γ_i as follows:

$$G^\dagger\gamma_i G = \sum_k O_{ik}\gamma_k, \qquad (8)$$

where $O\in \mathrm{O}(2n)$. Matchgates are parity-preserving two-qubit unitaries of the form

$$G(A,B) = \begin{pmatrix} A_{11} & 0 & 0 & A_{12} \\ 0 & B_{11} & B_{12} & 0 \\ 0 & B_{21} & B_{22} & 0 \\ A_{21} & 0 & 0 & A_{21} \end{pmatrix}, \qquad (9)$$

$$\det(A)=\det(B)=\pm 1, \qquad (10)$$

where the matrix is written in the $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ basis, and where A and B are complex unitary matrices. To relate matchgates and fermionic Gaussian unitaries, we first note that nearest-neighbor matchgate circuits (on a one-dimensional chain of qubits) can be generated from nearest-neighbor two-qubit gates of the form $\exp(i\theta X\otimes X)$ and single-qubit Z rotations $\exp(i\theta Z\otimes I)$, $\exp(i\theta I\otimes Z)$. This definition shows that fermionic Gaussian unitaries generated by $G(\theta)_{ii+1}$, where $G(\theta)_{ij}=\exp(\theta\gamma_i\gamma_j)$ with $i\neq j$, and nearest-neighbor matchgate circuits are equivalent since $iX_jX_{j+1}=\gamma_{2j}\gamma_{2j+1}$ and $iZ_j=\gamma_{2j-1}\gamma_{2j}$. Here, unitaries $G(\theta)_{ij}$ act on γ_k as follows:

$$G(\theta)_{ij}^\dagger\gamma_k G(\theta)_{ij} = \cos(2\theta)\gamma_i + \sin(2\theta)\gamma_j \quad k=i, \qquad (11)$$

$$G(\theta)_{ij}^\dagger\gamma_k G(\theta)_{ij} = -\sin(2\theta)\gamma_i + \cos(2\theta)\gamma_j \quad k=j, \qquad (12)$$

$$G(\theta)_{ij}^\dagger\gamma_k G(\theta)_{ij} = \gamma_k \quad k\notin\{i,j\}. \qquad (13)$$

This shows that the nearest-neighbor $X\otimes X$ rotations and single-qubit Z rotations mentioned earlier can be implemented as fermionic Gaussian unitaries $G(\theta)_{ii+1}$ corresponding to Givens rotations spanned by γ_i, γ_{i+1} for $i\in[2n-1]$, generating all rotations in $\mathrm{SO}(2n)$. Adding the operator X_1 can then be used to extend to rotations in $\mathrm{O}(2n)$ [13]. From here on, we will use fermionic Gaussian unitaries and nearest-neighbor matchgate circuits interchangeably.

Valiant showed that quantum circuits composed of nearest-neighbor matchgates on a one-dimensional chain of qubits can be classically simulated [12]. However, if these gates are allowed to act on arbitrary qubit pairs (or equivalently if the SWAP gate is added to the gate set), such circuits can perform universal quantum computation [29]. This result was strengthened in Ref. [9] to show that circuits with nearest-neighbor and next-nearest-neighbor matchgate circuits are quantum universal. Moreover, adding any one of the following gates to the gate set also gives quantum universality: controlled-Z, controlled-phase [16], or $\exp(i\pi Z_iZ_j/4)$ [11]. These gates can be written as non-Gaussian unitaries. For example, the gate $\exp(i\pi Z_iZ_j/4)$ can be written as $\exp(i\pi\gamma_{2i-1}\gamma_{2i}\gamma_{2j-1}\gamma_{2j}/4)$.

We now define the metric used to quantify the precision of our learning algorithm. The diamond-norm distance between

any two quantum channels $\mathcal{E}_1$ and $\mathcal{E}_2$ can be defined as follows:

$$\mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2) = \frac{1}{2} \max_\rho \|(\mathcal{E}_1 \otimes I)\rho - (\mathcal{E}_2 \otimes I)\rho\|_1, \quad (14)$$

where ρ is a density matrix on $2n$ qubits, and $\|.\|_1$ is the trace norm. Moreover, we denote the spectral norm (the largest singular value) as $\|.\|$ and denote the Frobenius norm as $\|.\|_2$, which is defined as follows:

$$\|A\|_2 = \sqrt{\mathrm{tr}[A^\dagger A]}. \quad (15)$$

We use α_x to denote the Hamming weight of the bit-string x. The projection on state $|z\rangle$ for the ith qubit is denoted by $\Pi_z^{(i)} = (1+(-1)^z Z_i)/2$. We denote single-qubit Paulis acting on the qubit labeled i as P_i, where $P \in \{X, Y, Z\}$.

III. RESULT

We now define our learning problem as follows. We are given black-box access to the unitary U_t with the following promise on its form:

$$U_t = G_t K_t \cdots G_1 K_1 G_0, \quad (16)$$

where G_i is a Gaussian unitary defined in Eq. (8), K_i is a non-Gaussian unitary generated by an even-weight product of Majorana operators with weight up to κ, and t is a constant. We take κ to be a constant because such unitaries (e.g., $\kappa = 4$ in Ref. [11]) suffice to implement universal quantum computation. We consider two cases. The first case is where U_t is implemented on n fermionic modes. Here, we specialize to parity-preserving Gaussian unitaries G_i. These unitaries correspond to orthogonal matrices in $\mathrm{SO}(2n)$ instead of $\mathrm{O}(2n)$ and can be implemented as time evolution under quadratic fermionic Hamiltonians composed of both hopping and pairing terms [10, 11]. The learning algorithm in this case must use input states that can be efficiently prepared on a fermionic quantum computer (i.e., states that can be obtained from parity-preserving unitaries). We refer to this setting as the *fermionic implementation*. The second case is where U_t is implemented on n qubits. Here, we consider Gaussian unitaries G_i that correspond to orthogonal matrices in $\mathrm{O}(2n)$ and are implemented as matchgates. We refer to this setting as the *qubit implementation*. We aim to find a description of a unitary channel $\mathcal{U}_t^{(\ell)}$ such that $\mathcal{D}_\diamond(\mathcal{U}_t^{(\ell)}, \mathcal{U}_t) \leq \epsilon$, where $\mathcal{U}_t$ is the quantum channel corresponding to U_t. The main result of this work is presented as follows.

Theorem 1. For a unitary U_t promised to have the form in Eq. (16), there is a learning algorithm that accesses the unitary $O(\mathrm{poly}(n, \epsilon^{-1}, \log \delta^{-1}))$ number of times and uses $O(\mathrm{poly}(n, \epsilon^{-1}, \log \delta^{-1}))$ classical processing time to produce a description of the quantum channel $\mathcal{U}_t^{(\ell)}$ such that $\mathcal{D}_\diamond(\mathcal{U}_t^{(\ell)}, \mathcal{U}_t) \leq \epsilon$, where $\mathcal{U}_t$ is the quantum channel corresponding to U_t, with probability $\geq 1-\delta$. The input states used in the algorithm have $O(\mathrm{poly}(n))$ gate complexity. Moreover, the channel description can be used to approximately implement the unitary U_t using $2m+1$ ancillary modes for the fermionic implementation or $2m$ ancillary qubits for the qubit implementation, where $m = M/2$ and $M = \kappa t$.

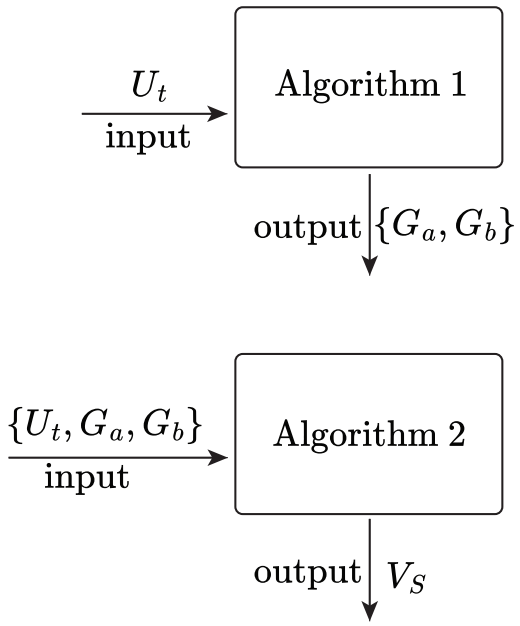

FIG. 1. The learning algorithm for the fermionic implementation. Algorithm 1 uses access to U_t to produce a description of Gaussian unitaries G_a and G_b. Algorithm 2 uses access to U_t, along with G_a and G_b, to learn the unitary $W_t = G_a^\dagger U_t G_b^\dagger$ on a constant number of modes and produce a description of the unitary V_S also suppported on a constant number of modes. The output of the learning algorithm is a description of the unitary $U_t^{(\ell)} = G_a V_S G_b$. For the qubit implementation, the learning algorithm is the same except that Algorithm 2 learns a description of $\bar{W}_t = \bar{U}_d^\dagger W_t \bar{U}_d$ instead of W_t.

Details of the learning guarantees are provided in Lemma 23 for the fermionic implementation and Lemma 22 for the qubit implementation. We remark that, since the resource requirements scale as $O(\mathrm{poly}(\log \delta^{-1}))$ in the failure probability δ, we can choose an exponentially small failure probability and still have an efficient algorithm. We remark that we need additional ancilla modes (qubits) to implement the learned unitary because our algorithm involves learning a constant-sized quantum channel that is only approximately unitary, and therefore needs additional ancilla qubits to be implemented as a unitary via Stinespring dilation [30].

As shown in Fig. 1, our learning algorithm can be described in two steps. In the first step, we perform a tomography scheme that constructs the matrix $c^{(1)} \in \mathbb{R}^{2n \times 2n}$ defined by

$$c_{jk}^{(1)} := \frac{1}{d} \mathrm{tr}\left[U_t^\dagger \gamma_k U_t \gamma_j\right], \quad (17)$$

where $d = 2^n$. The matrix element $c_{jk}^{(1)}$ can be described as follows. We evolve γ_k under U_t and then compute its overlap with the Majorana operator γ_j. The reason for the use of the superscript will be made clear later. Since we construct $c^{(1)}$

using tomography, we obtain the matrix $\hat{c}^{(1)}$ with error $E^{(1)}$ such that $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$. As shown later in Lemma 5, we can derive Gaussian unitaries G_a and G_b from $\hat{c}^{(1)}$ such that the unitary $W_t := G_a^\dagger U_t G_b^\dagger$ satisfies

$$[W_t, \gamma_i] \approx 0, \quad i > M. \tag{18}$$

We will refer to this property as Majorana decoupling. The error in this approximation can be made small by performing the tomography step with sufficiently high precision.

We now consider our two implementations. We start with the fermionic implementation, where we consider Gaussian G_j in Eq. (16) corresponding to orthogonal matrices in $\mathrm{SO}(2n)$. In this case, we can ensure W_t is a sum of even-weight Majorana strings by choosing G_a and G_b to be parity-preserving (i.e. generated by quadratic fermionic Hamiltonians). We can then show that $[W_t, \gamma_j] = 0$ for all $j > M$ implies that W_t is a sum of Majorana strings containing only Majorana operators γ_i with $i \leq M$, and therefore W_t only acts on modes $i \in [m]$. To prove this, for some $j > M$, let A_j be the sum of Majorana strings in W_t that contain γ_j. Since W_t has only even-weight Majorana strings $[W_t, \gamma_j] = 0$ implies $[A_j, \gamma_j] = 0$. Writing $A_j = B_j \gamma_j$, this immediately implies that $B_j = A_j = 0$. In Lemma 6, we extend this argument to the case where $[W_t, \gamma_j] = 0$ is replaced with $[W_t, \gamma_j] \approx 0$.

We now consider the qubit implementation. Gaussian unitaries G_j in Eq. (16) now correspond to orthogonal matrices in $\mathrm{O}(2n)$. In this case, since the Majorana weight of W_t can be odd, the condition in Eq. (18) does not imply that the unitary W_t acts trivially on the qubits labeled $i > m$. As a simple example, take $(n, m) = (2, 1)$ and consider $W_t = \gamma_1\gamma_3\gamma_4 = iX_1Z_2$. We remind the reader that γ_1 and γ_2 act on fermionic mode 1, while γ_3 and γ_4 act on fermionic mode 2 but on both qubits 1 and 2 due to Jordan-Wigner transformation. Even when $[W_t, \gamma_3] = [W_t, \gamma_4] = 0$, W_t acts non-trivially on qubit 2. In this case, we show that we can use a simple unitary transformation $\bar{U}_d$ to obtain a unitary $\bar{W}_t = \bar{U}_d^\dagger W_t \bar{U}_d$ that has no support on qubits labeled $i > m$ when Eq. (18) holds exactly. When Eq. (18) holds approximately, $\bar{W}_t$ has approximately no support on qubits $i > m$.

We now proceed to the second step of the learning algorithm. Once Algorithm 1 allows us to construct unitary transformations of U_t that can be approximated as m-mode (qubit) quantum channels for both fermionic and qubit implementations, we can learn those channels. In Algorithm 2, we learn these channels by measuring the expectation values of Pauli observables that act on the first m modes (qubits) via shadow tomography, and then constructing the corresponding Choi states. The Choi state can be used to compute the unitary Stinespring dilation V_S of the channels [31]. The channel can also be learned using brute force [1]. The result of our learning algorithm is a description of the unitary $U_t^{(\ell)} = G_a V_S G_b$ acting on $n+2m+1$ modes for the fermionic implementation and a description of the unitary $U_t^{(\ell)} = G_a \bar{U}_d V_S \bar{U}_d^\dagger G_b$ acting on $n + 2m$ qubits for the qubit implementation. The learned unitary satisfies $\mathcal{D}_\diamond(\mathcal{U}_t, \mathcal{U}_t^{(\ell)}) \leq \epsilon$, where $\mathcal{U}_t^{(\ell)}$ is the quantum channel obtained by applying the unitary $U_t^{(\ell)}$ and tracing out the ancillary modes (qubits). As shown in Fig. 2, for the fermionic implementation, the learned unitary can be implemented as a parity-preserving unitary using a unitary transformation on V_S, along with an additional ancilla mode [11].

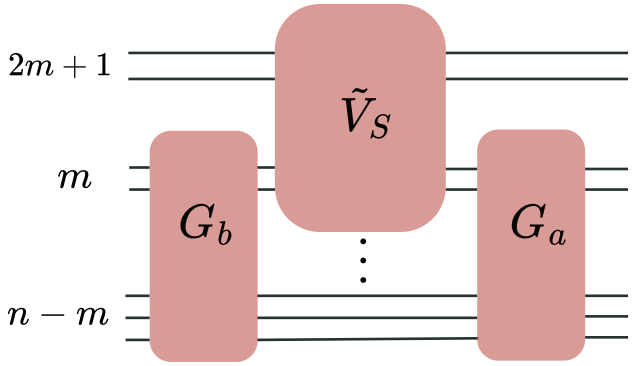

FIG. 2. This figure shows the implementation of the learned quantum channel $\mathcal{U}_t^{(\ell)}$ as a product of unitaries acting on $2m+1$ ancillary modes in the fermionic implementation. Here $\tilde{V}_S$ is a unitary transformation of the Stinespring dilation V_S of the reduced quantum channel $\mathcal{E}_m^{\mathcal{W}_t}$ corresponding to W_t, ensuring that $\tilde{V}_S$ is parity-preserving.

IV. METHODS

In this section, we first present an overview of the learning algorithm. Then, in Subsecs. IV A and IV B, we present details and lemmas for Algorithms 1 and 2, respectively.

Our learning algorithm is based on a minor modification of the result in Ref. [17] showing that U_t has the following decomposition.

Lemma 2 (Decomposition result for U_t)**.** For any given U_t in Eq. (16), there exist Gaussian unitaries G_A and G_B and unitary u_t such that

$$U_t = G_A u_t G_B, \tag{19}$$

where u_t is generated by even-weight Majorana strings containing Majorana operators γ_i with indices $i \in [M]$. Moreover, for the case where all G_j in Eq. (16) correspond to orthogonal matrices in $\mathrm{SO}(2n)$, there exist G_A and G_B that are in $\mathrm{SO}(2n)$.

See Appendix A for the proof of this lemma. We can use this result to show that U_t preserves the form of all but a constant number of transformed Majorana operators as follows.

Lemma 3 (Preserved Majoranas)**.** U_t preserves the form of transformed Majorana operators $G_A\gamma_i G_A^\dagger$, for $i = M+1, \ldots, 2n$, in the following sense:

$$U_t^\dagger G_A \gamma_i G_A^\dagger U_t = G_B^\dagger \gamma_i G_B. \tag{20}$$

Therefore, $G_A^\dagger U_t G_B^\dagger$ obeys the Majorana decoupling property

$$[G_A^\dagger U_t G_B^\dagger, \gamma_i] = 0, \quad i > M. \tag{21}$$

Proof. The left-hand side of Eq. (20) can be written as follows:

$$U_t^\dagger G_A \gamma_i G_A^\dagger U_t = G_B^\dagger u_t^\dagger \gamma_i u_t G_B \tag{22}$$

$$= G_B^\dagger \gamma_i G_B, \tag{23}$$

where we used the fact that $[u_t, \gamma_i] = 0$ from Lemma 2. Eq. (21) follows from Eq. (20). □

Lemma 3 shows that Eq. (19) implies the Majorana decoupling condition in Eq. (21). For the fermionic implementation, by choosing parity-preserving Gaussian G_A and G_B, we also ensure that Eq. (21) implies Eq. (19). On the other hand, for the qubit implementation, the existence of Gaussian G_a and G_b such that $W_t = G_a^\dagger U_t G_b^\dagger$ and $[W_t, \gamma_i] = 0$ for $i > M$ does not imply that G_a and G_b satisfy Eq. (19). This is illustrated for the case $(n, m) = (2, 1)$ and the example $U_t = \gamma_4$. Using $G_a = \gamma_1$ and $G_b = -\gamma_3$ gives us $W_t = \gamma_1\gamma_3\gamma_4$ which satisfies the Majorana decoupling condition but is not supported on Majorana operators γ_i with $i \in [2m]$. This is why, for the qubit implementation, we introduce notation G_a and G_b in addition to G_A and G_B. However, we will show that learning G_a, G_b satisfying the Majorana decoupling condition is sufficient to learn our unknown unitary. Since Lemma 3 shows there exist Gaussian unitaries G_a, G_b such that $W_t = G_a^\dagger U_t G_b^\dagger$ satisfies

$$[W_t, \gamma_i] = 0, \quad i > M, \tag{24}$$

we now proceed to devise a tomographic scheme that discovers these Gaussian unitaries. Consider the matrix $c_{xk} \in \mathbb{R}^{(T(n)+2n)\times 2n}$ defined as follows:

$$c_{xk} = \frac{1}{d} \operatorname{tr}\left[U_t^\dagger \gamma_k U_t \tilde{\gamma}_x\right], \tag{25}$$

where $d = 2^n$ is the Hilbert space dimension. Here $\tilde{\gamma}_x$ is defined as

$$\tilde{\gamma}_x = \gamma_x \text{ if } \gamma_x^\dagger = \gamma_x, \tag{26}$$

$$\tilde{\gamma}_x = i\gamma_x \text{ if } \gamma_x^\dagger = -\gamma_x, \tag{27}$$

where γ_x is a Majorana string defined by the $2n$ bit-string x as $\gamma_x = \gamma_1^{x_1} \ldots \gamma_{2n}^{x_{2n}}$. This definition ensures that our operator basis $\tilde{\gamma}_x$ is Hermitian. As shown in Fig. 3, c is made up of submatrices $c^{(1)}$, defined by Eq. (17), and $c^{(2)}$, defined as $c^{(2)}_{xk} = c_{xk}$ with $\alpha_x \geq 2$. Moreover, $c^{(1)}$ can be written using its singular-value decomposition as $c^{(1)} = U\Sigma V^T$. As a consequence of Lemma 3, $c^{(1)}$ has all but a constant number of singular values with value 1. Intuitively, this property is related to Eq. (20) which says that there are $2n - M$ Majorana operators $\{G_A\gamma_i G_A^\dagger\}$ that transform under U_t to another set of Majorana operators $\{G_B^\dagger \gamma_i G_B\}$, and the fact that $c^{(1)}$ describes how U_t transforms the Majorana operator γ_i to a linear combination of Majorana operators. This is described in the following result (see Appendix A for the proof).

Lemma 4 (Useful properties of the matrix c_{xk})**.** The matrix c_{xk} has orthonormal columns, making all its singular values

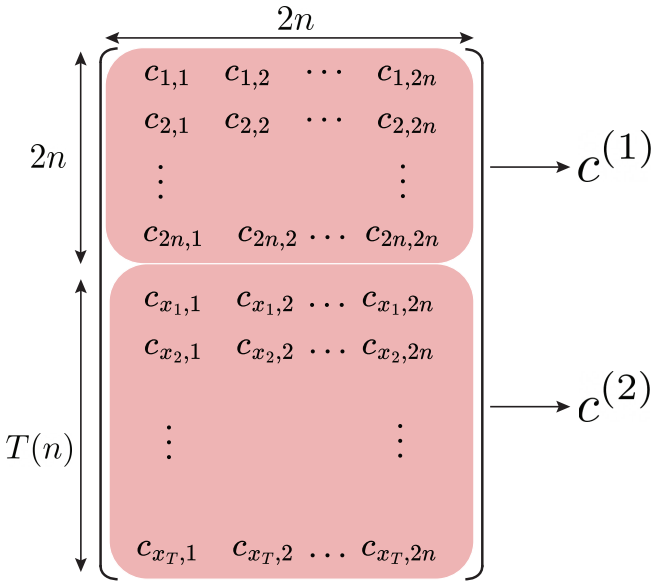

FIG. 3. The matrix c_{xk} defined in Eq. (25). Here $T(n)$ is a polynomial defined in Lemma 5.

equal to 1. The matrix $c^{(1)}$ has at least $2n - M$ singular values equal to 1. Moreover, the matrix $\hat{c}^{(1)}$, the learned version of $c^{(1)}$, has at least $2n - M$ singular values $\hat{d}_i$ that satisfy

$$|\hat{d}_i - 1| \leq \|E^{(1)}\|, \quad i = M+1, \ldots, 2n, \tag{28}$$

where $\hat{c}^{(1)}_{jk} = c^{(1)}_{jk} + E^{(1)}_{jk}$, and $E^{(1)}$ is the error from tomography.

