Multiqubit Clifford groups are unitary 3-designs

Huangjun Zhu*

Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada N2L 2Y5
and Institute for Theoretical Physics, University of Cologne, Cologne 50937, Germany

(Received 13 December 2016; published 29 December 2017)

Unitary t-designs are a ubiquitous tool in many research areas, including randomized benchmarking, quantum process tomography, and scrambling. Despite the intensive efforts of many researchers, little is known about unitary t-designs with $t \geqslant 3$ in the literature. We show that the multiqubit Clifford group in any even prime-power dimension is not only a unitary 2-design, but also a 3-design. Moreover, it is a minimal 3-design except for dimension 4. As an immediate consequence, any orbit of pure states of the multiqubit Clifford group forms a complex projective 3-design; in particular, the set of stabilizer states forms a 3-design. In addition, our study is helpful in studying higher moments of the Clifford group, which are useful in many research areas ranging from quantum information science to signal processing. Furthermore, we reveal a surprising connection between unitary 3-designs and the physics of discrete phase spaces and thereby offer a simple explanation of why no discrete Wigner function is covariant with respect to the multiqubit Clifford group, which is of intrinsic interest in studying quantum computation.

DOI: 10.1103/PhysRevA.96.062336

I. INTRODUCTION

Unitary designs are a ubiquitous tool in quantum information science [1–7]. They are particularly useful in derandomizing constructions that rely on random unitaries, such as randomized benchmarking [8–10], quantum process tomography [11,12], quantum cryptography [2,13], and data hiding [1]. In addition, they can generate complex projective designs [14–16], which are equally useful in derandomizing constructions that rely on random quantum states. Recently, projective and unitary designs also have found increasing applications beyond quantum information science, especially in the study of chaos and scrambling [17–20].

Most previous studies on this subject have focused on unitary 2-designs, among which the Clifford group is the most prominent [2–5,7–10,21,22] due to its extensive applications in various research areas, such as quantum computation, quantum error correction, and randomized benchmarking. Complex projective 2-designs constructed from Clifford orbits, including the set of stabilizer states in particular, are also of special interest [21–23]. By contrast, little is known about t-designs with $t \geqslant 3$ except for randomized constructions [16,24–27], despite intensive efforts of many researchers in the past decade. This situation has set a big barrier in realizing many tasks that rely on higher t-designs, such as quantum state discrimination [16,28], quantum tomography [12,29,30], phase retrieval [31,32], and reduction of query complexity [33].

Here we show that the multiqubit (including single-qubit) Clifford group is not only a unitary 2-design, but also a 3-design. Moreover, it is minimal except for dimension 4 in the sense that it does not contain any proper subgroup that is also a unitary 3-design. As a consequence, any orbit of pure states of the multiqubit Clifford group, including the set of stabilizer states in particular, forms a 3-design, which extends the result in Ref. [34]. Our study not only provides infinite families of well-structured 3-designs, but also paves the way for constructing t-designs with even higher strengths [35]. Recently, these results have found satisfactory applications in quantum state discrimination [36] and phase retrieval [37]. Furthermore, our work is helpful in studying multipartite entanglement in stabilizer tensor networks, which stand as an effective tool for understanding holographic duality [38].

In addition, our study leads to a simple explanation of the distinction between discrete Wigner functions in even prime-power dimensions and those in odd prime-power dimensions [22,39,40]. This distinction has been an elusive question and has profound implications for various interesting subjects, such as computational speedup and contextuality [23,41,42]. In each odd prime-power dimension, the discrete Wigner function introduced by Wootters [39] is covariant with respect to the Clifford group [22,40]; by contrast, none is covariant with respect to the multiqubit Clifford group [40]. Here we reveal a surprising connection between unitary 3-designs and the physics of discrete phase spaces and thereby clarify the reason behind this distinction.

II. PRELIMINARIES

A set of pure quantum states $\{|\psi_j\rangle\}$ in a d-dimensional Hilbert space $\mathcal{H}$ is a (complex projective) t-design for a positive integer t if $\sum_j (|\psi_j\rangle\langle\psi_j|)^{\otimes t}$ is proportional to the projector onto the symmetric subspace of $\mathcal{H}^{\otimes t}$ [14–16,43]. A set of K unitary operators $\{U_j\}$ acting on $\mathcal{H}$ is a unitary t-design [3–5] if it satisfies

$$\frac{1}{K}\sum_j U_j^{\otimes t} M \big(U_j^{\otimes t}\big)^\dagger = \int dU\, U^{\otimes t} M (U^{\otimes t})^\dagger \tag{1}$$

for any linear operator M acting on $\mathcal{H}^{\otimes t}$, where the dagger stands for the Hermitian conjugate and the integral is taken with respect to the normalized Haar measure. By definition, a unitary t-design is also a t'-design for $t' < t$. Note that the above equation remains intact when U_j are multiplied by arbitrary phase factors, so what we are concerned with

*hzhu1@uni-koeln.de; zhuhuangjun@gmail.com

are actually projective unitary t-designs. Alternatively, the set $\{U_j\}$ is a unitary t-design if the tth frame potential

$$\Phi_t(\{U_j\}) := \frac{1}{K^2}\sum_{j,k}|\operatorname{tr}(U_j U_k^\dagger)|^{2t} \tag{2}$$

attains the minimum $\gamma(t,d) := \int dU|\operatorname{tr}(U)|^{2t}$ [5,6,11]. Here we only need $\gamma(t,d)$ in two special cases [11,44]

$$\gamma(t,d) = \begin{cases} \frac{(2t)!}{t!(t+1)!}, & d=2,\\ t!, & d\geqslant t. \end{cases} \tag{3}$$

Besides the current application, frame potentials also play an important role in studying chaos and circuit complexity [17–20].

