npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-025-01015-y

# Unified framework for matchgate classical shadows

Check for updates

Valentin Heyraud[1], Héloise Chomet[2] & Jules Tilly[2]

Estimating quantum fermionic properties is a computationally difficult yet crucial task for the study of electronic systems. Recent developments have begun to address this challenge by introducing classical shadows protocols relying on sampling of Fermionic Gaussian Unitaries (FGUs): a class of transformations in fermionic space which can be conveniently mapped to matchgates circuits. The different protocols proposed in the literature use different sub-ensembles of the orthogonal group O(2*n*) to which FGUs can be associated. We propose an approach that unifies these different protocols, proving their equivalence, and deriving from it an optimal sampling scheme. We begin by demonstrating that the first three moments of the FGU ensemble associated with SO(2*n*) and of its intersection with the Clifford group are equal, generalizing a result known for O(2*n*) and addressing a question raised in previous works. Building on this proof, we establish the equivalence between the shadows protocols resulting from FGU ensembles analyzed in the literature. Finally, from our results, we propose a sampling scheme for a small sub-ensemble of matchgates circuits that is optimal in terms of number of gates and that inherits the performances guarantees of the previous ensembles.

Understanding the physics of correlated electronic systems is crucial for quantum chemistry[1–3] and condensed matter physics[4,5], with potential far-reaching applications in drug discovery[6], chemical engineering[7] and material science[8]. Simulating such many-body quantum systems on a classical computer is challenging due to the exponential scaling of the system's wavefunction. This difficult task was one of the first applications envisioned for quantum computers[9–13] and it remains one of the most promising[14–20]. However, current quantum devices are noisy and of limited size, which puts severe restrictions on the quantum algorithms that can be reliably executed. In that context, variational quantum algorithms[21] have emerged as a popular class of algorithms addressing these hardware constraints. These versatile algorithms rely on a classical optimization of a variational ansatz obtained by applying a parameterized quantum circuit to some fixed initial state. Among these algorithms, the variational quantum eigensolver[22–24] has attracted lot of attention in view of the simulation of many-body systems on near-term devices.

A critical step of this algorithm is the estimation of the expectation values of a set of observables. This operation occurs repeatedly during the optimization of the variational ansatz, which requires measuring the system Hamiltonian, and at the end of the algorithm to characterize the obtained quantum state. To this end, typical quantities of interest are the $k$-body reduced density matrices ($k$-RDM), which encode many relevant physical properties of the simulated systems[25]. For the study of fermionic systems on quantum devices, the 2-RDM can be used to estimate the system energy[26,27], the associated gradients[28,29] and multipole moments[30]; while the 3-RDM finds useful applications for condensed matter models[31,32]. Multiple methods have been developed to efficiently estimate fermionic $k$-RDM. Bonet-Monroig et al.[33] proposed a strategy based on the gathering of the target observables into cliques of commuting operators that can be measured simultaneously. Although nearly optimal for the 1- and 2-RDMs, the proposed methods cannot be easily generalized to larger values of $k$. Another similar strategy has been proposed in ref. 34 but requires the use of multiple ancillary qubits.

Recognizing these limitations, Zhao et al.[35] proposed a probabilistic strategy, building on the recent breakthrough of the classical shadows protocol[36,37]. This protocol consists in the construction of a classical representation of a quantum state obtained from the measurement performed on the system evolved according to a random unitary transformation. This representation is then used to build estimators of the quantities of interest. A key choice in this procedure is the ensemble of random unitary transformations used to derive the classical representation. The strategy proposed in ref. 35 relies on a subgroup of the group of Fermionic Gaussian Unitaries (FGUs), which is a particular subset of the transformations preserving the linear span of the $2n$ Majorana operators associated with $n$ fermionic modes (see Sec. Fermionic Gaussian Unitaries and Matchgate Circuits for more details). Under the Jordan-Wigner mapping[38], these transformations correspond to matchgate circuits[39], a class of efficiently classically simulable circuits generated by specific Pauli rotations

[1]InstaDeep, Paris, France. [2]InstaDeep, London, United Kingdom. e-mail: v.heyraud@instadeep.com

acting on adjacent pairs of a qubits chain[40,41]. Up to a global phase, FGUs are in one-to-one correspondence with the elements of the group of special orthogonal matrices SO($2n$). This allows for efficient classical simulation schemes that do not rely explicitly on the previous mapping[42–45], which in turns enables an efficient classical post-processing for the classical shadows protocol.

Zhao et al.[35] considered the subset of FGUs belonging to the Clifford group (under an arbitrary fermion-to-qubit mapping). The obtained ensemble corresponds to a subgroup of SO($2n$) solely composed of signed permutation matrices. Using this ensemble, they derived an asymptotically optimal classical shadows protocol for the estimation of fermionic $k$-RDMs. A limitation of the proposed method lies in the use of the subgroup of Clifford FGUs, which appears to single out a preferred basis of Majorana operators. Following this work, Wan et al.[46] introduced a classical shadows protocol using a larger ensemble, which we refer to as the generalized FGUs, in view of an application to hybrid quantum-classical quantum Monte-Carlo simulations (QC-QMC) of fermionic systems[47]. Similarly to FGUs, generalized FGUs are in one-to-one correspondence with the orthonormal group O($2n$) and correspond to matchgate circuits complemented with single-qubit Pauli gates under the Jordan-Wigner map. The authors prove that the first three moments of the uniform distributions on the generalized FGUs and on the subset of Clifford generalized FGUs are equal. This result enables them to simultaneously exploit the symmetries of the Clifford group and the invariance under rotation of the Haar measure on O($2n$), thereby avoiding singling out a preferred basis of Majorana operators. Leveraging this finding, they show that their scheme is efficient in estimating various quantities such as the overlap between an arbitrary pure state and a fermionic Gaussian state. In a related work, O'Gorman[48] provide a simplified analysis of the scheme presented in ref. 35, offering a corrected expression of the estimators variances within and showing the efficiency of the Clifford FGU ensemble for the classical shadows estimation of various quantities. They also considered a shadows protocol associated with a specific subgroup of permutation corresponding to the so-called perfect-matchings, and proved a partial equivalence with the results of ref. 35.

As noted by Zhao and Miyake[49], so far the group of FGU corresponding to the continuous matrix group SO($2n$) has not yet been analyzed in the context of classical shadows, and Wan et al.[46] left the possibility to extend the matchgate 3-design property to this ensemble as an open question. Furthermore, to this day, the link between the shadows protocols corresponding to different sub-ensembles of FGU remains unclear. In this paper, we investigate the use of the FGU ensemble associated with SO($2n$) for the classical shadows protocol. First, we consider the larger class of ensembles that can be decomposed into circuits with independent random Pauli rotations and show that under mild symmetry assumptions on the distributions of the random angles, these ensembles admit the same first three moments as their sub-ensembles belonging to the Clifford group. We refer to ensembles with this property as Clifford-3-cubatures. We find that the FGU ensemble associated with SO($2n$) is a Clifford-3-cubature, thereby providing a positive answer to the open question introduced in ref. 46. Our result proves that the SO($2n$) group leads to a shadows protocol that is equivalent to the one considered in ref. 35. Second, we show that classical shadows protocols using ensembles of Clifford FGUs are unaffected by the injection of reflections with respect to Majorana operators. Precisely, we complete the results of ref. 35 and show that the variances of the shadow estimators are invariant under such reflections. We also extend the results of ref. 48 and show that ensembles of FGU, which permutations correspond to the same perfect-matching also lead to shadow estimators with the same variances. This allow us to rigorously prove that the different FGU ensembles considered in the literature (in particular in refs. 35,46 and ref. 48) yield equivalent classical shadows protocols. Finally, we present and discuss new sampling schemes for different subsets of Clifford FGU. Building on the previous equivalence result, we derive a sampling scheme that is optimal in terms of a number of gates and that generates a FGU ensemble inheriting the best performance guarantees of the previous ensembles.

# Results

## Background

In the following we provide an overview of the background material necessary to develop and prove our results. First, we introduce some general notations and mathematical facts in sec. "Notations and mathematical preliminaries". Then, we review the classical shadows protocol in sec. "Classical shadows protocol". We gather useful definitions and results related to fermionic Gaussian unitaries and matchgate circuits in sec. "Fermionic Gaussian Unitaries and Matchgate Circuits". Finally, we review existing results related to shadows protocols based on FGU ensembles in sec. "Previous results".

**Notations and mathematical preliminaries**. Throughout this paper, we will denote $\mathbb{N}$ the set of non-negative integers, $[k] := \{1, \ldots, k\}$ and we write $\mathbb{N}^* := \mathbb{N}\backslash\{0\}$. For multi-indices $\boldsymbol{\mu}, \boldsymbol{\nu} \subset \mathbb{N}^*$ we write $\delta_{\boldsymbol{\mu\nu}}$ the generalized Kronecker symbol that is equal to 1 if $\boldsymbol{\mu} = \boldsymbol{\nu}$ and 0 otherwise. We follow ref. 35 and write Sym($2n$) the symmetric group on $2n$ objects. This group is faithfully represented by the group of $2n \times 2n$ permutation matrices, namely matrices, which columns and rows have only one non-zero entry equal to 1. We denote Sym($2, 2n$) the generalized symmetric group of cyclic order 2, which is defined as the wreath product $\mathbb{Z}_2 \wr$ Sym($2n$). The group Sym($2$, $2n$) is faithfully represented by permutation matrices whose non-zero entries take values in $\{-1, 1\}$. Every such matrix $M$ can be written $M = DP$ with $P$ a permutation matrix and $D$ a diagonal matrix with entries in $\{-1, 1\}$. The matrices $D$ can be seen as a faithful representation of $\mathbb{Z}_2^n \cong \{-1, 1\}^n$ and for two generalized permutations matrices $M_1$, $M_2$ we have the semi-direct product $M_1M_2 = (D_1P_1D_2P_1^{-1})(P_1P_2)$, so that $\mathrm{Sym}(2, 2n) = \mathbb{Z}_2^n \rtimes (\mathrm{Sym})\ (2n)$. We also write Sym$^+$($2n$) (respectively Sym$^+$($2$, $2n$) the subgroup of Sym($2n$) (respectively Sym($2$, $2n$)) corresponding to matrices with determinant + 1. Note that Sym$^+$($2n$) is exactly the alternating group, i.e. the subgroup of even parity permutations denoted Alt($2n$) in ref. 35. In the following we do not distinguish the previous groups and their matrix representations.

The Hilbert space of a system of $n$ qubits is denoted $\mathcal{H}_n \cong \mathbb{C}^{2^n}$. Since they have the same dimension, $\mathcal{H}_n$ is unitarily isomorphic to the state-space of a system $n$ fermionic modes, and upon fixing a fermion-to-qubits mapping we can identify both. Denote $\mathrm{U}(\mathcal{H}_n)$ the set of unitary operators on $\mathcal{H}_n$. Operators acting trivially on all but the $k$-th qubit are written with a lower index $k$. In particular, we denote $X_k$, $Y_k$, $Z_k$ the Pauli operators associated with the $k$-th qubit. The identity operator is denoted $I$. $\mathcal{H}_n$ is equipped with the usual canonical basis of eigenstates of the Pauli-$Z$ operators $\{|z\rangle,\ z \in \{0, 1\}^n\}$. We denote $\mathrm{P}_n$ the Pauli group, which contains all Pauli words of the form $P = \lambda \prod_{k=1}^n P_k$ with $P_k \in \{I, X_k, Y_k, Z_k\}$ and $\lambda \in \{1, -1, i, -i\}$. We write $\mathrm{Cl}_n$ for the Clifford group, which is defined as the group of unitary operators normalizing the Pauli group, namely $\mathrm{Cl}_n := \{C \in \mathrm{U}(\mathcal{H}_n) \,|\, C\mathrm{P}_nC^\dagger \subseteq \mathrm{P}_n\}$. Recall that up to global phases $\mathrm{Cl}_n$ is generated by the control-$Z$, the Hadamard and the phase gates, respectively denoted $CZ$, $H$ and $S$.

We write $\mathcal{L}(V)$ the space of linear operators on a complex vector space $V$. The set $\mathcal{L}(\mathcal{H}_n)$ is itself a Hilbert space equipped with the Hilbert-Schmidt inner product $\langle A, B\rangle_{HS} := \mathrm{Tr}[A^\dagger B]$. We write $\mathcal{L}(\mathcal{L}(\mathcal{H}_n))$ the vector space of superoperators on $\mathcal{L}(\mathcal{H}_n)$ and we call a quantum channel any superoperator that is completely positive and trace preserving[50]. In the following, superoperators will be denoted with calligraphic letters. In particular, for a unitary transformation $U$, we will write $\mathcal{U}$ the corresponding unitary quantum channel defined as $\mathcal{U}(A) := U^\dagger AU$ for $A \in \mathcal{L}(\mathcal{H}_n)$.

**Classical shadows protocol**. In this subsection we briefly review the classical shadows procedure introduced by Huang et al. in ref. 36. The aim of this protocol is to estimate the expectation values of a set of $M$ observables $\{O_1, \ldots, O_M\} \in \mathcal{L}(\mathcal{H}_n)$ with respect to an unknown quantum state $\rho$ of which we have multiple copies. The first step of the procedure is to chose a unitary ensemble $\mathbb{U}$ characterized by a probability measure $\eta$ over $\mathrm{U}(\mathcal{H}_n)$ (or some subset thereof) which can be efficiently sampled. For each copy of $\rho$, one then draw a random unitary transformation $\hat{U} \sim \mathbb{U}$, apply it to $\rho$ and perform a measurement of the resulting state in the computational basis. One then obtain a classical bit-string $\hat{z}$, whose probability distribution conditioned on $\hat{U}$ is given by Born's rule

$$\mathbb{P}\left[\hat{z} = z \mid \hat{U}\right] = \langle z|\hat{U}\rho\hat{U}^\dagger|z\rangle. \tag{1}$$

Applying the inverse unitary $\hat{U}^\dagger$ to the state $|\hat{z}\rangle$ and averaging over the realisations yields a mixed state that can be seen as the image of $\rho$ under the so-called measurement quantum channel

$$\begin{aligned}\mathcal{M}(\rho) &:= \mathbb{E}_{\hat{U},\hat{z}}\left[\hat{U}^\dagger|\hat{z}\rangle\langle\hat{z}|\hat{U}\right] \\ &= \mathbb{E}_{\hat{U}}\left[\sum_{z\in\{0,1\}^n}\langle z|\hat{U}\rho\hat{U}^\dagger|z\rangle\hat{U}^\dagger|z\rangle\langle z|\hat{U}\right],\end{aligned} \tag{2}$$

Assuming that $\mathcal{M}$ is invertible, one can define an estimator of $\rho$ as follow

$$\hat{\rho} := \mathcal{M}^{-1}\left(\hat{U}^\dagger|\hat{z}\rangle\langle\hat{z}|\hat{U}\right). \tag{3}$$

This estimator and its realisations are referred to as classical shadows in the literature. Note that the requirement that $\mathcal{M}$ must admit an inverse on the whole space $\mathcal{L}(\mathcal{H}_n)$ can be relaxed to $\mathcal{M}$ admitting an inverse on a subspace of $\mathcal{L}(\mathcal{H}_n)$, provided that both $\rho$ and $U^\dagger|z\rangle\langle z|U$ belong to this subspace for any $z \in \{0,1\}^n$ and $U \in \mathbb{U}$[46].

