Local unitary classes of states invariant under permutation subgroups

David W. Lyons ●,* Jesse R. Arnold,† and Ashley F. Swogger‡

Mathematical Sciences, Lebanon Valley College, Annville, Pennsylvania 17003, USA

The study of entanglement properties of multiqubit states that are invariant under permutations of qubits is motivated by potential applications in quantum computing, quantum communication, and quantum metrology. In this work we generalize the notions of symmetrization, Dicke states, and the Majorana representation to the alternating, cyclic, and dihedral subgroups of the full group of permutations. We use these tools to characterize states that are invariant under these subgroups and analyze their entanglement properties.

I. INTRODUCTION

Entangled states of many quantum bits are essential resources in emerging technologies, including quantum computing, secure communication, and measurement devices that promise to outperform "classical" digital technologies in fundamental ways. While such applications drive the study of multiparticle entanglement, a deeper motivation is to achieve insight in the foundations of physics.

In its full generality, entanglement is a hard problem: it is not reasonable to expect a full classification of multiparticle entanglement types [1]. A more modest, yet still valuable goal is to identify and classify families of entanglement types that are useful in protocols in quantum computation and communication.

One such family is the symmetric states, that is, states of composite systems that are invariant under permutations of the subsystems. Fruitful studies of permutation-invariant states where the general case remains intractable include geometric measure of entanglement [2–4], efficient tomography [5], classification of states equivalent under stochastic local operations and classical communication (SLOCC) [6,7], and our own work on classification of states equivalent under local unitary (LU) transformations [8,9]. Recent work [10] of Burchardt *et al.*, and also in this paper, generalizes the study of entanglement properties of permutationally invariant states to states that are invariant under the action of *subgroups* of the full permutation group.

The investigation in this paper is motivated by the following example. Higuchi and Sudbery [11] identified the state

$$|M_4\rangle = \frac{1}{\sqrt{6}}[(|0011\rangle + |1100\rangle) \\ + \omega(|1010\rangle + |0101\rangle) \\ + \omega^2(|1001\rangle + |0110\rangle)] \quad (1)$$

(where $\omega = e^{2\pi i/3}$) in a study seeking to analyze various maximal entanglement properties. The state $|M_4\rangle$ has the property that it has the maximum average two-qubit bipartite entanglement, averaged over all partitions into two-qubit subsystems. We found [12] that the state $|M_4\rangle$ and its conjugate $|\overline{M}_4\rangle$ are characterized, up to local unitary equivalence, by their invariance under the action of local unitary operators of the form $U^{\otimes 4}$ for arbitrary one-qubit unitaries U. An application of this fact is a code, using $|M_4\rangle$, $|\overline{M}_4\rangle$ for logical qubits $|0_L\rangle$, $|1_L\rangle$, that is unaffected by noise that takes the form of the same unitary evolution on each qubit. In addition to *local* unitary invariance properties, $|M_4\rangle$ has *nonlocal* permutation invariance under the subgroup A_4 of even permutations, that is, permutations that are products of an even number of transpositions of subsystems. The state $|M_4\rangle$ is *not* invariant under the full group of permutations of qubits: any odd number or transpositions of subsystems takes $|M_4\rangle$ to $|\overline{M}_4\rangle$, and vice versa.

Together, these observations about maximum entanglement properties, local unitary invariance, nonlocal permutation invariance, and potential application to quantum information protocols motivate the study of entanglement properties and potential applications of states that are invariant under subgroups of the full permutation group. We give a complete local unitary classification of states that are invariant under the alternating groups A_n in Sec. III and a partial classification for the cyclic groups C_n and the dihedral groups D_n in Sec. IV. We present evidence for applications in Sec. V. We begin, in Sec. II, by establishing basic definitions and tools for the study of G invariance, including generalizations of the S_n-invariant Dicke states and symmetrization constructions. Proofs of most Lemmas, Propositions, and Theorems are in the Appendix; a few short proofs are in the main body of the paper.