Most known examples of unitary designs are constructed from subgroups of the unitary group, which are referred to as (unitary) group designs. Given a finite group G of unitary operators on $\mathcal{H}$, in most cases we are only concerned with the quotient $\overline{G}$ of G over the phase factors. The frame potential of $\overline{G}$ takes on the form [5]

$$\Phi_t(\overline{G}) := \frac{1}{|\overline{G}|}\sum_{U\in\overline{G}}|\operatorname{tr}(U)|^{2t} = \frac{1}{|G|}\sum_{U\in G}|\operatorname{tr}(U)|^{2t}, \tag{4}$$

where $|\overline{G}|$ and $|G|$ denote the orders of $\overline{G}$ and G. Note that $\Phi_t(\overline{G})$ coincides with the sum of squared multiplicities of irreducible components of $\overline{G}_{(t)} := \{U^{\otimes t}|U\in\overline{G}\}$. The group $\overline{G}$ is a unitary t-design if and only if $\overline{G}_{(t)}$ has the same number of irreducible components as $\mathrm{U}_{(t)}$, where U denotes the group of all unitary operators acting on $\mathcal{H}$ [5]. For example, the group $\overline{G}$ is a unitary 1-design if and only if it is irreducible. It is a 2-design if $\overline{G}_{(2)}$ has two irreducible components, which correspond to the symmetric subspace and antisymmetric subspace of $\mathcal{H}^{\otimes 2}$. Prominent examples of unitary group 2-designs include Clifford groups and restricted Clifford groups in prime-power dimensions [1–5]. Not much is known about unitary t-designs with larger t.

Before presenting our main results, we need to introduce the (multipartite) Heisenberg-Weyl (HW) group. In prime dimension p, the HW group D is generated by the phase operator Z and the cyclic-shift operator X,

$$Z|u\rangle = \omega^u|u\rangle, \quad X|u\rangle = |u+1\rangle, \tag{5}$$

where $\omega = \mathrm{e}^{2\pi\mathrm{i}/p}$, $u\in\mathbb{F}_p$, and $\mathbb{F}_p$ is the field of integers modulo p (often written as $\mathbb{Z}_p$). When $p=2$, the operators Z and X reduce to the familiar Pauli operators σ_z and σ_x and the HW group reduces to the Pauli group. In this case, it is often more convenient to consider a variant of the HW group which includes the scalar i as an additional generator. However, these choices do not affect the following discussion since we are mostly concerned with the HW group modulo phase factors.

In prime-power dimension $q=p^n$, the HW group D is the tensor power of n copies of the HW group in dimension p. The elements in the HW group are called displacement operators (or Weyl operators). Up to phase factors, they can be labeled by vectors in $\mathbb{F}_p^{2n}$ as

$$D_\mu = \tau^{\sum_j \mu_j\mu_{n+j}}\prod_{j=1}^n X_j^{\mu_j}Z_j^{\mu_{n+j}}, \tag{6}$$

where $\tau = -e^{\pi\mathrm{i}/p}$, while Z_j and X_j are the phase operator and cyclic shift operator of the jth party. These operators satisfy the commutation relation

$$D_\mu D_\nu D_\mu^\dagger D_\nu^\dagger = \omega^{\langle\mu,\nu\rangle}, \tag{7}$$

where $\langle\mu,\nu\rangle = \mu^{\mathrm{T}}J\nu$ is the symplectic product with $J = \begin{pmatrix} 0_n & -1_n\\ 1_n & 0_n\end{pmatrix}$. The symplectic group $\mathrm{Sp}(2n,p)$ is the group of linear transformations on $\mathbb{F}_p^{2n}$ that preserves the symplectic product.

The (full) Clifford group $\overline{\mathrm{C}}$ is composed of all unitary transformations that map displacement operators to displacement operators up to phase factors [21,22,40,45–47]. It is referred to as the multiqubit Clifford group when the dimension is a power of 2 (including 2). In dimension 2, the Clifford group $\overline{\mathrm{C}}$ corresponds to the symmetry group of a cube inscribed in the Bloch sphere. In general, any Clifford unitary U induces a symplectic transformation F on the symplectic space $\mathbb{F}_p^{2n}$ that labels the displacement operators. Conversely, given any symplectic matrix F, there exist q^2 Clifford unitaries (up to phase factors) that induce F [45–47]. The quotient $\overline{\mathrm{C}}/\overline{D}$ can be identified with the symplectic group $\mathrm{Sp}(2n,p)$ [45,46].