Using the classical shadow $\hat{\rho}$, one can then build estimators for the expectation values $o_i := \mathrm{Tr}[O_i\rho]$ for $i \in [1, M]$ by defining

$$\hat{o}_i := \mathrm{Tr}[O_i\hat{\rho}]. \tag{4}$$

Remark that these estimators are to be computed classically from the knowledge of the sampled unitaries $\hat{U}$ and measurement outcomes $\hat{z}$. By construction, the classical shadows and the corresponding estimators are unbiased. In particular, the only part of the variance of $\hat{o}_i$ affected by the choice of $\mathbb{U}$ is the raw second moment $\mathbb{E}\left[\hat{o}_i^2\right]$, which is also a simple majorant of $\mathrm{Var}\left[\hat{o}_i\right]$. Huang et al.[36] also introduced another useful majorant of the previous variance, the so-called shadow norm which is defined as the supremum of the second raw moment over all possible states $\rho$. Using a median-of-mean estimator and the associated concentration inequalities[36,51], it can be shown that a sample size

$$N \propto \frac{1}{\epsilon^2}\log\left(\frac{M}{\delta}\right)\max_{1\le i\le M}\left(\mathrm{Var}\left[\hat{o}_i\right]\right) \tag{5}$$

is sufficient to estimate all the $M$ expectation values up to an error $\epsilon$ and with a probability of failure $\delta$. ref. 36 motivates the use of a median-of-mean estimator by the obtention of a logarithmic scaling in both $M$ and $\delta$. Depending on the observables to measure and on the unitary ensemble considered, the observables estimators might be bounded. In that case, a direct application of the Hoeffding inequality[52] shows that a simple mean-of-sample estimator can be used, leading to a similar scaling for $N$ (upon replacing the variances by the range of the estimators in Eq. (5)). However, as the inverse of the measurement channel might not be a quantum channel itself, the classical shadows are not well defined quantum states in general. In particular, $\hat{\rho}$ might fail to be positive, which can make it difficult to bound for $\mathrm{Tr}[O_i\hat{\rho}]$.

In order to better appreciate the role of the chosen unitary ensemble in the classical shadows protocol, it is insightful to introduce the $t$-fold twirl[53] (or simply $t$-fold[54]) channel of $\mathbb{U}$, whose action on $A \in \mathcal{L}(\mathcal{H}_n^{\otimes t})$ is given by

$$\mathcal{E}^{(t)}(A) := \int_{\mathrm{U}(\mathcal{H}_n)}(U^\dagger)^{\otimes t}AU^{\otimes t}\eta(\mathrm{d}U) \tag{6}$$

with $\eta$ the probability measure defining $\mathbb{U}$. The $t$-fold channel completely characterizes the first $t$ moments of the distribution $\eta$. Random unitary ensembles whose $t$-fold channel matches the $t$-fold channel of the Haar measure[55] on $\mathrm{U}(\mathcal{H}_n)$ are said to be unitary $t$-designs. As an example, it is well known that the Clifford group $\mathrm{Cl}_n$ equipped with the uniform distribution is a 3-design although it fails to be a 4-design[56,57]. The notion of $t$-design have also been extended to other unitary groups (see e.g. ref. 58) and to continuous variable systems in ref. 59. These ensembles have found numerous useful applications in quantum information theory[54,60–65]. In particular, the use of the uniform Clifford ensemble for the classical shadows protocol was investigated in ref. 36.

Having defined the $t$-fold channel of $\mathbb{U}$, one can use the linearity of both the trace and the expectation to rewrite the measurement channel as

$$\mathcal{M}(\rho) = \sum_{z\in\{0,1\}^n}\mathrm{Tr}_1\left[\mathcal{E}^{(2)}(|z\rangle\langle z|^{\otimes 2})(\rho\otimes I)\right], \tag{7}$$

where $\mathrm{Tr}_1$ denotes the partial trace over the first tensor component. Likewise, using the fact that $\mathrm{Tr}[\mathcal{M}^{-1}(A)B] = \mathrm{Tr}[A\mathcal{M}^{-1}(B)]$, one can write the second raw moment $\mathbb{E}\left[\hat{o}_i^2\right]$ as follow

$$\sum_{z\in\{0,1\}^n}\mathrm{Tr}\left[\mathcal{E}^{(3)}(|z\rangle\langle z|^{\otimes 3})(\rho\otimes\mathcal{M}^{-1}(O_i)\otimes\mathcal{M}^{-1}(O_i))\right]. \tag{8}$$

These expressions show that unitary ensembles sharing the same 3-fold channel yield classical shadows protocols whose efficiencies are essentially equal. As for the results presented in ref. 46, many of our results will rely on this observation.

**Fermionic Gaussian Unitaries and Matchgate Circuits.** In the next paragraphs, we introduce some notations and definitions related to many-body fermionic systems. Then, we review the various ensembles of fermionic Gaussian unitaries used in the literature and give some of the associated results in the context of classical shadows.

Consider a system of $n$ fermionic modes whose creation and annihilation operators are denoted $a_i$, $a_i^\dagger$ with $i \in [n]$. The fermionic modes can equivalently be represented by the $2n$ Majorana operators

$$\gamma_{2p-1} := a_p^\dagger + a_p, \quad \gamma_{2p} := i\left(a_p^\dagger - a_p\right), \tag{9}$$

which are self-adjoint and satisfy the anti-commutation relations $\left\{\gamma_k, \gamma_l\right\} = 2\delta_{kl}I$. In the following we will denote $\binom{[2n]}{k}$ the set of subsets of $[2n]$ with $k$ elements, and identify an element $\boldsymbol{\mu} \in \binom{[2n]}{k}$ with the corresponding $k$-multi-index $\boldsymbol{\mu} := (\mu_1, \ldots, \mu_k)$ which elements are sorted in increasing order $1 \le \mu_1 < \cdots < \mu_k \le 2n$. For any such $\boldsymbol{\mu}$, define the associated $k$-degree Majorana operator

$$\gamma_{\boldsymbol{\mu}} := \gamma_{\mu_1}\cdots\gamma_{\mu_k}. \tag{10}$$

These operators form an orthogonal family for the Hilbert-Schmidt inner product.

The $k$-RDM of a state $\rho$ is defined as the tensor of order $2k$ whose entries are written

$${}^kD^{p_1\cdots p_k}_{q_1\cdots q_k} := \mathrm{Tr}\left[a_{p_1}^\dagger\ldots a_{p_k}^\dagger a_{q_1}\ldots a_{q_k}\rho\right]. \tag{11}$$

In order to estimate the $k$-RDM using a quantum computer, one needs to map the system of $n$ fermionic modes to a system of qubits. For the sake of clarity, we will use the Jordan-Wigner (JW) transformation throughout this paper, which we recall at the end of the Methods section "Fermion-to-qubit mapping." Having fixed a fermion-to-qubit mapping, we will no longer distinguish the fermionic from the qubit transformations. Note that the results presented in this paper are independent of the exact mapping used, as long as Majorana operators are mapped to Pauli ones.

Zhao et al.[35] proposed a classical shadows protocol tailored for the estimation of fermionic $k$-RDMs relying on a subset of the continuous group of fermionic Gaussian unitary transformations. A FGU is a unitary transformation $U_Q \in \mathcal{L}(\mathcal{H}_n)$ associated with some $Q \in \mathrm{SO}(2n)$ such that

$$U_Q^\dagger \gamma_k U_Q = \sum_{k=1}^{2n} Q_{kl}\gamma_l \tag{12}$$

for every $k \in [2n]$. As before, we denote $\mathcal{U}_Q$ the corresponding unitary quantum channel. Using the Leibnitz formula for determinants and the commutation relation of the Majorana operators, we have

$$U_Q^\dagger \gamma_{\boldsymbol{\mu}} U_Q = \sum_{\boldsymbol{\nu} \in \binom{[2n]}{|\boldsymbol{\mu}|}} \det\left(Q_{\boldsymbol{\mu}\boldsymbol{\nu}}\right)\gamma_{\boldsymbol{\nu}}, \tag{13}$$

where $Q_{\boldsymbol{\mu}\boldsymbol{\nu}} \in \mathbb{R}^{|\boldsymbol{\mu}| \times |\boldsymbol{\mu}|}$ is defined by $(Q_{\boldsymbol{\mu}\boldsymbol{\nu}})_{ij} = Q_{\mu_i \nu_j}$ for $1 \le i, j \le |\boldsymbol{\mu}| = |\boldsymbol{\nu}|$. Hence, every FGU is characterized up to a global phase by its associated element $Q \in \mathrm{SO}(2n)$. In particular, the map $Q \mapsto \mathcal{U}_Q$ yields a faithful representation of $\mathrm{SO}(2n)$ on $\mathcal{L}(\mathcal{H}_n)$ that satisfies

$$\mathcal{U}_{Q'}\,\mathcal{U}_Q = \mathcal{U}_{QQ'} \tag{14}$$

for all $Q, Q' \in \mathrm{SO}(2n)$. Using the Cauchy-Binet formula[66] and the matrix elements $\mathrm{Tr}[\gamma_{\boldsymbol{\nu}}^\dagger \mathcal{U}_Q(\gamma_{\boldsymbol{\mu}})]$ in Liouville representation, one can show that this representation is orthogonal[35].

The existence of an homomorphism from $\mathrm{SO}(2n)$ to $\mathcal{L}(\mathcal{L}(\mathcal{H}_n))$ allows to transform a decomposition of the element $Q$ in elementary building blocks into a decomposition of the corresponding $U_Q$. Of note are the decompositions in terms of Givens rotations[67], which are rotations in planes spanned by two coordinate axes of $\mathbb{R}^{2n}$. More precisely, a Givens rotation $g_{ij}(\theta)$ of axes $i, j \in [\![1, 2n]\!]$ and angle $\theta \in (-\pi, \pi]$ is defined as the rotation whose matrix in the canonical basis of $\mathbb{R}^{2n}$ reads

$$\begin{array}{cc} & \begin{array}{ccccccc} \phantom{1} & \phantom{\cdots} & i & \phantom{\cdots} & j & \phantom{\cdots} & \phantom{0} \end{array} \\ \begin{array}{c} \\ \\ i \\ \\ j \\ \\ \\ \end{array} & \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & \cos(\theta) & \cdots & -\sin(\theta) & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & \sin(\theta) & \cdots & \cos(\theta) & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \end{array}. \tag{15}$$

Defining

$$G_{ij}(\theta) = \exp\left(-\frac{\theta}{2}\gamma_i\gamma_j\right), \tag{16}$$

and writting $\mathcal{G}_{ij}(\theta)$ the corresponding channel, we have

$$\begin{aligned} \mathcal{G}_{ij}(\theta)(\gamma_k) &:= G_{ij}(\theta)^\dagger \gamma_k G_{ij}(\theta) \\ &= \sum_{l=1}^{2n} [g_{ij}(\theta)]_{kl}\gamma_l, \end{aligned} \tag{17}$$

that is $g_{ij}(\theta)$ is represented by $\mathcal{G}_{ij}(\theta)$. From what precedes, decomposing $Q \in \mathrm{SO}(2n)$ as a product of $g_{ij}(\theta)$ yields a decomposition of $\mathcal{U}_Q$ as a composition of $\mathcal{G}_{ij}(\theta)$. Such decompositions have found useful applications in the literature related to FGU and the simulation of fermionic systems[15,16,68].

Under the JW mapping, the FGUs correspond to the so-called matchgate circuits. A matchgate is defined as a two-qubits Pauli rotation of the form

$$\begin{aligned} U(\theta) &= \exp\left(i\tfrac{\theta}{2} P \otimes P'\right), \\ P \otimes P' &\in \{Z \otimes I,\ I \otimes Z,\ X \otimes X\}. \end{aligned} \tag{18}$$

Considering that the $n$ qubits are placed on a line, matchgate circuits are then defined as the quantum circuits composed of matchgates acting on pairs of adjacent qubits. This correspondence between FGU and matchgate circuits, which was first proven in ref. 42, can be elucidated as follow. First, notice that

$$iZ_k = \gamma_{2k-1}\gamma_{2k}, \quad iX_kX_{k+1} = \gamma_{2k}\gamma_{2k+1}, \tag{19}$$

so that matchgates correspond to Givens rotations on adjacent qubits. In the following we write $g_k(\theta) := g_{k-1k}(\theta)$ these Givens rotations, and likewise for $G_k(\theta)$ and $\mathcal{G}_k(\theta)$ for $2 \le k \le 2n$. Then, remark that any elements of $\mathrm{SO}(2n)$ can be decomposed as a product of $g_k(\theta)$. We review an important scheme introduced in ref. 69 that achieves such a decomposition in the next section.

The classical shadows introduced in ref. 35 are built using the subgroup of FGU belonging to the Clifford group. Considering a fermion-to-qubit transformation mapping the Pauli operators to the Majorana ones, a FGU is in the Clifford group if and only if its matrix $Q$ belongs to $\mathrm{Sym}^+(2, 2n)$. The corresponding matchgate circuits are generated by matchgates with angles belonging to $\left\{0, \pi, \frac{\pi}{2}, -\frac{\pi}{2}\right\}$, which we refer to as the Clifford angles. To see this, remark that any rotation generated by a Pauli string can be transformed into a single-qubit $Z$-rotation upon conjugating with the adequate Clifford gates, and that the only $Z$-rotations in the Clifford group are the ones for which $\theta$ belongs to the Clifford angles (the angles $0, \pi, \frac{\pi}{2}, -\frac{\pi}{2}$ correspond respectively to the gates $I$, $Z$, $S$ and $S^\dagger$, up to global phases).

The previous definition of FGU and of the corresponding matchgate circuits can be extended to include transformations satisfying Eq. (12) with $Q \in \mathrm{O}(2n)$, which we refer to as generalized FGU. Notice that most of the previous discussion on FGU remains valid for these transformations, and in particular Eqs. (13) and (14) hold true. Generalized FGU form a group comprising the previous FGU together with unitary transformations implementing reflections, namely transformations that map $\gamma_k$ to $-\gamma_k$ for some $k \in [2n]$ and leave all over Majorana operators invariants. Adding such reflections allows to navigate between both connected components of $\mathrm{O}(2n)$ corresponding to matrices with determinant $+1$ and $-1$. Note that it suffices to add a single reflection to the group of FGU to generate the whole group of generalized FGU. A simple choice is to include the reflection with respect to the last Majorana operator $\gamma_{2n}$. In terms of qubits, this amount to allow the addition of the single-qubit Pauli gate $X_n$ to the previous matchgate circuits, as can be checked from Eq. (92). We refer to the corresponding circuits as generalized matchgate circuits. Remark that by using Eq. (92) one may verify that the reflections with respect to $\gamma_{2k-1}$ and $\gamma_{2k}$ correspond respectively to $X_k\Pi_{l>k}Z_l$ and $Y_k\Pi_{l>k}Z_l$, which can easily be decomposed into products of $X_n$ and matchgates.

Due to the connection between matchgate circuits and FGU, we write respectively $\mathrm{M}_n^+$ and $\mathrm{M}_n$ for the groups of FGU and generalized FGU.

**Previous results**. Having reintroduced the relevant ensembles, we can now recall some of the results on FGU shadows protocols established in previous works. Zhao et al.[35] derived an exact expression for the measurement channel for the ensemble $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$ that reads

$$\mathcal{M}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n} = \sum_{k=1}^{n} \binom{n}{k}\binom{2n}{2k}^{-1} \mathcal{P}_{2k} \tag{20}$$

with $\mathcal{P}_{2k}$ the projector on the subspace of Majorana operators of degree $2k$. This measurement channel is diagonal in the basis of Majorana operators and we write $\lambda_{k,n} := \binom{n}{k}\binom{2n}{2k}^{-1}$ its eigenvalues. Thanks to its diagonal form, this channel can be easily inverted. Moreover, a simple calculation shows that for a $2k$-degree Majorana operator $\gamma_{\boldsymbol{\mu}}$ the shadow norm is given by $\lambda_{k,n}^{-1}$, which yields an upper bound on the variance of the corresponding shadow estimator. The authors prove that this bound is optimal in the sense that there is no subgroup of Clifford FGU resulting in a strictly lower shadow norm. Another important result from ref. 35 is the fact that the measurement channel of an ensemble of FGU associated with a set of generalized permutation matrices is independent of the signs of the matrices entries. In particular, the authors show that the sub-ensembles of Clifford FGU corresponding to the groups $\mathrm{Sym}^{+}(2, 2n)$ and $\mathrm{Sym}^{+}(2n)$ result in the same measurement channel given by Eq. (20). This result seems to indicate an equivalence between the different ensembles of Clifford FGU. However, the equality of the measurement channels does not guarantee that the corresponding shadow estimators have the same variance, even though the authors showed that the corresponding shadow norms are the same. Besides, a potential limitation of the approach taken in ref. 35 lies in the restriction to the subgroup of Clifford FGU. In fact, focusing on this subgroup appears to single out a preferred basis of Majorana operators, and the bounds on the variance of the corresponding shadow estimators do not necessary hold for rotated bases of Majorana operators of the form $\tilde{\gamma}_k := \mathcal{U}_Q(\gamma_k)$ for some $Q \in \mathrm{O}(2n)$.