We now show that the singular values of $c^{(1)}$ with value 1 correspond to the Majorana operators satisfying Eq. (24). This can be seen from the following computation. Consider the unitary $W_t = G_a^\dagger U_t G_b^\dagger$, where

$$G_a \gamma_i G_a^\dagger = \sum_k O^a_{ki} \gamma_k, \tag{29}$$

$$G_b \gamma_i G_b^\dagger = \sum_k O^b_{ki} \gamma_k. \tag{30}$$

We can compute the evolved Majorana operator $W_t^\dagger \gamma_i W_t$ with $i > M$ as follows:

$$W_t^\dagger \gamma_i W_t = \sum_j (c^{(1)} O^a)_{ji} G_b \gamma_j G_b^\dagger + \sum_{x:2\leq\alpha_x\leq w} (c^{(2)} O^a)_{xi} G_b \gamma_x G_b^\dagger, \tag{31}$$

where $c^{(2)}_{xi}$ is a submatrix of c_{xi} such that $\alpha_x \geq 2$ (α_x is the Hamming weight of x). In the second term, it is sufficient to consider strings with weights upper-bounded by a constant $w = (\kappa + 1)^t$. This property follows from the facts that Gaussian unitaries do not increase the Majorana weight of a Majorana string under conjugation, and that U_t only contains

a constant number of non-Gaussian unitaries, which can increase the Majorana weight. For more details, see Lemma 14 in Appendix A. Assuming that the basis is ordered such that $\Sigma_{ii} = 1$ for $i > M$, and using $O^a = V$ then gives us

$$W_t^\dagger \gamma_i W_t = \sum_j U_{ji} G_b \gamma_j G_b^\dagger, \tag{32}$$

where we used the fact that $\Sigma_{ii} = 1$, and that c_{xk} has orthonormal columns. Finally, using Eq. (30) and $O^b = U^T$ gives us Eq. (24). Since we have access to $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$ instead of $c^{(1)}$, where $E^{(1)}$ is the tomography error, we have the following result (see Appendix A for the proof).

Lemma 5 (Constructing the unitary W_t)**.** Given $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$, we can compute descriptions of Gaussian unitaries G_a and G_b such that $W_t = G_a^\dagger U_t G_b^\dagger$ satisfies the following property:

$$\|[W_t, \gamma_i]\| \leq \epsilon_0, \quad i > M, \tag{33}$$

where ϵ_0 obeys the following bound:

$$\epsilon_0 \leq T_1(n) \|E^{(1)}\|^{1/2}, \tag{34}$$

where $T_1(n)$ is a polynomial defined by $T_1(n) = (\sqrt{5}T(n) + 2n + 1)$ with $T(n) = \sum_{x:2\leq\alpha_x\leq w} 1 = \text{poly}(n)$. Here x is a bitstring of length $2n$, and $w = (\kappa+1)^t$ is a constant defined in Lemma 14. Here G_a and G_b are defined in Eqs. (29) and (30), where $O^a = V$ and $O^b = U^T$. The orthogonal matrices U and V are defined from the singular-value decomposition of $\hat{c}^{(1)}$ as $\hat{c}^{(1)} = U\Sigma V^T$, where $\Sigma = \text{diag}(\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_{2n})$ with $\hat{d}_i$ the singular values and where U, V are orthogonal matrices. Moreover, we can always modify O^a and O^b suitably such that they are in SO$(2n)$ and Eq. (33) holds.

We therefore have that by learning $\hat{c}^{(1)}$ and performing its singular-value decomposition, we obtain a unitary $W_t = G_a^\dagger U_t G_b^\dagger$ that approximately commutes with the Majorana operators γ_i with $i > M$. In Algorithm 1, we measure observables in states obtained from applications of the unitary U_t to learn the matrix $c^{(1)}$ and use it to compute the descriptions of G_a and G_b. Details of this algorithm are presented in Subsec. IV A.

We now proceed to show how the Majorana decoupling condition for W_t from Eq. (18) helps us learn the unitary U_t. As discussed in Sec. III, for the fermionic implementation, this condition can be used to show that the unitary W_t acts almost as the identity on modes labeled $i > m$. This is described in the following result (see Appendix D for the proof).

Lemma 6 (Majorana decoupling for W_t in the fermionic implementation implies Pauli decoupling for modes $i > m$)**.** Consider the fermionic implementation where the Gaussian unitaries G_j in U_t correspond to orthogonal matrices in SO$(2n)$, and the unitary W_t is obtained from Algorithm 1. Then W_t satisfies the following:

$$\frac{1}{2} \sum_{P\in\{X,Y,Z\}} \|[W_t, P_i]\| \leq 3n\epsilon_0, \quad i > m+1, \tag{35}$$

given $\|[W_t, \gamma_j]\| \leq \epsilon_0$ for $j > M$ (see Lemma 5).

We will refer to the property obeyed by the unitary in Eq. (35) as (approximate) Pauli decoupling. As we will see later, this can be used to show that the unitary acts approximately as the identity on modes labeled $i > m$.

We now consider the qubit implementation where we allow Gaussian unitaries G_j to correspond to orthogonal matrices in O$(2n)$. As discussed in Sec. III, since such unitaries can have odd Majorana weight, the condition in Eq. (18) does not imply that W_t has no support on qubits labeled $i > m$. Instead, we consider the unitary $\bar{W}_t$ defined as follows.

Definition 7. We define the unitary $\bar{W}_t$ as follows:

$$\bar{W}_t = \bar{U}_d^\dagger W_t \bar{U}_d, \tag{36}$$

where $\bar{U}_d = V_d U_d$. The real diagonal unitaries U_d and V_d are defined as

$$V_d = \sum_x p(\alpha_x) |x\rangle\langle x|_{AB}, \tag{37}$$

$$U_d = \sum_{x'} p(\alpha_{x'}) |x'\rangle\langle x'|_A. \tag{38}$$

Here U_d acts on register A (which contains qubits labeled $i \in [m]$), register B contains qubits labeled $i > m$, V_d acts on all qubits, α_x is the Hamming weight of the state $|x\rangle$, and $p(\alpha) = (-1)^{\alpha(\alpha-1)/2}$.

In the case where $[W_t, \gamma_i] = 0$ holds for $i > M$, we can show that $\bar{W}_t = \langle 0| W_t |0\rangle_A \otimes I_B$ (see Lemma 16 in Appendix B for more details). We now consider the practical case where $\|[W_t, \gamma_i]\| \leq \epsilon_0$ as in Eq. (33). As shown in Lemma 18 in Appendix B, $\bar{W}_t$ now satisfies the following:

$$\frac{1}{2} \sum_{P\in\{X,Y,Z\}} \left\|[\bar{W}_t, P_i]\right\| \leq \epsilon_P, \quad \epsilon_P = (2n+3)\epsilon_0, \tag{39}$$

for all qubits in register B.

We now aim to approximate unitaries W_t ($\bar{W}_t$) for the fermionic (qubit) implementation as quantum channels on a constant number of modes (qubits). From this channel, we can then obtain a unitary V_S from the Stinespring dilation applied to the learned quantum channel. To this end, for an arbitrary n-mode (qubit) unitary U, we introduce the reduced quantum channel $\mathcal{E}_m^{\mathcal{U}}$ acting on m modes (qubits), defined as follows (see Definition 1 in Ref. [8] for more details).

Definition 8 (Reduced quantum channel [8])**.** For a given unitary U, we define the reduced channel $\mathcal{E}_m^{\mathcal{U}}(\rho)$ that acts on the first m qubits as follows:

$$\mathcal{E}_m^{\mathcal{U}}(\rho) = \text{tr}_{\geq m+1}\left(U\rho \otimes \frac{I_B}{2^{n-m}} U^\dagger\right), \tag{40}$$

where $\mathcal{U}$ is the quantum channel corresponding to the unitary U, I_B corresponds to modes (qubits) in register B, and $\text{tr}_{\geq m+1}$ denotes tracing over modes (qubits) $m+1, \ldots, n$ in register B.

Using ideas developed in Ref. [8], Eqs. (35) and (39) can be used to show that the unitary acts approximately as the identity on modes (qubits) in register B. In fact, the reduced quantum channel can be used as a proxy for the unitary channel as shown in the following result.

Lemma 9 (Approximating a unitary channel as a reduced quantum channel)**.** The channel $\mathcal{E}_m^{\mathcal{U}}$ is a CPTP (completely positive and trace preserving) map that satisfies

$$\mathcal{D}_\diamond\Big(\mathcal{U}, \mathcal{E}_m^{\mathcal{U}} \otimes \mathcal{I}_B\Big) \leq n\epsilon, \tag{41}$$

where $\mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2)$ is defined in Eq. (14), and $\mathcal{I}_B$ is the identity channel on register B, given the following condition holds:

$$\frac{1}{2} \sum_{P \in \{X,Y,Z\}} \|[U, P_i]\| \leq \epsilon, \tag{42}$$

where $i \geq m+1$.

We now proceed to use the above result to approximate the unitaries W_t and $\bar{W}_t$ in the fermionic and qubit implementations, respectively, as reduced quantum channels. For the fermionic implementation, the property from Eq. (35) and Lemma 9 allows us to show that the m-mode channel $\mathcal{E}_m^{\mathcal{W}_t} \otimes \mathcal{I}$, where $\mathcal{E}_m^{\mathcal{W}_t}$ acts on register A, is close in diamond distance to the channel corresponding to the unitary W_t on n modes, as described in Eq. (41). Similarly, for the qubit implementation, the property from Eq. (39) and Lemma 9 allows us to show that the m-qubit quantum channel $\mathcal{E}_m^{\bar{\mathcal{W}}_t} \otimes \mathcal{I}$, where $\mathcal{E}_m^{\bar{\mathcal{W}}_t}$ acts on register A, is close in diamond distance to the channel corresponding to the unitary $\bar{W}_t$ on n qubits, as described in Eq. (41).

We now proceed to learn the m-mode (qubit) channels. Any channel $\mathcal{E}$ on m modes (qubits) can be described via its Choi state

$$J(\mathcal{E}) = \frac{1}{d_0} \sum_{ij} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j|, \tag{43}$$

where $d_0 = 2^m$. Since the Choi state $J(\mathcal{E})$ corresponds to a CPTP map, it also satisfies the following two conditions:

$$J(\mathcal{E}) \geq 0, \tag{44}$$

$$\mathrm{tr}_A[J(\mathcal{E})] = I/d_0, \tag{45}$$

where A denotes the first register in Eq. (43). In Algorithm 2, we use shadow tomography of Pauli observables [8] to learn the Choi state of the channel as $J(\hat{\mathcal{E}})$ up to some error by measuring

$$f_{\alpha\beta} := \frac{1}{2^n} \mathrm{tr}\big[S^\dagger(\bar{P}_\beta \otimes I_B) S (\bar{P}_\alpha \otimes I_B)\big], \tag{46}$$

where $S = W_t$ for the fermionic implementation and $S = \bar{W}_t$ for the qubit implementation, and $\alpha, \beta \in \{I, X, Y, Z\}^{\otimes m}$. Note that we use black-box access to W_t or $\bar{W}_t$ when running the tomography process to measure $f_{\alpha\beta}$. As detailed in Section IV B, the coefficients $f_{\alpha\beta}$ can be used to reconstruct the Choi state corresponding to the reduced quantum channels. Since the state $J(\hat{\mathcal{E}})$ is learned up to some error, it may not satisfy the CPTP conditions in Eqs. (44) and (45). Therefore $J(\hat{\mathcal{E}})$ is projected (see Subsec. IV B) to a state J_p which satisfies the CPTP conditions, giving us the following diamond distance bound between the channel $\mathcal{E}^{\mathcal{W}_t}$ and the channel corresponding to the Choi state J_p denoted as $\mathcal{E}_{\text{proj}}^{\mathcal{W}_t}$:

$$\mathcal{D}_\diamond(\mathcal{E}^{\mathcal{W}_t}, \mathcal{E}_{\text{proj}}^{\mathcal{W}_t}) \leq C_3 \epsilon_2, \tag{47}$$

where $C_3 = d_0^{11}(3d_0^2 + 1)/2$ and $\epsilon_2 = \max_{\alpha,\beta} |\hat{f}_{\alpha\beta} - f_{\alpha\beta}|$. The same result holds for the channel $\mathcal{E}^{\bar{\mathcal{W}}_t}$ in the qubit implementation. The Choi state J_p can be used to construct the channel's unitary Stinespring dilation V_S acting on $3m$ modes (qubits) [30], as shown in Fig. 2.

This concludes the high-level overview of our learning algorithm. We now describe in detail the main lemmas used to define Algorithms 1 and 2.

A. Algorithm 1

We now explain in detail the main ideas and methods used to formulate Algorithm 1. We first consider the qubit implementation. Using methods in Ref. [25], we can estimate c_{xk} by measuring observables O_k^+ in some state prepared by the application of the unknown unitary U_t. This leads to the following result (see Appendix A for the proof).

Lemma 10 (Finding the coefficients c_{xk} (qubit implementation))**.** Let $\mathcal{A}$ be the $d = 2^n$ dimensional Hilbert space upon which the unitary U_t acts. Furthermore, let $\mathcal{B}$ be the Hilbert space of an ancilla register of the same size, and let $\mathcal{C}$ be the Hilbert space of another single ancilla qubit. Consider the state $|\psi_x\rangle$ defined as

$$\begin{aligned} |\psi_x\rangle = &\frac{1}{\sqrt{2}}\big[(U_t \otimes I)\,|\Phi_d\rangle_{\mathcal{AB}}\,|0\rangle_{\mathcal{C}} \\ &+ (U_t \otimes I)(\gamma_x^\dagger \otimes I)\,|\Phi_d\rangle_{\mathcal{AB}}\,|1\rangle_{\mathcal{C}}\big], \end{aligned} \tag{48}$$

where $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i,i\rangle_{\mathcal{AB}}$ is the maximally entangled state between systems $\mathcal{A}$ and $\mathcal{B}$, and $\gamma_x = \gamma_1^{x_1} \ldots \gamma_{2n}^{x_{2n}}$. The coefficients c_{xk} [defined in Eq. (25)] can be obtained using expectation values of observables

$$O_k^+ = O_k + O_k^\dagger = (\gamma_k \otimes I)_{\mathcal{AB}} \otimes X_{\mathcal{C}}, \tag{49}$$

$$O_k^- = iO_k - iO_k^\dagger = (\gamma_k \otimes I)_{\mathcal{AB}} \otimes Y_{\mathcal{C}}, \tag{50}$$

such that $c_{xk} = \mathrm{tr}\big[|\psi_x\rangle\langle\psi_x|\, O_k^+\big]$ for $\gamma_x^\dagger = \gamma_x$, and $c_{xk} = \mathrm{tr}\big[|\psi_x\rangle\langle\psi_x|\, O_k^-\big]$ for $\gamma_x^\dagger = -\gamma_x$.

We can apply the above result to measure the matrix elements of $c^{(1)}$ as expectation values of observables O_k^+ in states $|\psi_j\rangle := |\psi_{x^{(j)}}\rangle$, where $x^{(j)}$ is a weight-1 bit string with $x_j = 1$. The tomography scheme is defined as follows. We first reorder the Hilbert spaces as $\mathcal{C} \otimes \mathcal{A} \otimes \mathcal{B}$ so that observables O_k^+ can be written as Majorana strings of weight two.

This defines new Majorana operators $\hat{\gamma}_i$ on the Hilbert space $\mathcal{C} \otimes \mathcal{A} \otimes \mathcal{B}$ as follows:

$$\hat{\gamma}_1 = X_{\mathcal{C}}, \tag{51}$$
$$\hat{\gamma}_2 = Y_{\mathcal{C}}, \tag{52}$$
$$\hat{\gamma}_i = Z_{\mathcal{C}}\gamma_{i-2}, \quad i = 3, \ldots, 4n+2, \tag{53}$$

where γ_i are the Majorana operators defined in the same way as in Eqs. (5) and (6) on $\mathcal{A} \otimes \mathcal{B}$ containing qubits $1, \ldots, 4n$. We can then use the shadow tomography scheme based on the fermionic Gaussian unitary ensemble in Ref. [26] to obtain estimates of $c^{(1)}_{jk}$, giving us the following result (see Appendix A for the proof).

Lemma 11 (Estimating the matrix $c^{(1)}$ through shadow tomography for the qubit implementation)**.** Using shadow tomography with the fermionic Gaussian unitary ensemble [26], we can estimate the matrix $c^{(1)}_{jk} = \operatorname{tr}\left[U_t^\dagger \gamma_k U_t \gamma_j\right]/d$ by measuring the expectation values of the operators O_k^+ in state $|\psi_j\rangle$. With probability $\geq 1-\delta$, we obtain the matrix $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$ such that $\|E^{(1)}\| \leq \|E^{(1)}\|_2 \leq \epsilon$. For each row $j \in [2n]$ of $c^{(1)}_{jk}$, we need N_c copies of the state $|\psi_j\rangle$, where

$$N_c = \left(1 + \frac{\epsilon}{6n}\right) \log\left(8n^2/\delta\right) \frac{4n^2(4n+1)}{\epsilon^2}. \tag{54}$$

Moreover, the required classical post-processing to compute the expectation values can be done efficiently [26].

For the fermionic implementation, the same result holds except that we use states that can be obtained from a parity-preserving quantum circuit, and the observables $O_k^\pm$ are modified accordingly. For more details, see see Appendix D.

We remark that, while the shadow tomography step used to construct the matrix $c^{(1)}$ does not flag cases where it produces an inaccurate reconstruction of the matrix, we can make the failure probability δ of this step to be exponentially small in n because of the dependence of N_c on δ in Eqs. (54).

B. Algorithm 2

We now explain in detail the main ideas and methods used to formulate Algorithm 2. The Choi state of any channel $\mathcal{E}$ acting on m modes (qubits), defined in Eq. (43), can be written as follows:

$$J(\mathcal{E}) = \frac{1}{d_0} \sum_{ijkl} \sum_{\alpha\beta} c_{\alpha,ij} c_{\beta,lk} \operatorname{tr}\left[\mathcal{E}(\bar{P}_\alpha)\bar{P}_\beta\right] |k\rangle\langle l| \otimes |i\rangle\langle j|, \tag{55}$$

where $d_0 = 2^m$, $ijkl$ are indices over the computational basis elements of the m-mode (qubit) Hilbert space, $\alpha\beta$ are indices used to describe the Pauli string $\bar{P}_\alpha \in \{I, X, Y, Z\}^{\otimes m}$, and $c_{\alpha,ij} = \operatorname{tr}\left[|i\rangle\langle j|\, \bar{P}_\alpha\right]/d_0$. As shown in Lemma 19 in Appendix C, we can use the result

$$\frac{1}{d_0} \operatorname{tr}\left[\mathcal{E}(\bar{P}_\alpha)\bar{P}_\beta\right] = f_{\alpha\beta} \tag{56}$$

Algorithm 1: Algorithm for learning the matrix $c^{(1)}$ and descriptions of orthogonal matrices O^a and O^b defining G_a and G_b, respectively.

Input: Accuracy ϵ, failure probability δ.
Qubit implementation: N_c copies of the state $|\psi_j\rangle$ for each $j \in [2n]$, where an upper bound on N_c and the definition of $|\psi_j\rangle$ are given in Eqs. (54) and (48), respectively.
Fermionic implementation: N_c^{f} copies of the state $\left|\psi_j^{\mathrm{f}}\right\rangle$ for each $j \in [2n]$, where N_c^{f} and $\left|\psi_j^{\mathrm{f}}\right\rangle$ are defined in Eqs. (D14) and (D9), respectively.
Output: Matrices V and U obtained from a classical description of the matrix $\hat{c}^{(1)}$ such that $\hat{c}^{(1)} = U\Sigma V^T$, and $\|\hat{c}^{(1)} - c^{(1)}\| \leq \epsilon$ with probability $\geq 1-\delta$.

1 For each $j \in [2n]$, perform shadow tomography using the fermionic Gaussian unitary ensemble to estimate Majorana observables O_k^+ for all $k \in [2n]$, defined in Eq. (49) for the qubit implementation and Eq. (D12) for the fermionic implementation. Construct the matrix $\hat{c}^{(1)}$ (see Lemma 10 for more details) ;
2 Compute the singular value decomposition of $\hat{c}^{(1)} = U\Sigma V^T$, and reorder the basis such that the singular values are written in ascending order;
3 **return** V and U.

to express $J(\mathcal{E})$ in terms of the matrix elements $f_{\alpha\beta}$, defined in Eq. (46).

We first consider the qubit implementation. We can measure the matrix $f_{\alpha\beta}$ in a similar way to how we measured the matrix $c^{(1)}$, i.e. by constructing Pauli observables whose expectation values in states obtained from the application of the unknown unitary U_t give $f_{\alpha\beta}$. This is described for the qubit implementation in the following result.

Lemma 12 (Learning Pauli observables with shadow tomography for the qubit implementation)**.** The entries of the matrix $f_{\alpha\beta}$ defined as

$$f_{\alpha\beta} = \frac{1}{2^n} \operatorname{tr}\left[S^\dagger(\bar{P}_\beta \otimes I_B) S (\bar{P}_\alpha \otimes I_B)\right], \tag{57}$$

where $S = \bar{W}_t$ from Eq. (36), $\bar{P}_\alpha \in \{I, X, Y, Z\}^{\otimes m}$ are Pauli strings supported on the first m qubits and α, β are indices for the set of Pauli strings, can be learned using shadow tomography as follows. We estimate the expectation values of observables

$$\bar{O}_\beta = (\bar{P}_\beta \otimes I)_{\mathcal{AB}} \otimes |1\rangle\langle 0|_{\mathcal{C}}, \tag{58}$$

in states

$$|\bar{\psi}_\alpha\rangle = \frac{1}{\sqrt{2}}\left[(\bar{W}_t \otimes I)\, |\Phi_d\rangle_{\mathcal{AB}} |0\rangle_{\mathcal{C}} + (\bar{W}_t \otimes I)_{\mathcal{AB}} (\bar{P}_\alpha \otimes I)_{\mathcal{AB}} |\Phi_d\rangle\, |1\rangle_{\mathcal{C}}\right], \tag{59}$$

where $|\Phi_d\rangle$ is the maximally entangled state $\frac{1}{d}\sum_i |i,i\rangle_{\mathcal{AB}}$, and then construct each row of $\hat{f}_{\alpha\beta}$ (where $\alpha, \beta \in$

$\{I,X,Y,Z\}^{\otimes m}$) such that $\max_{\alpha,\beta}|\hat{f}_{\alpha\beta} - f_{\alpha\beta}| \leq \epsilon$ with probability $\geq 1-\delta$. The protocol needs $\bar{N}_c$ copies of the state $|\bar{\psi}_\alpha\rangle$, where

$$\bar{N}_c = C_1 \frac{\log(C_2/\delta)}{\epsilon^2}, \tag{60}$$

with $C_1 = 68(3^m)$, $C_2 = 2^{2m+1}$.