II. PERMUTATION SUBGROUP INVARIANCE

A. Invariance up to phase

Let G be a subgroup of the permutation group S_n. A permutation σ in G acts on the Hilbert space $(\mathbb{C}^2)^{\otimes n}$ of n-qubit

---

*lyons@lvc.edu
†jra005@lvc.edu
‡afs004@lvc.edu

TABLE I. Values of t_σ for $\sigma \in A_4$ acting on $|M_4\rangle$, where $\omega = e^{2\pi i/3}$.

σ	t_σ	σ	t_σ	σ	t_σ
e	1	(12)(34)	1	(123)	ω
		(13)(24)	1	(132)	ω^2
		(14)(23)	1	(124)	ω^2
				(142)	ω
				(234)	ω^2
				(243)	ω
				(134)	ω
				(143)	ω^2

states by

$$\sigma(|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle)$$
$$= |\phi_{\sigma^{-1}(1)}\rangle \otimes |\phi_{\sigma^{-1}(2)}\rangle \otimes \cdots \otimes |\phi_{\sigma^{-1}(n)}\rangle, \qquad (2)$$

where the $|\phi_k\rangle$ are one-qubit states. The effect of σ is to move the entry in position j to the position $\sigma(j)$. We say that an n-qubit state $|\psi\rangle$ is G-invariant *up to phase* if, for all $\sigma \in G$, there exists a nonzero scalar t_σ such that

$$\sigma|\psi\rangle = t_\sigma|\psi\rangle. \qquad (3)$$

Invariance up to phase is a generalization of belonging to the *symmetric subspace*, that is, having the property that $t_\sigma = 1$ for all σ. The state $|M_4\rangle$ (see (1) above) is invariant up to phase, but $|M_4\rangle$ is not in the A_4-symmetric subspace. For example, we have $(132)|M_4\rangle = \omega^2|M_4\rangle$, where $\omega = e^{2\pi i/2}$ and (132) denotes the 3-cycle permutation $1 \to 3 \to 2 \to 1$. Table I shows a complete list of values t_σ. *[Notation convention: In Table I, and throughout this paper, we use standard cycle notation to denote permutations. For distinct integers $a_1, a_2, \ldots, a_k$ in the range $1 \leqslant a_i \leqslant n$, the symbols $(a_1 a_2 \ldots a_k)$ denote the cyclic permutation*

$$a_1 \to a_2 \to a_3 \to \cdots \to a_n \to a_1.$$

Products of cycles $\kappa_1 \kappa_2 \ldots \kappa_t$ are read from right to left as function compositions.]

Because Eq. (2) defines a group action of G on n-qubit space, the function $t : G \to U(1)$ in Eq. (3) has the property that $t_{\sigma\tau} = t_\sigma t_\tau$ for all σ, τ, in G. In other words, t is a homomorphism of groups. From this we obtain useful properties such as the following:

(i) $t_e = 1$, where $e \in G$ is the identity permutation
(ii) $t_{\sigma^{-1}} = t_\sigma^{-1}$ for $\sigma \in G$
(iii) if $\sigma^m = 1$ then $t_\sigma^m = 1$

We record this key observation as a Proposition.

Proposition 1. Let G be a subgroup of S_n, let $|\psi\rangle$ be a G-invariant state, and let $t : G \to U(1)$ be given by $\sigma|\psi\rangle = t_\sigma|\psi\rangle$. Then t is a group homomorphism. That is, we have $t_{\sigma\tau} = t_\sigma t_\tau$ for all σ, τ in G.

In mathematical terminology, the homomorphism in Proposition 1 is an element of the *dual group* of G [13]. In place of saying "dual group element," we will use the unofficial but more descriptive term *phase homomorphism* to refer to a map $G \to U(1)$ arising from a G-invariant state $|\psi\rangle$ by the equations $\sigma|\psi\rangle = t_\sigma|\psi\rangle$ for $\sigma \in G$.

We conclude this section with a remark about invariance up to phase for $G = S_n$. An example of a permutationally invariant state that is not in the symmetric subspace is $|s\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, for which we have $(12)|s\rangle = -|s\rangle$. The following proposition shows that $|s\rangle$ is the *only* example for S_n invariance up to phase is different from belonging to the symmetric subspace. The proof is in the Appendix.