Building on the work of ref. 35, Wan et al.[46] proposed to use ensembles of generalized matchgate circuits. Most of their results stem from an important property which they prove, namely that the 3-fold channels of the ensembles $\mathrm{M}_n$ and $\mathrm{M}_n \cap \mathrm{Cl}_n$ are equal:

$$\mathcal{E}^{(3)}_{\mathrm{M}_n} = \mathcal{E}^{(3)}_{\mathrm{M}_n \cap \mathrm{Cl}_n}. \tag{21}$$

This result is reminiscent of the 3-design property of the Clifford group[56,58,70], and the authors informally summarize it by saying that the group of Clifford generalized matchgate circuits form a matchgate 3-design. As a consequence of this result, the ensembles $\mathrm{M}_n \cap \mathrm{Cl}_n$ and $\mathrm{M}_n$ are equivalent for the classical shadows protocol, and they yields the same measurement channels as well as shadow estimators with the same variance. Moreover, it is shown that the measurement channel is equal to the one obtained in ref. 35 for $\mathrm{M}_n^{+}$, such that

$$\mathcal{M}_{\mathrm{M}_n} = \mathcal{M}_{\mathrm{M}_n \cap \mathrm{Cl}_n} = \mathcal{M}_{\mathrm{M}_n^{+} \cap \mathrm{Cl}_n}. \tag{22}$$

The authors also derive improved variance bounds for Majorana operators as well as for other types observables, including some important overlaps quantities for hybrid quantum-classical Monte Carlo simulations. The equivalence between $\mathrm{M}_n \cap \mathrm{Cl}_n$ and $\mathrm{M}_n$ enables to use the symmetries of the Clifford group while preserving the invariance under rotations and reflections of the generalized matchgate group. This allows the authors to evade the specification of a preferred set of operators and to apply their bounds to any rotated bases of Majorana operators.

O'Gorman[48] extend the results of ref. 35 and provide a simplified analysis of the protocol as well as a corrected expression of the variance of the shadow estimators. Moreover, they show that the measurement channel of any sub-ensemble of $\mathrm{M}_n^{+} \cap \mathrm{Cl}_n$ only depends on the perfect-matching associated with each (signed) permutation of the ensemble. The perfect-matching associated with a permutation $\sigma : [2n] \mapsto [2n]$ is defined as

$$\mathrm{PerfMatch}(\sigma) := \left\{ \left\{ \sigma(2i-1), \sigma(2i) \right\},\ i \in [n] \right\}. \tag{23}$$

As such, $\mathrm{PerfMatch}(\sigma)$ is the equivalence class of permutations that differs from $\sigma$ by transposition acting on pairs of the form $(2i-1, 2i)$ and by permutations preserving these pairs. For $Q \in \mathrm{Sym}(2, 2n)$, we define $\mathrm{PerfMatch}(Q)$ as the perfect-matching of the corresponding unsigned permutation. We denote $\mathrm{PerfMatch}(2n)$ the set of all possible perfect-matching of $[2n]$. A complete set of representatives of $\mathrm{PerfMatch}(2n)$ is a subset of $\mathrm{Sym}(2, 2n)$ composed of exactly one representative per class in $\mathrm{PerfMatch}(2n)$. Using their result, the authors show that any such set equipped with a uniform measure leads to the same measurement channel as $\mathrm{M}_n^{+} \cap \mathrm{Cl}_n$. Hence, they find a strict sub-ensemble of $\mathrm{M}_n^{+} \cap \mathrm{Cl}_n$ admitting the same measurement-channel. As before, note that this imply an equality of the corresponding shadow norms but not necessarily of the variance of the shadow estimators. Besides their results, the authors conjecture the existence of an efficient sampling scheme for some complete sets of representatives of $\mathrm{PerfMatch}(2n)$.

**Table 1 | Sub-ensembles of the generalized matchgate used in the literature and the corresponding subsets $S \subseteq \mathrm{O}(2n)$**

| $\mathbb{U} := \{\mathcal{U}_{Q},\ Q \in S\}$ | $S \subset \mathrm{O}(2n)$ | ref. |
|---|---|---|
| $\mathrm{M}_n$ | $\mathrm{O}(2n)$ | 46 |
| $\mathrm{M}_n \cap \mathrm{Cl}_n$ | $\mathrm{Sym}(2, 2n)$ | 46 |
| $\mathrm{M}_n^{+}$ | $\mathrm{SO}(2n)$ | This work |
| $\mathrm{M}_n^{+} \cap \mathrm{Cl}_n$ | $\mathrm{Sym}^{+}(2, 2n)$ | 35 |
| n.a. | $\mathrm{Sym}^{+}(2n)$ | 35 |
| n.a. | $S \cong \mathrm{PerfMatch}(2n)$ | 48 |

In this work, we show that these ensembles yield equivalent classical shadows protocols. The last line correspond to subsets that are complete sets of representatives of PerfMatch(2n), i.e. sets that are isomorphic to PerfMatch(2n) under the associated natural projection.

Other works in the literature investigated the use of FGUs for classical shadows protocols. Wu and Koh[71] presented an error-mitigated version of the protocol of ref. 35. Statistical properties of the matchgate shadows of ref. 46 were investigated in refs. 72 and [73] in the respective context of quantum chemistry and QC-QMC. This protocol was also numerically and experimentally investigated in ref. 74, again in view of QC-QMC simulations. The authors show that the matchgate shadows protocol is robust to noise, connecting with earlier results of this nature[53,75]. They also show that the post-processing of the data remains a challenging bottleneck for an application to QC-QMC. Another classical shadows scheme based on the subset of number-conserving generalized FGU was investigated in ref. 76 for the particular case of quantum states with a fixed particle number. Low[76] found an exponential improvement for average variance of their estimator over the worst-case bounds obtained in ref. 35. However, this protocol suffers some limitations that are discussed in ref. 46'[77] and [78] introduced FGU-based shadow protocols adapted to the estimation of fermionic correlations on analog quantum simulator. Ref. 77 proposed a sampling scheme for a subgroup of FGU utilizing beam-splitter operations, enabling the estimation of 2- and 4-point fermionic correlations in ultra-cold atom experiments. In ref. 78, the authors explored protocols adapted to current experimental platforms, relying on translationally-invariant FGU. Zhao and Miyake[49] proposed a quantum error-mitigation strategy using classical shadow tomography and relying on symmetries of the system of interest. They apply their method in the context of matchgate shadows protocols and derive an optimal sampling of the continuous matchgate group. At last, the generalized FGU group was also explored in ref. 79 in the context of randomized benchmarking.

The different ensembles of generalized matchgates studied in this work and their corresponding matrix groups are summarized in Table 1.

## Clifford 3-cubatures and Matchgate Ensembles

Here we investigate the use of the ensemble $\mathrm{M}_n^{+}$ corresponding to the matrix group $\mathrm{SO}(2n)$ for the classical shadows protocol. As pointed out in ref. 46, so far it was unclear whether the matchgate 3-design property holds for $\mathrm{M}_n^{+}$. Here, we provide a positive answer to this question. Consequently, we obtain that the group $\mathrm{M}_n^{+}$ leads to a classical shadows protocol that is equivalent to one of the group $\mathrm{M}_n^{+} \cap \mathrm{Cl}_n$ analyzed in ref. 35.

To prove our claim, we first derive a general result in sec. "Locally random ensembles and Clifford 3-cubatures" which extends the relationship between the unitary group and its Clifford subset to non-uniform ensembles admitting a decomposition into independent local random rotations. Then, in sec. "Matchgate 3-desig", we show that $\mathrm{M}_n^{+}$ falls within the scope of the previous result, on which we build to conclude.

**Locally random ensembles and Clifford 3-cubatures**. To present our result, it is convenient to first introduce a type of ensemble that generalizes the notion of $t$-design to non-uniform distributions, which we call $t$-cubatures. Akin to unitary designs that were introduced as the unitary analogs of spherical designs, we define unitary $t$-cubatures as the analogs of positive cubatures appearing in the literature on numerical integration (see for instance refs. 80–84). Recall that the $t$-fold channel $\mathcal{E}_{\mathbb{U}}^{(t)}$ of a unitary ensemble $\mathbb{U}$ is given by Eq. (6).

**Definition 1**. (Unitary $t$-cubature). Let $\mathbb{U} \subseteq \mathrm{U}(\mathcal{H}_n)$ be a unitary ensemble. We say that a finite sub-ensemble $\{U_j, j \in J\} \subseteq \mathbb{U}$ with an associated probability distribution $(p_j)_{j\in J}$ is a $t$-cubature of $\mathbb{U}$ (or $(\mathbb{U}, t)$-cubature) if it satisfies

$$\mathcal{E}_{\mathbb{U}}^{(t)} = \sum_{j\in J} p_j \mathcal{U}_j^{\otimes t}. \tag{24}$$

We call a Clifford $t$-cubature any $t$-cubature whose elements belong to $\mathrm{Cl}_n$, and we say that $\mathbb{U}$ admits a (Clifford) $t$-cubature if there exists a (Clifford) $(\mathbb{U}, t)$-cubature.

Consistently with the definition of unitary $t$-design, we will call a $(\mathbb{U}, t)$-design any $(\mathbb{U}, t)$-cubature associated with a uniform distribution $p_j = 1/|J|, \forall j \in J$. Equipped with the previous definition, we can now state the main result of this section.

**Theorem 1**. Let $\mathbb{U}$ be a unitary ensemble generated by a quantum circuit composed of fixed Clifford gates and Pauli rotations with independent random angles distributed symmetrically about the Clifford angles. Then $\mathbb{U}$ admits a Clifford 3-cubature.

Recall that a random angle $\theta$ is symmetrically distributed about an angle $\theta_0$ if and only if $\mathbb{E}\left[f(\theta-\theta_0)\right] = \mathbb{E}\left[f(\theta_0-\theta)\right]$ for any bounded function $f$. To prove our theorem, we only need to focus on unitary ensembles generated by a random Pauli rotation of the form

$$\left\{U(\theta) := \exp\left(-i\frac{\theta}{2}P\right), \theta \sim \nu\right\} \tag{25}$$

with $P \in \mathrm{P}_n$ and $\nu$ a probability measure on $(-\pi, \pi]$. In fact, for an ensemble $\mathbb{U}$ generated by a circuit with a fixed architecture composed of Clifford gates and independent random rotations, if the unitary ensembles corresponding to the random rotations admit a Clifford $t$-cubature, then so does $\mathbb{U}$ by independence of the angles and linearity of the quantum channels. Furthermore, as for every Pauli string $P$ there exists a Clifford unitary $C \in \mathrm{Cl}_n$ such that $C^\dagger P C = Z_1$, one can simply focus on the particular case of a single-qubit random $Z$-rotation. For instance, Fig. 1 gives such a decomposition for the rotations generated by $P = X \otimes X$ which represents Givens rotations under the JW mapping. Let us denote $R_\theta := e^{-i\frac{\theta}{2}Z}$, and recall that up to a global phase we have

$$R_0 = I,\ R_{\frac{\pi}{2}} = S,\ R_\pi = Z,\ R_{\frac{3\pi}{2}} = S^\dagger. \tag{26}$$

As before, we write respectively $\mathcal{R}_\theta, \mathcal{I}, \mathcal{S}, \mathcal{Z}$ and $\mathcal{S}^\dagger$ the corresponding unitary channels. We prove the following lemma in the Methods section " Proof of Lemma 1."

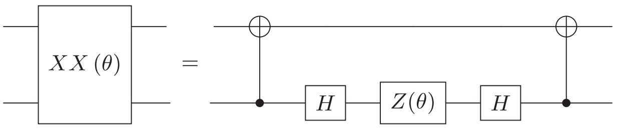

**Fig. 1** | Decomposition of the 2-qubits rotation generated by $X \otimes X$ into Clifford gates and single-qubit $Z$-rotation.

**Lemma 1**. Let $\nu$ be a probability distribution on $(-\pi, \pi]$ symmetric about the Clifford angles and $\theta \sim \nu$. Then

$$\mathbb{E}\left[\mathcal{R}_\theta^{\otimes 3}\right] = \frac{(1-p)}{2}\left(\mathcal{I}^{\otimes 3} + \mathcal{Z}^{\otimes 3}\right) + \frac{p}{2}\left(\mathcal{S}^{\otimes 3} + \mathcal{S}^{\dagger\otimes 3}\right) \tag{27}$$

with $p := \mathbb{E}\left[\sin(\theta)^2\right]$.

This shows that under the constraints on angle distribution state in the Lemma, the unitary ensemble corresponding to a random $Z$-rotation admits a Clifford 3-cubature, and the proof of Theorem 1 follows.

Note that Theorem 1 and Lemma 1 above are generalizations of previous results presented in ref. 85 that focused on Clifford 2-cubatures. Intuitively, these results can be interpreted as the outcomes of a decoherence effect induced by a random choice of the angles. It is natural to wonder whether or not the previous lemma generalizes to $k$-fold channels with $k \geq 4$. We provide a negative answer to this question and discuss some related implications in the Methods section "Absence of Clifford 4-cubature for single random Pauli rotations."

**Matchgate 3-designs**. To show that matchgate circuits are encompassed by the previous result, we rely on a well-known decomposition of elements of SO(2$n$) into Givens rotations as well as an associated sampling method introduced in ref. 69. Consider a matrix $Q \in \mathrm{SO}(2n)$, one can show that there exists Givens rotations $g_k^l(\theta_k^l)$ acting on axes $(k-1, k)$ with $1 \leq l < 2n+2-k \leq 2n$ such that

$$Q = (g_2^1 g_3^1 \ldots g_{2n}^1)\ldots(g_2^{2n-2} g_3^{2n-2})(g_2^{2n-1}), \tag{28}$$

where we dropped the angles for clarity. Detailed proofs of this decomposition can be found in refs. 86,87. To this decomposition corresponds a matchgate circuit. Figure 2 show this circuit for $2n = 2$. In the general case, that circuit is composed of $n(2n-1)$ rotations of angles $\theta_k^l$ that can be adjusted to generate any FGU. By sampling the rotation angles according to the right distributions, one can use this circuit to sample uniformly over $\mathrm{M}_n^+$. This result is encapsulated in the following proposition, which is adapted of a result given in ref. 86. Details on our modifications of the original proposition can be found in the Methods section "Distribution of the angles of Givens rotations."

**Proposition 1**. (Proposition 1.6 in ref. 86, adapted.). Let $Q$ be a random matrix defined by Eq. (28) for random independent angles $\theta_k^l$. If

$$\theta_k^l \sim f_k(\theta) := \frac{\Gamma\left(\frac{k}{2}\right)}{2\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{k-1}{2}\right)}|\sin(\theta)|^{k-2} \tag{29}$$

for all $l$ and $k$, then $Q$ is uniformly distributed on SO(2$n$).

Note that there exists other decompositions similar to the one presented here, some of which rely on Givens rotations with non-adjacent axes (see for instance ref. 88), and other ones with a different order of the Givens rotations (see ref. 89).

As the distributions of Eq. (29) are symmetric with respect to the Clifford angles, Theorem 1 applies to the random matchgate circuits corresponding to the decomposition of Proposition 1, as long as Majorana operators are mapped to Pauli strings under the considered. This is independent of the exact fermion-to-qubit mapping. This allows us to prove the following proposition, which generalizes the matchgate 3-design result of ref. 46 to $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$.