The symplectic space $\mathbb{F}_p^{2n}$ can also be identified with a two-dimensional vector space over the field $\mathbb{F}_q$. The special linear group $\mathrm{SL}(2,q)$ on this space is an extension-field-type subgroup of $\mathrm{Sp}(2n,p)$. The restricted Clifford group $\overline{\mathrm{C}}_{\mathrm{r}}$ (coinciding with the full Clifford group when q is a prime) is the subgroup of $\overline{\mathrm{C}}$ whose quotient $\overline{\mathrm{C}}_{\mathrm{r}}/\overline{D}$ corresponds to $\mathrm{SL}(2,q)$; see Refs. [5,22,48,49] for more details.

III. MULTIQUBIT CLIFFORD GROUPS ARE UNITARY 3-DESIGNS

In this section we prove our main result that the multiqubit Clifford group is a unitary 3-design. Consequently, any orbit of the Clifford group, including the orbit of stabilizer states, forms a complex projective 3-design. To achieve this goal, we determine the frame potentials of the Clifford group up to order 4. Furthermore, we show that, except in dimension 4, the multiqubit Clifford group contains no proper subgroup that forms a unitary 3-design. Recently, these results have found applications in many research areas both within and beyond quantum information science.

Theorem 1. The multiqubit Clifford group is a unitary 3-design but not a 4-design. The Clifford group in any odd prime-power dimension is only a unitary 2-design. The restricted Clifford group in any prime-power dimension is only a unitary 2-design except for dimension 2.

Corollary 1. Any orbit of pure states of the multiqubit Clifford group forms a 3-design; in particular, the set of multiqubit stabilizer states forms a 3-design.

The conclusion on stabilizer states was also proved directly by Kueng and Gross [34].

Theorem 1 is a simple corollary of Eq. (3) and the following lemma, which is proved in Appendix A by virtue of Lemma 2 below.

Lemma 1. In prime-power dimension p^n, the Clifford group $\overline{\mathrm{C}}$ has frame potentials

$$\Phi_2(\overline{\mathrm{C}}) = 2, \tag{8}$$

$$\Phi_3(\overline{\mathrm{C}}) = \begin{cases} 2p+1, & n=1, \\ 2p+2, & n \geqslant 2, \end{cases} \tag{9}$$

$$\Phi_4(\overline{\mathrm{C}}) = \begin{cases} p^3+p^2+p+1, & n=1, \\ 2p^3+2p^2+2p+1, & n=2, \\ 2(p^3+p^2+p+1), & n \geqslant 3. \end{cases} \tag{10}$$

The restricted Clifford group $\overline{\mathrm{C}}_{\mathrm{r}}$ has frame potentials

$$\Phi_t(\overline{\mathrm{C}}_{\mathrm{r}}) = \frac{q(q^{2t-4}-1)}{q^2-1} + q^{t-2} + 1 \quad \forall t \geqslant 1. \tag{11}$$

It is worth pointing out that Eqs. (8)–(10) also apply to subgroups of the Clifford group whose quotients over the HW group are isomorphic to $\mathrm{Sp}(2m,p^k)$ with $mk = n$ if n and p are replaced by m and p^k, respectively. Besides proving Theorem 1, Lemma 1 shows that the Clifford group in dimension 2 is quite close to a unitary 4-design. The one in dimension 3 is quite close to a unitary 3-design; the larger the prime p is, the further away the Clifford group is from being a unitary 3-design. In addition, the frame potentials presented in Lemma 1 are crucial to analyzing the fourth tensor power of the Clifford group and to constructing 4-designs from Clifford orbits [35,50], which are useful in quantum state discrimination [36] and phase retrieval [37]. Recently, these results also found an application in studying multipartite entanglement in stabilizer tensor networks, which are instructive in understanding holographic duality [38]. Furthermore, our study is helpful in exploring chaos and circuit complexity [19,20].

The following lemma is useful not only in proving Lemma 1, but also in computing frame potentials of subgroups of the Clifford group that contain the HW group. See Appendix B for a proof.

Lemma 2. Suppose $\overline{G} \geqslant \overline{D}$ is a subgroup of the Clifford group $\overline{\mathrm{C}}$ in dimension $q = p^n$ and $R = \overline{G}/\overline{D}$ [taken as a subgroup of $\mathrm{Sp}(2n,p)$]. Then

$$\Phi_t(\overline{G}) = \frac{1}{|R|} \sum_{F \in R} f(F)^{t-1}, \tag{12}$$

where $|R|$ is the order of R and $f(F)$ is the number of fixed points of F in $\mathbb{F}_p^{2n}$. Moreover, $\Phi_t(\overline{G})$ is equal to the number of orbits of R on $(\mathbb{F}_p^{2n})^{\times(t-1)}$. The group $\overline{G}$ is a unitary 2-design if and only if R is transitive on $\mathbb{F}_p^{2n*}$. It is a unitary 3-design if and only if R is 2-transitive when $n=1$ and is a rank-3 permutation group when $n \geqslant 2$.