Proposition 2. Let $|\psi\rangle$ be an n-qubit state for $n \neq 2$. Suppose that $\sigma|\psi\rangle = t_\sigma|\psi\rangle$ for every σ in S_n, where the S_n action on n-qubit vector space is given by (2). Then $t_\sigma = 1$ for all σ.

B. Generalized Dicke forms

In this section we develop a key tool for the analysis of G-invariant states that generalizes the Dicke states for S_n-invariant states. Let G be a subgroup of S_n. The group G acts on n-bit strings by

$$g(i_1 i_2 \ldots i_n) = i_{g^{-1}(1)} i_{g^{-1}(2)} \ldots i_{g^{-1}(n)} \qquad (4)$$

for $g \in G$. We will write $[I]$ to denote the G orbit

$$[I] = \{gI : g \in G\},$$

and we will write Stab_I^G to denote the stabilizer subgroup

$$\text{Stab}_I^G = \{g \in G : gI = I\}$$

of the bit string I.

Let $|\psi\rangle$ be a G-invariant state (throughout this paper we adopt (3) for the definition of G-invariant state and will omit the phrase "up to phase"). Let $|\psi\rangle = \sum_I c_I|I\rangle$ be the expansion of $|\psi\rangle$ in the computational basis. For $g \in G$, we have

$$g|\psi\rangle = t_g|\psi\rangle = \sum_I t_g c_I|I\rangle \qquad (5)$$

and we also have

$$g|\psi\rangle = \sum_I c_I|gI\rangle. \qquad (6)$$

Comparing the $|J\rangle = |gI\rangle$ term in Eqs. (5) and (6) above, we have

$$c_I = t_g c_J \text{ for all } g \in G \text{ such that } gI = J. \qquad (7)$$

It follows that if $c_I \neq 0$ and $gI = I$, then $t_g = 1$. Thus we have the following:

Observation. If $|\psi\rangle$ is G invariant, with phase homomorphism $t : G \to U(1)$ given by $g|\psi\rangle = t_g|\psi\rangle$ for all $g \in G$, then t is constant on Stab_I^G for all I such that $c_I \neq 0$. This observation leads to the following representations of the G-invariant state $|\psi\rangle$ that generalize the Dicke form for S_n-invariant states. For each G orbit $[I]$, choose a fixed representative $L_{[I]}$. (For example, we could choose $L_{[I]}$ to be the bit string that represents the largest binary integer among all the elements of $[I]$.) We will write $c_{[I]}$ to denote $c_{L_{[I]}}$. We have the following *generalized Dicke forms* for $|\psi\rangle$:

$$|\psi\rangle = \sum_{[I]} \frac{c_{[I]}}{\sqrt{|\text{Stab}_I^G|}} \sum_{g \in G} t_g^{-1}|gI\rangle \qquad (8)$$

$$= \sum_{[I]} c_{[I]} \sum_{J \in [I]} t_g^{-1}|J\rangle \text{ (where } gL_{[I]} = J). \qquad (9)$$

That the expression t_g in (9) is independent of the choice of g (as long as $gL_{[I]} = J$) is justified by (7).

We have shown that any G-invariant state has a Dicke form. Now we show the converse (the proof is in the Appendix).

Proposition 3. Let G be a subgroup of S_n, let $c_{[I]}$ be complex constants, one for each G orbit on n-bit strings, and let $t : G \to U(1)$ be a homomorphism that is constant on any stabilizer Stab_I^G for which $c_I \neq 0$. The state

$$|\psi\rangle = \sum_{[I]} c_{[I]} \sum_{J \in [I]} t_g^{-1} |J\rangle \quad \text{(where } gL_{[I]} = J)$$

is G invariant and satisfies $g|\psi\rangle = t_g|\psi\rangle$ for all $g \in G$.