See Appendix C for the proof. For the fermionic implementation, the same result holds as above except that we use states that can be prepared by a parity-preserving quantum circuit, and the observables O_β^+ are modified accordingly. For more details, see Appendix D.

We remark that, while the shadow tomography step used to construct the matrix $f_{\alpha\beta}$ does not flag cases where it produces an inaccurate reconstruction of the matrix, we can make the failure probability of this step δ to be exponentially small in n because of the dependence of $\bar{N}_c$ on δ in Eqs. (60).

Now that we have the learned version of the Choi state $J(\hat{\mathcal{E}})$ obtained by $\hat{f}_{\alpha\beta}$ from Algorithm 2, we construct the projected Choi state J_p that satisfies the CPTP conditions in Eqs. (44) and (45). The projection scheme is based on ideas in Ref. [32]. The state $J(\hat{\mathcal{E}})$ is first projected onto a completely positive map denoted by J_1. The state J_1 is then projected onto a trace-preserving map denoted by J_2. Since J_2 may have negative eigenvalues, we construct the final state J_p defined by

$$J_p = (1-p)J_2 + \frac{p}{d_0^2}\mathbb{1}\otimes\mathbb{1}, \tag{61}$$

where p is the solution to the equation $(1-p)\lambda_{\min} + p/d_0^2 = 0$, and $\lambda_{\min}$ is the minimum eigenvalue of J_2. One can find this eigenvalue efficiently since the channel has constant dimension. This choice of p ensures J_p has non-negative eigenvalues. We can then show that, given $\|J(\hat{\mathcal{E}}) - J(\mathcal{E})\| \leq \epsilon_1$, the projected Choi state J_p obeys $\|J(\mathcal{E}) - J_p\|_1 \leq C_r\epsilon_1$, where $C_r = 3d_0^4 + d_0^2$, giving us the channel distance bound in Eq. (47). For more details of the projection scheme, see Lemma 20 in Appendix C. The Choi state J_p on modes (qubits) labeled $1,\ldots,m$, can then be used to construct the unitary Stinespring dilation V_S, as shown in Fig. 2. Using descriptions of G_a, G_b (and $\bar{U}_d$ for the qubit implementation), we obtain the description of the unitary $U_t^{(\ell)}$ that approximates U_t. This concludes our exposition of the learning algorithm.

Algorithm 2: Algorithm for learning the Choi state $J(\hat{\mathcal{E}})$ corresponding to the reduced quantum channel.

Input: Accuracy ϵ, failure probability δ,
Qubit implementation: $\bar{N}_c$, defined in Eq. (60), copies of the states $|\bar{\psi}_\alpha\rangle$, defined in Eq. (59), for each $\alpha \in \{I,X,Y,Z\}^{\otimes m}$.
Fermionic implementation: $\bar{N}_c^{\mathrm{f}}$, defined in Eq. (D20), copies of the states $|\bar{\psi}_\alpha^{\mathrm{f}}\rangle$, defined in Eq. (D15), for each $\alpha \in \{I,X,Y,Z\}^{\otimes m}$.

Output: A classical description of the state $J(\hat{\mathcal{E}})$ such that $\max_{\alpha\beta}|\hat{f}_{\alpha\beta} - f_{\alpha\beta}| \leq \epsilon$, and $\|J(\hat{\mathcal{E}}) - J(\mathcal{E})\| \leq d_0^6\epsilon$, where $J(\mathcal{E})$ is the Choi state corresponding to the channel $\mathcal{E} = \mathcal{E}_m^{\mathcal{W}_t}$ for the fermionic implementation, and the channel $\mathcal{E} = \mathcal{E}_m^{\bar{\mathcal{W}}_t}$ for the qubit implementation.

For each α, perform shadow tomography using the local Clifford unitary ensemble to estimate Pauli observables $\bar{O}_\beta^+$ defined in Eq. (C4) and Eq. (D19) for the qubit implementation and the fermionic implementation, respectively, to construct the matrix $\hat{f}_{\alpha\beta}$ (see Lemma 12 and Appendix D for more details) ;

Compute the classical description of the learned Choi state $J(\hat{\mathcal{E}})$ from the matrix elements $\hat{f}_{\alpha\beta}$;

return $J(\hat{\mathcal{E}})$

V. MATCHGATE HIERARCHY

In this section, we show that fermionic unitaries with a constant number of non-Gaussian gates are, in general, not within the matchgate hierarchy [33]. For n qubits (modes), we define an infinite family of gates $\mathcal{M}_k$ called the matchgate hierarchy. We define the set $\Gamma_1 = \{\gamma_\mu : \mu \in [2n]\}$. Each set $\mathcal{M}_k$ can then be defined recursively as follows:

$$\mathcal{M}_1 = \{M \in U(2^n) : M = \sum_\mu a_\mu\gamma_\mu, a_\mu \in \mathbb{R}\}, \tag{62}$$

$$\mathcal{M}_k = \{M \in U(2^n) : M\Gamma_1 M^\dagger \subseteq \mathcal{M}_{k-1}\}, \quad k \geq 2. \tag{63}$$

We note here that $\mathcal{M}_2$ corresponds to Gaussian unitaries. Recent work [33] has shown that there is an efficient algorithm for learning unitaries in any finite level of the matchgate hierarchy. We show that arbitrary fermionic unitaries with just two non-Gaussian gates (belonging to the third level of the matchgate hierarchy) lie outside any finite level of the matchgate hierarchy. This is stated in the following lemma.

Lemma 13 (Example of U_t outside the matchgate hierarchy)**.** The unitary $U_t = KG(\theta)K$ with two non-Gaussian gates K, where

$$K = \exp(i\pi\gamma_1\gamma_2\gamma_3\gamma_4/4), \tag{64}$$

$$G(\theta) = \exp(\theta\gamma_1\gamma_5), \tag{65}$$

$\theta = \pi/p$, and p is an odd integer, does not belong to any finite level of the matchgate hierarchy.

This result can be proved by contradiction. For any unitary U_t to lie in some finite level, say k, of the matchgate hierarchy, the unitary $F_1 = U_t\gamma_\mu U_t^\dagger$, for any $\mu \in [2n]$, must lie in $\mathcal{M}_{k-1}$. We can define the unitaries

$$F_k := F_{k-1}\gamma_\mu F_{k-1}^\dagger, \quad k \geq 2. \tag{66}$$

Extending the same argument shows that F_{k-2} must lie in $\mathcal{M}_2$ i.e., F_{k-2} is Gaussian. Explicit computation for $\mu = 2$ shows that F_{k-2} is not Gaussian, showing that U_t does not belong to any finite level of the matchgate hierarchy. See Appendix E for the proof of this lemma.

VI. CONCLUSION

In Ref. [17], it was shown that there is an efficient algorithm to learn quantum states obtained from fermionic Gaussian unitaries with a constant number of non-Gaussian gates. In this work, we have solved an open problem from Ref. [17] by providing an efficient algorithm for learning these types of fermionic Gaussian unitaries. We have also shown that such unitaries generally do not fall under the matchgate hierarchy. A few directions for future work could include improving our algorithm by reducing the number of ancilla qubits required to implement the learned unitary or reducing the resource requirements for the learning algorithm. It may be interesting to apply our techniques for learning fermionic channels which in some cases are known to be efficiently simulatable [34]. Another possible future direction is that of studying property testing for fermionic unitaries such as those we studied [35, 36]. It would also be interesting to explore applications of our learning algorithm to single-parameter and multi-parameter quantum sensing [37]. Our work contributes to a clear understanding about the kinds of quantum processses that can be learned, verified, and benchmarked efficiently, paving the way for accurate and verifiable quantum computation.

VII. ACKNOWLEDGMENTS

S.A. acknowledges helpful correspondence with Josh Cudby. S.A. and A.V.G. acknowledge support from the U.S. Department of Energy, Office of Science, Accelerated Research in Quantum Computing, Fundamental Algorithmic Research toward Quantum Utility (FAR-Qu). S.A. and A.V.G. were also supported in part by the DoE ASCR Quantum Testbed Pathfinder program (awards No. DE-SC0019040 and No. DE-SC0024220), NSF QLCI (award No. OMA-2120757), NSF STAQ program, AFOSR MURI, DARPA SAVaNT ADVENT, and NQVL:QSTD:Pilot:FTL. S.A. and A.V.G. also acknowledge support from the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. M.E.S.M. acknowledges support from the U.S. Department of Defense through a QuICS Hartree Fellowship.

Note added: While we were polishing the manuscript, a related paper was posted to arXiv [38]. Ref. [38] solves the same problem as the one solved by Theorem 1 for the qubit implementation, i.e. when the unknown operator has Gaussian unitaries in $\mathrm{O}(2n)$. Moreover, in Ref. [38], a property testing procedure for testing the closeness of an unknown unitary to unitaries with a constant number of non-Gaussian gates is also considered.

[1] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455–2467 (1997).
[2] M. Mohseni, A. T. Rezakhani, and D. A. Lidar, Phys. Rev. A **77**, 032322 (2008).
[3] G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **86**, 4195 (2001).
[4] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, Phys. Rev. Lett. **93**, 080502 (2004).
[5] J. Haah, R. Kothari, R. O'Donnell, and E. Tang, in *FOCS* (2023).
[6] L. Leone, S. F. E. Oliviero, S. Lloyd, and A. Hamma, Phys. Rev. A **109**, 022429 (2024).
[7] H. Zhao, L. Lewis, I. Kannan, Y. Quek, H.-Y. Huang, and M. C. Caro, PRX Quantum **5**, 040306 (2024).
[8] H.-Y. Huang, Y. Liu, M. Broughton, I. Kim, A. Anshu, Z. Landau, and J. R. McClean, in *STOC* (2024) p. 1343–1351.
[9] R. Jozsa and A. Miyake, Proc. R. Soc. A: Math **464**, 3089–3106 (2008).
[10] B. M. Terhal and D. P. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).
[11] S. B. Bravyi and A. Y. Kitaev, Ann. Phys. (N. Y.). **298**, 210–226 (2002).
[12] L. G. Valiant, SIAM J. Comput. **31**, 1229 (2002).
[13] K. Wan, W. J. Huggins, J. Lee, and R. Babbush, Commun. Math. Phys. **404**, 629–700 (2023).
[14] M. Oszmaniec, N. Dangniam, M. E. Morales, and Z. Zimborás, PRX Quantum **3**, 020328 (2022).
[15] J. Cudby and S. Strelchuk, Learning gaussian operations and the matchgate hierarchy (2024), arXiv:2407.12649 [quant-ph].
[16] D. J. Brod and E. F. Galvão, Phys. Rev. A **84**, 022310 (2011).
[17] A. A. Mele and Y. Herasymenko, PRX Quantum **6**, 010319 (2025).
[18] D. González-Cuadra, D. Bluvstein, M. Kalinowski, R. Kaubruegger, N. Maskara, P. Naldesi, T. V. Zache, A. M. Kaufman, M. D. Lukin, H. Pichler, B. Vermersch, J. Ye, and P. Zoller, Proc. Natl. Acad. Sci. **120** (2023).
[19] R. Ott, D. González-Cuadra, T. V. Zache, P. Zoller, A. M. Kaufman, and H. Pichler, Error-corrected fermionic quantum processors with neutral atoms (2024), arXiv:2412.16081 [quant-ph].
[20] A. Schuckert, E. Crane, A. V. Gorshkov, M. Hafezi, and M. J. Gullans, Fermion-qubit fault-tolerant quantum computing (2024), arXiv:2411.08955 [quant-ph].
[21] B. Dias and R. Koenig, Quantum **8**, 1350 (2024).
[22] O. Reardon-Smith, M. Oszmaniec, and K. Korzekwa, Quantum **8**, 1549 (2024).
[23] A. Mocherla, L. Lao, and D. E. Browne, Extending matchgate simulation methods to universal quantum circuits (2024), arXiv:2302.02654 [quant-ph].
[24] A. Bampounis, R. S. Barbosa, and N. de Silva, Matchgate hierarchy: A clifford-like hierarchy for deterministic gate teleportation in matchgate circuits (2024), arXiv:2410.01887 [quant-ph].
[25] J. Castaneda and N. Wiebe, Hamiltonian learning via shadow

tomography of pseudo-choi states (2023), arXiv:2308.13020 [quant-ph].
[26] A. Zhao, N. C. Rubin, and A. Miyake, Phys. Rev. Lett. **127**, 110504 (2021).
[27] H.-Y. Huang and R. Kueng, Predicting features of quantum systems from very few measurements (2019), arXiv:1908.08909 [quant-ph].
[28] R. Levy, D. Luo, and B. K. Clark, Phys. Rev. Res. **6**, 013029 (2024).
[29] J. Kempe, D. Bacon, D. P. DiVincenzo, and K. B. Whaley, Encoded universality from a single physical interaction (2001), arXiv:quant-ph/0112013 [quant-ph].
[30] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
[31] J. Watrous, *The Theory of Quantum Information*, 1st ed. (Cambridge University Press, USA, 2018).
[32] T. Surawy-Stepney, J. Kahn, R. Kueng, and M. Guta, Quantum **6**, 844 (2022).
[33] J. Cudby and S. Strelchuk, Gaussian decomposition of magic states for matchgate computations (2023), arXiv:2307.12654 [quant-ph].
[34] S. Bravyi and R. Koenig, Classical simulation of dissipative fermionic linear optics (2011), arXiv:1112.2184 [quant-ph].
[35] L. Bittel, A. A. Mele, J. Eisert, and L. Leone, Optimal trace-distance bounds for free-fermionic states: Testing and improved tomography (2025), arXiv:2409.17953 [quant-ph].
[36] X. Lyu and K. Bu, Fermionic gaussian testing and non-gaussian measures via convolution (2024), arXiv:2409.08180 [quant-ph].
[37] J. Liu, H. Yuan, X.-M. Lu, and X. Wang, J. Phys. A: Math. Theor. **53**, 023001 (2020).
[38] V. Iyer, Mildly-interacting fermionic unitaries are efficiently learnable (2025), arXiv:2504.11318 [quant-ph].
[39] G. Stewart, Linear Algebra and its Applications **28**, 213 (1979).
[40] M. Kliesch and I. Roth, PRX Quantum **2**, 010201 (2021).
[41] A. Hahn, D. Burgarth, and K. Yuasa, New J. Phys. **24**, 063027 (2022).

Appendix A: Details of Algorithm 1

In this Appendix, we present proofs for several lemmas related to Algorithm 1. The following lemma describes the decomposition result (Theorem 4 in Ref. [17]) with minor modifications.

Lemma 2 (Decomposition result for U_t)**.** For any given U_t in Eq. (16), there exist Gaussian unitaries G_A and G_B and unitary u_t such that

$$U_t = G_A u_t G_B, \tag{19}$$

where u_t is generated by even-weight Majorana strings containing Majorana operators γ_i with indices $i \in [M]$. Moreover, for the case where all G_j in Eq. (16) correspond to orthogonal matrices in $\mathrm{SO}(2n)$, there exist G_A and G_B that are in $\mathrm{SO}(2n)$.

Proof. As in Eq. (B3) of Ref. [17], we can rewrite U_t from Eq. (16) as $U_t = \tilde{G}_t \prod_{t'=1}^{t} \tilde{K}_{t'}$, where $\tilde{K}_{t'} = \tilde{G}_{t'-1}^{\dagger} K_{t'} \tilde{G}_{t'-1}$ and $\tilde{G}_{t'} = G_{t'} \dots G_0$. We can then write U_t as follows:

$$U_t = \tilde{G}_t G_{\text{aux}} \prod_{t'=1}^{t} (G_{\text{aux}}^{\dagger} \tilde{K}_{t'} G_{\text{aux}}) G_{\text{aux}}^{\dagger}. \tag{A1}$$

This equation holds for an arbitrary G_{aux}. It is possible to find a G_{aux} such that the Majoranas that generate each $K_{t'}$ transform under $\tilde{G}_{t-1} G_{\text{aux}}$ such that they are mapped to the first $M = \kappa t$ Majorana modes. This translates to the condition

$$\mathbf{e}_q^T O_{\text{aux}}^T \mathbf{v}_j = 0, \tag{A2}$$

where $q \in \{M+1, \dots, 2n\}$, $\mathbf{v}_j \in \{\tilde{O}_{t'-1}^T \mathbf{e}_{\mu(t')}\}$, and $\tilde{O}_{t'}$ corresponds to the Gaussian $\tilde{G}_{t'}$ via Eq. (8). Here $\mu(t')$ indexes the Majorana operators in $K_{t'}$ e.g., for $K_1 = \exp(i\theta\gamma_1\gamma_2\gamma_5\gamma_7)$, we have $\mu(1) \in \{1,2,5,7\}$. Since $K_{t'}$ is generated by a Majorana string with weight κ, and $t' \in [t]$, we have $j \in [\kappa t]$. We can choose O_{aux} such that it maps the span of $\{\mathbf{v}_j\}$ to the first $M = \kappa t$ basis vectors, satisfying Eq. (A2). Moreover, without loss of generality, we can choose O_{aux} to be in $\mathrm{SO}(2n)$. Concretely, we can define $O_{\text{aux}}^T = \sum_{k=1}^{M} \mathbf{e}_k \mathbf{s}_k^T + \sum_{k=M+1}^{2n} \mathbf{e}_k \bar{\mathbf{s}}_k^T$, where $\{\mathbf{s}_i\}$ are orthonormal basis vectors that span $\{\mathbf{v}_j\}$, and $\{\bar{\mathbf{s}}_i\}$ are orthonormal vectors outside the span of $\{\mathbf{v}_j\}$. In case O_{aux}^T is not in $\mathrm{SO}(2n)$, we can redefine $O_{\text{aux}}^T \to O_1 O_{\text{aux}}^T$ where $O_1 = \mathrm{diag}(-1, 1, \dots, 1)$, ensuring O_{aux} is in $\mathrm{SO}(2n)$ and satisfies Eq. (A2). We can then write

$$U_t = G_A u_t G_B, \tag{A3}$$

where $G_A = \tilde{G}_t G_{\text{aux}}$, $G_B = G_{\text{aux}}^{\dagger}$, and $u_t = \prod_{t'}^{t} G_{\text{aux}}^{\dagger} \tilde{K}_{t'} G_{\text{aux}}$. In the case all $G_{t'}$ correspond to $\mathrm{SO}(2n)$, it follows that both G_A and G_B correspond to $\mathrm{SO}(2n)$. □

We proceed by establishing a bound on the weight of Majorana strings appearing in $U_t^{\dagger} \gamma_i U_t$ for $i \in [M]$. This result is necessary to prove the subsequent lemmas.

Lemma 14 (A bound on the Majorana weight)**.** The transformed Majorana operators $\bar{\gamma}_i := U_t^{\dagger} \gamma_i U_t$ are sums of Majorana strings with weight upper bounded by $w := (\kappa+1)^t$.

Proof. First, consider the non-Gaussian unitary K_l as defined in Eq. (16). Let K_l be generated by R_l, a product of κ Majorana operators. Since Majorana strings are in the Pauli group, they either commute or anticommute with each other. This means that we need to consider the two cases $R_l = R_l^{\dagger}$ and $R_l = -R_l^{\dagger}$.

Let's consider the case $R_l = R_l^{\dagger}$. We can then write $K_l = e^{-iR_l s}$ (where s is some unknown real parameter). The evolved Majorana operator $\bar{\gamma}_i(s) := K_l^{\dagger} \gamma_i K_l$ is the solution to the differential equation

$$\frac{d}{dy} \bar{\gamma}_i(y) = i e^{iR_l y} [R_l, \gamma_i] e^{-iR_l y}. \tag{A4}$$

In the trivial case wherein $[R_l, \gamma_i] = 0$, we have $\bar{\gamma}_i(s) = \gamma_i$, leaving the Majorana weight unchanged. In the case $\{R_l, \gamma_i\} = 0$, we have

$$\frac{d}{dy}\bar{\gamma}_i(y) = 2iR_l\bar{\gamma}_i(y), \tag{A5}$$

where we used the fact that $\{R_l, \gamma_i\} = 0 \implies [R_l, \gamma_i] = 2R_l\gamma_i$. Eq. (A5) has the solution

$$\bar{\gamma}_i(s) = \cos 2s\gamma_i + i \sin 2sR_l\gamma_i, \tag{A6}$$

where we used the fact that $R_l^2 = 1$ (from the condition that $R_l = R_l^\dagger$ and $R_l R_l^\dagger = 1$). This shows that $\bar{\gamma}_i(s)$ is a sum of operators with Majorana weight $\leq \kappa + 1$.

We now consider the case $R_l = -R_l^\dagger$. We can then write $K_l = e^{R_l s}$. The evolved Majorana operator $\bar{\gamma}_i = K_l^\dagger \gamma_i K_l$ then obeys the differential equation

$$\frac{d}{dy}\bar{\gamma}_i(y) = e^{R_l y}[R_l, \gamma_i]e^{-R_l y}. \tag{A7}$$

In the trivial case wherein $[R_l, \gamma_i] = 0$, we have $\bar{\gamma}_i(s) = \gamma_i$, leaving the Majorana weight unchanged. In the case $\{R_l, \gamma_i\} = 0$, Eq. (A7) then becomes

$$\frac{d}{dy}\bar{\gamma}_i(y) = 2R_l\bar{\gamma}_i(y), \tag{A8}$$

which has the solution

$$\bar{\gamma}_i(s) = \cos 2s\gamma_i + \sin 2sR_l\gamma_i, \tag{A9}$$

where we use the fact that $R_l^2 = -1$ (from the condition that $R_l = -R_l^\dagger$ and $R_l R_l^\dagger = 1$). This shows that $\bar{\gamma}_i(s)$ is a sum of operators with Majorana weight $\leq \kappa + 1$. We therefore have that

$$K_l^\dagger \gamma_i K_l = \sum_{x|\alpha_x \leq \kappa+1} \alpha_x \gamma_x, \tag{A10}$$

where x is a bit-string of length $2n$, $\gamma_x := \gamma_1^{x_1} \cdots \gamma_{2n}^{x_{2n}}$, and α_x denotes the Hamming weight of x.