Remark 1. $\mathbb{F}_p^{2n*}$ is the set of nonzero vectors in $\mathbb{F}_p^{2n}$. A subgroup of $\mathrm{Sp}(2n,p)$ is transitive if it can map any nonzero vector in $\mathbb{F}_p^{2n}$ to any other and 2-transitive or doubly transitive if it can map any ordered pair of distinct nonzero vectors to any other pair. It is a rank-3 permutation group if it is transitive and each point stabilizer has three orbits on $\mathbb{F}_p^{2n*}$ including the orbit of the fixed point [51–53]. The relation between transitive subgroups of the symplectic group and unitary 2-designs was noticed previously in Ref. [5].

In many applications, unitary designs with fewer elements are desirable. Is there any proper subgroup of the multiqubit Clifford group that forms a 3-design? The answer turns out to be negative except for dimension 4. The following theorem is proved in Appendix C. It shows that, in a sense, the multiqubit Clifford group is the most economical in constructing a unitary 3-design.

Theorem 2. The multiqubit Clifford group $\overline{\mathrm{C}}$ is a minimal unitary 3-design except for dimension 4, in which case it has a unique proper subgroup that is a unitary 3-design.

Remark 2. In dimension 4, $\overline{\mathrm{C}}/\overline{D} \simeq \mathrm{Sp}(4,2) \simeq S_6$ contains a unique subgroup that is isomorphic to A_6 [54], where S_m and A_m denote the symmetric group and alternating group on m letters. The preimage of A_6 in $\overline{\mathrm{C}}$ is a unitary 3-design.

IV. APPLICATIONS TO DISCRETE WIGNER FUNCTIONS

Discrete Wigner functions are the analogs of the familiar Wigner function in the continuous scenario. They are useful in many research areas, including quantum tomography and quantum computation. In each odd prime-power dimension, the Wootters discrete Wigner function is distinguished because it is covariant with respect to the Clifford group [22,39,40]. In this quasiprobability representation, Clifford transformations can be understood as permutations on the discrete phase space. In addition, a pure state has a non-negative Wootters discrete Wigner function if and only if it is a stabilizer state according to the discrete Hudson theorem [22]. In particular, stabilizer states can be represented as probability distributions on the discrete phase space. These facts offer a simple explanation of the famous Gottesman-Knill theorem which states that stabilizer quantum computation can be efficiently simulated classically [55]. In other words, negativity in the Wootters discrete Wigner function is a necessary resource to achieve universal quantum computation [41]. Incidentally, this negativity is also tied to the prominent nonclassical phenomenon known as contextuality [23].

In the multiqubit setting, which is the most relevant to realizing practical quantum computation, however, no discrete Wigner function is covariant with respect to the Clifford group [40]. Consequently, it is more difficult to come up with a simple geometric picture that illustrates the Gottesman-Knill theorem. Also, it is more difficult to clarify the origin of computational speedup in quantum computation based on qubits. A focus of ongoing research is to understand the distinction between multiqubit systems and systems of odd local dimensions [23,40–42].

Here we show that the nonexistence of a Clifford covariant discrete Wigner function in an even prime-power dimension is closely tied to the fact that the multiqubit Clifford group is a unitary 3-design. To elucidate this point, it suffices to show that no operator basis is covariant with respect to the multiqubit Clifford group; note that any Clifford covariant discrete Wigner function determines a Clifford covariant operator basis. For example, in an odd prime-power dimension, the Wootters discrete Wigner function [39] determines the operator basis composed of phase point operators and vice versa [22,40]. Here an operator basis $\{L_j\}$ is covariant with respect to the group $\overline{G}$ of unitary transformations if $\overline{G}$ leaves this basis invariant and acts transitively on the basis operators. In particular, each $U \in \overline{G}$ induces a permutation among the basis operators.

Theorem 3. No operator basis is covariant with respect to any unitary group 3-design. No discrete Wigner function is covariant with respect to the multiqubit Clifford group.

This theorem is proved in Appendix D. It offers a simple explanation of the distinction between multiqubit systems and systems of odd local dimensions, which is of intrinsic interest in studying quantum computation. Moreover, it reveals a surprising connection between unitary t-designs and the physics of discrete phase spaces, which may have profound implications for the cross fertilization of the two active research fields.

V. SUMMARY

We showed that the multiqubit Clifford group is a unitary 3-design. It is also a minimal 3-design except for dimension 4. As a consequence, any orbit of pure states of the multiqubit Clifford group is a 3-design; in particular, the set of multiqubit stabilizer states is a 3-design. The methods and conclusions presented here are also useful in studying higher moments of the Clifford group. These results are of interest in many research areas both within and beyond quantum information science.

Moreover, we offered a simple explanation of why no discrete Wigner function is covariant with respect to the multiqubit Clifford group by proving that no operator basis is covariant with respect to any group that forms a unitary 3-design. This result reveals a surprising connection between unitary designs and the physics of discrete phase spaces, which is of interest in studying quantum computation and a number of nonclassical phenomena, such as negativity and contextuality.

Note added. Recently, we noticed a comprehensive math paper by Guralnick and Tiep [56], from which it is possible to deduce our Theorems 1 and 2 with some additional work. However, this paper mentions neither t-designs nor the Clifford group explicitly. In addition, some of their results rely on Hering's theorem, which relies on the classification of finite simple groups (CFSGs). Our proofs are completely independent of the CFSGs and are thus simpler and more transparent. In addition, Webb also recently proved that the multiqubit Clifford group is a unitary 3-design [57], which offers a perspective complementary to our approach.