We note here that the Dicke form (9) is indeed a generalization of the decomposition $|\psi\rangle = \sum_{w=0}^{n} d_w|D_n^w\rangle$ of a state $|\psi\rangle$ in the (S_n-)symmetric subspace, where

$$\left|D_n^w\right\rangle = \frac{1}{\sqrt{\binom{n}{w}}} \sum_{I:\mathrm{wt}I=w} |I\rangle \tag{10}$$

is the weight w Dicke state. [Here the symbols "wt$I$" denote the (Hamming) weight of the binary string I, that is, the number of 1's in I.]

We conclude this section with a definition of the *generalized Dicke states.* Given a homomorphism $t : G \to U(1)$ and a G orbit $[I]$ such that t is constant on Stab_I^G, we refer to the states

$$\left|\widetilde{D}_t^{[I]}\right\rangle = \sum_{J \in [I]} t_g^{-1}|J\rangle \quad \text{(where } gL_{[I]} = J), \tag{11}$$

$$\left|D_t^{[I]}\right\rangle = \frac{1}{\sqrt{|[I]|}}\left|\widetilde{D}_t^{[I]}\right\rangle, \tag{12}$$

as the un-normalized (respectively, normalized) generalized Dicke state for the G orbit $[I]$ with respect to the homomorphism t.

C. The permutation subgroups A_n, C_n, and D_n

In this paper we consider the following permutation subgroups—the alternating group A_n, the cyclic group C_n, and the dihedral group D_n, defined as follows:

A_n the alternating group is the set of permutations that can be written as a product of an even number of permutations

C_n the cyclic group is the group generated by the full cycle $\epsilon = (12 \cdots n)$

D_n the dihedral group is the group generated by the full cycle $\epsilon = (12 \cdots n)$ and the "mirror reflection" $\tau = \prod_{j=1}^{\lfloor \frac{n+1}{2} \rfloor}(j, n+1-j)$

In terms of the action (4) of permutations on bit strings, the effect of τ is string reversal, that is, we have

$$\tau(i_1 i_2 \cdots i_{n-1} i_n) = (i_n i_{n-1} \cdots i_2 i_1).$$

In what follows we will use the facts that A_n is generated by 3-cycles [14], that C_n is generated by ϵ (by definition), and that D_n is generated by ϵ and τ:

$$A_n = \langle(ijk)\rangle \quad (1 \leqslant i, j, k \leqslant n, \ i, j, k \text{ distinct})$$

$$C_n = \langle\epsilon\rangle$$

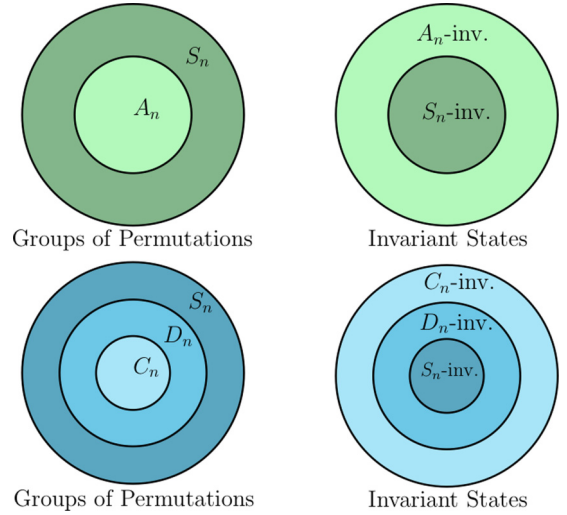$$D_n = \langle\epsilon, \tau\rangle.$$

FIG. 1. Subgroups of S_n and corresponding sets of invariant states.

Figure 1 illustrates the inclusions among the groups S_n, A_n, D_n, and C_n, and the reversed inclusions among the corresponding invariant states. In the sections that follow, we focus on the characterization of states that lie in the annular rings of Fig. 1, that is, we characterize states that are A_n invariant and are *not* fully S_n invariant, and states that are C_n invariant and are *not* D_n invariant. Table II shows a summary table of the (unnormalized) generalized Dicke states (11) for $G = S_n, C_n, D_n$ (the case of A_n is treated in Sec. III A).