Now consider the unitary-evolved operator $U_t^\dagger \gamma_i U_t$, where $U_t = G_t K_t \cdots G_1 K_1 G_0$. Since evolution under Gaussian unitaries doesn't change the weight of a Majorana operator, Eq. (A10) shows that the operator $U_t^\dagger \gamma_i U_t$ is a sum of Majorana strings with weight $\leq w := (\kappa + 1)^t$. □

We now prove Lemma 4 regarding the singular values of the matrices c, $c^{(1)}$, and $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$, where $E^{(1)}$ denotes the tomography error in measuring $c^{(1)}$ using Algorithm 1.

Lemma 4 (Useful properties of the matrix c_{xk})**.** The matrix c_{xk} has orthonormal columns, making all its singular values equal to 1. The matrix $c^{(1)}$ has at least $2n - M$ singular values equal to 1. Moreover, the matrix $\hat{c}^{(1)}$, the learned version of $c^{(1)}$, has at least $2n - M$ singular values $\hat{d}_i$ that satisfy

$$|\hat{d}_i - 1| \leq \|E^{(1)}\|, \quad i = M + 1, \ldots, 2n, \tag{28}$$

where $\hat{c}^{(1)}_{jk} = c^{(1)}_{jk} + E^{(1)}_{jk}$, and $E^{(1)}$ is the error from tomography.

Proof. We first describe the properties of γ_x and $\tilde{\gamma}_x$, where $\gamma_x = \gamma_1^{x_1} \ldots \gamma_{2n}^{x_{2n}}$, and $\tilde{\gamma}_x$ is defined as

$$\tilde{\gamma}_x = \gamma_x \quad \text{for } \gamma_x^\dagger = \gamma_x, \tag{A11a}$$
$$\tilde{\gamma}_x = i\gamma_x \quad \text{for } \gamma_x^\dagger = -\gamma_x, \tag{A11b}$$

making $\tilde{\gamma}_x$ Hermitian. Since γ_x satisfy the property

$$\mathrm{tr}\left[\gamma_x \gamma_y^\dagger\right] = d\delta_{x,y}, \tag{A12}$$

where $d = 2^n$, using Eqs. (A11) and (A12), we get

$$\mathrm{tr}[\tilde{\gamma}_x \tilde{\gamma}_y] = d\delta_{x,y}. \tag{A13}$$

For $x \neq y$, $\mathrm{tr}[\tilde{\gamma}_x \tilde{\gamma}_y] = 0$ follows from Eq. (A12). The relation $\mathrm{tr}\left[\tilde{\gamma}_x^2\right] = d$ follows from considering the cases $\gamma_x^\dagger = \gamma_x$ and $\gamma_x^\dagger = -\gamma_x$ separately. For $\gamma_x^\dagger = \gamma_x$, $\mathrm{tr}\left[\tilde{\gamma}_x^2\right] = \mathrm{tr}[\gamma_x \gamma_x] = \mathrm{tr}\left[\gamma_x \gamma_x^\dagger\right] = d$. For $\gamma_x^\dagger = -\gamma_x$, $\mathrm{tr}\left[\tilde{\gamma}_x^2\right] = \mathrm{tr}[(i\gamma_x)(i\gamma_x)] = \mathrm{tr}[\gamma_x(-\gamma_x)] = \mathrm{tr}\left[\gamma_x \gamma_x^\dagger\right] = d$.

We first show that the columns of c are orthonormal. From the definition of c_{xk}, we have

$$U_t^\dagger \gamma_k U_t = \sum_{x \in \{0,1\}^{2n}} c_{xk} \tilde{\gamma}_x. \tag{A14}$$

We then have

$$(U_t^\dagger \gamma_j U_t)(U_t^\dagger \gamma_k U_t) = \sum_{xy} c_{xj} c_{yk} \tilde{\gamma}_x \tilde{\gamma}_y, \tag{A15}$$

$$U_t^\dagger \gamma_j \gamma_k U_t = \sum_{xy} c_{xj} c_{yk} \tilde{\gamma}_x \tilde{\gamma}_y. \tag{A16}$$

Taking $j = k$, and taking the trace of both sides gives us

$$\sum_x c_{xj}^2 = 1, \tag{A17}$$

where we used the fact that $\mathrm{tr}[\tilde{\gamma}_x \tilde{\gamma}_y] = d\delta_{xy}$ from Eq. (A13). Using $j \neq k$, and taking the trace of both sides of Eq. (A16) gives us

$$\sum_x c_{xj} c_{xk} = 0, \tag{A18}$$

where we use Eq. (A13). Since c has orthonormal columns, $c^T c = I$, showing that all singular values of c are 1.

We now focus on the singular values of $c^{(1)}$. Let $c^{(2)}$ contain the rows of c that are not inside $c^{(1)}$. The matrices $\hat{c}^{(1)}$, $\hat{c}^{(2)}$, $E^{(1)}$, and $E^{(2)}$ are defined in the same way, i.e. $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$ and $\hat{c}^{(2)} = c^{(2)} + E^{(2)}$. We first define G_A and G_B using orthogonal matrices O^A and O^B as follows:

$$G_A \gamma_i G_A^\dagger = \sum_{k=1}^{2n} O^A_{ki} \gamma_k, \tag{A19}$$

$$G_B \gamma_i G_B^\dagger = \sum_{k=1}^{2n} O^B_{ki} \gamma_k. \tag{A20}$$

We can expand both sides of Eq. (20) in terms of O^A, O^B, $c^{(1)}$, and $c^{(2)}$ as follows:

$$\sum_j (c^{(1)}O^A)_{ji}\gamma_j + \sum_{x:\alpha_x\geq 2} (c^{(2)}O^A)_{xi}\tilde{\gamma}_x = \sum_j O^B_{ij}\gamma_j, \tag{A21}$$

giving us the equations

$$(c^{(1)}O^A)_{ji} = O^B_{ij}, \tag{A22}$$
$$(c^{(2)}O^A)_{xi} = 0. \tag{A23}$$

Now note that the matrix cO^A also has orthonormal columns from the following computation:

$$\begin{aligned}&(U_t^\dagger G_A\gamma_j G_A^\dagger U_t)(U_t^\dagger G_A\gamma_k G_A^\dagger U_t)\\ &= \sum_{x,y}(cO^A)_{xj}(cO^A)_{yk}\tilde{\gamma}_x\tilde{\gamma}_y,\end{aligned} \tag{A24}$$

$$\begin{aligned}&U_t^\dagger G_A\gamma_j\gamma_k G_A^\dagger U_t\\ &= \sum_{xy}(cO^A)_{xj}(cO^A)_{yk}\tilde{\gamma}_x\tilde{\gamma}_y,\end{aligned} \tag{A25}$$

where we use $U_t^\dagger G_A\gamma_i G_A^\dagger U_t = \sum_k O^A_{ki}U_t^\dagger\gamma_k U_t = \sum_k O^A_{ki}\sum_x c_{xk}\tilde{\gamma}_x = \sum_x (cO^A)_{xi}\tilde{\gamma}_x$. Considering the case $j = k$ and taking the trace of both sides of Eq. (A25) and using Eq. (A13) gives us $\sum_x (cO^A)_{xj}(cO^A)_{xj} = 1$. Taking the case $j \neq k$ and taking the trace of both sides of Eq. (A25) and using Eq. (A13) gives us $\sum_x (cO^A)_{xj}(cO^A)_{xk} = 0$. This means that we can write cO^A as follows:

$$cO^A = \begin{pmatrix} w_1, \ldots, w_M, v_{M+1}, \ldots, v_{2n}\end{pmatrix}, \tag{A26}$$

where vectors w_i and v_i are real orthonormal column vectors with row-index x, where x is a binary string of weight $\leq w$ defined in Lemma 14. Now Eqs. (A22) and (A23) say that the columns $i = M+1, \ldots, 2n$ of cO^A are orthonormal and are nonzero only on the first $2n$ rows of cO^A. We then have

$$c^{(1)}O^A = \begin{pmatrix}\bar{w}_1, \cdots \bar{w}_M, \bar{v}_{M+1}, \cdots \bar{v}_{2n}\end{pmatrix}, \tag{A27}$$

where $\bar{w}_i$ and $\bar{v}_i$ are the truncated versions of w_i and v_i, respectively, such that they contain the first $2n$ elements. Eqs. (A22) and (A23) say that the vectors v_i are supported on the first $2n$ slots and are orthonormal, giving us the conditions

$$\bar{v}_i^T\bar{v}_j = v_i^T v_j = \delta_{ij}, \quad i,j = M+1, \ldots, 2n. \tag{A28}$$

We now compute Y^TY with $Y = c^{(1)}O^A$ as follows:

$$Y^TY = \begin{pmatrix} A & B\\ C & D\end{pmatrix}, \tag{A29}$$

where

$$A_{ij} = \bar{w}_i^T\bar{w}_j, \quad i = 1, \ldots, M, j = 1, \ldots, M, \tag{A30}$$
$$B_{ij} = \bar{w}_i^T\bar{v}_j, \quad i = 1, \ldots, M, j = M+1, \ldots, 2n, \tag{A31}$$
$$C_{ij} = \bar{v}_i^T\bar{w}_j, \quad i = M+1, \ldots, 2n, j = 1, \ldots, M, \tag{A32}$$
$$D_{ij} = \bar{v}_i^T\bar{v}_j, \quad i = M+1, \ldots, 2n, j = M+1, \ldots, 2n. \tag{A33}$$

Since v_i is only supported on the first $2n$ slots, and cO^A has orthonormal columns, we have $B_{ij} = \bar{w}_i^T\bar{v}_j = w_i^T v_j = 0$. Similarly, $C_{ij} = \bar{v}_i^T\bar{w}_j = v_i^T w_j = 0$. Finally, $D_{ij} = \bar{v}_i^T\bar{v}_i = \delta_{ij}$, giving us the block diagonal matrix

$$Y^TY = \begin{pmatrix} A & 0\\ 0 & I\end{pmatrix}, \tag{A34}$$

giving us the result that $c^{(1)}O^A$ has at least $2n - M$ singular values with value 1. Since multiplication by orthogonal matrices doesn't change singular values, it follows that $c^{(1)}$ also has at least $2n - M$ singular values 1.

We now consider the case with errors. We first state Weyl's theorem as follows:

Theorem 15 (Weyl's theorem [39])**.** *Let A be a rectangular matrix with singular values $\sigma_1, \ldots, \sigma_n$, and let $\tilde{A} = A + E$ be a perturbation of A such that $\tilde{A}$ has singular values $\tilde{\sigma}_1, \ldots \tilde{\sigma}_n$. Then the following holds:*

$$|\sigma_i - \tilde{\sigma}_i| \leq \|E\| \quad (i = 1, 2, \ldots, n). \tag{A35}$$

Using the above shows that the matrix $\hat{c}^{(1)}_{xk} = c_{xk} + E^{(1)}_{xk}$ has at least $2n - M$ singular values that obey Eq. (28).

□

We now prove Lemma 5, which shows that the unitary $W_t = G_a^\dagger U_t G_b^\dagger$ approximately satisfies the Majorana decoupling condition in Eq. (24).

Lemma 5 (Constructing the unitary W_t)**.** Given $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$, we can compute descriptions of Gaussian unitaries G_a and G_b such that $W_t = G_a^\dagger U_t G_b^\dagger$ satisfies the following property:

$$\|[W_t, \gamma_i]\| \leq \epsilon_0, \quad i > M, \tag{33}$$

where ϵ_0 obeys the following bound:

$$\epsilon_0 \leq T_1(n)\|E^{(1)}\|^{1/2}, \tag{34}$$

where $T_1(n)$ is a polynomial defined by $T_1(n) = (\sqrt{5}T(n) + 2n + 1)$ with $T(n) = \sum_{x:2\leq\alpha_x\leq w} 1 = \text{poly}(n)$. Here x is a bitstring of length $2n$, and $w = (\kappa+1)^t$ is a constant defined in Lemma 14. Here G_a and G_b are defined in Eqs. (29) and (30), where $O^a = V$ and $O^b = U^T$. The orthogonal matrices U and V are defined from the singular-value decomposition of $\hat{c}^{(1)}$ as $\hat{c}^{(1)} = U\Sigma V^T$, where $\Sigma = \text{diag}(\hat{d}_1, \hat{d}_2, \ldots, \hat{d}_{2n})$ with $\hat{d}_i$ the singular values and where U, V are orthogonal matrices. Moreover, we can always modify O^a and O^b suitably such that they are in SO$(2n)$ and Eq. (33) holds.

Proof. We first order the basis such that for $\hat{c}^{(1)} = U\Sigma V^T$, $\Sigma e_i = \hat{d}_i e_i$, and $\hat{d}_i$ satisfies Eq. (28) for $i = M+1, \ldots, 2n$. We define $\tilde{U}_t = G_a^\dagger U_t$, where G_a is defined by the equation $G_a\gamma_i G_a^\dagger = \sum_k O^a_{ki}\gamma_k$ and $O^a = V$. We can then compute

$\tilde{U}_t^\dagger \gamma_i \tilde{U}_t$ as follows:

$$\tilde{U}_t^\dagger \gamma_i \tilde{U}_t = \sum_k O^a_{ki} U_t^\dagger \gamma_k U_t \tag{A36}$$
$$= \sum_k O^a_{ki} \sum_x c_{xk} \gamma_x \tag{A37}$$
$$= \sum_j (c^{(1)} O^a)_{ji} \gamma_j + \sum_{x:2\le\alpha_x\le w} (c^{(2)} O^a)_{xi} \tilde{\gamma}_x \tag{A38}$$
$$= \sum_j (\hat{c}^{(1)} O^a)_{ji} \gamma_j - \sum_j (E^{(1)} O^a)_{ji} \gamma_j + \sum_{x:2\le\alpha_x\le w} (c^{(2)} O^a)_{xi} \tilde{\gamma}_x \tag{A39}$$
$$= \sum_j U_{ji} \hat{d}_i \gamma_j - \sum_j (E^{(1)} V)_{ji} \gamma_j + \sum_{x:2\le\alpha_x\le w} (c^{(2)} V)_{xi} \tilde{\gamma}_x \tag{A40}$$
$$= \sum_j \hat{d}_i U_{ji} \gamma_j - \sum_j (E^{(1)} V e_i)_j \gamma_j + \sum_{x:2\le\alpha_x\le w} (c^{(2)} V e_i)_x \tilde{\gamma}_x, \tag{A41}$$

where α_x denotes the Hamming weight of x, and w is a constant defined in Lemma 14. In Eq. (A36), we use Eq. (A14). In Eq. (A39), we use $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$. In Eq. (A40), we use $O^a_{ki} = (Ve_i)_k$, where $\Sigma e_i = \hat{d}_i e_i$. In Eq. (A41), we use the fact that $V_{ki} = (Ve_i)_k$, where e_i is the ith computational basis state.

We now compute $W_t^\dagger \gamma_i W_t$, where $W_t = \tilde{U}_t G_b^\dagger$ with $G_b \gamma_i G_b^\dagger = \sum_k O^b_{ki} \gamma_k$ and $O^b = U^T$, as follows:

$$\begin{aligned} &W_t^\dagger \gamma_i W_t \\ =&\sum_k (O^b U)_{ki} \hat{d}_i \gamma_k - \sum_k (E^{(1)} V e_i)_j G_b \gamma_j G_b^\dagger \\ &+ \sum_{x:\alpha_x\ge 2} (c^{(2)} V e_i)_x G_b \tilde{\gamma}_x G_b^\dagger \end{aligned} \tag{A42}$$
$$= \hat{d}_i \gamma_i - \sum_j (E^{(1)} V e_i)_j G_b \gamma_j G_b^\dagger + \sum_{x:\alpha_x\ge 2} (c^{(2)} V e_i)_x G_b \tilde{\gamma}_x G_b^\dagger. \tag{A43}$$

We can then obtain the bound

$$\begin{aligned} &\|W_t^\dagger \gamma_i W_t - \gamma_i\| \\ \le& |\hat{d}_i - 1| + \sum_j |(E^{(1)} V e_i)_j| + \sum_{x:2\le\alpha_x\le w} |(c^{(2)} V e_i)_x| \end{aligned} \tag{A44}$$
$$\le |\hat{d}_i - 1| + |E^{(1)} V e_i| \sum_j 1 + |c^{(2)} V e_i| \sum_{x:2\le\alpha_x\le w} 1 \tag{A45}$$
$$\le |\hat{d}_i - 1| + 2n |E^{(1)} V e_i| + |c^{(2)} V e_i| T(n) \tag{A46}$$
$$\le |\hat{d}_i - 1| + 2n \|E^{(1)}\| + |c^{(2)} V e_i| T(n), \tag{A47}$$

where we use the triangle inequality, the facts that $\|\tilde{\gamma}_x\| = 1$ and $\|.\|$ is unitarily invariant. We define $T(n) := \sum_{x:2\le\alpha_x\le w} 1$. We use here the fact that the Majorana weight of $\tilde{\gamma}_x$ in the above equations is bounded by the constant w from Lemma 14. To simplify the last term in the expression above, let us first consider the following:

$$|cVe_i|^2 = |c^{(1)} V e_i|^2 + |c^{(2)} V e_i|^2 \tag{A48}$$
$$= |\hat{c}^{(1)} V e_i - E^{(1)} V e_i|^2 + |c^{(2)} V e_i|^2 \tag{A49}$$
$$= |\hat{c}^{(1)} V e_i|^2 + |E^{(1)} V e_i|^2 - 2(\hat{c}^{(1)} V e_i) \cdot (E^{(1)} V e_i) + |c^{(2)} V e_i|^2, \tag{A50}$$

where we use $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$ in Eq. (A49), giving us

$$|c^{(2)} V e_i|^2 = |cVe_i|^2 - |\hat{c}^{(1)} V e_i|^2 - |E^{(1)} V e_i|^2 + 2(\hat{c}^{(1)} V e_i) \cdot (E^{(1)} V e_i). \tag{A51}$$

Using the results

$$|cVe_i|^2 \le \|c\|^2 \le 1, \tag{A52}$$
$$(1 - \|E^{(1)}\|)^2 \le |\hat{c}^{(1)} V e_i|^2 = \hat{d}_i^2 \le (1 + \|E^{(1)}\|)^2, \tag{A53}$$
$$|E^{(1)} V e_i|^2 \ge 0, \tag{A54}$$
$$-\hat{d}_i \|E^{(1)}\| \le (\hat{c}^{(1)} V e_i) \cdot (E^{(1)} V e_i) \le \hat{d}_i \|E^{(1)}\|, \tag{A55}$$

where inequality (A52) follows from Lemma 4, inequality (A53) follows from $\hat{c}^{(1)} = U\Sigma V^T$ (and the condition that $\|E^{(1)}\| \le 1$) and Lemma 4, and inequality (A55) follows from Cauchy's inequality. Using these inequalities, Eq. (A51) becomes

$$\begin{aligned} |c^{(2)} V e_i|^2 &\le 1 - (1 - \|E^{(1)}\|)^2 + 2\hat{d}_i \|E^{(1)}\| \\ &\le \|E^{(1)}\|(2 - \|E^{(1)}\|) + 2\|E^{(1)}\|(1 + \|E^{(1)}\|) \\ &\le 5\|E^{(1)}\|, \end{aligned} \tag{A56}$$

where we used the condition $\|E^{(1)}\| \le 1$. Using the above in inequality (A47) gives us

$$\begin{aligned} \|[W_t, \gamma_i]\| &= \|W_t^\dagger \gamma_i W_t - \gamma_i\| \\ &\le (2n+1)\|E^{(1)}\| + (5\|E^{(1)}\|)^{1/2} T(n) \\ &\le T_1(n) \|E^{(1)}\|^{1/2}, \end{aligned} \tag{A57}$$

where $T_1(n)$ is a polynomial defined by $T_1(n) = (\sqrt{5}T(n) + 2n + 1)$.

We now consider the case where either U or V are outside of SO($2n$). The idea is that we can set $G_a \to G_a(\bar{G})^p$ and $G_b \to (\bar{G})^q G_b$, where $p = 1$ ($q = 1$) if U (V) is outside SO($2n$) and $p = 0$ ($q = 0$) if U (V) is inside SO($2n$). We can then consider the unitary $\hat{W}_t = (\bar{G}^\dagger)^p W_t (\bar{G}^\dagger)^q$, where $\bar{G}$ corresponds to the orthogonal matrix $\bar{O} = \mathrm{diag}(-1, 1, \ldots, 1)$ using Eq. (8). Computing $\hat{W}_t^\dagger \gamma_i \hat{W}_t$ for $i > M$ as follows

$$\hat{W}_t^\dagger \gamma_i \hat{W}_t = (\bar{G})^q W_t^\dagger (\bar{G})^p \gamma_i (\bar{G}^\dagger)^p W_t (\bar{G}^\dagger)^q \tag{A58}$$
$$= (\bar{G})^q W_t^\dagger \gamma_i W_t (\bar{G}^\dagger)^q \tag{A59}$$
$$= (\bar{G})^q \gamma_i (\bar{G}^\dagger)^q + (\bar{G})^q W_t^\dagger [\gamma_i, W_t] (\bar{G}^\dagger)^q \tag{A60}$$
$$= \gamma_i + (\bar{G})^q W_t^\dagger [\gamma_i, W_t] (\bar{G}^\dagger)^q \tag{A61}$$

gives us $\|[\hat{W}_t, \gamma_i]\| \leq \epsilon_0$. Here we used the fact that $\|[W_t, \gamma_i]\| \leq \epsilon_0$, that $\|.\|$ is unitarily invariant, and that $\bar{G}\gamma_i\bar{G}^\dagger = \gamma_i$ for $i > M$ from the definition of $\bar{G}$. □

We now prove Lemma 10, which shows that, in the qubit implementation, the matrix elements c_{xk} can be obtained by measuring observables in states prepared using the unitary U_t. This lemma is used in defining Algorithm 1 which constructs the matrix $c^{(1)}$, a submatrix of c_{xk}. For the fermionic implementation, the analogous result is proved in Appendix D.