**Proposition 2**. The uniform FGU group $\mathrm{M}_n^+$ admits a Clifford 3-design, i.e.

$$\mathcal{E}_{\mathrm{M}_n^+}^{(3)} = \mathcal{E}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n}^{(3)}. \tag{30}$$

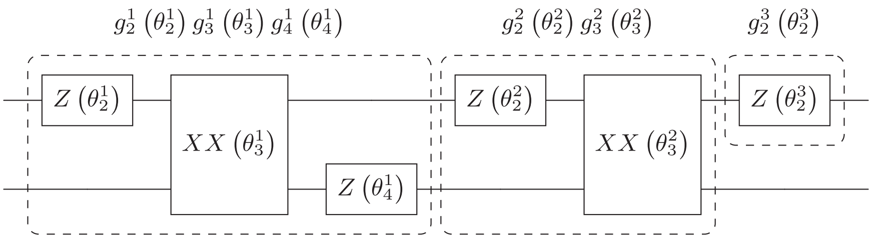
$g_2^1\left(\theta_2^1\right) g_3^1\left(\theta_3^1\right) g_4^1\left(\theta_4^1\right)$
$g_2^2\left(\theta_2^2\right) g_3^2\left(\theta_3^2\right)$
$g_2^3\left(\theta_2^3\right)$
$Z\left(\theta_2^1\right)$
$XX\left(\theta_3^1\right)$
$Z\left(\theta_4^1\right)$
$Z\left(\theta_2^2\right)$
$XX\left(\theta_3^2\right)$
$Z\left(\theta_2^3\right)$

**Fig. 2** | Example of matchgate circuit corresponding to the decomposition of Eq. (28) for the Jordan-Wigner mapping and $n = 2$ qubits.

**Proof**. From Theorem 1, there exists a Clifford 3-cubature $\{\mathcal{C}_j, j \in J\} \subset \mathrm{M}_n^+ \cap \mathrm{Cl}_n$ with a probability distribution $(p_j)_{j \in J}$ such that

$$\mathcal{E}^{(3)}_{\mathrm{M}_n^+} = \sum_{j \in J} p_j \mathcal{C}_j^{\otimes 3}. \tag{31}$$

The 3-fold channel $\mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n}$ can be written

$$\mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n} = \frac{1}{|\mathrm{M}_n^+ \cap \mathrm{Cl}_n|} \sum_{\mathcal{C} \in \mathrm{M}_n^+ \cap \mathrm{Cl}_n} \mathcal{C}^{\otimes 3}. \tag{32}$$

Composing this equation on the left with $\mathcal{E}^{(3)}_{\mathrm{M}_n^+}$ gives

$$\begin{aligned} \mathcal{E}^{(3)}_{\mathrm{M}_n^+} \mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n} &= \tfrac{1}{|\mathrm{M}_n^+ \cap \mathrm{Cl}_n|} \sum_{\mathcal{C} \in \mathrm{M}_n^+ \cap \mathrm{Cl}_n} \mathcal{E}^{(3)}_{\mathrm{M}_n^+} \mathcal{C}^{\otimes 3} \\ &= \tfrac{1}{|\mathrm{M}_n^+ \cap \mathrm{Cl}_n|} \sum_{\mathcal{C} \in \mathrm{M}_n^+ \cap \mathrm{Cl}_n} \mathcal{E}^{(3)}_{\mathrm{M}_n^+} \\ &= \mathcal{E}^{(3)}_{\mathrm{M}_n^+}, \end{aligned} \tag{33}$$

where we used the left-invariance of the Haar measure on $\mathrm{M}_n^+$ on the second line. Likewise, using Eq. (31) and the right-invariance of the Haar measure on $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$, we have

$$\begin{aligned} \mathcal{E}^{(3)}_{\mathrm{M}_n^+} \mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n} &= \sum_{j \in J} p_j \mathcal{C}_j^{\otimes 3} \mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n} \\ &= \sum_{j \in J} p_j \mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n} \\ &= \mathcal{E}^{(3)}_{\mathrm{M}_n^+ \cap \mathrm{Cl}_n}, \end{aligned} \tag{34}$$

and equating Eqs. (33) and (34) yields the desired result. □

Remark that the analog of Proposition 2 holds true for the subgroup of unitary transformations belonging to the orthogonal group $\mathrm{O}(2^n) \subset \mathrm{U}(2^n)$[90]. The authors of ref. 91 recently conjectured that a similar result could extend to the symplectic group. Investigating whether our findings could aid in proving this conjecture would be interesting.

The preceding results can be summarized as follow. First, we proved in Lemma 1 that up to the third order random Pauli rotations can be written as convex sums of Clifford gates, provided their random rotation angle is symmetrically distributed according to the Clifford angles. This allowed us to prove the existence of a Clifford 3-cubature for a large class of random circuits in Theorem 1. Second, we provided a decomposition of the elements of the uniform FGU ensemble $\mathrm{M}_n^+$ associated with the matrix group $\mathrm{SO}(2n)$ into products of independent Givens rotations through Eq. (28) and Proposition 1. Under the considered fermion-to-qubit mapping, this yielded a decomposition of the corresponding matchgates circuits in terms of independent random Pauli rotations. Leveraging this decomposition and the previous theorem, we obtained the existence of a Clifford 3-cubature for $\mathrm{M}_n^+$. Finally, we used the invariance of the Haar measure on this group to derive the equality of the 3-fold channels of $\mathrm{M}_n^+$ and of its Clifford subgroup $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$, thereby proving the equivalence of the shadows protocols associated with the matrix groups $\mathrm{SO}(2n)$ and $\mathrm{Sym}^+(2, 2n)$.

## Invariances and equivalence of the Matchgate Shadows Protocols

The results of the previous section proves that the classical shadows protocols corresponding to the ensembles $\mathrm{M}_n^+$ and $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$ are equivalent. In this section we extend the results of refs. 35 and ref. 48 and show that, as for the measurement channels, the variances of the shadow estimators associated with the ensembles of generalized Clifford FGU corresponding to signed permutations are independent of the permutations signs and only depend on the associated perfect-matchings. From this, we identify the relevant properties of ensembles of matchgate circuits for the classical shadows protocol and we establish the equivalence between the different ensembles of Table 1. Importantly, this result allows us to transfer the performances guarantees associated with a given ensemble to the others. For instance, the results obtained in ref. 46 for $\mathrm{M}_n$ and $\mathrm{M}_n \cap \mathrm{Cl}_n$, which rely on the invariance of the shadows protocols under an arbitrary rotation of the basis of Majorana operators, can be generalized to the other ensembles.

One of the key ingredient used by Wan et al.[46] to derive their results is the invariance of the generalised FGU group $\mathrm{M}_n$ under arbitrary reflections. This invariance enables them to explicitly calculate the 3-fold channel $\mathcal{E}^{(3)}_{\mathrm{M}_n}$ and to establish the equality $\mathcal{E}^{(3)}_{\mathrm{M}_n} = \mathcal{E}^{(3)}_{\mathrm{M}_n \cap \mathrm{Cl}_n}$. Before we state and prove our results, let us introduce a few facts regarding reflections. These transformations are intimately related with the signs of the matrices in $\mathrm{Sym}(2, 2n)$ associated with Clifford generalized FGU. In fact, the channels implementing reflections with respect to Majorana operators are of the form $\mathcal{U}_D$ with $D \in \mathbb{Z}_2^{2n}$. Consider the channel $\mathcal{U}_Q$ with $Q \in \mathrm{Sym}(2, 2n)$. Recall that $Q$ admits a unique decomposition $Q = DP$ with $D \in \mathbb{Z}_2^{2n}$ and $P \in \mathrm{Sym}(2n)$, such that $\mathcal{U}_Q = \mathcal{U}_P \mathcal{U}_D$. For elements of $\mathrm{Sym}(2, 2n)$, define the equivalence relation $Q \sim Q'$ if and only if the entries of $Q$ and $Q'$ only differ by a sign, i.e. $Q = DQ'$ for some $D \in \mathbb{Z}_2^{2n}$. This equivalence relation can be lifted to the corresponding quantum channel and we write $\mathcal{U}_Q \sim \mathcal{U}_{Q'}$ if and only if $Q \sim Q'$. In the following, we will prove that for a unitary ensemble $\mathbb{U} \subset \mathrm{M}_n \cap \mathrm{Cl}_n$, the corresponding classical shadows protocol only depends on the equivalence classes of the elements of $\mathbb{U}$ for the equivalence relation ~ .

We define the $k$-fold channels associated with the ensemble of reflections (equipped with the corresponding Haar measure) as

$$\Lambda^{(k)} := \frac{1}{2^{2n}} \sum_{D \in \mathbb{Z}_2^{2n}} \mathcal{U}_D^{\otimes k}. \tag{35}$$

By the right invariance of the Haar measure, we have $\mathcal{U}_D^{\otimes k} \Lambda^{(k)} = \Lambda^{(k)}$ for all $D \in \mathbb{Z}_2^{2n}$. In particular, the following lemma holds true.

**Lemma 2**. Let $\mathcal{U}_Q, \mathcal{U}_{Q'}$ be a Clifford generalized FGUs such that $\mathcal{U}_Q \sim \mathcal{U}_{Q'}$. Then we have $\forall k \in \mathbb{N}^*$:

$$\mathcal{U}_Q^{\otimes k} \Lambda^{(k)} = \mathcal{U}_{Q'}^{\otimes k} \Lambda^{(k)}. \tag{36}$$

We can now prove the following proposition.

**Proposition 3**. Let $\mathbb{U} \subseteq \mathrm{M}_n \cap \mathrm{Cl}_n$ be a unitary ensemble of Clifford generalized FGU. For any $\mathcal{U}_Q \in \mathbb{U}$ with $Q \in \mathrm{Sym}(2, 2n)$, replacing $\mathcal{U}_Q$ by some $\mathcal{U}_{Q'} \sim \mathcal{U}_Q$ has no effect on the measurement channel and on the variance of the estimators of the resulting classical shadows protocol.

**Proof**. The invariance of measurement channel under such exchange was proven in ref. 35. We can thus focus on the variance of the shadow estimators. Let us write $\{\mathcal{U}_{Q_j},\, j\in J\}$ the elements of $\mathbb{U}$ and $(p_j)_{j\in J}$ the associated probability distribution. Denote $\mathcal{E}^{(3)}_{\mathbb{U}} = \sum_{j\in J} p_j \mathcal{U}^{\otimes 3}_{Q_j}$ the corresponding 3-fold channel. As recalled in sec. "Classical shadows protocol", for an observable $O\in\mathcal{L}(\mathcal{H}_n)$, the variance of the corresponding estimator $\hat{o}$ is essentially determined by the second raw moment $\mathbb{E}\left[\hat{o}^2\right]$ which expression is given in Eq. (8). Using the linearity of the trace, we can rewrite this expression

$$\mathbb{E}\left[\hat{o}^2\right] = \mathrm{Tr}\left[\Upsilon^{(3)}_{\mathbb{U}}(\rho\otimes\mathcal{M}^{-1}(O_i)\otimes\mathcal{M}^{-1}(O_i))\right] \tag{37}$$

where we defined

$$\Upsilon^{(3)}_{\mathbb{U}} := \mathcal{E}^{(3)}_{\mathbb{U}}\left(\sum_{z\in\{0,1\}^n} |z\rangle\langle z|^{\otimes 3}\right). \tag{38}$$

Remark that $\forall\ P\in \mathrm{P}_n$ the map $A\mapsto P^\dagger AP$ is bijective and maps bitstring states of the form $|z\rangle\langle z|$ to bitstring states, such that

$$P^{\dagger\otimes 3}\left(\sum_{z\in\{0,1\}^n} |z\rangle\langle z|^{\otimes 3}\right)P^{\otimes 3} = \sum_{z\in\{0,1\}^n} |z\rangle\langle z|^{\otimes 3}. \tag{39}$$

As reflections with respect to Majorana operators corresponds to Pauli strings under the JW mapping, we have

$$\Lambda^{(3)}\left(\sum_{z\in\{0,1\}^n} |z\rangle\langle z|^{\otimes 3}\right) = \sum_{z\in\{0,1\}^n} |z\rangle\langle z|^{\otimes 3} \tag{40}$$

and one can rewrite Eq. (38) as

$$\Upsilon^{(3)}_{\mathbb{U}} = \mathcal{E}^{(3)}_{\mathbb{U}}\Lambda^{(3)}\left(\sum_{z\in\{0,1\}^n} |z\rangle\langle z|^{\otimes 3}\right). \tag{41}$$

Hence we can replace $\mathcal{E}^{(3)}_{\mathbb{U}}$ by $\mathcal{E}^{(3)}_{\mathbb{U}}\Lambda^{(3)}$ in the expression of the variance. Finally, one can rewrite

$$\mathcal{E}^{(3)}_{\mathbb{U}}\Lambda^{(3)} = \sum_{j\in J} p_j \mathcal{U}^{\otimes 3}_{Q_i}\Lambda^{(3)} \tag{42}$$

and invoking Lemma 2 achieves the proof. □

Note that adapting this proof to the measurement channel is straightforward, so that we incidentally proved the result of ref. 35.

In the cases where elements of the considered ensemble $\mathbb{U}$ are obtained as products of more elementary Clifford generalized FGUs, we can likewise replace the elementary channels by any other equivalent channel. This is a direct consequence of Proposition 3 and of the following Lemma:

**Lemma 3**. Let $\mathcal{U}_Q$ be a Clifford generalized FGU, then

$$\mathcal{U}^{\otimes k}_Q\Lambda^{(k)} = \Lambda^{(k)}\mathcal{U}^{\otimes k}_Q, \quad \forall k\in\mathbb{N}^* \tag{43}$$

**Proof**. This lemma is easily proven. To lighten notations we take $k = 1$, the proof remaining valid for any $k$. Decomposing $Q$ as $Q = DP$ with $P\in \mathrm{Sym}(2n)$ and $D\in\mathbb{Z}_2^{2n}$, we have $\forall D'\in\mathbb{Z}_2^{2n}$:

$$\begin{aligned}\mathcal{U}_Q\mathcal{U}_{D'} &= \mathcal{U}_{D'Q} = \mathcal{U}_{D'DP}\\ &= \mathcal{U}_{DD'P}\\ &= \mathcal{U}_{DPP^{-1}D'P}\\ &= \mathcal{U}_{P^{-1}D'P}\mathcal{U}_Q\end{aligned} \tag{44}$$

Hence

$$\begin{aligned}\mathcal{U}_Q\Lambda^{(1)} &= \frac{1}{2^n}\sum_{D\in\mathbb{Z}_2^{2n}}\mathcal{U}_Q\mathcal{U}_D\\ &= \left(\frac{1}{2^n}\sum_{D\in\mathbb{Z}_2^{2n}}\mathcal{U}_{P^{-1}DP}\right)\mathcal{U}_Q\\ &= \Lambda^{(1)}\mathcal{U}_Q,\end{aligned} \tag{45}$$

using the fact that for any $P\in\mathrm{Sym}(2n)$ the map $D\mapsto P^{-1}DP$ is bijective an preserves $\mathbb{Z}_2^{2n}$. □

Proposition 3 and Lemma 3 clearly prove that the first five ensembles of Table 1 lead to equivalent classical shadows protocols. More generally, this equivalence holds between any unitary sub-ensembles of the generalized FGU admitting Clifford 3-cubatures whose elements differ only by reflections. In terms of matchgate circuits, one can rephrase this equivalence and state that inserting Pauli strings into any matchgates circuit of a sub-ensemble of $\mathrm{M}_n\cap\mathrm{Cl}_n$ has no effect on the corresponding classical shadows protocol. Note that the addition of reflections plays a crucial in the proof of the results of ref. 46. From our result, it appears that these reflections naturally stems from the measurement and averaging process of the shadows protocol, so that there is no need to explicitly add them to the circuits of the considered ensemble.

Having proved the previous equivalences, it remains to show that the shadows protocol only depends on the perfect-matching corresponding to permutation matrices of the considered ensemble. O'Gorman[48] proved this result for the measurement channels using arguments similar to the ones we use in the proof of Proposition 3. As before, we generalize it to the variance of the corresponding estimators.