D. G symmetrization

Here is a construction that produces G-invariant states. Let G be a subgroup of S_n and let $t : G \to U(1)$ be a group homomorphism. For one-qubit states $|\phi_1\rangle, \ldots, |\phi_n\rangle$, we define the G symmetrization of $|\phi_i\rangle_{i=1}^{n}$ by

$$\mathrm{GSym}_t(|\phi_1\rangle, \ldots, |\phi_n\rangle)$$
$$= K \sum_{\sigma \in G} t_\sigma^{-1} |\phi_{\sigma^{-1}(1)}\rangle \otimes \cdots \otimes |\phi_{\sigma^{-1}(n)}\rangle, \tag{13}$$

where K is a normalizing factor. [It is possible that G symmetrization produces the zero vector, which is not a state. For example, $\mathrm{GSym}_t(|0\rangle, |0\rangle) = 0$ for $G = S_2$ and $t : S_2 \to U(1)$ given by $t_{(12)} = -1$. In this case K can be assigned arbitrarily.] The following Proposition expresses that the G symmetrization of one-qubit states is in fact G invariant. The proof is in the Appendix.

Proposition 4. Let $|\psi\rangle = \mathrm{GSym}_t(|\phi_1\rangle, \ldots, |\phi_n\rangle)$ for some G, t, and states $|\phi_i\rangle$. Then we have

$$\sigma|\psi\rangle = t_\sigma|\psi\rangle$$

TABLE II. Un-normalized generalized Dicke states.

G	$|\widetilde{D}_t^{[I]}\rangle$
S_n	$\sum_{I:\mathrm{wt}I=w}|I\rangle$
C_n	$\sum_{k=0}^{n-1} t_\epsilon^{-k}|\epsilon^k I\rangle$
D_n	$\sum_{a=0}^{1}\sum_{k=0}^{n-1} t_\tau^a t_\epsilon^{-k}|\tau^a \epsilon^k I\rangle$

for all $\sigma \in G$, i.e., $|\psi\rangle$ is G invariant.

Corollary 1. Suppose that

$$|\psi\rangle = \text{GSym}_t(|\phi_1\rangle, \ldots, |\phi_n\rangle) \neq 0$$

for some subgroup G of S_n for some $n \geqslant 3$, and that t is not trivial. Then $|\psi\rangle$ is *not* S_n invariant.

Comments. For $G = S_n$ and for the trivial homomorphism t, the symmetrization (13) establishes a one-to-one correspondence between sets of n points on the Bloch sphere and S_n-symmetric states of n qubits:

$$\{|\phi_1\rangle, \ldots, |\phi_n\rangle\} \longleftrightarrow \text{GSym}_t(|\phi_1\rangle, \ldots, |\phi_n\rangle).$$

This remarkable fact is the well-known Majorana representation [6]. We show with examples that the one-to-one correspondence does not hold in general for symmetrization over subgroups of S_n.

Examples. Unlike the case for S_n, G symmetrization does not give a one-to-one correspondence between n tuples of points on the Bloch sphere and G-invariant states.

For $G = A_3 = C_3 = \langle (123) \rangle$ and t determined by $t_{(123)} = e^{4\pi i/3}$, and

$$|\alpha\rangle = \frac{1}{\sqrt{3}}(|100\rangle + \omega|010\rangle + \omega^2|001\rangle),$$

we have

$$|\alpha\rangle = \text{GSym}_t(|1\rangle, |0\rangle, |0\rangle)$$
$$= \text{GSym}_t(|0\rangle + |1\rangle, |0\rangle + \omega|1\rangle, |0\rangle + \omega^2|1\rangle).$$

For $G = A_4$ and $t : A_4 \to U(1)$ given by $t_{(123)} = e^{2\pi i/3}$, we have

$$|M_4\rangle = \text{GSym}_t(|1\rangle, |1\rangle, |0\rangle, |0\rangle)$$
$$= \text{GSym}_t(|+\rangle, |+\rangle, |-\rangle, |-\rangle)$$
$$= \text{GSym}_t(|1\rangle, |1\rangle, |+\rangle, |+\rangle).$$

We explore the structure of A_n symmetrizations in Sec. III C below.