ACKNOWLEDGMENTS

The author is grateful to David Gross, Richard Kueng, Debbie Leung, and Andreas Winter for discussions. This work was supported in part by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation. The author also acknowledges financial support from the Excellence Initiative of the German Federal and State Governments (Grant No. ZUK 81) and the DFG.

APPENDIX A: PROOF OF LEMMA 1

Proof. According to Lemma 2, the frame potential $\Phi_t(\overline{\mathrm{C}})$ is equal to the number of orbits of $\mathrm{Sp}(2n,p)$ on $(\mathbb{F}_p^{2n})^{\times(t-1)}$. The number is 2 when $t=2$ given that $\mathrm{Sp}(2n,p)$ is transitive [51,52]. When $t=3$, let $\mathbf{0}=(0,0,\dots,0)^{\mathrm{T}}$ and $\mathbf{1}=(1,0,\dots,0)^{\mathrm{T}}\in\mathbb{F}_p^{2n}$. Then any orbit on $(\mathbb{F}_p^{2n})^{\times 2}$ contains one of the elements $(\mathbf{0},\mathbf{0})$, $(\mathbf{0},\mathbf{1})$, $(\mathbf{1},\mathbf{0})$, $(\mathbf{1},\mathbf{1})$, and $(\mathbf{1},\mu)$, where $\mu\neq\mathbf{0},\mathbf{1}$. The vector μ is a fixed point of the stabilizer of $\mathbf{1}$ if and only if it is proportional to $\mathbf{1}$; there are $p-2$ such fixed points excluding $\mathbf{0},\mathbf{1}$. Suppose $\mu,\nu\in\mathbb{F}_p^{2n*}$ are not proportional to $\mathbf{1}$; then $(\mathbf{1},\mu)$ and $(\mathbf{1},\nu)$ are on the same orbit if and only if the symplectic products $\langle\mathbf{1},\mu\rangle$ and $\langle\mathbf{1},\nu\rangle$ are equal by Witt's lemma [58]. When $n>1$, $\langle\mathbf{1},\mu\rangle$ may take on any value in $\mathbb{F}_p$, while it is nonzero when $n=1$. So there are $2p+1$ orbits in total when $n=1$ and $2p+2$ orbits when $n>1$, from which we deduce Eq. (9). Equation (10) and frame potentials of higher orders can be derived using a similar reasoning.

For the restricted Clifford group, the summation over $f(F)^{t-1}$ in Eq. (12) can be evaluated explicitly. Equation (11) follows from the fact that $f(F)=q$ for the q^2-1 order-p elements in $\mathrm{SL}(2,q)$ and $f(F)=1$ for other q^3-q^2-q nonidentity elements [see Refs. [59–61] for the conjugacy classes of $\mathrm{SL}(2,q)$]. ■

APPENDIX B: PROOF OF LEMMA 2

Proof. Let $F\in R$ and U_F be a Clifford unitary that induces the transformation F; then $U_F D_\mu$ induces the same transformation for all $\mu\in\mathbb{F}_p^{2n}$. According to a similar argument used in the proof of Theorem 2.34 in Zauner's thesis [62] (see also Ref. [63]), $|\mathrm{tr}(U_F D_\mu)|^2$ is either zero or equal to the number of displacement operators that commute with U_F, which in turn is equal to the number $f(F)$ of fixed points of F in $\mathbb{F}_p^{2n}$. On the other hand, $\sum_\mu|\mathrm{tr}(U_F D_\mu)|=q^2$ given that the HW group is a unitary error basis. It follows that $|\mathrm{tr}(U_F D_\mu)|^2=f(F)$ for $q^2/f(F)$ of the q^2 displacement operators D_μ. Therefore,

$$\begin{aligned}\Phi_t(\overline{G})&=\frac{1}{q^2|R|}\sum_{F\in R}\sum_{\mu}|\mathrm{tr}(U_F D_\mu)|^{2t}\\&=\frac{1}{q^2|R|}\sum_{F\in R}f(F)^t\frac{q^2}{f(F)}=\frac{1}{|R|}\sum_{F\in R}f(F)^{t-1}.\end{aligned}\tag{B1}$$

According to the orbit-stabilizer relation, $\Phi_t(\overline{G})$ is equal to the number of orbits of R on $(\mathbb{F}_p^{2n})^{\times(t-1)}$.

In view of Eq. (3) and Lemma 2, the group $\overline{G}$ is a unitary 2-design if and only if R has two orbits on $\mathbb{F}_p^{2n}$ and is transitive on $\mathbb{F}_p^{2n*}$. The group $\overline{G}$ is a unitary 3-design if and only if R has five orbits on $(\mathbb{F}_p^{2n})^{\times 2}$ when $n=1$ and six orbits when $n\geqslant 2$; that is, R has two orbits on $(\mathbb{F}_p^{2n*})^{\times 2}$ and is 2-transitive when $n=1$ and it has three orbits and rank-3 when $n\geqslant 2$. ■