In what precedes we exploited the symmetry of the state $\sum_z|z\rangle\langle z|^{\otimes 3}$ under conjugation by 3-fold products of Pauli strings. This state is also clearly invariant under conjugation by any 3-fold product of single-qubit $Z$-rotations and *CNOT* gates. Since the transposition $T_i$ that exchange the pair $(\gamma_{2i-1},\gamma_{2i})$ corresponds to the $Z$-rotation on qubit $i$ (up to irrelevant signs), we get that

$$\mathcal{U}^{\otimes 3}_{T_i}\left(\sum_z |z\rangle\langle z|^{\otimes 3}\right) = \sum_z |z\rangle\langle z|^{\otimes 3}. \tag{46}$$

On the other hand, any permutation $\tilde{Q}$ preserving the pairs of the form $(2i-1, 2i)$ can be represented (again up to irrelevant signs) by products of *SWAP* gates, which are themselves products of *CNOT* gates. Hence, for any such generalized permutation, we also have

$$\mathcal{U}^{\otimes 3}_{\tilde{Q}}\left(\sum_z |z\rangle\langle z|^{\otimes 3}\right) = \sum_z |z\rangle\langle z|^{\otimes 3}. \tag{47}$$

With these invariances, the proof of Proposition 3 is straightforwardly adapted and the following proposition holds.

**Proposition 4**. Let $\mathbb{U}\subseteq\mathrm{M}_n\cap\mathrm{Cl}_n$ be a unitary ensemble of Clifford generalized FGU. For any $\mathcal{U}_Q\in\mathbb{U}$ with $Q\in\mathrm{Sym}(2,2n)$, replacing $\mathcal{U}_Q$ by some $\mathcal{U}_{Q'}$ with $Q'$ satisfying

$$\mathrm{PerfMatch}(Q) = \mathrm{PerfMatch}(Q') \tag{48}$$

has no effect on the measurement channel and on the variance of the estimators of the resulting classical shadows protocol.

This last result achieves the proof that the shadows protocols corresponding to the ensembles of Table 1 are all equivalent.

### Samplings of ensembles of matchgate circuits

Now we build on the results of secs. "Clifford 3-cubatures and Matchgate Ensembles " and "Invariances and equivalence of the Matchgate Shadows Protocols " to improve over the existing methods and derive a sampling scheme for a small sub-ensemble of $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$ that is optimal in terms of number of gates and that inherits the performance guarantees of the protocols considered previously. Before we present our optimal sampling scheme, we also introduce simple sampling schemes for sub-ensembles of generalized FGUs resulting in equivalent shadows protocols and based on the results of Section " Clifford 3-cubatures and Matchgate Ensembles." Note that a sampling scheme for a sub-ensemble of $\mathrm{M}_n^+$ can easily be extended to a sub-ensemble of $\mathrm{M}_n$ by randomly adding a single reflection (for instance with a Pauli $X$ gate on the last qubit) to the generated circuits with probability 1/2. Consequently, we focus on ensembles in $\mathrm{M}_n^+$ in this section.

**Algorithm 1**. Sampling of matchgates circuits for the classical shadows protocol
**Input:** Number of qubits $n$
**Output:** Random matchgates circuit

```
1. Sample a permutation $P \in \mathrm{Sym}(2n)$
2. Extract the corresponding perfect-matching PerfMatch($P$) = $\{\{P_{2i-1}, P_{2i}\}, i \in [n]\}$
3. $\forall\, i \in [n]$, sort the pair $\{P_{2i-1}, P_{2i}\}$ in increasing order
4. Sort the $n$ pairs by their first element in increasing order
5. Concatenate the sorted pairs to obtain a new permutation $P'$
6. Decompose the permutation $P'$ in a sequence of transpositions using the bubblesort algorithm
7. Compile the quantum circuit by turning each transposition into a Givens rotation with angles $\pi/2$
```

The decomposition of Proposition 1 directly provides a method to sample circuits uniformly in $\mathrm{M}_n^+$, relying on single-and-two qubits random rotations. Although simple, this sampling scheme is not necessarily efficient. An efficient sampling schemes for $\mathrm{M}_n^+$ can be found in ref. 49.

Proposition 1 and Lemma 1 yields a simple sampling scheme for $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$. In fact, assuming that the distribution of random angles $\theta$ satisfy the constraints of Lemma 1, Eq. (27) can be rewritten for random Givens rotations $\mathcal{G}_k(\theta)$ as:

$$\begin{aligned}\mathbb{E}\left[\mathcal{G}_k^{\otimes 3}(\theta)\right] = {} & \frac{(1-p)}{2}\left(\mathcal{G}_k^{\otimes 3}(0)+\mathcal{G}_k^{\otimes 3}(\pi)\right) \\ & + \frac{p}{2}\left(\mathcal{G}_k^{\otimes 3}\left(\frac{\pi}{2}\right)+\mathcal{G}_k^{\otimes 3}\left(-\frac{\pi}{2}\right)\right).\end{aligned} \tag{49}$$

For $\theta_k^l$ distributed according to the probability density of Eq. (29) we have (by identifying a ratio of Wallis integrals)

$$\mathbb{E}\left[\sin^2(\theta_k^l)\right] = \frac{k-1}{k}. \tag{50}$$

As a result, to generate a circuit uniformly over $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$, it suffices to consider the matchgate circuits corresponding to the decomposition of Eq. (28) and to independently sample each angle $\theta_k^l$ from the set of Clifford angles according to the distribution

$$p_0 = p_\pi = \frac{1}{2k}, \quad p_{\frac{\pi}{2}} = p_{-\frac{\pi}{2}} = \frac{k-1}{2k}. \tag{51}$$

In the context of the classical shadows protocol, one can use the invariance under composition by reflections to further refine this distribution. Remarking that the Givens rotation $\mathcal{G}_k(\pi)$ is equal to the composition of the reflections with respect to $\gamma_{k-1}$ and $\gamma_k$, we have $\mathcal{G}_k(0) \sim \mathcal{G}_k(\pi)$ and $\mathcal{G}_k(\pi/2) \sim \mathcal{G}_k(-\pi/2)$. Hence, for the shadows protocol one can simply use the decomposition of Eq. (28) and sample each angle $\theta_k^l$ independently from $\{0, \pi/2\}$ according to the distribution

$$p_0 = \frac{1}{k}, \quad p_{\frac{\pi}{2}} = \frac{k-1}{k}. \tag{52}$$

From the results of ec. "Invariances and equivalence of the Matchgate Shadows Protocols", each rotation gate with an angle $\theta = \pm\,\pi/2$ corresponds, up to a reflection, to the application of a transposition. Therefore, the previous sampling scheme can be seen as a way to sequentially build a random permutation from independent random transpositions. Note that the structure of the circuit obtained by this sampling is not optimal in depth, due to inverted triangular shape that prevents an efficient parallelization. We provide a simple method to turn each circuit with the corresponding structure into an equivalent (up to reflections) more compact "brick-wall" structure in the Methods section "Brick-wall and triangular circuits structure." Unfortunately, this conversion does not allow to preserves the locality of the sampling, in the sense that the resulting random brick-wall circuit cannot be expressed as a product of local random gates.

We investigate numerically and compare the performances of the shadows protocol associated with previous sampling methods to estimate the 1-RDM of a simple system of 8 qubits. Specifically, we consider random matchgates circuits with the triangular structure of Fig. 2 and random angles sampled according either to the distribution of Eq. (29) or to the distributions of Eqs. (52) and (51). Figure 3 shows the corresponding results. We use the absolute error for each of the observable estimators as measures of performance, and we plot the related relevant statistics averaged over the set of considered observables. As expected, the different sampling schemes yield shadow estimators with equivalent performances.

The sampling methods considered so far yield circuits with a large number of gates. In view of obtaining an ensemble of matchgate circuits for the classical shadows protocol that are optimal in number of gates, we focus on sub-ensembles of $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$ in the following. For the samplings corresponding to Eqs. (52) and (51), one could try to reduce the number of gates by scanning the layers of the circuit and pruning the redundant gates. We leave the exploration of this path for future works.

Here, we propose another method leveraging the results of sec. "Invariances and equivalence of the Matchgate Shadows Protocols". Since the signs of the generalized permutations corresponding to the ensemble of Clifford matchgate circuits are irrelevant, one can first a draw a uniformly random permutation $P$. Then, we build the corresponding circuit by decomposing the permutation into a sequence of transposition and by using the equivalence between transpositions and Givens rotations with angle $\pm\,\pi/2$. Due to this equivalence, to obtain a minimal number of gates in the circuit amount to decompose $P$ into a minimal number of transpositions. The optimal decomposition can be computed using a bubblesort[92], which will produce a circuit with a triangular structure and minimal number of gates. Using the method of the Methods section "Brick-wall and triangular circuits structure," we can finally to turn this circuit into an equivalent circuit with a brick-wall structure and the same number of gates. As the minimal number of transpositions required to decompose $P$ is equal to the number of its inversion[92], so is the number of gates in the associated circuit. As the expected number of inversion in a random permutation of the set $[2n]$ is equal to $n(2n-1)/2$, a circuit obtained with this method will present the same expected number of gates. Eventually, as the shadows protocol is only

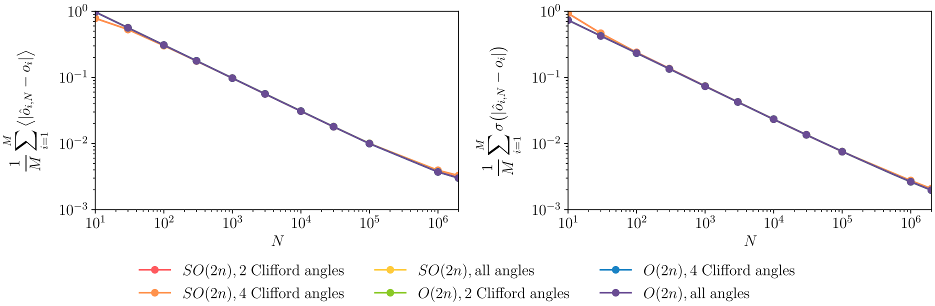

**Fig. 3 | Statistics of the error of the shadow estimators as a function of the number of shadows for the different samplings of the rotation angles.** The input state is an 8-qubit state obtained from CCSD calculation on a fictitious $H^4$ molecule. The set of observables considered are the Majorana operators of order 2, namely $\{\gamma_p\gamma_q,\ p<q,\ p,q\in[2n]\}$. The left panel shows the mean value of the shadow estimators absolute error for a given number $N$ of shadow shots, averaged over all of the observables. The right panel shows the standard deviation of the same quantity. We simulate a total of 2e6 shadows samples, and the results are obtained using a bootstrap sampling with a bootstrap sample size of 1e3.

sensitive to the perfect matching associated with the previous permutation, one can replace $P$ by any other permutation $P'$ satisfying $\mathrm{PerfMatch}(P) = \mathrm{PerfMatch}(P')$. To obtain a circuit with an optimal number of gates, we can chose the permutation $P'$ resulting in a minimal number of inversions. Given the perfect matching $\mathrm{PerfMatch}(P) = \{\{p_{2i-1}, p_{2i}\}, i\in[n]\}$, it suffices to consider the permutation obtained by first sorting each pair $\{p_{2i-1}, p_{2i}\}$ and then sorting the pairs by their first element. This clearly produces the permutation with the lowest number of inversion and thus the circuit with the lowest number of gates among the corresponding equivalence class. The average number of gates is then $n(n-1)/2$, with a maximal depth of $2n$ layers of commuting Givens rotations. We verify the scaling of the average gate count numerically on Fig. 4. The procedure above is summarized in Algorithm 1, and the corresponding optimality result is encapsulated in the following proposition.

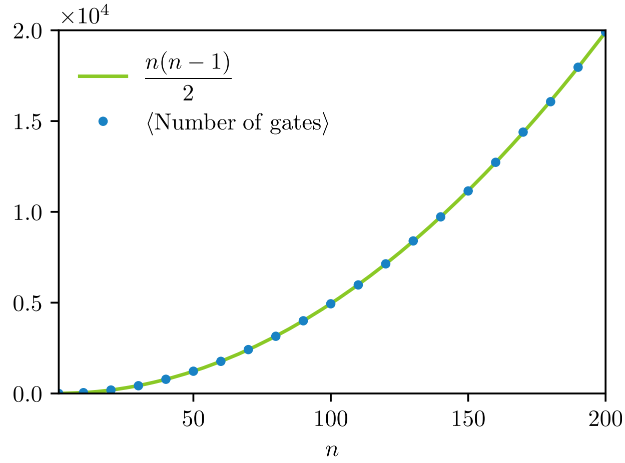

**Fig. 4 | Average number of gates in circuits produced with Algorithm 1.** For each $n$, we use $100\lfloor\sqrt{n}\rfloor$ samples.

**Proposition 5**. Algorithm 1 produces circuits with the lowest number of gates among the class of circuits that are equivalent under the symmetries considered in Sec. "Invariances and equivalence of the Matchgate Shadows Protocols". Furthermore, the shadows protocol corresponding to the sub-ensemble of $\mathrm{M}_n^+ \cap \mathrm{Cl}_n$ generated by this algorithm is equivalent to the protocols associated with the ensembles of Table 1.

Although this method is optimal in the number of gates, it is unclear whether it could be used to confirm the conjecture of ref. 48, as it would require a more detailed investigation of the average depth of the circuits obtained. Also, it would be interesting to explore the combination of the previous sampling scheme with the method presented in ref. 49 and the compilation scheme for Clifford circuits of ref. 93. We leave these investigations for future work.

## Discussion

In this paper, we investigated the matchgate classical shadows protocol associated with matrix group SO($2n$), which remained unanalyzed in the previous related literature. Our approach relied on a decomposition of random matchgate circuits in products of independent Pauli rotations. By decomposing the quantum channels corresponding to these random rotations into convex sums of Clifford channels, we were able to show that the considered unitary ensemble admits the same first three moments as its intersection with the Clifford group. Thereby, we generalized a result that was previously known for the group of generalized matchgate circuits associated with O($2n$). Extending existing results related to Clifford matchgate circuits, we further proved the equivalence between the shadows protocols corresponding to the various ensembles of matchgates studied in the literature. Building on our results, we also proposed new sampling schemes for different sub-ensembles of Clifford FGU, including a sampling scheme based on perfect-matching that is optimal in terms of number of gates.

We believe that our unifying results will prove very useful in future applications, as they allow to transfer the results obtained for specific FGU ensembles to many others. In particular, our results show that one can use our gate-count optimal sampling scheme with the same performances guarantees as for the shadows protocol relying on the full ensemble of generalized FGUs, which is a clear improvement over the existing protocols. Along the way, we proved the existence of Clifford 3-cubatures for a large class of circuits of independent random Pauli rotations. We expect this result to find relevant applications in the contexts of randomized benchmarking and of variational quantum algorithms.

Many open questions and interesting research avenues remain. In this work, we derived a sampling method for the matchgate shadows protocol that is optimal in the number of gates. It would be interesting to analyze the scaling of the proposed scheme in terms of circuit depth. In particular, whether one could rely on the symmetry invariances of sec. "Invariances and equivalence of the Matchgate Shadows Protocols" to sample circuits with a proven minimal depth is unclear at this point. To further optimize the sampling scheme for matchgate shadows, a potentially fruitful research path would be to investigate the use of approximate matchgate design. This approach has recently proven successful in ref. 94, where the authors show that such an approximate ensemble can be used for Clifford shadows to obtain circuits with a logarithmic depth in the number of qubits. To obtain this approximate ensemble, one could for instance rely on classical random walks obtained from Markov chains applying random transpositions at each step. It is known that the mixing time of such Markov chain scales as $n^p\log(n)$[95], with $p = 2$ for random transpositions of nearest neighbors and $p = 1$ for transpositions between any pairs of the $n$ indices. Thus, depending on the connectivity of the considered device, it might possible to derive a sampling scheme yielding circuits with a sub-linear depth. However, it is unclear how to reliably build an estimator based on such an approximate ensemble, for the corresponding unitary ensemble would yields $t$-fold channels that would only approximate the ones of the matchgate ensemble. In the same spirit, and in view of the dependence of the shadows protocol on perfect-matchings, it would be worth exploring possible links with random phylo-genetic trees which can be seen as random perfect-matchings[96].