III. A_n-INVARIANT STATES

A. Phase homomorphisms for A_n-invariant states

We start by showing that the phase homomorphism $t : A_n \to U(1)$ cannot be trivial for a state that is A_n invariant but *not* S_n invariant.

Lemma 1. Let $n \geqslant 3$, and let $|\psi\rangle$ be A_n invariant. Suppose $\sigma|\psi\rangle = |\psi\rangle$ for all σ in A_n. Then $|\psi\rangle$ is S_n invariant.

Proof. Suppose there is an I such that $1 \leqslant \text{wt} I \leqslant n - 1$ and $c_I \neq 0$. Choose j, k, ℓ such that $i_k = i_\ell$ and $i_j \neq i_\ell$. Then we have $I = (jk\ell)(k\ell)I$, but $(jk\ell)(k\ell) = (kj)$ and $(kj)I \neq I$. Therefore $\text{wt} I = 0$ or $\text{wt} I = n$. Thus $|\psi\rangle$ is S_n invariant.

Corollary 2. Suppose that $|\psi\rangle$ is an A_n-invariant but not S_n-invariant state for $n \geqslant 3$, and suppose that $\sigma|\psi\rangle = t_\sigma|\psi\rangle$ for all σ in A_n. Then there exists a 3-cycle τ such that $t_\tau \neq 1$.

Proof. The Corollary follows directly from Lemma 1 with the observation that A_n is generated by its 3-cycles.

The proofs of the next two statements, Corollary 3 and Proposition 5, are in the Appendix.

Corollary 3. (t_σ *values for 3-cycles and products of disjoint 2-cycles*) For a 3-cycle σ, we have $t_\sigma = 1, \omega, \omega^2$, where $\omega = e^{2\pi i/3}$. If τ is a a product of disjoint 2-cycles, then $t_\tau = 1$.

Proposition 5. For $n \geqslant 5$, there are no pure states that are A_n invariant and not S_n invariant.

Now we use the Dicke form (9) and the above results about the phase homomorphism $t : A_n \to U(1)$ to determine the form of a state $|\psi\rangle$ that is A_n invariant and not S_n invariant. By Proposition 5 we need only consider the cases $n = 3$ and $n = 4$. For $n = 3$, the homomorphism t is determined by choosing one of the two values $t_{(123)} = \omega, \omega^*$, where $\omega = e^{2\pi i/3}$. If the coefficient of $|100\rangle$ in the expansion $|\psi\rangle = \sum_I |I\rangle$ is c_{100}, then the weight-1 terms in $|\psi\rangle$ must have the form

$$c_{100}(|100\rangle + \omega|010\rangle + \omega^2|001\rangle)$$

or the conjugate of that expression, depending on the value of $t_{(123)}$. A similar observation holds for the weight-2 terms. It is easy to see that the weight-0 and weight-3 terms must be zero. Let us define the following three-qubit states, where $\omega = e^{2\pi i/3}$ and a, b are some complex constants with $|a|^2 + |b|^2 = 1$:

$$|\alpha\rangle = \frac{1}{\sqrt{3}}(|100\rangle + \omega|010\rangle + \omega^2|001\rangle)$$

$$|\beta\rangle = \frac{1}{\sqrt{3}}(|110\rangle + \omega|011\rangle + \omega^2|101\rangle)$$

$$|M_3(a, b)\rangle = a|\alpha\rangle + b|\beta\rangle.$$

The discussion in the previous paragraph establishes the following:

Proposition 6. If $|\psi\rangle$ is A_3 invariant and not S_3 invariant, then there are complex numbers a, b with $|a|^2 + |b|^2 = 1$ such that $|\psi\rangle$ equals $|M_3(a, b)\rangle$ or its conjugate, up to a global phase factor.