APPENDIX C: PROOF OF THEOREM 2

Proof. Suppose $\overline{G}$ is a subgroup of the n-qubit Clifford group that is a unitary 3-design. Let $\overline{H}=\overline{GD}$ and $R=\overline{H}/\overline{D}$. Then $\overline{H}$ is also a unitary 3-design. By Lemma 2, R is 2-transitive when $n=1$ and has rank-3 when $n\geqslant 2$. According to Theorem 4 below, $R=\mathrm{Sp}(2n,2)$ or $n=2$ and $R=A_6$

[the conclusion for $n=1$ follows from the observation that $\mathrm{Sp}(2,2)\simeq S_3$]. Here S_m and A_m denote the symmetric group and alternating group on m letters. To complete the proof it remains to show that $\overline{G}\geqslant\overline{D}$. Suppose this is not the case; then $\overline{G}$ cannot contain any nontrivial displacement operator given that R is transitive. Therefore, $\overline{G}$ is a complement of the HW group and is isomorphic to $\mathrm{Sp}(2n,2)$ when $n\neq 2$; when $n=2$, $\overline{G}$ is isomorphic to either $\mathrm{Sp}(4,2)$ or A_6. On the other hand, any unitary 3-design in dimension d has at least $d^2(d^4-3d^2+6)/2$ elements [6], which means 20 and 1712 elements for dimensions 2 and 4 and leads to a contradiction when $n=1,2$. In addition, the HW group is not complemented in the n-qubit Clifford group when $n\geqslant 2$ according to Theorem 7 in Ref. [46]. This contradiction confirms Theorem 2. ∎

Theorem 4. The group $\mathrm{Sp}(2n,2)$ with $n\geqslant 2$ has no proper rank-3 subgroup except when $n=2$, in which case it has a unique proper rank-3 subgroup, that is, the alternating group A_6 embedded in $\mathrm{Sp}(4,2)$.

This theorem follows from the work of Cameron and Kantor [64,65], although it is not easy to spot an explicit statement in these references. To prove this theorem, we need to introduce a few auxiliary concepts and results. A subgroup of $\mathrm{Sp}(2n,2)$ is primitive if it acts transitively on nonzero vectors in $\mathbb{F}_2^{2n}$ and preserves no nontrivial partition. It is antiflag transitive if it acts transitively on all pairs (μ,H) of nonzero vectors and hyperplanes in $\mathbb{F}_2^{2n}$ with $\mu\notin H$ [64,65].

Lemma 3. Any rank-3 subgroup of $\mathrm{Sp}(2n,2)$ for $n\geqslant 2$ is primitive.

Proof. Let R be a rank-3 subgroup of $\mathrm{Sp}(2n,2)$; then R is transitive and the point stabilizer of any nonzero vector μ partitions the remaining nonzero vectors into two orbits according to their symplectic products with μ. Therefore, the stabilizer has two orbits on $\mathbb{F}_2^{2n*}$ of lengths $2^{2n-1}-2$ and 2^{2n-1}, respectively. If R is not primitive, then any block in a nontrivial partition has size either $2^{2n-1}-1$ or $2^{2n-1}+1$. On the other hand, the size must be a divisor of $2^{2n}-1$. This contradiction shows that R is primitive. ∎

Lemma 4. Any rank-3 subgroup of $\mathrm{Sp}(2n,2)$ for $n\geqslant 2$ is antiflag transitive.

Proof. Let R be a rank-3 subgroup; then R is transitive and the point stabilizer of any nonzero vector μ has two orbits on the remaining nonzero vectors. Denote by $\mu^\perp$ the hyperplane composed of all vectors that are orthogonal to μ with respect to the given symplectic product. Then the map $\mu\mapsto\mu^\perp$ sets a one-to-one correspondence between vectors and hyperplanes, which is preserved by the symplectic group, that is, $F\mu^\perp=(F\mu)^\perp$ for any $F\in\mathrm{Sp}(2n,2)$. Let $\nu_1^\perp$ and $\nu_2^\perp$ be two hyperplanes that do not contain μ, that is, $\langle\mu,\nu_1\rangle=\langle\mu,\nu_2\rangle=1$. Then the point stabilizer of μ within R can map ν_1 to ν_2 and, accordingly, $\nu_1^\perp$ to $\nu_2^\perp$. So R is antiflag transitive. ∎

Proof of Theorem 4. Let R be a rank-3 subgroup of $\mathrm{Sp}(2n,2)$ with $n\geqslant 2$; then R is primitive and antiflag transitive, but not 2-transitive. Now Theorem 4 follows from Theorem 5.2 and Proposition 6.2 in Ref. [64]. Alternatively, it can be proved based on Theorem 2.2 in Ref. [65]. ∎

APPENDIX D: PROOF OF THEOREM 3

Proof. In view of Theorem 1, it suffices to prove the statement that no operator basis is covariant with respect to a unitary group 3-design. Suppose, on the contrary, that $\{L_j\}$ is an operator basis on the Hilbert space $\mathcal{H}$ of dimension d that is covariant with respect to a unitary group 3-design $\overline{G}$. Then $\Phi_2(\overline{G})=2$ and $\Phi_3(\overline{G})=6$ [$\Phi_3(\overline{G})=5$ when $d=2$] according to Eq. (3). Note that $\{L_j\otimes L_k\}$ and $\{L_j\otimes L_k\otimes L_l\}$ form operator bases for $\mathcal{H}^{\otimes 2}$ and $\mathcal{H}^{\otimes 3}$, respectively. According to Lemma 1 in Ref. [40] (cf. Lemma 7.2 in Ref. [63]), $\overline{G}$ acts transitively on ordered pairs of distinct operators in $\{L_j\}$ and has two orbits (one orbit when $d=2$) on ordered triples. The triple products $\mathrm{tr}(L_jL_kL_l)$ for distinct j,k,l must all be equal and thus real when $d=2$, while they can take on at most two different values when $d\geqslant 3$.