## Methods

### Proof of Lemma 1

In this section we prove Lemma 1 of the main text. Recall that we denote

$$R_\theta := e^{-i\frac{\theta}{2}Z} = e^{-i\frac{\theta}{2}}\Pi_0 + e^{i\frac{\theta}{2}}\Pi_1, \tag{53}$$

with $\Pi_0 := |0\rangle\langle 0|$ and $\Pi_1 := |1\rangle\langle 1|$, and that

$$R_0 = I,\ R_{\frac{\pi}{2}} = S,\ R_\pi = Z,\ R_{\frac{3\pi}{2}} = S^\dagger. \tag{54}$$

The corresponding channels are respectively written $\mathcal{R}_\theta, \mathcal{I}, \mathcal{S}, \mathcal{Z}$ and $\mathcal{S}^\dagger$.

**Proof**. For $1 \le k \le 3$, define the projector onto the subspace of constant Hamming weight $k$

$$\Lambda_k := \sum_{\substack{k_1, k_2, k_3 \in \{0,1\} \\ k_1 + k_2 + k_3 = k}} \Pi_{k_1} \otimes \Pi_{k_2} \otimes \Pi_{k_3}. \tag{55}$$

We have

$$\begin{aligned} R_\theta^{\otimes 3} &= e^{-i\frac{3\theta}{2}}\Lambda_0 + e^{-i\frac{\theta}{2}}\Lambda_1 + e^{i\frac{\theta}{2}}\Lambda_2 + e^{i\frac{3\theta}{2}}\Lambda_3 \\ &= e^{-i\frac{3\theta}{2}} \sum_{k=0}^{3} e^{ik\theta}\Lambda_k \end{aligned} \tag{56}$$

such that

$$\mathcal{R}_\theta^{\otimes 3}(\rho) = \sum_{k,l=0}^{3} e^{i\theta(k-l)}\Lambda_k \rho \Lambda_l. \tag{57}$$

For $\theta$ symmetrically distributed around 0, we have $\mathbb{E}_\theta\left[e^{in\theta}\right] = \mathbb{E}_\theta\left[e^{-in\theta}\right] = \mathbb{E}_\theta[\cos(n\theta)]$ for all $n \in \mathbb{N}$, and it comes

$$\mathbb{E}\left[\mathcal{R}_\theta^{\otimes 3}\right](\rho) = \sum_{k,l=0}^{3} \mathbb{E}[\cos(\theta(k-l))]\Lambda_k \rho \Lambda_l. \tag{58}$$

Using the parity of cos and setting $n = l - k$, we can reorder the sum to obtain

$$\mathbb{E}\left[\mathcal{R}_\theta^{\otimes 3}\right](\rho) = \sum_{k=0}^{3}\sum_{n=0}^{3-k} \mathbb{E}[\cos(\theta n)]\mathcal{U}_{kn}(\rho), \tag{59}$$

where we defined

$$\mathcal{U}_{kn}(\rho) := \Lambda_k \hat{\rho} \Lambda_{k+n} + \Lambda_{k+n}\rho\Lambda_k - \delta_{n0}\Lambda_k\hat{\rho}\Lambda_k. \tag{60}$$

Let $\delta(\theta)$ denote the Dirac distribution. Applying Eq. (59) for $\theta$ following the even distributions $\delta(\theta - \pi)$, $\delta(\theta)$ and $\frac{1}{2}\left(\delta(\theta - \frac{\pi}{2}) + \delta(\theta + \frac{\pi}{2})\right)$ gives

$$\begin{aligned} \mathcal{Z}^{\otimes 3} &= \sum_{k=0}^{3}\sum_{n=0}^{3-k} (-1)^n \mathcal{U}_{kn}, \\ \mathcal{I}^{\otimes 3} &= \sum_{k=0}^{3}\sum_{n=0}^{3-k} \mathcal{U}_{kn}, \\ \frac{1}{2}\left(\mathcal{S}^{\otimes 3} + \mathcal{S}^{\dagger\otimes 3}\right) &= \sum_{k=0}^{3}\sum_{n=0}^{3-k} (\delta_{n0} - \delta_{n2})\mathcal{U}_{kn}. \end{aligned} \tag{61}$$

Recombining the previous equations, we get

$$\begin{aligned} \frac{1}{4}\left(\mathcal{I}^{\otimes 3} + \mathcal{Z}^{\otimes 3} + \mathcal{S}^{\otimes 3} + \mathcal{S}^{\dagger\otimes 3}\right) &= \sum_{k=0}^{3}\sum_{n=0}^{3-k} \delta_{n0}\mathcal{U}_{kn} \\ \frac{1}{4}\left(\mathcal{I}^{\otimes 3} + \mathcal{Z}^{\otimes 3} - \mathcal{S}^{\otimes 3} - \mathcal{S}^{\dagger\otimes 3}\right) &= \sum_{k=0}^{3}\sum_{n=0}^{3-k} \delta_{n2}\mathcal{U}_{kn} \end{aligned} \tag{62}$$

Assuming further that $\theta$ is symmetrically distributed around $\frac{\pi}{2}$, and thus that $\theta$ is symmetric around every Clifford angle, we have that $\mathbb{E}[\cos(n\theta)] = 0$ for $n = 1$ and $n = 3$, but not necessarily for $n = 2$. In that case, injecting Eq. (62) in Eq. (59) yields

$$\begin{aligned} \mathbb{E}\left[\mathcal{R}_\theta^{\otimes 3}\right] = &\frac{1}{4}\left(\mathcal{I}^{\otimes 3} + \mathcal{Z}^{\otimes 3} + \mathcal{S}^{\otimes 3} + \mathcal{S}^{\dagger\otimes 3}\right) \\ &+ \tfrac{\mathbb{E}[\cos(2\theta)]}{4}\left(\mathcal{I}^{\otimes 3} + \mathcal{Z}^{\otimes 3} - \mathcal{S}^{\otimes 3} - \mathcal{S}^{\dagger\otimes 3}\right), \end{aligned} \tag{63}$$

which gives the result outlined in Eq. (27). □

### Absence of Clifford 4-cubature for single random Pauli rotations

Here we show that Lemma 1 cannot be generalized to the 4-fold channel by proving the following result.

**Lemma 4**. Let $\nu$ be a probability distribution on $(-\pi, \pi]$ symmetric about the Clifford angles and $\theta \sim \nu$. If $\nu$ is not only supported by the set of Clifford angles, then the ensemble $\{\mathcal{R}_\theta, \theta \sim \nu\}$ admits no Clifford 4-cubature.

**Proof**. As before, we write

$$R_\theta := \exp\left(-i\frac{\theta}{2}Z\right) \tag{64}$$

and $\mathcal{R}_\theta$ the corresponding quantum channel. Let us denote $\mathbb{U} = \{\mathcal{R}_\theta, \theta \sim \nu\}$ the unitary ensemble associated with the random rotation angle $\theta$ distributed according to $\nu$. The distribution $\nu$ is not supported by the set of Clifford angles if it cannot be written as

$$\nu = \sum_{k=0}^{3} p_k \delta_{k\pi/2} \tag{65}$$

with $p_k \ge 0$ and $\sum_{k=0}^{3} p_k = 1$. Suppose that $\mathbb{U}$ admits a Clifford 4-cubature $\{(\mathcal{C}_j, p_j),\ j \in J\}$ such that

$$\mathbb{E}\left[\mathcal{R}_\theta^{\otimes 4}\right] = \sum_{j\in J} p_j \mathcal{C}_j^{\otimes 4}. \tag{66}$$

For every $j \in J$, there is a unique Pauli operator $P_j \in \{I, X, Y, Z\}$ satisfying $\mathcal{C}_j(X) = \lambda_j P_j$ with $|\lambda_j| = 1$. We denote

$$\Gamma := \sum_{P\in\{I,X,Y,Z\}^{\otimes 4}} \frac{1}{2^4}\left|\mathrm{Tr}\left\{P\mathbb{E}\left[\mathcal{R}_\theta(X)^{\otimes 4}\right]\right\}\right|, \tag{67}$$

and from the above we have

$$\begin{aligned} \Gamma &= \sum_{P\in\{I,X,Y,Z\}^{\otimes 4}} \left|\sum_{j\in J} \tfrac{p_j}{2^4}\mathrm{Tr}\left\{P\mathcal{C}_j(X)^{\otimes 4}\right\}\right| \\ &\le \sum_{P\in\{I,X,Y,Z\}^{\otimes 4}} \sum_{j\in J} \tfrac{p_j}{2^4}\left|\mathrm{Tr}\left\{PP_j^{\otimes 4}\right\}\right| \\ &\le \sum_{j\in J} p_j = 1. \end{aligned} \tag{68}$$

On the other hand, for all $\theta \in [-\pi, \pi)$ we have

$$\mathcal{R}_\theta(X) = \cos(\theta)X + \sin(\theta)Y \tag{69}$$

such that

$$\mathbb{E}\left[\mathcal{R}_\theta(X)^{\otimes 4}\right] = \mathbb{E}\left[(\cos(\theta)X + \sin(\theta)Y)^{\otimes 4}\right]. \tag{70}$$

Developing this equation, we obtain

$$\begin{aligned}\mathbb{E}\left[\mathcal{R}_\theta(X)^{\otimes 4}\right] = {} & \mathbb{E}\left[\cos(\theta)^4\right]XXXX + \mathbb{E}\left[\sin(\theta)^4\right]YYYY \\ & + \mathbb{E}\left[\cos(\theta)\sin(\theta)^3\right](XYYY + YXYY + YYXY + YYYX) \\ & + \mathbb{E}\left[\cos(\theta)^3\sin(\theta)\right](YXXX + XYXX + XXYX + XXXY) \\ & + \mathbb{E}\left[\cos(\theta)^2\sin(\theta)^2\right](XXYY + YYXX + XYXY \\ & + YXYX + XYYX + YXXY),\end{aligned} \tag{71}$$

where we dropped the tensor products for clarity. Assuming that $\theta$ is symmetrically distributed about the Clifford angles, we have

$$\mathbb{E}\left[\cos(\theta)\sin(\theta)^3\right] = \mathbb{E}\left[\cos(\theta)^3\sin(\theta)\right] = 0, \tag{72}$$

which gives

$$\begin{aligned}\Gamma &= \mathbb{E}\left[\cos(\theta)^4\right] + \mathbb{E}\left[\sin(\theta)^4\right] + 6\mathbb{E}\left[\cos(\theta)^2\sin(\theta)^2\right] \\ &= \mathbb{E}\left[\cos(\theta)^4 + \sin(\theta)^4 + 6\cos(\theta)^2\sin(\theta)^2\right] \\ &= \mathbb{E}\left[\left(\cos(\theta)^2 + \sin(\theta)^2\right)^2 + 4\cos(\theta)^2\sin(\theta)^2\right] \\ &= \mathbb{E}\left[1 + 4\cos(\theta)^2\sin(\theta)^2\right] \\ &= 1 + 4\mathbb{E}\left[\cos(\theta)^2\sin(\theta)^2\right].\end{aligned} \tag{73}$$

Writing $f(\theta) = \cos(\theta)^2\sin(\theta)^2$, we have $f(\theta) \geq 0$ such that $\{f \geq 0\} = (-\pi, \pi]$. Moreover, $f(\theta) = 0$ if and only if $\sin(\theta)^2 = 0$ or $\cos(\theta)^2 = 0$, that is if and only if $\theta \in \{\frac{k\pi}{2}, k \in \{-1, 0, 1, 2\}\}$. As a result, we have

$$\begin{aligned}\{f = 0\} &= \left\{\tfrac{k\pi}{2}, k \in \{-1, 0, 1, 2\}\right\} \\ \{f > 0\} &= (-\pi, \pi] \setminus \{f = 0\}.\end{aligned} \tag{74}$$

Furthermore, $\int_{(-\pi,\pi]} f(\theta)\nu(d\theta) = 0$ if and only if $f$ vanishes $\nu$-almost everywhere (see[97], Theorem 1.39-(a)) and thus if and only if the support of $\nu$ is included in the set of Clifford angles. Hence, if $\nu$ is not supported only on the set of Clifford angles, we have $\mathbb{E}\left[\cos(\theta)^2\sin(\theta)^2\right] > 0$ such that $\Gamma > 1$. This contradicts Eq. (68), hence $\mathbb{U}$ do not admit any Clifford 4-cubature. □

The previous result rules out the existence of Clifford 4-cubature for a single layer of Pauli rotations of the form

$$\hat{U}(\boldsymbol{\theta}) = \bigotimes_{j \in J} e^{i\theta_j P_j/2}, \tag{75}$$

provided that the $P_j$ acts on different sets of qubits and that any of the marginal distribution of one of the angles is not supported on the set of Clifford angles. In fact, by conjugating with adequate Clifford gates, this transformation can be transformed to

$$\hat{V}(\boldsymbol{\theta}) = \bigotimes_{k=1}^{|J|} e^{i\theta_j Z_j/2} \tag{76}$$

with $Z_j$ acting only on the $j$-th qubit. Supposing that the marginal distribution of $\theta_k$ is not solely supported by the set of Clifford angles, we can repeat the previous proof by replacing $\mathcal{R}_\theta(X)$ by the action of $\hat{V}(\boldsymbol{\theta})$ on $X_k$, namely

$$\hat{V}(\boldsymbol{\theta})^\dagger X_k \hat{V}(\boldsymbol{\theta}) = \mathcal{R}_{\theta_k}(X_k). \tag{77}$$

However, this reasoning does not extends easily to the case of multiple such layers applied successively. In particular, even if Lemma 4 shows that the matchgate group does not admit any 4-Clifford cubature for $n = 1$, this does not necessary imply that this is the case when $n \geq 2$, which remains an open question for future work.

The $t$-fold channels of unitary ensembles admitting a Clifford $t$-cubature are stabilizer-preserving channels, for which efficient classical simulation schemes exists (see for instance ref. 98). Remark that determining the degree of non-stabilizerness of a quantum state or operation (often referred to as the "magic" in the literature) is a delicate task[99,100]. Interestingly, the previous lemma suggests that correlations between random single-qubit Pauli rotations can be a source of magic for the corresponding 1-fold average channel.

### Distribution of the angles of Givens rotations

This section provide details and justify our adaptation of the Proposition 1.6. of ref. 86. Up to a change of notations, the original version of the proposition proves the result for following distribution for the independent rotations angles

$$\theta_2^l \sim \frac{d\theta_2^l}{2\pi} \quad \text{on} \quad [0, 2\pi) \tag{78}$$

and $\forall k \in (2, 2n]$,

$$\theta_k^l \sim \frac{\Gamma\left(\frac{k-1}{2}\right)}{2\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{k-2}{2}\right)}\sin(\theta)^{k-2} \quad \text{on} \quad [0, \pi). \tag{79}$$

The proof of ref. 86 relies on a colmun-by-column construction of the random rotation matrix $Q$. Before we review this construction, we recall some facts related to random vectors on spheres. Let $\mathbb{S}^{n-1} \subset \mathbb{R}^n$ be the $(n-1)$-sphere, a vector $\mathbf{v} \in \mathbb{S}^{n-1}$ is characterized by its associated Euler angles $\theta_1, \ldots, \theta_{n-1}$ as follow

$$\mathbf{v} = \begin{pmatrix} \sin(\theta_{n-1})\ldots\sin(\theta_2)\sin(\theta_1) \\ \sin(\theta_{n-1})\ldots\sin(\theta_2)\cos(\theta_1) \\ \vdots \\ \sin(\theta_{n-1})\cos(\theta_{n-2}) \\ \cos(\theta_{n-1}) \end{pmatrix}, \tag{80}$$

with $0 \leq \theta_1 < 2\pi$ and $0 \leq \theta_k \leq \pi$ for $2 \leq k \geq n - 1$. For $\mathbf{v}$ to be uniformly distributed over $\mathbb{S}^{n-1}$, it suffices that its Euler angles are distributed according to the measure

$$d\mu_{\mathbb{S}^{n-1}} := \frac{\Gamma\left(\frac{n}{2}\right)}{(2\pi)^{n/2}}\left(\prod_{k=2}^{n}\sin^{k-1}(\theta_k)\mathbf{1}_{[0,\pi)}(\theta_k)d\theta_k\right)d\theta_1, \tag{81}$$

where $\mathbf{1}_A$ is the indicator function of the set $A$.