Lemma 10 (Finding the coefficients c_{xk} (qubit implementation))**.** Let $\mathcal{A}$ be the $d = 2^n$ dimensional Hilbert space upon which the unitary U_t acts. Furthermore, let $\mathcal{B}$ be the Hilbert space of an ancilla register of the same size, and let $\mathcal{C}$ be the Hilbert space of another single ancilla qubit. Consider the state $|\psi_x\rangle$ defined as

$$\begin{aligned}|\psi_x\rangle =& \frac{1}{\sqrt{2}}\big[(U_t \otimes I)\,|\Phi_d\rangle_{\mathcal{AB}}\,|0\rangle_{\mathcal{C}} \\ &+ (U_t \otimes I)(\gamma_x^\dagger \otimes I)\,|\Phi_d\rangle_{\mathcal{AB}}\,|1\rangle_{\mathcal{C}}\big],\end{aligned} \tag{48}$$

where $|\Phi_d\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i,i\rangle_{\mathcal{AB}}$ is the maximally entangled state between systems $\mathcal{A}$ and $\mathcal{B}$, and $\gamma_x = \gamma_1^{x_1}\ldots\gamma_{2n}^{x_{2n}}$. The coefficients c_{xk} [defined in Eq. (25)] can be obtained using expectation values of observables

$$O_k^+ = O_k + O_k^\dagger = (\gamma_k \otimes I)_{\mathcal{AB}} \otimes X_{\mathcal{C}}, \tag{49}$$

$$O_k^- = iO_k - iO_k^\dagger = (\gamma_k \otimes I)_{\mathcal{AB}} \otimes Y_{\mathcal{C}}, \tag{50}$$

such that $c_{xk} = \operatorname{tr}\left[|\psi_x\rangle\langle\psi_x|\,O_k^+\right]$ for $\gamma_x^\dagger = \gamma_x$, and $c_{xk} = \operatorname{tr}\left[|\psi_x\rangle\langle\psi_x|\,O_k^-\right]$ for $\gamma_x^\dagger = -\gamma_x$.

Proof. Let $\rho_x = |\psi_x\rangle\langle\psi_x|$. We show that the operator

$$O_k = (\gamma_k \otimes I)_{\mathcal{AB}} \otimes |1\rangle\langle 0|_{\mathcal{C}}\,, \tag{A62}$$

can be used to estimate c_{xk} from the following computation. We can write $\rho_x O_k$ as follows:

$$\begin{aligned}\rho_x O_k =& \frac{1}{2}\big[(U_t \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\,(\gamma_x U_t^\dagger \gamma_k \otimes I) \otimes |0\rangle\langle 0| \\ &+ (U_t\gamma_x^\dagger \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\,(\gamma_x U_t^\dagger \gamma_k \otimes I) \otimes |1\rangle\langle 0|\,\big].\end{aligned} \tag{A63}$$

Computing the trace on both sides gives us

$$\begin{aligned}\operatorname{tr}[\rho_x O_k] &= \frac{1}{2}\operatorname{tr}\left[(U_t \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\,(\gamma_x U_t^\dagger \gamma_k \otimes I)\right] \\ &= \frac{1}{2}\operatorname{tr}\left[(\gamma_x U_t^\dagger \gamma_k U_t \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\right] \\ &= \frac{1}{2}\langle\Phi_d|\,\gamma_x U_t^\dagger \gamma_k U_t \otimes I\,|\Phi_d\rangle \\ &= \frac{1}{2d}\sum_i \langle i|\,\gamma_x U_t^\dagger \gamma_k U_t\,|i\rangle \\ &= \frac{1}{2d}\operatorname{tr}_{\mathcal{A}}\left[U_t^\dagger \gamma_k U_t \gamma_x\right].\end{aligned} \tag{A64}$$

Let $a_{xk} = \operatorname{tr}[\rho_x O_k]$. First, consider the case $\gamma_x^\dagger = \gamma_x$. We have

$$\begin{aligned}a_{xk}^* &= \frac{1}{2d}\operatorname{tr}\left[(U_t^\dagger \gamma_k U_t \gamma_x)^\dagger\right] \\ &= \frac{1}{2d}\operatorname{tr}\left[U_t^\dagger \gamma_k U_t \gamma_x^\dagger\right] \\ &= a_{xk},\end{aligned} \tag{A65}$$

showing $\operatorname{tr}[\rho_x O_k]$ is real. We can compute $\operatorname{tr}\left[\rho_x O_k^+\right]$ using Eq. (49) as follows:

$$\begin{aligned}\operatorname{tr}\left[\rho_x O_k^+\right] &= \operatorname{tr}[\rho_x O_k] + \operatorname{tr}\left[\rho_x O_k^\dagger\right] \\ &= \operatorname{tr}[\rho_x O_k] + \operatorname{tr}\left[(\rho_x O_k)^\dagger\right] \\ &= 2\operatorname{Re}\operatorname{tr}[\rho_x O_k] \\ &= 2\operatorname{tr}[\rho_x O_k],\end{aligned} \tag{A66}$$

where we used the fact that $\operatorname{tr}[\rho_x O_k]$ is real. We now consider $\gamma_x^\dagger = -\gamma_x$. We then have

$$\begin{aligned}a_{xk}^* &= \frac{1}{2d}\operatorname{tr}\left[U_t^\dagger \gamma_k U_t \gamma_x^\dagger\right] \\ &= -\frac{1}{2d}\operatorname{tr}\left[U_t^\dagger \gamma_k U_t \gamma_x\right] \\ &= -a_{xk},\end{aligned} \tag{A67}$$

showing $\operatorname{tr}[\rho_x O_k]$ is imaginary. We can compute $\operatorname{tr}\left[\rho_x O_k^-\right]$ using Eq. (50) as follows:

$$\begin{aligned}\operatorname{tr}\left[\rho_x O_k^-\right] &= i\operatorname{tr}[\rho_x O_k] - i\operatorname{tr}\left[\rho_x O_k^\dagger\right] \\ &= i\operatorname{tr}[\rho_x O_k] - i\operatorname{tr}\left[(\rho_x O_k)^\dagger\right] \\ &= i\operatorname{tr}[\rho_x O_k] - i\operatorname{tr}[\rho_x O_k]^* \\ &= -2\operatorname{Im}\operatorname{tr}[\rho_x O_k] \\ &= 2i\operatorname{tr}[\rho_x O_k],\end{aligned} \tag{A68}$$

where we use the fact that $\operatorname{tr}[\rho_x O_k]$ is imaginary. Finally, the coefficient c_x can be written as

$$c_{xk} = 2\operatorname{tr}[\rho_x O_k] = \operatorname{tr}\left[\rho_x O_k^+\right] \quad \text{for } \gamma_x^\dagger = \gamma_x, \tag{A69}$$

$$c_{xk} = 2i\operatorname{tr}[\rho_x O_k] = \operatorname{tr}\left[\rho_x O_k^-\right] \quad \text{for } \gamma_x^\dagger = -\gamma_x, \tag{A70}$$

where we use the definition of c_x in Eq. (25), as well as Eqs. (A66) and (A68). We can specialize to the case where $\alpha_x = 1$ and $x_j = 1$, which makes $c_{jk}^{(1)}$ a real matrix. In this case, we only measure O_k^+ since $O_k \propto (O_k^+ - iO_k^-)$ and $c_{jk}^{(1)} \propto \operatorname{tr}[\rho_j O_k]$ (since $c_{jk}^{(1)}$ is a real matrix). □

We now prove Lemma 11 that gives, for the qubit implementation, guarantees on the error in measuring the matrix $c^{(1)}$ using shadow tomography. The analogous result for the fermionic implementation is proved in Appendix D.

Lemma 11 (Estimating the matrix $c^{(1)}$ through shadow tomography for the qubit implementation)**.** Using shadow tomography with the fermionic Gaussian unitary ensemble [26],

we can estimate the matrix $c^{(1)}_{jk} = \mathrm{tr}\left[U_t^\dagger \gamma_k U_t \gamma_j\right]/d$ by measuring the expectation values of the operators O_k^+ in state $|\psi_j\rangle$. With probability $\geq 1-\delta$, we obtain the matrix $\hat{c}^{(1)} = c^{(1)} + E^{(1)}$ such that $\|E^{(1)}\| \leq \|E^{(1)}\|_2 \leq \epsilon$. For each row $j \in [2n]$ of $c^{(1)}_{jk}$, we need N_c copies of the state $|\psi_j\rangle$, where

$$N_c = \left(1 + \frac{\epsilon}{6n}\right) \log\left(8n^2/\delta\right) \frac{4n^2(4n+1)}{\epsilon^2}. \tag{54}$$

Moreover, the required classical post-processing to compute the expectation values can be done efficiently [26].

Proof. We first reorder the Hilbert spaces as $\mathcal{C} \otimes \mathcal{A} \otimes \mathcal{B}$ so that observables O_k^+ can be written as Majorana strings of weight two. We then define new Majorana operators $\hat{\gamma}_i$ as follows:

$$\hat{\gamma}_1 = X_{\mathcal{C}}, \tag{A71}$$
$$\hat{\gamma}_2 = Y_{\mathcal{C}}, \tag{A72}$$
$$\hat{\gamma}_i = Z_{\mathcal{C}} \gamma_{i-2}, \quad i = 3, \ldots, 4n+2, \tag{A73}$$

where γ_i are the Majorana operators defined in the same way as in Eqs. (5) and (6) on $\mathcal{A} \otimes \mathcal{B}$ containing qubits $1, \ldots, 4n$. This gives us the following representation of the operators $O_k^\pm$ defined in Eqs. (49) and (50):

$$O_k^+ = i\hat{\gamma}_{k+2}\hat{\gamma}_2, \tag{A74}$$
$$O_k^- = -i\hat{\gamma}_{k+2}\hat{\gamma}_1. \tag{A75}$$

From Eq. (12) in Theorem 2 of Supp. Mat. in Ref. [26], estimating a Majorana observable O_j with Majorana weight $2k$ with error ϵ with probability $\geq 1-\delta$ requires N_c copies of the state, where N_c is

$$N_c = \left(1 + \frac{\epsilon}{3}\right) \frac{\log(2L/\delta)}{\epsilon^2} \mathrm{max}_{1 \leq j \leq L} \|O_i\|^2_{\mathcal{U}}, \tag{A76}$$

where $\|O_i\|^2_{\mathcal{U}} = \binom{2\bar{n}}{2k} / \binom{\bar{n}}{k}$, where $\bar{n}$ is the number of qubits, and $2k$ is the Majorana weight of the observable O_j (equal to 2 in our case). Since each state $|\psi_j\rangle$ is used to construct each row of $c^{(1)}_{jk}$, we have $L = 2n$ observables. Moreover, because we want the entire error matrix $E^{(1)}$ to have Frobenius norm $\leq \epsilon$ with probability $\geq 1-\delta$, we set $\delta \to \delta/2n$, and $\epsilon \to \epsilon/2n$ to obtain Eq. (54). □

Appendix B: The Pauli decoupling theorem for $\bar{W}_t$ and guarantee for the reduced quantum channel

In this Appendix, we first show that $\bar{W}_t$ from Definition 7 satisfies the Pauli decoupling condition in Eq. (39). We then state and prove Lemma 9, which shows that the Pauli decoupling property satisfied by W_t in Eq. (35) and $\bar{W}_t$ in Eq. (39) ensures that these unitaries can be approximated by their corresponding reduced quantum channels from Definition 8.

Let's first consider the case where $[W_t, \gamma_i] = 0$ for $i > M$. We can then show that $\bar{W}_t$ acts only on the first m qubits. This is shown in the following lemma.

Lemma 16 (Properties of $\bar{W}_t$ for exact Majorana decoupling)**.** In the case where $[W_t, \gamma_i] = 0$ for $i = M+1, \ldots, 2n$, the following holds:

$$\bar{W}_t = \langle\bar{0}| W_t |\bar{0}\rangle_A \otimes I_B, \tag{B1}$$

where register A contains qubits labeled $1, \ldots, m$, register B contains qubits labeled $m+1, \ldots, n$, I_B is the identity on qubits in register B, $|\bar{0}\rangle$ is the state $|0^{n-m}\rangle$ defined on qubits in register B, and $\langle\bar{0}| W_t |\bar{0}\rangle$ is an operator defined on register A.

Proof. We first consider the following expression for W_t:

$$W_t = \sum_{\bar{x},\bar{y}} \langle\bar{x}| W_t |\bar{y}\rangle_A \otimes |\bar{x}\rangle\langle\bar{y}|_B, \tag{B2}$$

where $|\bar{x}(\bar{y})\rangle$ is a computational basis state on qubits $m+1, \ldots, n$. The first observation is that $\langle\bar{x}| W_t |\bar{y}\rangle = 0$ unless $\bar{x} = \bar{y}$. This is because $\Pi_{\bar{z}} := I^{[1]} \otimes |\bar{z}\rangle\langle\bar{z}|$, where $I^{[1]}$ is the identity on the qubit block [1] which consists of qubits $1, \ldots, m$, commutes with W_t for all $\bar{z}$. This follows because

$$\Pi_{\bar{z}} = \frac{1}{2^{n-m}}[1 + (-1)^{z_{m+1}}(-i\gamma_{2m+1}\gamma_{2m+2})] \cdots [1 + (-1)^{z_n}(-i\gamma_{2n-1}\gamma_{2n})], \tag{B3}$$

and $[W_t, \gamma_i] = 0$ for $i = 2m+1, \ldots, 2n$. Then $\langle\bar{x}| W_t |\bar{y}\rangle = \langle\bar{x}| W_t \Pi_{\bar{y}} |\bar{y}\rangle = \langle\bar{x}| \Pi_{\bar{y}} W_t |\bar{y}\rangle = 0$ unless $\bar{x} = \bar{y}$. This allows us to simplify W_t as follows:

$$W_t = \sum_{\bar{x}} \langle\bar{x}| W_t |\bar{x}\rangle_A |\bar{x}\rangle\langle\bar{x}|_B. \tag{B4}$$

We now relate $\langle\bar{x}| W_t |\bar{x}\rangle$ to $\langle\bar{0}| W_t |\bar{0}\rangle$ as follows:

$$\langle\bar{x}| W_t |\bar{x}\rangle = \sum_{x'y'} \langle x'\bar{x}| W_t |y'\bar{x}\rangle |x'\rangle\langle y'| \tag{B5}$$
$$= \sum_{x'y'} \langle 0| \Gamma^\dagger_{x'\bar{x}} W_t \Gamma_{y'\bar{x}} |0\rangle |x'\rangle\langle y'|, \tag{B6}$$

where $|0\rangle := |0_1 \cdots 0_n\rangle$ and

$$\Gamma_x := \gamma_1^{x_1} \gamma_3^{x_2} \ldots \gamma_{2n-1}^{x_n}. \tag{B7}$$

We further simplify the matrix element $\langle 0| \Gamma^\dagger_{x'\bar{x}} W_t \Gamma_{y'\bar{x}} |0\rangle$ as follows:

$$\langle 0| \Gamma^\dagger_{x'\bar{x}} W_t \Gamma_{y'\bar{x}} |0\rangle \tag{B8}$$
$$= \Gamma^2_{y'\bar{x}} \Gamma^2_{x'\bar{x}} \langle 0| \Gamma_{x'\bar{x}} W_t \Gamma^\dagger_{y'\bar{x}} |0\rangle \tag{B9}$$
$$= \Gamma^2_{y'\bar{x}} \Gamma^2_{x'\bar{x}} \langle 0| \Gamma_{x'} \Gamma_{\bar{x}} W_t \Gamma^\dagger_{\bar{x}} \Gamma^\dagger_{y'} |0\rangle \tag{B10}$$
$$= \Gamma^2_{y'\bar{x}} \Gamma^2_{x'\bar{x}} \langle 0| \Gamma_{x'} \Gamma_{\bar{x}} \Gamma^\dagger_{\bar{x}} W_t \Gamma^\dagger_{y'} |0\rangle \tag{B11}$$
$$= \Gamma^2_{y'\bar{x}} \Gamma^2_{x'\bar{x}} \langle 0| \Gamma_{x'} W_t \Gamma^\dagger_{y'} |0\rangle \tag{B12}$$
$$= \Gamma^2_{y'\bar{x}} \Gamma^2_{x'\bar{x}} \Gamma^2_{x'} \Gamma^2_{y'} \langle 0| \Gamma^\dagger_{x'} W_t \Gamma_{y'} |0\rangle \tag{B13}$$
$$= \Gamma^2_{y'\bar{x}} \Gamma^2_{x'\bar{x}} \Gamma^2_{x'} \Gamma^2_{y'} \langle x'\bar{0}| W_t |y'\bar{0}\rangle, \tag{B14}$$

where we use the following facts:

$$\Gamma_x = \Gamma_x^2 \Gamma_x^\dagger, \tag{B15}$$
$$\Gamma_x^2 = (\Gamma_x^2)^\dagger = \pm 1, \tag{B16}$$
$$\Gamma_{x'\bar{y}} = \Gamma_{x'} \Gamma_{\bar{y}}, \tag{B17}$$
$$[W_t, \Gamma_{\bar{x}}^\dagger] = 0, \tag{B18}$$
$$\Gamma_x \Gamma_x^\dagger = 1, \tag{B19}$$

where we define $\Gamma_{x'} = \Gamma_{x'0\ldots0}$ and $\Gamma_{\bar{x}} = \Gamma_{0\cdots0\bar{x}}$, with $x' = x_1, \ldots, x_m$ and $\bar{x} = x_{m+1}, \ldots, x_n$. This gives us

$$\langle \bar{x} | W_t | \bar{x} \rangle = \sum_{x'y'} \Gamma_{y'\bar{x}}^2 \Gamma_{x'\bar{x}}^2 \Gamma_{x'}^2 \Gamma_{y'}^2 \langle x'\bar{0} | W_t | y'\bar{0} \rangle | x' \rangle\langle y' | . \tag{B20}$$

We can then write

$$\langle \bar{x} | W_t | \bar{x} \rangle = U_d V_{\bar{x}} \langle \bar{0} | W_t | \bar{0} \rangle V_{\bar{x}} U_d, \tag{B21}$$

where $V_{\bar{x}}$ and U_d are diagonal unitaries on registers A and B, respectively, as follows:

$$V_{\bar{x}} | x' \rangle = \Gamma_{x'\bar{x}}^2 | x' \rangle , \tag{B22}$$
$$U_d | x' \rangle = \Gamma_{x'}^2 | x' \rangle . \tag{B23}$$

Using Eq. (B4), we then get

$$W_t = U_d V_d \left(\langle \bar{0} | W_t | \bar{0} \rangle \otimes \bar{I} \right) V_d U_d, \tag{B24}$$

where

$$V_d = \sum_{\bar{x}} V_{\bar{x}} \otimes | \bar{x} \rangle\langle \bar{x} |_B . \tag{B25}$$

Moreover, we can simplify the form of the unitary V as follows:

$$V_d = \sum_{\bar{x}} \sum_{x'y'} \langle x' | V_{\bar{x}} | y' \rangle | x'\bar{x} \rangle \langle y'\bar{x} | \tag{B26}$$
$$= \sum_{\bar{x}} \sum_{x'y'} \Gamma_{y'\bar{x}}^2 \langle x' | y' \rangle | x'\bar{x} \rangle\langle y'\bar{x} | \tag{B27}$$
$$= \sum_{x'\bar{x}} \Gamma_{x'\bar{x}}^2 | x'\bar{x} \rangle\langle x'\bar{x} | \tag{B28}$$
$$= \sum_{x} \Gamma_x^2 | x \rangle\langle x | . \tag{B29}$$

□

We now consider the practical case where $\|[W_t, \gamma_i]\| = \epsilon_0$ with $i \in [M]$. We first gather a few useful properties about the unitaries U_d and V_d that define $\bar{U}_d$ in $\bar{W}_t = \bar{U}_d^\dagger W_t \bar{U}_d$ via Eqs. (38) and (37) in the following lemma.

Lemma 17 (Some properties of unitaries U_d and V_d)**.** The unitaries U_d and V_d satisfy the following properties.

(a) The diagonal entries of U_d and V_d satisfy $\langle x' | U_d | x' \rangle = \Gamma_{x'}^2$ and $\langle x | V_d | x \rangle = \Gamma_x^2$, respectively, where x' is the computational basis state on qubits $1, \ldots, m$, x is the computational basis state on qubits $1, \ldots, n$, and Γ_x is defined in Eq. (B7). Moreover, we can show that $\Gamma_x^2 = p(\alpha_x)$, where α_x is the Hamming weight of x, and $p(\alpha) = (-1)^{\alpha(\alpha-1)/2}$ obeys the following recursive relation:

$$p(\alpha) = (-1)^{\alpha-1} p(\alpha - 1), \tag{B30}$$

with $p(0) = 1$. Both U_d and V_d can be efficiently implemented using Hamiltonian simulation of a 2-local Hamiltonian.

(b) For $k = 1, \ldots, n$, we have that

$$[Z_k, V_d] = 0, \tag{B31}$$
$$\Big(\prod_{l \neq k}^{n} Z_l \Big) X_k V_d X_k = V_d. \tag{B32}$$

(c) For $\|[W_t, \gamma_i]\| \leq \epsilon_0$, we have the following error bounds:

$$\left\| [W_t, (Z_{m+1}^{x_{m+1}} \cdots Z_n^{x_n})] \right\| \leq 2\alpha_y \epsilon_0, \tag{B33}$$

where $y = x_{m+1}, \ldots, x_n$ and α_x is the Hamming weight of x.

Proof.

(a) This follows from the definition of the unitaries in Eqs. (37) and (38). The recursive formula for Γ_x^2 follows from the definition of Γ_x.