For $n = 4$, any permutation σ in A_4 is either the product of disjoint transpositions $\sigma = (ij)(k\ell)$ or a 3-cycle $\sigma = (abc)$. For a 3-cycle, we have $(abc)^3 = e$, so we must have $t_{(abc)} = \omega, \omega^*$, where again, $\omega = e^{2\pi i/3}$. In the first case we have

$$\sigma = (ij)(k\ell) = (i\ell k)(ijk).$$

Thus for $\sigma = (ij)(k\ell) = (i\ell k)(ijk)$ we must have that t_σ is a power of ω. But $\sigma^2 = e$ implies $t_\sigma = \pm 1$. Therefore we must have $t_\sigma = 1$, since no power of ω can equal -1. The values of t_σ for $\sigma = (abc)$ are determined by equations like $(123)(124) = (13)(24)$, so $t_{(123)} = t_{(124)}^*$. With just a few calculations, we see that the values t_σ must either be the same as those given in Table I, or their conjugates. If $|\psi\rangle$ is A_4 invariant but not S_4 invariant, it cannot have any weight-1 terms with nonzero coefficients in its expansion in the computational basis. For example, the 2-cycle (123) fixes $|0001\rangle$, but $t_{(123)} \neq 1$. By similar considerations, $|\psi\rangle$ cannot have any nonzero terms in weights 0, 1, 3, or 4. One determines quickly that the weight-2 terms must be organized as for $|M_4\rangle$ or its conjugate (up to a global phase factor). Thus we have proved the following.

Proposition 7. If $|\psi\rangle$ is A_4 invariant and not S_4 invariant, then $|\psi\rangle$ equals $|M_4\rangle$ or its conjugate, up to a phase multiple.

B. Local unitary equivalence

In this section we classify the LU equivalence classes of states that are A_n invariant and not S_n invariant. For the case $n = 3$, we have the striking result that all of the states in the infinite family $|M_3(a, b)\rangle$, $|\overline{M_3(a, b)}\rangle$ are local unitary equivalent. The proof exploits the relationship between carefully chosen one-qubit operators U acting on the one-qubit state $a|0\rangle + b|1\rangle$ and suitably constructed three-qubit operators $V^{\otimes 3}$ acting on $|M_3(a, b)\rangle$, in such a way that a local equivalence between $a|0\rangle + b|1\rangle$ and $a'|0\rangle + b'|1\rangle$ yields a local equivalence between $|M_3(a, b)\rangle$ and $|M_3(a', b')\rangle$. A detailed proof is in the Appendix.

Theorem 1. Let $|\psi\rangle$ be A_3 invariant and not S_3 invariant. Then $|\psi\rangle$ is LU equivalent to

$$|M_3(1, 0)\rangle = \frac{1}{\sqrt{3}}(|100\rangle + \omega|010\rangle + \omega^2|001\rangle).$$

For the case $n = 4$, there are only two states to consider, namely, $|M_4\rangle$ and its conjugate. We refer the reader to [12] for a proof that there are LU invariants that distinguish the LU classes of $|M_4\rangle$ and its conjugate. We record the result here.

Proposition 8. The two states (up to global phase factor) that are A_4 invariant and not S_4 invariant, namely, $|M_4\rangle$ and its conjugate, are LU inequivalent.

C. A_n symmetrization

In this section we consider the question of under what conditions does A_n symmetrization produce an A_n-invariant state that is not also S_n invariant and also nonzero. In the Propositions below, we characterize the n-tuples $|\phi_1\rangle, \ldots, |\phi_n\rangle$ of one-qubit states and the homomorphisms $t : A_n \to U(1)$ such that for $G = A_n$ the state $\mathrm{GSym}_t(|\phi_1\rangle, \ldots, |\phi_n\rangle)$ is A_n invariant and not S_n invariant and also nonzero. The proofs are in the Appendix. By the results in the preceding section we need only consider $n = 3, 4$.

Proposition 9. Let $n = 3$, let $G = A_3$, and let $|\phi_i\rangle$ be one-qubit states for $i = 1, 2, 3$. The state $\mathrm{GSym}_t(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle)$ is A_3 invariant and not S_3 invariant and not zero if an only if $t_{(123)} \neq 1$ and the three states $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$ are not all the same (up to phase).

Proposition 10. Let $n = 4$, let $G = A_4$, and let $|\phi_i\rangle$ be 1-qubit states for $i = 1, 2, 3, 4$. Except for a set of measure zero, the state $\mathrm{GSym}_t(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle)$ is A_4-invariant and not S_4-invariant and not zero if and only if $t_{(123)} \neq 1$ and no three of the states $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle$ are equal (up to phase).