Remark that in the previous definition of the Euler angles, the domains of the $\theta_k$ for $2 \leq k \leq n - 1$ can be freely chosen to be either $[0, \pi]$ or $[-\pi, 0]$ without loss of generality. We use this freedom to extend the domain of the random Euler angles associated with uniformly distributed random vectors.

Let $\mathbf{v}(\theta_1, \ldots, \theta_{n-1})$ be defined by Eq. (80) with $\theta_1, \ldots\theta_{n-1}$ distributed according to the measure of Eq. (81). Since $\mathbf{v}$ is uniformly distributed, so is $Q'\mathbf{v}$ for any matrix $Q' \in O(n)$. Take $Q'$ to be the reflection with respect to the $i$-th axis and let $X$ be a Bernouilli random variable with

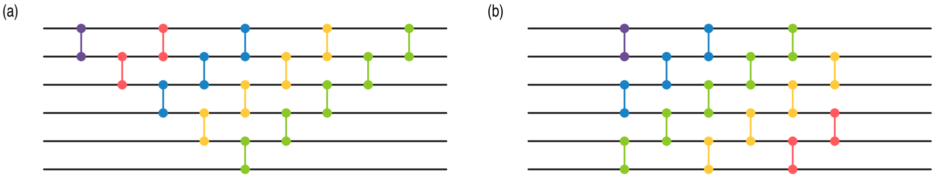

**Fig. 5 | Structures of the sequences of transposition considered in this work.** (**a**) triangular structure and (**b**) brick-wall structure. Each line corresponds to a single Majorana operator and connections between adjacent lines correspond to the application of either the identity or to the transposition of the two lines.

$\mathbb{P}(X=1)=\mathbb{P}(X=0)=1/2$, we have that

$$\mathbf{u}:=(1-X)\mathbf{v}+XQ'\mathbf{v} \tag{82}$$

is also uniformly distributed on $\mathbb{S}^{n-1}$, with

$$Q'\mathbf{v}=\mathbf{v}(\theta_1,\ldots,-\theta_i.\ldots\theta_{n-1}). \tag{83}$$

As a result, replacing

$$\sin^{i-1}(\theta_i)\boldsymbol{1}_{[0,\pi)}(\theta_i) \tag{84}$$

by

$$\frac{1}{2}|\sin(\theta_i)|^{i-1}=\frac{1}{2}\left(\sin^{i-1}(\theta_i)\mathbf{1}_{[0,\pi)]}(\theta_i)+\sin^{i-1}(-\theta_i)\mathbf{1}_{(-\pi,0]}(\theta_i)\right) \tag{85}$$

in the probability distribution of Eq. (81) above still yields a uniformly distributed vector. As this holds for any index $i$, we get that any vector defined by Eq. (80) such that $\theta_1,\ldots\theta_{n-1}$ follow the distribution

$$\mathrm{d}\tilde{\mu}_{\mathbb{S}^{n-1}}:=\frac{\Gamma\left(\frac{n}{2}\right)}{2^{n-1}(2\pi)^{n/2}}\left(\prod_{k=2}^{n}|\sin(\theta_k)|^{k-1}\mathrm{d}\theta_k\right)\mathrm{d}\theta_1 \tag{86}$$

is uniformly distributed on $\mathbb{S}^{n-1}$.

The constrution of a random element $Q\in \mathrm{SO}(2n)$ presented in ref. 86 then proceeds as follow. We write $\mathbf{q}_i$ the $i$-th column of the matrix $Q$. The first step of the construction is to draw the last column of $Q$, i.e. $\mathbf{q}_{2n}=Q\mathbf{e}_{2n}$, uniformly from the sphere $\mathbb{S}^{2n-1}$. To do so, one can take $\mathbf{q}_{2n}=Q_1\mathbf{e}_{2n}$ with $Q_1:=g_2^1g_3^1\ldots g_{2n}^1$. This vector has the form given in Eq. (80) and the vector Euler angles are the ones of the rotations $g_k^1$. From the above, choosing these angles randomly according the distribution of Eq. (86) yields a vector uniformly distributed on $\mathbb{S}^{2n-1}$. Then, the second-to-last column $\mathbf{q}_{2n-1}=Q\mathbf{e}_{2n-1}$ is uniformly sampled in the $(2n-2)$-sphere of the orthogonal complement of $Q\mathbf{e}_{2n}$, namely $\mathbb{S}^{2n-2}\cap\{Q\mathbf{e}_{2n}\}^{\perp}$. As before, it suffices to take the vector $Q_1Q_2\mathbf{e}_{2n-1}$ with $Q_2=g_2^2g_3^2\ldots g_{2n-1}^2$ and to sample the angles of $Q_2$ from the distribution of Eq. (86). Multiplying on the left by $Q_1$ allows to sample the resulting vector from the orthogonal complement of $\mathbf{q}_{2n}$, as we have

$$\begin{aligned}\langle\mathbf{q}_{2n},\mathbf{q}_{2n-1}\rangle&=\langle\mathbf{e}_{2n}Q_1^TQ_1Q_2\mathbf{e}_{2n-1}\rangle\\&=\langle\mathbf{e}_{2n}Q_2\mathbf{e}_{2n-1}\rangle\\&=0.\end{aligned} \tag{87}$$

Proceeding like that up to the first column yields a Haar-distributed random matrix $Q$ of the form given in the main text, that is

$$Q=(g_2^1g_3^1\ldots g_{2n}^1)\ldots(g_2^{2n-2}g_3^{2n-2})(g_2^{2n-1}). \tag{88}$$

Importantly, for each $1\le k\le 2n-1$ the angles of the Givens rotations $g_l^k(\theta_l^k)$ correspond to the random Euler angles of the column vector $Q\mathbf{e}_{2n+1-k}$. In particular, in the proof of ref. 86, the distribution of the angles is inherited from the probability distribution of Eq. (81) used to generated the various random vectors. Consequently, the proof remains valid if we replace the distribution of Eq. (81) by the one of Eq. (86) and our adapted version of the proposition follows.

## Brick-wall and triangular circuits structures

Here we give a simple method to transform circuits with a triangular structure described in the sampling scheme of sec. "Samplings of ensembles of matchgate circuits" into a circuit with a "brick-wall" structure that is equivalent for the classical shadows protocol.

We consider matchgate circuits that can be decomposed according to Eq. (28) with angles belonging to $\{0,\pi/2\}$. The corresponding quantum circuit is given for $n=1$ qubit in Fig. 2 for the JW mapping. Recall that under this mapping, each Pauli rotation corresponds to a Givens rotation acting on a pair of adjacent indices. From the invariance results of sec. "Invariances and equivalence of the Matchgate Shadows Protocols", each Givens rotation of angle $\pi/2$ acting on the pair of indices $(i,i+1)$ corresponds to a transposition of these indices. Thus, one can represent the equivalence class of circuits yielding the same permutation by a sequence of transposition. For the considered circuits, the obtained sequence is represented by a triangular "circuit" of transpositions as represented on the left panel of Fig. 5.

The triangular shape is inherited from the decomposition of Eq. (28). There exists other such decomposition in the literature. In particular, Clements et al.[101] provide an analog decomposition leading to a circuit of Givens rotations arranged in a rectangular structure, which we refer to as a "brick-wall" structure. Under the previous equivalence, this decomposition leads to circuits of transposition with the shape given on the right panel of Fig. 5.

In order to turn circuit in $\mathrm{M}_n\cap\mathrm{Cl}_n$ obtained from the sampling scheme of the sec. "Samplings of ensembles of matchgate circuits" into an equivalent circuit with a brick-wall structure, it suffices to transform its corresponding triangular circuit of transposition into a brick-wall one and chose a quantum circuit in the associated equivalence class.

To transform a triangular circuit of transpositions into a brick-wall one, we propose a simple strategy that consists in permuting the successive diagonals of transpositions as represented on Fig. 5. Denote $\tau_i$ the transposition of the indices $(i,i+1)$. It is well known that such transpositions satisfy the following braid relation

$$\tau_i\tau_{i+1}\tau_i=\tau_{i+1}\tau_i\tau_{i+1}. \tag{89}$$

Let $b\in\{0,1\}$, and write $\tau_i^b$ the permutation equal to $\tau_i$ if $b=1$ and that is the identity otherwise. A simple inspection shows that for all $b_1,b_2,b_3\in\{0,1\}$ there exists $b_1',b_2',b_3'\in\{0,1\}$ such that

$$\begin{gathered}\tau_i^{b_1}\tau_{i+1}^{b_2}\tau_i^{b_3}=\tau_{i+1}^{b_1'}\tau_i^{b_2'}\tau_{i+1}^{b_3'},\\b_1+b_2+b_3\ge b_1'+b_2'+b_3'.\end{gathered} \tag{90}$$

Figure 6 shows how the previous relation can be used to permute two diagonals. This is straightforwardly extended to diagonals of any size.

## Fermion-to-qubit mappings

We briefly review some facts about fermion-to-qubit mappings and recall the well-known Jordan-Wigner mapping. There exists a large variety of fermion-to-qubit mappings in the literature (see refs. 34,38,102–106, to cite but a few). Typically, such a mapping takes the form of a unitary transformation between the state-spaces of the considered fermionic and qubit systems. This transformation yields a homomorphism on the algebra of

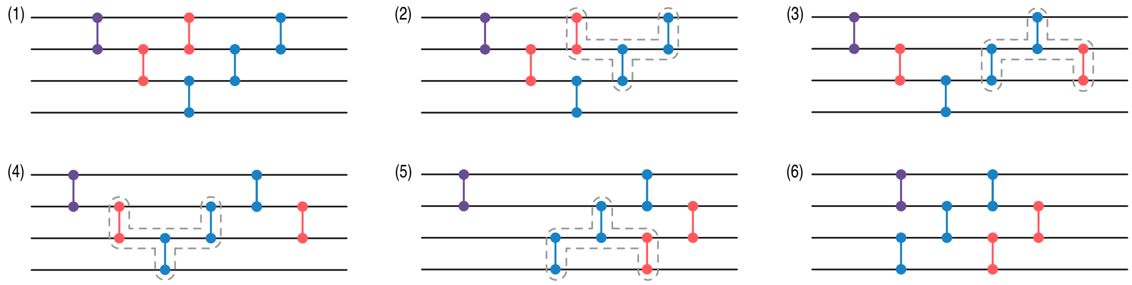

**Fig. 6 | Example of elementary transformations allowing to turn a triangular structure into a brick-wall one.** Subfigures (2) and (6)respectively show the intial and target structure. Subfigures (1) and (3)(resp. (4) and (5)) show the first (resp. second) steps of the the transformation. The outlined sets of connections represents equivalent groups of transpositions that are mapped to each other through Eq. (90). Generalizing and repeating this sequence of operations allows to exchange the order of the diagonals of different length in the structures of Fig. 5, which in turns allows to map triangular structures to brick-wall ones.

observables that preserves the algebraic properties of the operators. As the Majorana operators have the same algebraic properties as the Pauli operators, it is natural to require that the considered mapping sends Majorana operators to Pauli strings.

The Jordan-Wigner mapping identifies the fermionic Fock states $|z_1 \dots z_n\rangle$ of the fermionic modes $a_1, \dots, a_n$ with the states $\otimes_{i=1}^{n} |z_i\rangle$ of canonical basis of the $\mathcal{H}_n$, yielding the following correspondence between the Pauli and the mode operators:

$$\begin{aligned} X_k &= \left(\prod_{l<k} e^{i\pi a_k^\dagger a_k}\right)\left(a_k^\dagger + a_k\right), \\ Y_k &= \left(\prod_{l<k} e^{i\pi a_k^\dagger a_k}\right) i\left(a_k^\dagger - a_k\right), \\ Z_k &= 1 - 2a_k^\dagger a_k = \quad e^{i\pi a_k^\dagger a_k}. \end{aligned} \tag{91}$$

The mapping with the Majorana operators follows

$$\gamma_{2k-1} = \prod_{l<k} Z_l X_k, \quad \gamma_{2k} = \prod_{l<k} Z_l Y_k, \tag{92}$$

and states in the canonical basis can be written

$$|z\rangle\langle z| = \frac{1}{2^n}\prod_{k=1}^{n}\left(I - i(-1)^{z_k}\gamma_{2k-1}\gamma_{2k}\right). \tag{93}$$

## Data availability

The data used in this work are available from the corresponding author upon reasonable request.

## Code availability

The code used to produce the numerical results is available from the corresponding author upon reasonable request.

Received: 26 September 2024; Accepted: 19 March 2025;
Published online: 16 April 2025

## References

1. Deglmann, P., Schäfer, A. & Lennartz, C. Application of quantum calculations in the chemical industry—An overview. *Int. J. Quantum Chem.* **115**, 107 (2015).
2. Williams-Noonan, B. J., Yuriev, E. & Chalmers, D. K. Free Energy Methods in Drug Design: Prospects of “Alchemical Perturbation” in Medicinal Chemistry. *J. Med. Chem.* **61**, 638 (2018).
3. Heifetz, A. ed., https://doi.org/10.1007/978-1-0716-0282-9*Quantum Mechanics in Drug Discovery*, Methods in Molecular Biology, **2114** (Springer US, New York, NY, 2020).
4. Continentino, M. A. *Key Methods and Concepts in Condensed Matter Physics: Green’s Functions and Real Space Renormalization Group* (IOP Publishing, 2021).
5. Van der Ven, A., Deng, Z., Banerjee, S. & Ong, S. P. Rechargeable Alkali-Ion Battery Materials: Theory and Computation. *Chem. Rev.* **120**, 6977 (2020).
6. Blunt, N. S. et al. Perspective on the Current State-of-the-Art of Quantum Computing for Drug Discovery Applications. *J. Chem. Theory Comput.* **18**, 7001 (2022).
7. Lordi, V. & Nichol, J. M. Advances and opportunities in materials science for scalable quantum computing. *MRS Bull.* **46**, 589 (2021).
8. Cao, Y., Romero, J. & Aspuru-Guzik, A. Potential of quantum computing for drug discovery. *IBM J. Res. Dev.* **62**, 6:1 (2018).
9. Feynman, R. P. Simulating physics with computers. *Int. J. Theor. Phys.* **21**, 467 (1982).
10. Manin, Yu. I.*Vychislimoe i Nevychislimoe* (Sov. radio, 1980).
11. Ortiz, G., Gubernatis, J. E., Knill, E. & Laflamme, R. Quantum algorithms for fermionic simulations. *Phys. Rev. A* **64**, 022319 (2001).
12. Somma, R., Ortiz, G., Gubernatis, J. E., Knill, E. & Laflamme, R. Simulating physical phenomena by quantum networks. *Phys. Rev. A* **65**, 042323 (2002).
13. Somma, R., Ortiz, G., Knill, E. & Gubernatis, J. Quantum Simulations of Physics Problems. *Int. J. Quantum Inf.* **01**, 189 (2003).
14. Verstraete, F., Cirac, J. I. & Latorre, J. I. Quantum circuits for strongly correlated quantum systems. *Phys. Rev. A* **79**, 032316 (2009).
15. Wecker, D. et al. Solving strongly correlated electron models on a quantum computer. *Phys. Rev. A* **92**, 062318 (2015).
16. Jiang, Z., Sung, K. J., Kechedzhi, K., Smelyanskiy, V. N. & Boixo, S. Quantum Algorithms to Simulate Many-Body Physics of Correlated Fermions. *Phys. Rev. Appl.* **9**, 044036 (2018).
17. Smith, A., Kim, M. S., Pollmann, F. & Knolle, J. Simulating quantum many-body dynamics on a current digital quantum computer. *npj Quantum Inf.* **5**, 1 (2019).
18. Tacchino, F., Chiesa, A., Carretta, S. & Gerace, D. Quantum Computers as Universal Quantum Simulators: State-of-the-Art and Perspectives. *Adv. Quantum Technol.* **3**, 1900052 (2020).
19. Bharti, K. et al. Noisy intermediate-scale quantum algorithms. *Rev. Mod. Phys.* **94**, 015004 (2022).
20. Fauseweh, B. Quantum many-body simulations on digital quantum computers: State-of-the-art and future challenges. *Nat. Commun.* **15**, 2123 (2024).
21. Cerezo, M. et al. Variational quantum algorithms. *Nat. Rev. Phys.* **3**, 625 (2021).
22. Peruzzo, A. et al. A variational eigenvalue solver on a photonic quantum processor. *Nat. Commun.* **5**, 4213 (2014).
23. McClean, J. R., Romero, J., Babbush, R. & Aspuru-Guzik, A. The theory of variational hybrid quantum-classical algorithms. *N. J. Phys.* **18**, 023023 (2016).