(b) Since V_d and Z_k are diagonal unitaries, they commute. We now prove Eq. (B32). We can write V_d from Eq. (37) as follows:

$$V_d = \sum_{x \setminus x_k} \Gamma_{\beta_k}^2 | \beta_k \rangle\langle \beta_k | + \Gamma_{\beta_k'}^2 | \beta_k' \rangle\langle \beta_k' | , \tag{B34}$$

where $\beta_k = x_1 \ldots x_{k-1} 0_k x_{k+1} \ldots x_n$ and $\beta_k' = x_1 \ldots x_{k-1} 1_k x_{k+1} \ldots x_n$. First note that

$$X_k V_d X_k = \sum_{x \setminus x_k} \Gamma_{\beta_k'}^2 | \beta_k \rangle\langle \beta_k | + \Gamma_{\beta_k}^2 | \beta_k' \rangle\langle \beta_k' | . \tag{B35}$$

We can compute the left-hand side of Eq. (B32) as follows:

$$\Big(\prod_{l=1, l\neq k}^{n} Z_l \Big) X_k V_d X_k = \sum_{x \setminus x_k} \Gamma_{\beta_k'}^2 (-1)^{\alpha_k} | \beta_k \rangle\langle \beta_k | + \Gamma_{\beta_k}^2 (-1)^{\alpha_k} | \beta_k' \rangle\langle \beta_k' | , \tag{B36}$$

where we use $\alpha_k := \alpha_b$ with $b = \beta_k$. Finally, using the relation $\Gamma_{\beta_k'}^2 (-1)^{\alpha_k} = \Gamma_{\beta_k}^2$ from Eq. (B30), we obtain Eq. (B32).

(c) Using the commutator identity $[A, BC] = [A, B]C + B[A, C]$, the triangle inequality for the spectral norm, the fact that $\|U\| = 1$ for a unitary U, and $Z_i = -i\gamma_{2i-1}\gamma_{2i}$, we get Eq. (B33). □

We now prove Lemma 18, which shows that $\bar{W}_t$ satisfies the Pauli decoupling property in Eq. (39) when $[W_t, \gamma_i] \approx 0$ for $i > M$.

Lemma 18 (Locality property of $\bar{W}_t$)**.** We consider here the unitary $\bar{W}_t = U_d V_d W_t V_d U_d$, where W_t satisfies $\|[W_t, \gamma_i]\| \leq \|\epsilon_0\|$ for $i = 2m+1, \ldots, 2n$ from Eq. (33) in Lemma 5. Then $\bar{W}_t$ satisfies the following properties:

$$\|[\bar{W}_t, Z_k]\| \leq 2\epsilon_0, \tag{B37}$$
$$\|[\bar{W}_t, X_k]\| \leq (2n+1)\epsilon_0, \tag{B38}$$
$$\|[\bar{W}_t, Y_k]\| \leq 2(n+1)\epsilon_0, \tag{B39}$$

for $k = m+1, \ldots, n$. Here ϵ_0 is defined in Eq. (34). Moreover, we can then prove that $\bar{W}_t$ satisfies the Pauli decoupling property as follows:

$$\frac{1}{2} \sum_{P \in \{X,Y,Z\}} \big\|[\bar{W}_t, P_i]\big\| \leq \epsilon_P, \;\; \epsilon_P = (2n+3)\epsilon_0, \tag{39}$$

where P_i acts on the qubit labeled $i \in \{m+1, \ldots, n\}$.

Proof. We first prove Eq. (B37). We have

$$\bar{W}_t Z_k = U_d V_d W_t V_d U_d Z_k \tag{B40}$$
$$= U_d V_d W_t Z_k V_d U_d \tag{B41}$$
$$= U_d V_d Z_k W_t V_d U_d + \tilde{O}_3 \tag{B42}$$
$$= Z_k U_d V_d W_t V_d U_d + \tilde{O}_3, \tag{B43}$$

where we used the facts that U_d acts on qubits $1, \ldots, m$, Z_k commutes with V_d from Eq. (B31), and that $\tilde{O}_3 = U^{(1)}[W_t, Z_k]U^{(2)}$, for some unitaries $U^{(1)}$ and $U^{(2)}$, with $\|[W_t, Z_k]\| \leq 2\epsilon_0$ from Eq. (B33). This gives us Eq. (B37).

We now prove Eq. (B38). We first compute $X_k W_t X_k$ as follows:

$$X_k W_t X_k = (Z_1 \cdots Z_{k-1})\gamma_{2k-1} W_t \gamma_{2k-1} (Z_1 \cdots Z_{k-1}) \tag{B44}$$
$$= (Z_1 \cdots Z_{k-1}) W_t (Z_1 \cdots Z_{k-1}) + O_1 \tag{B45}$$
$$= (Z_1 \cdots Z_{k-1}) U_{z,k+1} U_{z,k+1} W_t (Z_1 \cdots Z_{k-1}) + O_1, \tag{B46}$$

where $O_1 = U^{(3)}[W_t, \gamma_{2k-1}]U^{(4)}$ for some unitaries $U^{(3)}$, $U^{(4)}$, and $U_{z,k+1} = \prod_{l=k+1}^{n} Z_l$. Continuing the calculation gives us

$$X_k W_t X_k = (Z_1 \cdots Z_{k-1}) U_{z,k+1} W_t U_{z,k+1} (Z_1 \cdots Z_{k-1}) + O_1 + O_2 \tag{B47}$$
$$= \Big(\prod_{l=1, l\neq k}^{n} Z_l\Big) W_t \Big(\prod_{l=1, l\neq k}^{n} Z_l\Big) + O_1 + O_2, \tag{B48}$$

where $O_2 = U^{(5)}[U_{z,k+1}, W_t]U^{(6)}$ for some unitaries $U^{(5)}$, $U^{(6)}$. We have $\|O_1\| \leq \epsilon_0$ from Eq. (33), and $\|O_2\| \leq 2n\epsilon_0$ from Eq. (B33). We can then compute the commutator in Eq. (B38) as follows. First, consider

$$\bar{W}_t X_k = U_d V_d W_t V_d U_d X_k \tag{B49}$$
$$= U_d X_k (X_k V_d X_k)(X_k W_t X_k)(X_k V_d X_k) U_d, \tag{B50}$$

where we insert the identity $X_k^2 = 1$ in Eq. (B50) and use the fact that U_d commutes with V_d. Inserting the expression for $X_k W_t X_k$ from Eq. (B48) and gives us

$$\bar{W}_t X_k = U_d X_k (X_k V_d X_k) \Big(\prod_{l=1, l\neq k}^{n} Z_l\Big) W_t \Big(\prod_{l=1, l\neq k}^{n} Z_l\Big)(X_k V_d X_k) U_d + \tilde{O}_1 + \tilde{O}_2 \tag{B51}$$
$$= X_k U_d V_d W_t V_d U_d + \tilde{O}_1 + \tilde{O}_2, \tag{B52}$$

where $\tilde{O}_i = U^{(i5)} O_i U^{(i6)}$ for some unitaries $U^{(i5)}$, $U^{(i6)}$. We use the fact that $\big(\prod_{l=1,l\neq k}^{n} Z_l\big)(X_k V_d X_k) = V_d$ from Eq. (B32), and $(X_k V_d X_k)\big(\prod_{l=1,l\neq k}^{n} Z_l\big) = V_d$ since both $X_k V_d X_k$ and $\big(\prod_{l=1,l\neq k}^{n} Z_l\big)$ are diagonal operators (see Eq. (B35) for the explicit form of $X_k V_d X_k$). This gives us $[\bar{W}_t, X_k] = \tilde{O}_1 + \tilde{O}_2$, where $||\tilde{O}_1|| \leq \epsilon_0$, $||\tilde{O}_2|| \leq 2n\epsilon_0$, proving Eq. (B38). Finally, using Eqs. (B38) and (B39) and the fact that $Y = iXZ$ gives us Eq. (B39). Finally, we can obtain Eq. (39) using Eqs. (B37–B39). □

We now prove Lemma 9, which shows that the Pauli decoupling property, shown to hold for W_t and $\bar{W}_t$ in Eqs. (35) and (39), respectively, leads to a reduced quantum channel that is close to the action of the unitary channel. This is proved in the following lemma.

Lemma 9 (Approximating a unitary channel as a reduced quantum channel)**.** The channel $\mathcal{E}_m^{\mathcal{U}}$ is a CPTP (completely positive and trace preserving) map that satisfies

$$\mathcal{D}_\diamond\Big(\mathcal{U}, \mathcal{E}_m^{\mathcal{U}} \otimes \mathcal{I}_B\Big) \leq n\epsilon, \tag{41}$$

where $\mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2)$ is defined in Eq. (14), and $\mathcal{I}_B$ is the identity channel on register B, given the following condition holds:

$$\frac{1}{2} \sum_{P \in \{X,Y,Z\}} \|[U, P_i]\| \leq \epsilon, \tag{42}$$

where $i \geq m+1$.

Proof. We first show here that $\mathcal{E}_m^U$ is a CPTP map. Let ρ be a quantum state over m qubits. The channel $\mathcal{E}_m^U$ can be rewritten as follows:

$$\mathcal{E}_m^{\mathcal{U}}(\rho) = \frac{1}{2^{n-m}} \operatorname{tr}_{\geq m}[U(\rho \otimes I)U^\dagger] \tag{B53}$$
$$= \frac{1}{2^{n-m}} \sum_{\bar{z}\bar{x}} \langle \bar{z}| U |\bar{x}\rangle\langle \bar{x}| (\rho \otimes I) U^\dagger |\bar{z}\rangle \tag{B54}$$
$$= \sum_{\bar{z}\bar{x}} E_{\bar{z}\bar{x}} \rho E_{\bar{z}\bar{x}}^\dagger, \tag{B55}$$

where $E_{\bar{z}\bar{x}} = \langle \bar{z}| U |\bar{x}\rangle / \sqrt{2^{n-m}}$ and $|\bar{x}\rangle = |x_{m+1} \dots x_n\rangle$ is a state on the qubits $m+1, \dots, n$. Since $\sum_{\bar{z}\bar{x}} E^{\dagger}_{\bar{z}\bar{x}} E_{\bar{z}\bar{x}} = I^{\otimes m}$, it follows that $\mathcal{E}^U_m$ is a CPTP map (see Corollary 2.27 in [31] for details).

We now prove Eq. (41). Let's first define qubit blocks such that qubits $1, \dots, m$ are denoted as $[1]$, qubits $m+1, \dots, n$ are denoted as $[2]$, qubits $n, \dots, 2n$ are denoted as $[3]$, and qubits $2n+1, \dots, 3n-m$ are denoted as $[4]$.

We denote concatenated qubit blocks as $[i, \dots, j]$, where $[i], [j]$ are the qubit blocks we defined earlier. Consider a state $\rho^{[1,2,3]}$ over registers $[1,2,3]$. We first note that

$$\left\| (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]})\rho^{[1,2,3]} - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[2,3]})\rho^{[1,2,3]} \right\|_1 \tag{B56}$$

$$= \left\| \operatorname{tr}_{[4]} \left[(\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3,4]}) \left(\rho^{[1,2,3]} \otimes \frac{I^{\otimes n-m}}{2^{n-m}} \right) \right] - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[2,3]})(\rho^{[1,2,3]}) \right\|_1 \tag{B57}$$

$$= \Bigg\| \operatorname{tr}_{[2]} \left[(\mathcal{S}_{[2],[4]} \circ (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3,4]})) \left(\rho^{[1,2,3]} \otimes \frac{I^{\otimes n-m}}{2^{n-m}} \right) \right] - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[4,3]})(\rho^{[1,4,3]}) \Bigg\|_1, \tag{B58}$$

where the swap unitary S between qubit blocks 2 and 4 is defined as follows:

$$\mathcal{S}_{[2],[4]} = \mathcal{S}_{m+1,2n+1} \circ \dots \circ \mathcal{S}_{n,3n-m}, \tag{B59}$$

and the channel corresponding to the swap is denoted by $\mathcal{S}$. Now we can use the triangle inequality to get

$$\left\| (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]})\rho^{[1,2,3]} - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[2,3]})\rho^{[1,2,3]} \right\|_1 \tag{B60}$$

$$\leq \Bigg\| \operatorname{tr}_{[2]} \left[(\mathcal{S}_{m+1,2n+1} \circ \dots \circ (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3,4]}) \circ \mathcal{S}_{n,3n-m}) \left(\rho^{[1,2,3]} \otimes \frac{I^{\otimes n-m}}{2^{n-m}} \right) \right] - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[4,3]})\rho^{[1,4,3]} \Bigg\|_1 + \left\| \mathcal{S}_{m+1,2n+1} \circ \dots \circ \mathcal{C}_1 \left(\rho^{[1,2,3]} \otimes \frac{I^{\otimes n-m}}{2^{n-m}} \right) \right\|_1, \tag{B61}$$

where $\mathcal{C}_1 = \mathcal{S}_{n,3n-m} \circ (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]}) - (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]}) \circ \mathcal{S}_{n,3n-m}$, and we used the fact that partial trace cannot increase $\|.\|_1$. Since all $\mathcal{S}_{i,j}$ are unitary channels, the last term in Eq. (B61) can be simplified to

$$\left\| (S_{m+1,2n+1} \circ \dots \circ \mathcal{C}_1)(\rho_1) \right\|_1$$

$$= \left\| \mathcal{C}_1(\rho_1) \right\|_1 \tag{B62}$$

$$= \left\| \operatorname{tr}_{[5]} \left[\mathcal{C}_1 \otimes \mathcal{I}^{[5]} \left(\rho_1 \otimes \frac{I^{\otimes 3n-m}}{2^{3n-m}} \right) \right] \right\|_1 \tag{B63}$$

$$\leq \left\| \mathcal{C}_1 \otimes \mathcal{I}^{[5]} \left(\rho_1 \otimes \frac{I^{\otimes 3n-m}}{2^{3n-m}} \right) \right\|_1 \tag{B64}$$

$$\leq 2\mathcal{D}_{\diamond}(\mathcal{S}_{n,3n-m} \circ (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]}), (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]}) \circ \mathcal{S}_{n,3n-m}) \tag{B65}$$

$$\leq 2\epsilon, \tag{B66}$$

where $\rho_1 = \left(\rho \otimes \frac{I^{\otimes n-m}}{2^{n-m}} \right)$, the qubit block $[5]$ is defined by the qubits $3n-m+1, \dots, 2(3n-m+1)$, and in Eq. (B65), we use the following result from Eq. (45) in Ref. [8]:

$$\|\mathcal{S}_{i,j}(\mathcal{U} \otimes I_r) - (\mathcal{U} \otimes I_r)\mathcal{S}_{i,j}\|_{\diamond} \leq 2\epsilon, \tag{B67}$$

where $\mathcal{S}_{i,j}$ is the unitary channel corresponding to the swap operator between qubit i in the first n qubits and qubit j in the ancilla register of arbitrary size r. To bound the first term in Eq. (B61), we repeat the same procedure as before with the other swap operators. Repeating the same step for the jth time gives the jth error term as follows:

$$\left\| \mathcal{S}_{m+1,2n+1} \circ \dots \circ C_j \circ \dots \circ S_{n,3n-m}(\rho_1) \right\|_1 \tag{B68}$$

$$= \left\| \mathcal{S}_{m+1,2n+1} \circ \dots \circ C_j(\rho_j) \right\|_1 \tag{B69}$$

$$= \left\| C_j(\rho_j) \right\|_1 \tag{B70}$$

$$\leq 2\epsilon, \tag{B71}$$

where ρ_j is a normalized density matrix since it is ρ_1 acted upon some unitary channels. Summing all the error terms then gives us the result from Eq. (B61) as

$$\left\| (\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3]})\rho^{[1,2,3]} - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[2,3]})\rho^{[1,2,3]} \right\|_1$$

$$\leq \Bigg\| \operatorname{tr}_{[2]} \left[(\mathcal{U}^{[1,2]} \otimes \mathcal{I}^{[3,4]}) \circ \mathcal{S}_{[2],[4]} \left(\rho^{[1,2,3]} \otimes \frac{I^{\otimes n-m}}{2^{n-m}} \right) \right] - (\mathcal{E}^{\mathcal{U},[1]}_m \otimes \mathcal{I}^{[4,3]})(\rho^{[1,4,3]}) \Bigg\|_1 + 2(n-m)\epsilon \tag{B72}$$

$$\leq 2(n-m)\epsilon. \tag{B73}$$

In line (B72), the first term is zero because $\mathrm{tr}_{[2]}(.)$ is the definition of $(\mathcal{E}_m^{\mathcal{U},[1]} \otimes \mathcal{I}^{[4,3]})\rho^{[1,4,3]}$. Finally, using the definition of $\mathcal{D}_\diamond(.)$ from Eq. (14) gives us the result in Eq. (41). □

Appendix C: Details of Algorithm 2

In this Appendix, we gather a few technical lemmas to prove the guarantees provided in Algorithm 2. In Appendix C 1, we prove Lemma 12 that shows how to measure $f_{\alpha\beta}$ used to construct the Choi state of the quantum channel $\mathcal{E}_m^{\bar{\mathcal{W}}_t}$ for the qubit implementation. The analogous result for the fermionic implementation is provided in Appendix D. In Appendix C 2, we prove technical lemmas regarding the Choi states corresponding to the reduced quantum channels learned in Algorithm 2 for both fermionic and qubit implementations. We also provide the learning guarantee for the qubit implementation (see Appendix D for the learning guarantee in the fermionic implementation).

1. Learning the matrix $f_{\alpha\beta}$

Lemma 12 (Learning Pauli observables with shadow tomography for the qubit implementation)**.** The entries of the matrix $f_{\alpha\beta}$ defined as

$$f_{\alpha\beta} = \frac{1}{2^n}\,\mathrm{tr}\big[S^\dagger(\bar{P}_\beta \otimes I_B)S(\bar{P}_\alpha \otimes I_B)\big], \tag{57}$$

where $S = \bar{W}_t$ from Eq. (36), $\bar{P}_\alpha \in \{I,X,Y,Z\}^{\otimes m}$ are Pauli strings supported on the first m qubits and α,β are indices for the set of Pauli strings, can be learned using shadow tomography as follows. We estimate the expectation values of observables

$$\bar{O}_\beta = (\bar{P}_\beta \otimes I)_{\mathcal{AB}} \otimes |1\rangle\langle 0|_{\mathcal{C}}\,, \tag{58}$$

in states

$$\begin{aligned}|\bar{\psi}_\alpha\rangle =& \frac{1}{\sqrt{2}}\big[(\bar{W}_t \otimes I)\,|\Phi_d\rangle_{\mathcal{AB}}\,|0\rangle_{\mathcal{C}} \\ &+ (\bar{W}_t \otimes I)_{\mathcal{AB}}(\bar{P}_\alpha \otimes I)_{\mathcal{AB}}\,|\Phi_d\rangle\,|1\rangle_{\mathcal{C}}\,\big],\end{aligned} \tag{59}$$

where $|\Phi_d\rangle$ is the maximally entangled state $\frac{1}{d}\sum_i |i,i\rangle_{\mathcal{AB}}$, and then construct each row of $\hat{f}_{\alpha\beta}$ (where $\alpha,\beta \in \{I,X,Y,Z\}^{\otimes m}$) such that $\max_{\alpha,\beta}|\hat{f}_{\alpha\beta} - f_{\alpha\beta}| \leq \epsilon$ with probability $\geq 1-\delta$. The protocol needs $\bar{N}_c$ copies of the state $|\bar{\psi}_\alpha\rangle$, where

$$\bar{N}_c = C_1\frac{\log(C_2/\delta)}{\epsilon^2}, \tag{60}$$

with $C_1 = 68(3^m)$, $C_2 = 2^{2m+1}$.

Proof. We can compute $\bar{\rho}_\alpha O_\beta$, where $\bar{\rho}_\alpha = |\bar{\psi}_\alpha\rangle\langle\bar{\psi}_\alpha|$, as follows:

$$\begin{aligned}\bar{\rho}_\alpha\bar{O}_\beta =& \frac{1}{2}\big[(\bar{W}_t \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\,(\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta \otimes I) \otimes |0\rangle\langle 0|_{\mathcal{C}} \\ &+ (\bar{W}_t\bar{P}_\alpha \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\,(\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta \otimes I) \otimes |1\rangle\langle 0|_{\mathcal{C}}\,\big].\end{aligned} \tag{C1}$$

Taking the trace of the above gives us

$$\begin{aligned}\mathrm{tr}\big[\bar{\rho}_\alpha\bar{O}_\beta\big] &= \frac{1}{2}\,\mathrm{tr}\Big[(\bar{W}_t \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\,(\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta \otimes I)\Big] \\ &= \frac{1}{2}\,\mathrm{tr}\Big[(\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta\bar{W}_t \otimes I)\,|\Phi_d\rangle\langle\Phi_d|\Big] \\ &= \frac{1}{2}\,\langle\Phi_d|\,\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta\bar{W}_t \otimes I\,|\Phi_d\rangle \\ &= \frac{1}{2d}\sum_i \langle i|\,\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta\bar{W}_t\,|i\rangle \\ &= \frac{1}{2}\frac{1}{2^n}\,\mathrm{tr}\Big[\bar{P}_\alpha\bar{W}_t^\dagger\bar{P}_\beta\bar{W}_t\Big] \\ &= \frac{1}{2}f_{\alpha\beta},\end{aligned} \tag{C2}$$

where we use $d = 2^n$. We can then write the operator $\bar{O}_\beta$ as

$$\bar{O}_\beta = \frac{1}{2}(\bar{O}_\beta^+ - i\bar{O}_\beta^-), \tag{C3}$$

where $\bar{O}_\beta^\pm$ are Hermitian operators defined as

$$\bar{O}_\beta^+ = (\bar{P}_\beta \otimes I)_{\mathcal{AB}} \otimes X_{\mathcal{C}}, \tag{C4}$$

$$\bar{O}_\beta^- = (\bar{P}_\beta \otimes I)_{\mathcal{AB}} \otimes Y_{\mathcal{C}}, \tag{C5}$$

giving us $f_{\alpha\beta} = \mathrm{tr}[\bar{\rho}_\alpha\bar{O}_\beta^+] - i\,\mathrm{tr}[\bar{\rho}_\alpha\bar{O}_\beta^-]$. Since $f_{\alpha\beta}$ is a real matrix, we have $f_{\alpha\beta} = \mathrm{tr}[\bar{\rho}_\alpha\bar{O}_\beta^+]$. Ref. [27] on shadow tomography using the local Clifford unitary ensemble shows that estimating the expectation value of tensored single-qubit Paulis acting non-trivially on k qubits in some state, with probability $\geq 1-\delta$ and error ϵ, needs $68.3^k\log(2L/\delta)\epsilon^2$ copies of the state. Here L is the number of observables. For additional details, see Eqs. (S13) and (S50) in Ref. [27]. Since we want to construct the matrix $\hat{f}_{\alpha\beta}$ such that $\max_{\alpha\beta}|\hat{f}_{\alpha\beta} - f_{\alpha\beta}| \leq \epsilon$, we need to estimate observables $\bar{O}_\beta^+$ for each state $|\bar{\psi}_\alpha\rangle$ with error ϵ with probability $\geq 1-\delta/4^m$ (since the index α has $\leq 4^m$ many values). The number of copies $\bar{N}_c$ of each state $|\bar{\psi}_\alpha\rangle$ is

$$\bar{N}_c = \frac{68}{\epsilon^2}3^m\log\big(2^{2m+1}/\delta\big), \tag{C6}$$

where we use the facts that there are $\leq 4^m$ observables for each α and that the observables $\bar{O}_\beta^+$ have Pauli weight $\leq m+1$. □

2. Technical lemmas for Choi states

In this subsection, we state and prove key technical lemmas regarding the Choi state learned in Algorithm 2. The results presented here apply for channels corresponding to the unitaries W_t (for the fermionic implementation) and $\bar{W}_t$ (for the qubit implementation).