However, these triple products cannot all be real, since otherwise the basis operators would commute with each other and thus cannot form an operator basis. When $d=2$, this contradiction confirms the theorem. When $d\geqslant 3$, these triple products must take on two distinct values, which are complex conjugates of each other. Consequently, $\overline{G}$ acts transitively on unordered triples; in other words, $\overline{G}$ is 3-homogeneous in the language of permutation groups [51–53]. According to Theorem 1 of Ref. [66] (see also Theorem 9.4B in Ref. [51] and Lemma 2 in Ref. [53]), any 3-homogeneous permutation group on m objects with $m\geqslant 9$ a perfect square is 3-transitive. Therefore, $\overline{G}$ acts transitively on ordered triples, which means all triple products $\mathrm{tr}(L_jL_kL_l)$ are real, in contradiction with the previous observation. ∎

[1] D. P. DiVincenzo, D. Leung, and B. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory **48**, 580 (2002).

[2] H. F. Chau, Unconditionally secure key distribution in higher dimensions by depolarization, IEEE Trans. Inf. Theory **51**, 1451 (2005).

[3] C. Dankert, Efficient Simulation of Random Quantum States and Operators, Master thesis, University of Waterloo (2005), arXiv:quant-ph/0512217.

[4] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, Phys. Rev. A **80**, 012304 (2009).

[5] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, J. Math. Phys. **48**, 052104 (2007).

[6] A. Roy and A. J. Scott, Unitary designs and codes, Des. Codes Cryptogr. **53**, 13 (2009).

[7] R. Cleve, D. Leung, L. Liu, and C. Wang, Near-linear constructions of exact unitary 2-designs, Quantum Inf. Comput. **16**, 0721 (2016).

[8] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Randomized benchmarking of quantum gates, Phys. Rev. A **77**, 012307 (2008).

[9] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, Phys. Rev. Lett. **106**, 180504 (2011).

[10] J. J. Wallman and S. T. Flammia, Randomized benchmarking with confidence, New J. Phys. **16**, 103032 (2014).

[11] A. J. Scott, Optimizing quantum process tomography with unitary 2-designs, J. Phys. A: Math. Theor. **41**, 055308 (2008).

[12] S. Kimmel and Y.-K. Liu, Phase Retrieval Using Unitary 2-Designs, arXiv:1510.08887.

[13] A. Ambainis, J. Bouda, and A. Winter, Nonmalleable encryption of quantum information, J. Math. Phys. **50**, 042106 (2009).

[14] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. **45**, 2171 (2004).

[15] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A: Math. Gen. **39**, 13507 (2006).

[16] A. Ambainis and J. Emerson, Quantum t-designs: t-wise independence in the quantum world, in *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)* (IEEE, New York, 2007), pp. 129–140.

[17] P. Hayden and J. Preskill, Black holes as mirrors: quantum information in random subsystems, J. High Energy Phys. 09 (2007) 120.

[18] Y. Sekino and L. Susskind, Fast scramblers, J. High Energy Phys. 10 (2008) 065.

[19] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, Chaos in quantum channels, J. High Energy Phys. 02 (2016) 004.

[20] D. A. Roberts and B. Yoshida, Chaos and complexity by design, J. High Energy Phys. 04 (2017) 121.

[21] D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. thesis, California Institute of Technology (1997), arXiv:quant-ph/9705052.

[22] D. Gross, Hudson's theorem for finite-dimensional quantum systems, J. Math. Phys. **47**, 122107 (2006).

[23] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Contextuality supplies the 'magic' for quantum computation, Nature **510**, 351 (2014).

[24] A. W. Harrow and R. A. Low, Random quantum circuits are approximate 2-designs, Commun. Math. Phys. **291**, 257 (2009).

[25] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Efficient Quantum Pseudorandomness, Phys. Rev. Lett. **116**, 170502 (2016).

[26] P. Ćwikliński, M. Horodecki, M. Mozrzymas, Ł. Pankowski, and M. Studziński, Local random quantum circuits are approximate polynomial-designs: Numerical results, J. Phys. A: Math. Theor. **46**, 305301 (2013).

[27] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics, Phys. Rev. X **7**, 021006 (2017).

[28] W. Matthews, S. Wehner, and A. Winter, Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding, Commun. Math. Phys. **291**, 813 (2009).

[29] A. Hayashi, T. Hashimoto, and M. Horibe, Reexamination of optimal quantum state estimation of pure states, Phys. Rev. A **72**, 032325 (2005).

[30] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Quantum State Tomography Via Compressed Sensing, Phys. Rev. Lett. **105**, 150401 (2010).