24. Tilly, J. et al. The Variational Quantum Eigensolver: A review of methods and best practices, https://doi.org/10.1016/j.physrep.2022.08.003 *Physics Reports* The Variational Quantum Eigensolver: A Review of Methods and Best Practices, **986**, 1 (2022).
25. Coleman, A. J. & Absar, I. Reduced hamiltonian orbitals. III. Unitarily invariant decomposition of hermitian operators. *Int. J. Quantum Chem.* **18**, 1279 (1980).
26. Rubin, N. C., Babbush, R. & McClean, J. Application of fermionic marginal constraints to hybrid quantum algorithms. *N. J. Phys.* **20**, 053020 (2018).
27. Tilly, J. et al. Reduced density matrix sampling: Self-consistent embedding and multiscale electronic structure on current generation quantum computers. *Phys. Rev. Res.* **3**, 033230 (2021).
28. O'Brien, T. E. et al. Calculating energy derivatives for quantum chemistry on a quantum computer. *npj Quantum Inf.* **5**, 1 (2019).
29. Overy, C. et al. Unbiased reduced density matrices and electronic properties from full configuration interaction quantum Monte Carlo. *J. Chem. Phys.* **141**, 244117 (2014).
30. Gidofalvi, G. & Mazziotti, D. A. Molecular properties from variational reduced-density-matrix theory with three-particle N-representability conditions. *J. Chem. Phys.* **126**, 024105 (2007).
31. Tsuneyuki, S. Transcorrelated Method: Another Possible Way towards Electronic Structure Calculation of Solids. *Prog. Theor. Phys. Suppl.* **176**, 134 (2008).
32. Peterson, M. R. & Nayak, C. More realistic Hamiltonians for the fractional quantum Hall regime in GaAs and graphene. *Phys. Rev. B* **87**, 245129 (2013).
33. Bonet-Monroig, X., Babbush, R. & O'Brien, T. E. Nearly Optimal Measurement Scheduling for Partial Tomography of Quantum States. *Phys. Rev. X* **10**, 031064 (2020).
34. Jiang, Z., Kalev, A., Mruczkiewicz, W. & Neven, H. Optimal fermion-to-qubit mapping via ternary trees with applications to reduced quantum states learning. *Quantum* **4**, 276 (2020).
35. Zhao, A., Rubin, N. C. & Miyake, A. Fermionic partial tomography via classical shadows. *Phys. Rev. Lett.* **127**, 110504 (2021).
36. Huang, H.-Y., Kueng, R. & Preskill, J. Predicting Many Properties of a Quantum System from Very Few Measurements. *Nat. Phys.* **16**, 1050 (2020).
37. Elben, A. et al. The randomized measurement toolbox. *Nat. Rev. Phys.* **5**, 9 (2023).
38. Jordan, P. & Wigner, E. Über das Paulische Äquivalenzverbot. *Z. f.ür. Phys.* **47**, 631 (1928).
39. Terhal, B. M. & DiVincenzo, D. P. Classical simulation of noninteracting-fermion quantum circuits. *Phys. Rev. A* **65**, 032325 (2002).
40. Valiant, L. G. Quantum computers that can be simulated classically in polynomial time, in *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, STOC '01 https://doi.org/10.1145/380752.380785 (Association for Computing Machinery, New York, NY, USA, 2001) pp. 114–123.
41. Jozsa, R. & Miyake, A. Matchgates and classical simulation of quantum circuits. *Proc. R. Soc. A: Math., Phys. Eng. Sci.* **464**, 3089 (2008).
42. Knill, E. Fermionic Linear Optics and Matchgates https://doi.org/10.48550/arXiv.quant-ph/0108033 (2001).
43. DiVincenzo, D. P. & Terhal, B. M. Fermionic Linear Optics Revisited. *Found. Phys.* **35**, 1967 (2005).
44. Bravyi, S. Lagrangian representation for fermionic linear optics. *Quantum Inf. Comput.* **5**, 216 (2005).
45. Cai, J.-Y., Choudhary, V. & Lu, P. On the Theory of Matchgate Computations. *Theory Comput. Syst.* **45**, 108 (2009).
46. Wan, K., Huggins, W. J., Lee, J. & Babbush, R. Matchgate Shadows for Fermionic Quantum Simulation. *Commun. Math. Phys.* **404**, 629 (2023).
47. Huggins, W. J. et al. Unbiasing fermionic quantum Monte Carlo with a quantum computer. *Nature* **603**, 416 (2022).
48. O'Gorman, B. Fermionic tomography and learning https://doi.org/10.48550/arXiv.2207.14787 (2022).
49. Zhao, A. & Miyake, A. Group-theoretic error mitigation enabled by classical shadows and symmetries https://doi.org/10.48550/arXiv.2310.03071 (2023).
50. Watrous, J. *The Theory of Quantum Information* (Cambridge University Press, 2018).
51. Lerasle, M. Lecture Notes: Selected topics on robust statistical learning theory https://doi.org/10.48550/arXiv.1908.10761 (2019)
52. Hoeffding, W. Probability Inequalities for sums of Bounded Random Variables, in *The Collected Works of Wassily Hoeffding*, edited by N. I. Fisher and P. K. Sen https://doi.org/10.1007/978-1-4612-0865-5_26 (Springer, New York, NY, 1994) pp. 409–426.
53. Koh, D. E. & Grewal, S. Classical Shadows With Noise. *Quantum* **6**, 776 (2022).
54. Roberts, D. A. & Yoshida, B. Chaos and complexity by design. *J. High. Energy Phys.* **2017**, 121 (2017).
55. Mele, A. A. Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial. *Quantum* **8**, 1340 (2024).
56. Webb, Z. The Clifford group forms a unitary 3-design. *Quantum Inf. Comput.* **16**, 1379 (2016).
57. Zhu, H., Kueng, R., Grassl, M. & Gross, D., The Clifford group fails gracefully to be a unitary 4-design https://doi.org/10.48550/arXiv.1609.08172 (2016).
58. Mitsuhashi, Y. & Yoshioka, N., Clifford Group and Unitary Designs under Symmetry https://doi.org/10.48550/arXiv.2306.17559 (2023).
59. Iosue, J. T., Sharma, K., Gullans, M. J. & Albert, V. V. Continuous-Variable Quantum State Designs: Theory and Applications. *Phys. Rev. X* **14**, 011013 (2024).
60. Gross, D., Audenaert, K. & Eisert, J. Evenly distributed unitaries: On the structure of unitary designs. *J. Math. Phys.* **48**, 052104 (2007).
61. Harrow, A. W. & Low, R. A. Random Quantum Circuits are Approximate 2-designs. *Commun. Math. Phys.* **291**, 257 (2009).
62. Roy, A. & Scott, A. J. Unitary designs and codes. *Des., Codes Cryptogr.* **53**, 13 (2009).
63. Nakaji, K. & Yamamoto, N. Expressibility of the alternating layered ansatz for quantum computation. *Quantum* **5**, 434 (2021).
64. Haferkamp, J. Random quantum circuits are approximate unitary *t*-designs in depth $O\left(nt^{5+o(1)}\right)$.Quantum 6, 795 (2022).
65. Holmes, Z., Sharma, K., Cerezo, M. & Coles, P. J. Connecting Ansatz Expressibility to Gradient Magnitudes and Barren Plateaus. *PRX Quantum* **3**, 010313 (2022).
66. Tao, T. *Topics in Random Matrix Theory* (American Mathematical Soc., 2012)
67. Givens, W. Computation of Plain Unitary Rotations Transforming a General Matrix to Triangular Form. *J. Soc. Ind. Appl. Math.* **6**, 26 (1958).
68. Kivlichan, I. D. et al. Quantum Simulation of Electronic Structure with Linear Depth and Connectivity. *Phys. Rev. Lett.* **120**, 110501 (2018).
69. Hurwitz, A. Über die Erzeugung der Invarianten durch Integration. *Nachrichten von. der Ges. der Wissenschaften zu Göttingen, Mathematisch-Physikalische Kl.* **1897**, 71 (1897).
70. Zhu, H. Multiqubit Clifford groups are unitary 3-designs. *Phys. Rev. A* **96**, 062336 (2017).
71. Wu, B. & Koh, D. E. Error-mitigated fermionic classical shadows on noisy quantum devices. *npj Quantum Inf.* **10**, 1 (2024).
72. Scheurer, M., Anselmetti, G.-L. R., Oumarou, O., Gogolin, C. & Rubin, N. C. Tailored and Externally Corrected Coupled Cluster with Quantum Inputs https://doi.org/10.48550/arXiv.2312.08110 (2024).
73. Kiser, M. et al. Classical and quantum cost of measurement strategies for quantum-enhanced auxiliary field quantum Monte Carlo. *N. J. Phys.* **26**, 033022 (2024).

74. Huang, B. et al. Evaluating a quantum-classical quantum Monte Carlo algorithm with Matchgate shadows https://doi.org/10.48550/arXiv.2404.18303 (2024).

75. Chen, S., Yu, W., Zeng, P. & Flammia, S. T. Robust Shadow Estimation. *PRX Quantum* **2**, 030348 (2021).

76. Low, G. H. Classical shadows of fermions with particle number symmetry https://doi.org/10.48550/arXiv.2208.08964 (2022).

77. Naldesi, P. et al. Fermionic correlation functions from randomized measurements in programmable atomic quantum devices. *Phys. Rev. Lett.* **131**, 060601 (2023).

78. Denzler, J., Mele, A. A., Derbyshire, E., Guaita, T. & Eisert, J. Learning fermionic correlations by evolving with random translationally invariant hamiltonians. *Phys. Rev. Lett.* **133**, 240604 (2024).

79. Helsen, J., Nezami, S., Reagor, M. & Walter, M. Matchgate benchmarking: Scalable benchmarking of a continuous family of many-qubit gates. *Quantum* **6**, 657 (2022).

80. Sobolev, S. L. Theory of Cubature Formulas, in *Selected Works of S.L. Sobolev: Volume I: Mathematical Physics, Computational Mathematics, and Cubature Formulas*, edited by G. V. Demidenko and V. L. Vaskevich https://doi.org/10.1007/978-0-387-34149-1_26 (Springer US, Boston, MA, 2006) pp. 491–511.

81. Cools, R. Constructing cubature formulae: The science behind the art. *Acta Numerica* **6**, 1 (1997).

82. de la Harpe, P. & Pache, C. Cubature Formulas, Geometrical Designs, Reproducing Kernels, and Markov Operators, in *Infinite Groups: Geometric, Combinatorial and Dynamical Aspects*, edited by L. Bartholdi, T. Ceccherini-Silberstein, T. Smirnova-Nagnibeda and A. Zuk https://doi.org/10.1007/3-7643-7447-0_6 (Birkhäuser, Basel, 2005) pp. 219–267.

83. Goethals, J. M. & Seidel, J. J. Cubature Formulae, Polytopes, and Spherical Designs, in *The Geometric Vein*, edited by C. Davis, B. Grünbaum and F. A. Sherk https://doi.org/10.1007/978-1-4612-5648-9_13 (Springer, New York, NY, 1981) pp. 203–218.

84. Prestin, J. & Roşca, D. On some cubature formulas on the sphere. *J. Approx. Theory* **142**, 1 (2006).

85. Heyraud, V., Li, Z., Donatella, K., Le Boité, A. & Ciuti, C. Efficient Estimation of Trainability for Variational Quantum Circuits. *PRX Quantum* **4**, 040335 (2023).

86. Meckes, E. S., *The Random Matrix Theory of the Classical Compact Groups* (Cambridge University Press, 2019).

87. Diaconis, P. and Forrester, P. J., A. Hurwitz and the origins of random matrix theory in mathematics https://doi.org/10.48550/arXiv.1512.09229 (2016).

88. Heiss, W. D. Distributions of angles of a random unit vector and random orthogonal matrices. *Z. f.ür. Phys. A Hadrons Nucl.* **349**, 9 (1994).

89. Diaconis, P. & Saloff-Coste, L. Bounds for Kac's Master Equation. *Commun. Math. Phys.* **209**, 729 (2000).

90. Hashagen, A. K., Flammia, S. T., Gross, D. & Wallman, J. J. Real Randomized Benchmarking. *Quantum* **2**, 85 (2018).

91. West, M., Mele, A. A., Larocca, M. & Cerezo, M. Random ensembles of symplectic and unitary states are indistinguishable https://arxiv.org/abs/2409.16500 (2024).

92. Knuth, D. E. *The Art of Computer Programming: Sorting and Searching, Volume 3* (Addison-Wesley Professional, 1998).

93. Bravyi, S. & Maslov, D. Hadamard-free circuits expose the structure of the clifford group. *IEEE Trans. Inf. Theory* **67**, 4546 (2021).

94. Schuster, T., Haferkamp, J. & Huang, H.-Y. Random unitaries in extremely low depth, https://arxiv.org/abs/2407.07754 (2024).

95. Levin, D. A. & Peres, Y. *Markov Chains and Mixing Times*, **107** (American Mathematical Soc., 2017).

96. Holmes, S. & Diaconis, P. Random walks on trees and matchings, *Electro. J. Probab.* **7** (2002).

97. Rudin, W. et al. *Principles of mathematical analysis*, **3** (McGraw-hill New York, 1964).

98. Howard, M. & Campbell, E. Application of a Resource Theory for Magic States to Fault-Tolerant Quantum Computing. *Phys. Rev. Lett.* **118**, 090501 (2017).

99. Seddon, J. R. & Campbell, E. T. Quantifying magic for multi-qubit operations. *Proc. R. Soc. A* **475**, 20190251 (2019).

100. Haug, T. & Kim, M. Scalable Measures of Magic Resource for Quantum Computers. *PRX Quantum* **4**, 010301 (2023).

101. Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walmsley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460 (2016).

102. Bravyi, S. B. & Kitaev, A. Y. Fermionic Quantum Computation. *Ann. Phys.* **298**, 210 (2002).

103. Verstraete, F. & Cirac, J. I. Mapping local Hamiltonians of fermions to local Hamiltonians of spins. *J. Stat. Mech.: Theory Exp.* **2005**, P09012 (2005).

104. Steudtner, M. & Wehner, S. Fermion-to-qubit mappings with varying resource requirements for quantum simulation. *N. J. Phys.* **20**, 063010 (2018).

105. Miller, A., Zimborás, Z., Knecht, S., Maniscalco, S. & García-Pérez, G. Bonsai Algorithm: Grow Your Own Fermion-to-Qubit Mappings. *PRX Quantum* **4**, 030314 (2023).

106. Chiew, M. & Strelchuk, S. Discovering optimal fermion-qubit mappings through algorithmic enumeration. *Quantum* **7**, 1145 (2023).

## Acknowledgements

The authors acknowledge that this work was supported by Innovate UK - UKRI through grant 1468/10074167. We thank Thomas D. Barrett for his helpful suggestions during the writing of this paper.

## Author contributions

The analytic calculations were led by V.H. and discussed with H.C. and J.T. H.C. and V.H. carried the numerical experiments. The manuscript was written by V.H. and improved by H.C. and J.T. All authors read and approved the final manuscript.

## Competing interests

The authors declare no competing interests.

## Additional information

**Correspondence** and requests for materials should be addressed to Valentin Heyraud.

**Reprints and permissions information** is available at http://www.nature.com/reprints

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2025