Lemma 19 (Learning the reduced quantum channel $\mathcal{E}_m^{\mathcal{Q}}$ from shadow tomography)**.** We can learn the Choi state of the reduced quantum channel $\mathcal{E}_m^{\mathcal{Q}}$, corresponding to the unitary Q,

such that the distance between the learned Choi state $J(\hat{\mathcal{E}})$ and the Choi state $J(\mathcal{E})$ corresponding to $\mathcal{E}_m^{\mathcal{Q}}$ is bounded as

$$\|J(\hat{\mathcal{E}}) - J(\mathcal{E})\| \leq d_0^6 \delta, \tag{C7}$$

where $\delta = \max_{\alpha\beta}|q_{\alpha,\beta} - \hat{q}_{\alpha,\beta}|$, $q_{\alpha,\beta}$ is defined as

$$q_{\alpha\beta} := \frac{1}{2^n} \operatorname{tr}\left[Q^\dagger(\bar{P}_\beta \otimes I_B)Q(\bar{P}_\alpha \otimes I_B)\right], \tag{C8}$$

and $\hat{q}$ is the learned version of q.

Proof. We have that

$$\begin{aligned} & d_0 q_{\alpha\beta} && \text{(C9)}\\ =& \frac{1}{2^{n-m}} \operatorname{tr}\left[Q^\dagger(\bar{P}_\beta \otimes I_B)Q(\bar{P}_\alpha \otimes I_B)\right] \\ =& \frac{1}{2^{n-m}} \operatorname{tr}\left[Q(\bar{P}_\alpha \otimes I_B)Q^\dagger(\bar{P}_\beta \otimes I_B)\right] \\ =& \frac{1}{2^{n-m}} \operatorname{tr}\left(\operatorname{tr}_{\geq m+1}[Q(\bar{P}_\alpha \otimes I_B)Q^\dagger(\bar{P}_\beta \otimes I_B)]\right) \\ =& \frac{1}{2^{n-m}} \operatorname{tr}\left(\operatorname{tr}_{\geq m+1}[Q(\bar{P}_\alpha \otimes I_B)Q^\dagger]\bar{P}_\beta\right) \\ =& \operatorname{tr}\left(\mathcal{E}_m^{\mathcal{Q}}(\bar{P}_\alpha)\bar{P}_\beta\right), && \text{(C10)} \end{aligned}$$

giving us the result

$$2^m q_{\alpha\beta} = \operatorname{tr}\left(\mathcal{E}_m^{\mathcal{Q}}(\bar{P}_\alpha)\bar{P}_\beta\right). \tag{C11}$$

For any channel $\mathcal{E}$ on m modes (qubits), we can write the Choi-Jamiolkowski state $J(\mathcal{E})$ as follows:

$$J(\mathcal{E}) = \frac{1}{d_0} \sum_{ij} \mathcal{E}(|i\rangle\langle j|) \otimes |i\rangle\langle j|, \tag{C12}$$

where $|i\rangle$ is a computational basis state on m modes (qubits), and $d_0 = 2^m$. We can expand $J(\mathcal{E})$ as follows:

$$\begin{aligned} J(\mathcal{E}) &= \frac{1}{d_0} \sum_{ijkl} \operatorname{tr}[\mathcal{E}(|i\rangle\langle j|)\,|l\rangle\langle k|]\,|k\rangle\langle l| \otimes |i\rangle\langle j| && \text{(C13)}\\ &= \frac{1}{d_0} \sum_{ijkl} \sum_{\alpha\beta} c_{\alpha,ij} c_{\beta,lk} \operatorname{tr}\left[\mathcal{E}(\bar{P}_\alpha)\bar{P}_\beta\right] |k\rangle\langle l| \otimes |i\rangle\langle j| && \text{(C14)}\\ &= \sum_{ijkl} \sum_{\alpha\beta} c_{\alpha,ij} c_{\beta,lk} q_{\alpha\beta}\, |k\rangle\langle l| \otimes |i\rangle\langle j|\,. && \text{(C15)} \end{aligned}$$

We can then bound $\|J(\hat{\mathcal{E}}) - J(\mathcal{E})\|$, where $J(\hat{\mathcal{E}})$ corresponds to the Choi state constructed using $\hat{q}_{\alpha\beta}$, as follows:

$$\begin{aligned} & \|J(\hat{\mathcal{E}}) - J(\mathcal{E})\| \\ \leq & \sum_{ijkl} \sum_{\alpha\beta} |c_{\alpha,ij} c_{\beta,lk}| |\hat{q}_{\alpha\beta} - q_{\alpha\beta}| \| |k\rangle\langle l| \otimes |i\rangle\langle j| \|. && \text{(C16)} \end{aligned}$$

We used the facts that $\| |k\rangle\langle l| \otimes |i\rangle\langle j| \| \leq 1$ and $c_{\alpha,ij} \leq 1/2^m$ from $c_{\alpha,ij} = \operatorname{tr}\left[|i\rangle\langle j|\,\bar{P}_\alpha\right]/2^m = \langle j|\,\bar{P}_\alpha\,|i\rangle\,/2^m$. Equation (C16) then becomes

$$\begin{aligned} \|J(\hat{\mathcal{E}}) - J(\mathcal{E})\| &\leq \frac{\delta}{2^{2m}} \sum_{ijkl} \sum_{\alpha\beta} 1 \\ &= 2^{6m}\delta, && \text{(C17)} \end{aligned}$$

where we use $\sum_i 1 = 2^m$ and $\sum_\alpha 1 \leq 4^m$. Taking $\delta = \max_{\alpha,\beta}|\hat{q}_{\alpha\beta} - q_{\alpha\beta}|$ then gives us the result in Eq. (C7). We also get the inequality

$$\|J(\hat{\mathcal{E}}) - J(\mathcal{E})\|_1 \leq d_0^8 \delta \tag{C18}$$

from using the inequality $\|X\|_1 \leq \operatorname{rank}(X)\|X\|$ (see Lemma 11 in Ref. [40] for details). □

Once we have the Choi state $J(\mathcal{E})$, we project it using the steps outlined in Subsec. IV B and show that the projected Choi state J_p is close to the Choi state $J(\mathcal{E})$ as follows.

Lemma 20 (CPTP-projecting a Choi state)**.** Let $J(\mathcal{E})$ be the Choi state corresponding to some m-mode (qubit) channel $\mathcal{E}$, and let $J(\hat{\mathcal{E}})$ be the learned version of the Choi state such that $\|J(\hat{\mathcal{E}}) - J(\mathcal{E})\|_2^2 \leq \epsilon_1^2$. The projected Choi state J_p satisfies the bound

$$\|J(\mathcal{E}) - J_p\|_1 \leq \epsilon_l, \tag{C19}$$

where $\epsilon_l = C_0\epsilon_1$ (with C_0 being a constant).

Proof. The projection, with respect to the Frobenius norm (defined as $\|A\|_2 = \sqrt{\operatorname{tr}[A^\dagger A]}$), to a trace-preserving map is defined as

$$\begin{aligned} \text{Proj}_{\text{TP}}[X] &= \text{argmin}_{X'} \|X - X'\|_2 && \text{(C20)}\\ \text{s.t. } \operatorname{tr}_A[X'] &= \frac{\mathbb{1}}{d_0}. && \text{(C21)} \end{aligned}$$

The unique solution satisfies the inequality

$$\|\text{Proj}_{\text{TP}}[X] - Y\|_2^2 \leq \|X - Y\|_2^2, \tag{C22}$$

where Y corresponds to a trace preserving map, and X is an arbitrary matrix. We note that this unique solution has an exact analytical form given in Proposition 11 of Ref. [32], which means we can find the projection by computing this expression with a classical computer. The projection, with respect to the Frobenius norm, to a completely positive map is defined as

$$\begin{aligned} \text{Proj}_{\text{CP}}[X] &= \text{argmin}_{X'} \|X - X'\|_2^2, && \text{(C23)}\\ \text{s.t. } X' &\geq 0. && \text{(C24)} \end{aligned}$$

The unique solution satisfies the following inequality:

$$\|\text{Proj}_{\text{CP}}[X] - Y\|_2^2 \leq \|X - Y\|_2^2, \tag{C25}$$

where $Y \geq 0$ and X is arbitary. This unique solution has an exact analytical expression which can be found in Proposition 12 of Ref. [32].

Let us define $J_1 := \text{Proj}_{\text{CP}}[J(\hat{\mathcal{E}})]$ and $J_2 := \text{Proj}_{\text{TP}}[J_1]$. Let λ_i be the eigenvalues of J_2, and let $\lambda_{\min}$ be the minimum eigenvalue. First note that

$$\begin{aligned} \|J_2 - J(\mathcal{E})\|_2^2 &= \|\text{Proj}_{\text{TP}}[J_1] - J(\mathcal{E})\|_2^2 && \text{(C26)}\\ &\leq \|J_1 - J(\mathcal{E})\|_2^2 && \text{(C27)}\\ &= \|\text{Proj}_{\text{CP}}[J(\hat{\mathcal{E}})] - J(\mathcal{E})\|_2^2 && \text{(C28)}\\ &\leq \|J(\hat{\mathcal{E}}) - J(\mathcal{E})\|_2^2 && \text{(C29)}\\ &\leq \epsilon_1^2, && \text{(C30)} \end{aligned}$$

where we use Eq. (C22) in Eq. (C27) and use Eq. (C25) in Eq. (C29). In the case $\lambda_{\min} \geq 0$, we choose $J_p = J_2$ as the projected Choi state that satisfies $\|J_2 - J(\mathcal{E})\|_1 \leq d_0^2\epsilon_1$. In the case $\lambda_{\min} < 0$, we set $J_p = J_3$, where J_3 is defined as follows:

$$J_3 = (1-p)J_2 + \frac{p}{d_0^2}\mathbb{1}\otimes\mathbb{1}, \tag{C31}$$

$$(1-p)\lambda_{\min} + \frac{p}{d_0^2} = 0. \tag{C32}$$

From the condition in Eq. (C32), we have $J_3 \geq 0$ (resulting in complete positivity of the corresponding channel). Taking the partial trace of J_3 over the first subsystem, which we denote as system A, gives us $\mathrm{tr}_A[J_3] = \mathbb{1}/d_0$ (we use the fact that $\mathrm{tr}_A[J_2] = \mathbb{1}/d_0$). Before we bound $\|J_3 - J(\mathcal{E})\|_1$, we gather here a few facts. Since $J(\mathcal{E})$ corresponds to a CPTP state, it has eigenvalues between 0 and 1. Using Weyl's perturbation theorem in Theorem 15 and the fact that $\|J_2 - J(\mathcal{E})\| \leq \|J_2 - J(\mathcal{E})\|_2 \leq \epsilon_1$ gives us $\|J_2\| \leq 1 + \epsilon_1$ and $\lambda_{\min} \geq -\epsilon_1$. Using these facts with Eq. (C32) gives us

$$p = \frac{-\lambda_{\min}}{1/d_0^2 - \lambda_{\min}} \leq d_0^2\epsilon_1, \tag{C33}$$

$$\|J_2\| \leq 1 + \epsilon_1. \tag{C34}$$

Using the above results and the definition of J_3 from Eq. (C31) gives us

$$\|J_3 - J_2\| \leq p\|J_2\| + \frac{p}{d_0^2} \tag{C35}$$

$$\leq p(1+\epsilon_1) + \frac{p}{d_0^2} \tag{C36}$$

$$\leq 3d_0^2\epsilon_1, \tag{C37}$$

where we assume $\epsilon_1 < 1$. We can then finally bound $\|J_3 - J(\mathcal{E})\|_1$ as follows:

$$\begin{aligned}\|J_3 - J(\mathcal{E})\|_1 &\leq \|J_3 - J_2\|_1 + \|J_2 - J(\mathcal{E})\|_1 \\ &\leq d_0^2\|J_3 - J_2\| + d_0^2\|J_2 - J\| \\ &\leq d_0^2\|J_3 - J_2\| + d_0^2\|J_2 - J\|_2 \\ &\leq (3d_0^4 + d_0^2)\epsilon_1 \\ &= C_0\epsilon_1 \\ &= \epsilon_l,\end{aligned} \tag{C38}$$

where we use the triangle inequality, Eqs. (C30) and (C37), and the property $\|A\|_1 \leq \mathrm{rank}(A)\|A\|$. □

Since the projected Choi state J_p is close to the Choi state $J(\mathcal{E})$, we can prove the following distance bound between the channel $\mathcal{E}_m^{\mathcal{Q}}$ (corresponding to the Choi state $J(\mathcal{E})$) and the channel $\mathcal{E}_{m,\mathrm{proj}}^{\mathcal{Q}}$ (corresponding to the Choi state J_p).

Corollary 21. *(*Distance between the learned channel and the projected channel) We can obtain the following bound on the diamond distance between the channel $\mathcal{E}_m^{\mathcal{Q}}$ and the channel $\mathcal{E}_{m,\mathrm{proj}}^{\mathcal{Q}}$:

$$\mathcal{D}_\diamond(\mathcal{E}_m^{\mathcal{Q}}, \mathcal{E}_{m,\mathrm{proj}}^{\mathcal{Q}}) \leq C_3\epsilon_2, \tag{C39}$$

where $C_3 = d_0^{11}(3d_0^2+1)/2$, $\epsilon_2 = \max_{\alpha,\beta}|\hat{q}_{\alpha\beta} - q_{\alpha\beta}|$, $d_0 = 2^m$, and $m = \kappa t/2$. Here $\mathcal{E}_{m,\mathrm{proj}}^{\mathcal{Q}}$ is obtained by projecting the learned Choi state of the channel $\mathcal{E}_m^{\mathcal{Q}}$ from Lemma 20.

Proof. This result follows from the following computation:

$$\mathcal{D}_\diamond(\mathcal{E}_m^{\mathcal{Q}}, \mathcal{E}_{m,\mathrm{proj}}^{\mathcal{Q}}) \leq \frac{d_0}{2}\|J(\mathcal{E}) - J_p\|_1 \tag{C40}$$

$$\leq \frac{d_0}{2}C_0\epsilon_1. \tag{C41}$$

In Eq. (C40), we use the following bound from Lemma 26 in Ref. [41]:

$$\mathcal{D}_\diamond(\mathcal{E}_1, \mathcal{E}_2) \leq \frac{d_0}{2}\|J(\mathcal{E}_1) - J(\mathcal{E}_2)\|_1. \tag{C42}$$

In Eq. (C41), we use Eq. (C19) from Lemma 20, where $\|J(\mathcal{E}) - J_p\|_2 \leq \epsilon_1$ and $\|J(\mathcal{E}) - J_p\|_1 \leq C_0\epsilon_1$. Now note that $\|J(\mathcal{E}) - J_p\|_2 \leq d_0^2\|J(\mathcal{E}) - J_p\| \leq d_0^8\epsilon_2$, where we use Eq. (C7) and $\epsilon_2 = \max_{\alpha,\beta}|\hat{q}_{\alpha\beta} - q_{\alpha\beta}|$. Therefore, we can choose $\epsilon_1 = d_0^8\epsilon_2$ to get

$$\mathcal{D}_\diamond(\mathcal{E}_m^{\mathcal{Q}}, \mathcal{E}_{m,\mathrm{proj}}^{\mathcal{Q}}) \leq \frac{d_0^9}{2}C_0\epsilon_2 \tag{C43}$$

and the result in Eq. (C39). □

We now proceed to provide the learning guarantee for our algorithm in the qubit implementation. The analogous result for the fermionic implementation is provided in Appendix D.

Lemma 22 (Learning algorithm guarantee for the qubit implementation)**.** Let U_t be the unknown unitary defined in Eq. (16) with a qubit implementation. There is a learning algorithm that learns the unknown unitary as the m-qubit channel $\mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t}$ satisfying the distance bound

$$\mathcal{D}_\diamond(\bar{\mathcal{W}}_t, \mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t}\otimes\mathcal{I}_B) \leq T_2(n)\epsilon \tag{C44}$$

with probability $\geq 1-\delta$, using $O(\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1}))$ accesses to U_t and $O(\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1}))$ classical processing time. Here $T_2(n) = \mathrm{poly}(n)$.

Proof. Running Algorithm 1 with input parameters $(\epsilon^2, \delta/2)$ and some postprocessing gives the reduced channel $\mathcal{E}_m^{\bar{\mathcal{W}}_t}$ with the bound $\mathcal{D}_\diamond(\bar{\mathcal{W}}_t, \mathcal{E}_m^{\bar{\mathcal{W}}_t}\otimes\mathcal{I}_B) \leq n(2n+3)T_1(n)\epsilon$, where $\bar{\mathcal{W}}_t$ is the unitary channel corresponding to the unitary $\bar{W}_t$, with probability $\geq 1-\delta/2$. This follows from the following computation:

$$\mathcal{D}_\diamond(\bar{\mathcal{W}}_t, \mathcal{E}_m^{\bar{\mathcal{W}}_t}\otimes\mathcal{I}_B) \leq n(2n+3)\epsilon_0 \tag{C45}$$

$$\leq n(2n+3)T_1(n)\epsilon, \tag{C46}$$

where line (C45) follows from Eq. (41) in Lemma 9 and Eq. (39). To obtain Eq. (C46), we use Eq. (34) from Lemma 5. Running Algorithm 2 with input parameters $(\epsilon, \delta/2)$ to learn the reduced quantum channel $\mathcal{E}_m^{\bar{\mathcal{W}}_t}$ and projecting using our scheme gives us the following bound between the channels $\mathcal{E}_m^{\bar{\mathcal{W}}_t}$ and the projected channel $\mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t}$ from Corollary 21:

$$\mathcal{D}_\diamond(\mathcal{E}_m^{\bar{\mathcal{W}}_t}, \mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t}) \leq C_3\epsilon, \tag{C47}$$

with probability $\geq 1-\delta/2$. Here C_3 is a constant defined in Eq. (C39). We can then use the triangle inequality to obtain the channel distance bound between the channel $\bar{\mathcal{W}}_t$ and the projected version of the learned channel $\mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t}$ as follows:

$$\begin{aligned}
&\mathcal{D}_\diamond(\bar{\mathcal{W}}_t, \mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t} \otimes \mathcal{I}_B) \\
\leq &\mathcal{D}_\diamond(\bar{\mathcal{W}}_t, \mathcal{E}_m^{\bar{\mathcal{W}}_t} \otimes \mathcal{I}_B) + \mathcal{D}_\diamond(\mathcal{E}_m^{\bar{\mathcal{W}}_t}, \mathcal{E}_{m,\mathrm{proj}}^{\bar{\mathcal{W}}_t}) && \text{(C48)} \\
\leq &T_2(n)\epsilon, && \text{(C49)}
\end{aligned}$$

where $T_2(n) = n(2n+3)T_1(n) + C_3 = \mathrm{poly}(n)$. From the union bound, the algorithm succeeds with probability $\geq 1-\delta$. From the ϵ-dependence of the number of states required for Algorithms 1 and 2, the learning algorithm uses $N_c + \bar{N}_c = O(\mathrm{poly}(n, \epsilon, \log\delta^{-1}))$ accesses of the unknown unitary U_t to achieve error ϵ in Eq. (C49), where N_c and $\bar{N}_c$ are defined in Algorithms 1 and 2, respectively. Moreover, each step of the learning algorithm requires $\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1})$ classical processing time. □

Appendix D: Technical lemmas for the fermionic implementation

In this section, we prove key technical lemmas for the fermionic implementation.

We first prove Lemma 6, which shows that, in the fermionic implementation, we can construct W_t such that the condition $[W_t, \gamma_i] \approx 0$ for $i > M$ implies that W_t is Pauli decoupled from modes $i > m$.

Lemma 6 (Majorana decoupling for W_t in the fermionic implementation implies Pauli decoupling for modes $i > m$)**.** Consider the fermionic implementation where the Gaussian unitaries G_j in U_t correspond to orthogonal matrices in $\mathrm{SO}(2n)$, and the unitary W_t is obtained from Algorithm 1. Then W_t satisfies the following:

$$\frac{1}{2}\sum_{P\in\{X,Y,Z\}} \|[W_t, P_i]\| \leq 3n\epsilon_0, \quad i > m+1, \tag{35}$$

given $\|[W_t, \gamma_j]\| \leq \epsilon_0$ for $j > M$ (see Lemma 5).