[31] D. Gross, F. Krahmer, and R. Kueng, A partial derandomization of PhaseLift using spherical designs, J. Fourier Anal. Appl. **21**, 229 (2014).

[32] R. Kueng, H. Rauhut, and U. Terstiege, Low rank matrix recovery from rank one measurements, Appl. Comput. Harmon. Anal. **42**, 88 (2017).

[33] F. G. S. L. Brandão and M. Horodecki, Exponential quantum speed-ups are generic, Quantum Inf. Comput. **13**, 0901 (2013).

[34] R. Kueng and D. Gross, Qubit stabilizer states are complex projective 3-designs, arXiv:1510.02767.

[35] H. Zhu, R. Kueng, M. Grassl, and D. Gross, The Clifford group fails gracefully to be a unitary 4-design, arXiv:1609.08172.

[36] R. Kueng, H. Zhu, and D. Gross, Distinguishing quantum states using Clifford orbits, arXiv:1609.08595.

[37] R. Kueng, H. Zhu, and D. Gross, Low rank matrix recovery from Clifford orbits, arXiv:1610.08070.

[38] S. Nezami and M. Walter, Multipartite Entanglement in Stabilizer Tensor Networks, arXiv:1608.02595.

[39] W. K. Wootters, A Wigner-function formulation of finite-state quantum-mechanics, Ann. Phys. **176**, 1 (1987).

[40] H. Zhu, Permutation Symmetry Determines the Discrete Wigner Function, Phys. Rev. Lett. **116**, 040501 (2016).

[41] V. Veitch, C. Ferrie, D. Gross, and J. Emerson, Negative quasi-probability as a resource for quantum computation, New J. Phys. **14**, 113011 (2012).

[42] N. Delfosse, P. Allard Guerin, J. Bian, and R. Raussendorf, Wigner Function Negativity and Contextuality in Quantum Computation on Rebits, Phys. Rev. X **5**, 021003 (2015).

[43] D. M. Appleby, C. A. Fuchs, and H. Zhu, Group theoretic, Lie algebraic and Jordan algebraic formulations of the SIC existence problem, Quantum Inf. Comput. **15**, 61 (2015).

[44] E. M. Rains, Increasing subsequences and the classical groups, Electron. J. Combin. **5**, R12 (1998).

[45] B. Bolt, T. G. Room, and G. E. Wall, On the Clifford collineation, transform and similarity groups. I., J. Austral. Math. Soc. **2**, 60 (1961).

[46] B. Bolt, T. G. Room, and G. E. Wall, On the Clifford collineation, transform and similarity groups. II., J. Austral. Math. Soc. **2**, 80 (1961).

[47] H. Zhu, Sharply covariant mutually unbiased bases, arXiv:1503.00003.

[48] D. M. Appleby, Properties of the extended Clifford group with applications to SIC-POVMs and MUBs, arXiv:0909.5233.

[49] H. Zhu, Mutually unbiased bases as minimal Clifford covariant 2-designs, Phys. Rev. A **91**, 060301(R) (2015).

[50] J. Helsen, J. J. Wallman, and S. Wehner, Representations of the multi-qubit Clifford group, (2016), arXiv:1609.08188.

[51] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics (Springer, New York, 1996), Vol. 163.

[52] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts (Cambridge University Press, Cambridge, UK, 1999), Vol. 45.

[53] H. Zhu, Super-symmetric informationally complete measurements, Ann. Phys. **362**, 311 (2015).

[54] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics (Springer, London, 2009), Vol. 251.
[55] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[56] R. M. Guralnick and P. H. Tiep, Decompositions of small tensor powers and Larsen's conjecture, Representation Theory **9**, 138 (2005).
[57] Z. Webb, The Clifford group forms a unitary 3-design, Quantum Inf. Comput. **16**, 1379 (2016), arXiv:1510.02769.
[58] P. J. Cameron, Notes on classical groups (2000), available at http://www.maths.qmul.ac.uk/∼pjc/class_gps/cg.pdf.
[59] J. E. Humphreys, Representations of SL(2, p), Am. Math. Mon. **82**, 21 (1975).
[60] D. M. Appleby, I. Bengtsson, and S. Chaturvedi, Spectra of phase point operators in odd prime dimensions and the extended Clifford group, J. Math. Phys. **49**, 012102 (2008).
[61] H. Zhu, SIC POVMs and Clifford groups in prime dimensions, J. Phys. A: Math. Theor. **43**, 305305 (2010).
[62] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, Int. J. Quantum. Inform. **09**, 445 (2011).
[63] H. Zhu, Quantum State Estimation and Symmetric Informationally Complete POMs, Ph.D. thesis, National University of Singapore (2012), available at http://scholarbank.nus.edu.sg/bitstream/10635/35247/1/ZhuHJthesis.pdf.
[64] P. J. Cameron and W. M. Kantor, 2-transitive and antiflag transitive collineation groups of finite projective spaces, J. Algebra **60**, 384 (1979).
[65] P. J. Cameron and W. M. Kantor, Antiflag-transitive collineation groups revisited, (2002), available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.64.2238&rep=rep1&type=pdf.
[66] W. M. Kantor, k-homogeneous groups, Math. Z. **124**, 261 (1972).