Proof. In the case where we are given that $G_{t'}$ in U_t correspond to $\mathrm{SO}(2n)$, it follows from Lemmas 2 and 5 that $W_t = G_a^\dagger U_t G_b^\dagger$ obtained from Algorithm 1 has the form $G_1 u_t G_2$, where both G_1 and G_2 correspond to orthogonal matrices in $\mathrm{SO}(2n)$ since both G_a and G_b can be chosen to correspond to $\mathrm{SO}(2n)$. This means that W_t is a sum of Majorana strings of even weight and satisfies Eq. (33) in Lemma 5. We note that W_t can be written as

$$W_t = W_t^{\mathrm{L}} + W_t^{\mathrm{NL}}, \tag{D1}$$

where W_t^{L} is supported on the first M Majorana operators, and W_t^{NL} contains Majorana strings $\tilde{\gamma}_x$ containing at least one Majorana operator γ_i with $i > M$. We first introduce the following notation. Let f_j and $\bar{f}_j$ be functions defined on operators as follows:

$$f_j(X) = \frac{1}{2}[X, \gamma_j]\gamma_j, \tag{D2}$$

$$\bar{f}_j(X) = \frac{1}{2}\{X, \gamma_j\}\gamma_j, \tag{D3}$$

where X is any operator. For any operator X, we can always write $X = X_j + \bar{X}_j$, where $\{X_j, \gamma_j\} = 0$, and $[\bar{X}_j, \gamma_j] = 0$. This is because X can be written as a sum of Majorana strings $\tilde{\gamma}_x$, and each $\tilde{\gamma}_x$ either commutes or anticommutes with γ_j (since $\tilde{\gamma}_x$ and γ_j are in the Pauli group). The function f_j then satisfies $f_j(X) = X_j$ and $\bar{f}_j(X) = \bar{X}_j$. Additionally, we have the following result:

$$\|f_j \bar{f}_k(X)\| \leq \|f_j(X)\|, \tag{D4}$$

for any X and $j \neq k$. This follows from the triangle inequality and the following computation:

$$\begin{aligned}
f_j \circ \bar{f}_k(X) &= \frac{1}{2}[\bar{f}_k(X), \gamma_j]\gamma_j \\
&= \frac{1}{4}[X + \gamma_k X \gamma_k, \gamma_j]\gamma_j \\
&= \frac{1}{4}\Big([X, \gamma_j]\gamma_j + \gamma_k[X, \gamma_j]\gamma_j\gamma_k\Big) \\
&= \frac{1}{2}(f_j(X) + \gamma_k f_j(X)\gamma_k). && \text{(D5)}
\end{aligned}$$

We first write W_t^{NL} as follows:

$$W_t^{\mathrm{NL}} = f_{M+1}(W_t^{\mathrm{NL}}) + \sum_{k=M+2}^{2n} f_k \bar{f}_{k-1}\bar{f}_{k-2}\cdots\bar{f}_{M+1}(W_t^{\mathrm{NL}}), \tag{D6}$$

where we use the notation $\bar{f}_{i_1} \circ f_{i_2} \circ \cdots \circ f_{i_n}(X) =: \bar{f}_{i_1} f_{i_2} \ldots f_{i_n}(X)$. The decomposition in Eq. (D6) follows from the following computation:

$$\begin{aligned}
&W_t^{\mathrm{NL}} \\
=&f_{M+1}(W_t^{\mathrm{NL}}) + \bar{f}_{M+1}(W_t^{\mathrm{NL}}) \\
=&f_{M+1}(W_t^{\mathrm{NL}}) + f_{M+2}\bar{f}_{M+1}(W_t^{\mathrm{NL}}) + \bar{f}_{M+2}\bar{f}_{M+1}(W_t^{\mathrm{NL}}) \\
=&f_{M+1}(W_t^{\mathrm{NL}}) + f_{M+2}\bar{f}_{M+1}(W_t^{\mathrm{NL}}) + \\
&\cdots + f_{2n}\bar{f}_{2n-1}\cdots\bar{f}_{M+1}(W_t^{\mathrm{NL}}), && \text{(D7)}
\end{aligned}$$

where we use the fact that all terms in W_t^{NL} contain at least one γ_i with $i > M$. We now proceed to bound W_t^{NL} as follows:

$$\begin{aligned}
&\|W_t^{\mathrm{NL}}\| \\
\leq &\|f_{M+1}(W_t^{\mathrm{NL}})\| + \sum_{k=M+2}^{2n} \|f_k \bar{f}_{k-1}\bar{f}_{k-2}\cdots\bar{f}_{M+1}(W_t^{\mathrm{NL}})\| \\
\leq &\|f_{M+1}(W_t^{\mathrm{NL}})\| + \sum_{k=M+2}^{2n} \|f_k(W_t^{\mathrm{NL}})\| \\
\leq &(2n-M)\max_{k>M}\|f_k(W_t^{\mathrm{NL}})\|,
\end{aligned}$$

where we use the fact that $\|f_{i_1}\bar{f}_{i_2}\cdots\cdots\bar{f}_{i_n}(X)\| \leq \|f_{i_1}(X)\|$, which in turn follows from using Eq. (D4) repeatedly. Now note that we can write $f_k(W_t^{\mathrm{NL}}) = f_k(W_t)$ since W_t^{L} commutes with γ_k for $k > M$ (since W_t contains Majorana strings $\tilde{\gamma}_x$ with even weight). Then the result $\|[W_t, \gamma_k]\| \leq \epsilon_0$ from Eq. (33) gives us $\|f_k(W_t)\| \leq \epsilon_0/2$ and the following result:

$$\|W_t^{\mathrm{NL}}\| \leq n\epsilon_0. \tag{D8}$$

The above equation then gives us the result in Eq. (35) using the fact that, for $i > m$, $\|[W_t, P_i]\| = \|[W_t^{\mathrm{NL}}, P_i]\| \leq 2\|W_t^{\mathrm{NL}}\|\|P_i\| \leq 2n\epsilon_0$. □

We now show how to modify the learning algorithm for the fermionic implementation. For Algorithms 1 and 2, we modify the states (and the corresponding observables) used in the shadow tomography protocols to ones that can be prepared on a fermionic computer (i.e., states that can be prepared by a parity-preserving quantum circuit). Throughout this section, we will often describe our fermionic unitaries as parity-preserving qubit unitaries, related to the actual fermionic ones we have in mind through the Jordan-Wigner transformation.

1. Fermionic implementation: states and observables for Algorithm 1

In Lemma 10, we perform state tomography on some qubit state $|\psi_j\rangle$ (where the index j corresponds to the bitstring x with weight 1 and $x_j = 1$) to estimate physical observables O_k^+ and construct the matrix $c^{(1)}$. For the fermionic implementation, we modify the states and observables as follows. We use the mapping between fermionic and qubit states where any computational basis state on qubits $|z_1 \ldots z_n\rangle$ is identified with the corresponding fermionic state in the occupation basis. We prepare the fermionic state $|\psi_j^{\mathrm{f}}\rangle$ defined as

$$|\psi_j^{\mathrm{f}}\rangle = (U_t \otimes I)\,|\phi_j^{\mathrm{f}}\rangle\,, \tag{D9}$$

$$|\phi_j^{\mathrm{f}}\rangle = \frac{1}{\sqrt{2}} U_j^{\mathrm{f}}(|00\rangle - |11\rangle)_{\mathcal{A}_1\mathcal{A}_2}\,|\Phi_d\rangle\,, \tag{D10}$$

where $|\Phi_d\rangle \propto \sum_{z\in\{0,1\}^n} |z,z\rangle$, where $|z\rangle$ are the occupation basis states on n modes. $|\phi_j^{\mathrm{f}}\rangle$ is a fermionic state defined on modes $\mathcal{A}_1, \mathcal{A}_2, 1, \ldots, 4n$, and U_j^{f} is a fermionic unitary defined as $U_j^{\mathrm{f}} = (1 - a_{\mathcal{A}_2}^\dagger a_{\mathcal{A}_2}) + a_{\mathcal{A}_2}^\dagger a_{\mathcal{A}_2}\gamma_{\mathcal{A}_1}\gamma_j$, where $j \in \{1, \ldots, 2n\}$. The unitary U_t acts on modes labeled $1, \ldots, n$. We write $U_t \otimes I$ to emphasize the fact that U_t only acts on modes $1, \ldots, n$. The state $|\phi_j^{\mathrm{f}}\rangle$ can be simplified as follows:

$$|\phi_j^{\mathrm{f}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle\,|\Phi_d\rangle + a_{\mathcal{A}_2}^\dagger\gamma_j\,|00\rangle\,|\Phi_d\rangle). \tag{D11}$$

We note here that the state $(|00\rangle - |11\rangle)\,|\Phi_d\rangle$ can be prepared by a fermionic circuit efficiently using the facts that the qubit version of this state can be prepared by a circuit composed of parity-preserving two-qubit gates as shown in Fig. 4, and that any two-qubit parity-preserving gate can be implemented as a series of fermionic gates [11].

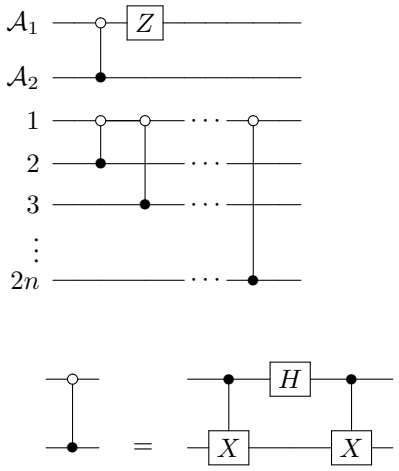

FIG. 4. The qubit unitary, composed of parity-preserving two-qubit unitaries, needed to prepare the qubit state $(|00\rangle - |11\rangle)\,|\Phi_d\rangle$ in Eq. (D10). This implies that this state, now thought of as a fermionic state in the occupation basis, can be prepared on a fermionic quantum computer [11].

The observables in Eqs. (49) and (50) are redefined to

$$O_k^+ = (a_{\mathcal{A}_2}^\dagger - a_{\mathcal{A}_2})\gamma_k, \tag{D12}$$

$$O_k^- = i(a_{\mathcal{A}_2}^\dagger + a_{\mathcal{A}_2})\gamma_k, \tag{D13}$$

giving us $O_k = a_{\mathcal{A}_2}^\dagger\gamma_k = (O_k^+ - iO_k^-)/2$ in place of Eq. (A62) with the desired expectation value in Eq. (A64). We measure only O_k^+ since $O_k \propto (O_k^+ - iO_k^-)$ and $c_{jk}^{(1)} \propto \mathrm{tr}[\rho_j O_k]$ (since $c_{jk}^{(1)}$ is a real matrix). The shadow tomography step can be implemented on the fermionic platform by first applying a unitary from the fermionic Gaussian ensemble, performing a basis measurement in the occupation basis, and then performing classical post-processing on a classical computer (e.g. by representing Majorana operators via the Jordan-Wigner encoding). Since the state is defined on a different number of modes, the shadow tomography step in Algorithm 1 needs

$$N_c^{\mathrm{f}} = \left(1 + \frac{\epsilon}{6n}\right)\log\left(8n^2/\delta\right)\frac{4n^2(4n+3)}{\epsilon^2} \tag{D14}$$

copies of state $|\psi_j^{\mathrm{f}}\rangle$ (for more details, see discussion surrounding Eq. (A76) in Lemma 11). This step gives us the matrix $c^{(1)}$, which can be processed, as described in Lemma 5, to give us the unitaries G_a, G_b, and the unitary $W_t = G_a^\dagger U_t G_b^\dagger$ that satisfies the Majorana decoupling property in Eq. (33).

2. Fermionic implementation: states and observables for Algorithm 2

We now modify the states and observables in Algorithm 2 used to construct the Choi state $J(\hat{\mathcal{E}})$ for the reduced quantum channel corresponding to the unitary W_t. We define states on the fermionic modes $\mathcal{A}_1, \mathcal{A}_2, 1, \ldots, 2n$, where $\mathcal{A}_1$, $\mathcal{A}_2$ are ancilla modes. Instead of using the state defined in Eq. (59),

we use the state

$$|\bar{\psi}^{\mathrm{f}}_{\alpha}\rangle = (W_t \otimes I)\,|\bar{\phi}^{\mathrm{f}}_{\alpha}\rangle\,, \tag{D15}$$

$$|\bar{\phi}^{\mathrm{f}}_{\alpha}\rangle = \frac{1}{\sqrt{2}}\bar{U}^{\mathrm{fp}}_{\alpha}\big(\,|00\rangle_{\mathcal{A}_1\mathcal{A}_2} + |11\rangle_{\mathcal{A}_1\mathcal{A}_2}\big)\,|\Phi_d\rangle\,, \tag{D16}$$

where $\alpha \in \{I, X, Y, Z\}^{\otimes m}$ and W_t acts on modes $1, \ldots, n$. Here $p = 0$ when the Pauli observable $\bar{P}_\alpha$ is parity-preserving and $p = 1$ when it is not. The unitary $\bar{U}^{\mathrm{fp}}_{\alpha}$ is defined as follows:

$$\bar{U}^{\mathrm{fp}}_{\alpha} = (|0\rangle\langle 0|_{\mathcal{A}_1} \otimes I + |1\rangle\langle 1|_{\mathcal{A}_1} \otimes (X_{\mathcal{A}_2})^p \bar{P}_\alpha), \tag{D17}$$

where $\bar{P}_\alpha$ acts on modes $1, \ldots, m$. We note that, due to the Jordan-Wigner transformation, $X_{\mathcal{A}_2}$ acts on both modes $\mathcal{A}_2$ and $\mathcal{A}_1$. We also note here that the qubit version of state $(|00\rangle_{\mathcal{A}_1\mathcal{A}_2} + |11\rangle_{\mathcal{A}_1\mathcal{A}_2})\,|\Phi_d\rangle$ can be prepared using a circuit composed of parity-preserving two-qubit gates (similar to the circuit in Fig. 4). Moreover, the unitary $\bar{U}^{\mathrm{fp}}_{\alpha}$ is a parity-preserving gate, ensuring that the state $|\bar{\psi}^{\mathrm{f}}_{\alpha}\rangle$ can be implemented on a fermionic quantum computer. We can then employ shadow tomography using the local Clifford unitary ensemble to estimate the expectation value of the operator $\bar{O}^{+}_{\beta}$ defined as

$$\bar{O}^{+}_{\beta} = X_{\mathcal{A}_1} X_{\mathcal{A}_2} \otimes \bar{P}_\beta \tag{D18}$$

for $p = 0$. For the case where $p = 1$, we use the observable $\bar{O}^{+}_{\beta}$ defined as

$$\bar{O}^{+}_{\beta} = X_{\mathcal{A}_1} Z_{\mathcal{A}_2} \otimes \bar{P}_\beta. \tag{D19}$$

The number of copies required for shadow tomography using the local Clifford ensemble (for the cases $p = 0$ and $p = 1$) is given by

$$\bar{N}^{\mathrm{f}}_{c} = C'_1 \log(C'_2/\delta)/\epsilon^2, \tag{D20}$$

where $C'_1 = 68(3^{m+2})$ and $C_2 = 2(4^{2m})$. The choice of observables in Eqs. (D18) and (D19) ensures that $\mathrm{tr}\left[\bar{O}^{+}_{\beta}|\bar{\psi}^{\mathrm{f}}_{\alpha}\rangle\langle\bar{\psi}^{\mathrm{f}}_{\alpha}|\right] = f_{\alpha\beta}$, where $f_{\alpha\beta}$ is defined in Eq. (46) for $S = W_t$, and $\alpha, \beta \in \{I, X, Y, Z\}^{\otimes m}$.

We now show how to implement any unitary U_c from the local Clifford ensemble for the shadow tomography step. First, consider the case where U_c is parity-preserving. In that case, we can implement the gate built from fermionic gates [11]. For the case where U_c doesn't preserve parity, as shown in Ref. [11], we can define the following gate:

$$\tilde{U}_c = V_p^{\dagger}(I \otimes U_c)V_p, \tag{D21}$$

using an ancilla mode labeled 0, where $V_p\,|z_0, z_1, \cdots, z_N\rangle = |z_p, z_1, \ldots, z_N\rangle$ with $z_p = z_0 + z_1 + \ldots + z_N$, making $\tilde{U}_c$ parity-preserving. We can then decompose $\tilde{U}_c$ into a product of two-qubit parity-preserving gates, each of which can be implemented on a fermionic quantum computer using a series of fermionic gates [11].

By implementing Algorithm 2, we can construct the projected Choi state J_p of the reduced channel corresponding to $\mathcal{W}_t$. In the final step, where the Stinespring dilation V_S (using $2m$ ancilla fermionic modes) is constructed from the projected Choi state J_p, a parity-preserving unitary $\tilde{V}_S$ can be constructed using the same trick that defines $\tilde{U}_c$ in Eq. (D21). $\tilde{V}_S$ can then be used to implement the reduced quantum channel as shown in Fig. 2.

Lemma 23 (Learning algorithm guarantees for the fermionic implementation)**.** Let U_t be the unknown unitary defined in Eq. (16) in a fermionic implementation. There is a learning algorithm that learns the unknown unitary as the m-mode channel $\mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}}$ satisfying the distance bound

$$\mathcal{D}_\diamond(\mathcal{W}_t, \mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}} \otimes \mathcal{I}_B) \leq T^{\mathrm{f}}_2(n)\epsilon \tag{D22}$$

with probability $\geq 1 - \delta$, using $O(\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1}))$ accesses to U_t and $O(\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1}))$ classical processing time. Here $T^{\mathrm{f}}_2(n) = \mathrm{poly}(n)$.

Proof. Running Algorithm 1 with input parameters $(\epsilon^2, \delta/2)$ and some postprocessing gives the reduced channel $\mathcal{E}^{\mathcal{W}_t}$ with the bound $\mathcal{D}_\diamond(\mathcal{W}_t, \mathcal{E}^{\mathcal{W}_t} \otimes \mathcal{I}_B) \leq 3n^2 T_1(n)\epsilon$, where $\mathcal{W}_t$ is the unitary channel corresponding to the unitary W_t, with probability $\geq 1 - \delta/2$. This follows from the following computation:

$$\mathcal{D}_\diamond(\mathcal{W}_t, \mathcal{E}^{\mathcal{W}_t}_{m} \otimes \mathcal{I}_B) \leq 3n^2\epsilon_0 \tag{D23}$$

$$\leq 3n^2 T_1(n)\epsilon, \tag{D24}$$

where line (D23) follows from Eq. (41) in Lemma 9 and Eq. (35) in Lemma 6. Line (D24) follows from Eq. (34) in Lemma 5. Running Algorithm 2 with input parameters $(\epsilon, \delta/2)$ to learn the reduced quantum channel and then projecting it to a CPTP map gives us the following bound on the distance between the channel $\mathcal{E}^{\mathcal{W}_t}_{m}$ and the projected channel $\mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}}$ from Corollary 21:

$$\mathcal{D}_\diamond(\mathcal{E}^{\mathcal{W}_t}_{m}, \mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}}) \leq C_3\epsilon, \tag{D25}$$

with probability $\geq 1 - \delta/2$. Here C_3 is a constant defined in Eq. (C39). We can then use the triangle inequality to obtain the channel distance bound between the channel $\mathcal{W}_t$ and the projected version of the learned channel $\mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}}$ as follows:

$$\mathcal{D}_\diamond(\mathcal{W}_t, \mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}} \otimes \mathcal{I}_B)$$

$$\leq \mathcal{D}_\diamond(\mathcal{W}_t, \mathcal{E}^{\mathcal{W}_t}_{m} \otimes \mathcal{I}_B) + \mathcal{D}_\diamond(\mathcal{E}^{\mathcal{W}_t}_{m}, \mathcal{E}^{\mathcal{W}_t}_{m,\mathrm{proj}}) \tag{D26}$$

$$\leq T^{\mathrm{f}}_2(n)\epsilon, \tag{D27}$$

where $T^{\mathrm{f}}_2(n) = 3n^2 T_1(n) + C_3 = \mathrm{poly}(n)$. From the union bound, the algorithm succeeds with probability $\geq 1 - \delta$. From the ϵ-dependence of the number of states required for Algorithms 1 and 2, the learning algorithm uses $N^{\mathrm{f}}_c + \bar{N}^{\mathrm{f}}_c = O(\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1}))$ accesses to the unknown unitary U_t to achieve error ϵ in Eq. (D27), where N^{f}_c and $\bar{N}^{\mathrm{f}}_c$ are defined in Algorithms 1 and 2, respectively. Moreover, each step of the learning algorithm requires $\mathrm{poly}(n, \epsilon^{-1}, \log\delta^{-1})$ classical processing time. □

Appendix E: Fermionic unitaries and the matchgate hierarchy

In this section, we state and prove Lemma 13, which shows that, generally, fermionic unitaries with just two non-Gaussian gates lie outside the matchgate hierarchy.

Lemma 13 (Example of U_t outside the matchgate hierarchy)**.** The unitary $U_t = KG(\theta)K$ with two non-Gaussian gates K, where

$$K = \exp(i\pi\gamma_1\gamma_2\gamma_3\gamma_4/4), \tag{64}$$
$$G(\theta) = \exp(\theta\gamma_1\gamma_5), \tag{65}$$

$\theta = \pi/p$, and p is an odd integer, does not belong to any finite level of the matchgate hierarchy.

Proof. We assume that U_t is in some finite level, say k, of the matchgate hierarchy. Then the unitary $F_1 = U_t\gamma_\mu U_t^\dagger$ must be in $\mathcal{M}_{k-1}$ from the definition of the matchgate hierarchy, where $\mu \in [2n]$. We define the unitaries

$$F_j := F_{j-1}\gamma_\mu F_{j-1}^\dagger, \quad j \geq 2. \tag{E1}$$

Extending the same argument as above shows that F_{k-2} must belong to $\mathcal{M}_{k-2}$. For $U_t = KG(\theta)K$ and $\mu = 2$, the following results hold:

$$F_1 = -\gamma_2(\cos(2\theta) + i\sin(2\theta)\gamma_2\gamma_3\gamma_4\gamma_5), \tag{E2}$$
$$F_j = \gamma_2(\cos(2^j\theta) + i\sin(2^j\theta)\gamma_2\gamma_3\gamma_4\gamma_5), \quad j \geq 2. \tag{E3}$$

Choosing $\theta = \pi/p$, where p is an odd integer, shows that F_j always has a Majorana string with weight > 1. This means that F_{k-2} is not Gaussian because $F_{k-2}\gamma_2 F_{k-2}^\dagger = F_{k-1}$ has a Majorana weight > 1, proving the claim that U_t does not belong to any finite level of the matchgate hierarchy. □