IV. C_n- AND D_n-INVARIANT STATES

A. Necklace diagrams

A regular n-gon with vertices colored white or black encodes the cycle class of an n-bit string as follows. Starting at any vertex, label the vertices $v_1, v_2, \ldots, v_n$ traveling counterclockwise around the polygon. Let the bit string $I = i_1 i_2 \ldots i_n$ be defined by $i_k = 0$ if v_k is white and let $i_k = 1$ if v_k is black. If we perform the same procedure starting at a different vertex, say $w_1 = v_\ell$, we obtain the bit string $J = \epsilon^\ell I$, where $\epsilon = (12 \cdots n)$. This type of figure, called a *necklace diagram*, encodes the C_n orbit $[I]$ of the bit string I. Figure 2 illustrates with an example.
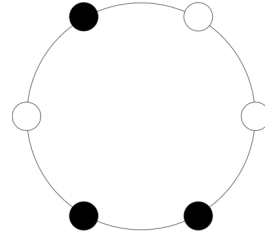

FIG. 2. Necklace diagram for the cycle class [101100].

In what follows we will develop criteria for cyclic and dihedral symmetry for states constructed from necklace diagrams in terms of lines of mirror symmetry. For n odd, any line of mirror symmetry passes through one vertex, say v_0, labeled by a bit a_0, and one of the bit strings in the cycle class of the necklace has the form $A = (a_\ell \ldots a_2 a_1 a_0 a_1 a_2 \ldots a_\ell)$ so that $\tau A = A$. For n even, there are two possible types of mirror lines of symmetry: a line may pass through no vertices, and a line may pass through two vertices. In the no-vertex case, the necklace encodes a palindromic bit string of the form $B = (b_1 b_2 \ldots b_\ell b_\ell \ldots b_2 b_1)$ so that $\tau B = B$. In the two-vertex case, the necklace encodes a bit string of the form $C = (a_\ell \cdots a_2 a_1 c_0 a_1 a_2 \ldots a_\ell c_1)$, so that $\tau C = \epsilon C$. See Fig. 3.

Terminology: We will use the following terms for types of necklaces. A necklace $[I]$ of length n is

[SP] *self-palindromic* or *palindromic on the string level*, denoted SP, if $[I]$ has at least one 0-vertex line of symmetry (if n is even) or at least one 1-vertex line of symmetry (if n is odd)

[CP] *class-palindromic* or *palindromic on the class level*, denoted CP, if n is even and $[I]$ has at least one 2-vertex line of symmetry and no 0-vertex lines of symmetry

[chiral] *chiral,* or *nonpalindromic*, if $[I]$ has no lines of symmetry

We say that the *cycle order* of a necklace diagram $[I]$ is the number of distinct bit strings in the G orbit $[I]$. Equivalently, we can define the cycle order of a bit string I to be the smallest positive integer m such that $\epsilon^m I = I$.
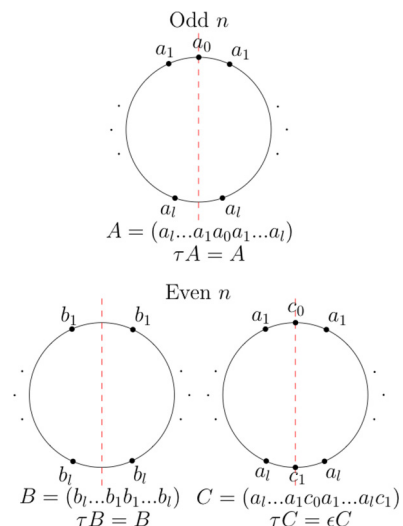

FIG. 3. Lines of symmetry through zero, one, and two vertices.

The following Proposition will be used in the characterization of states that are C_n invariant and not D_n invariant. The proof is in the Appendix.

Proposition 11. Let J be an n-bit string with even cycle order, say m. Suppose $\tau \epsilon^k J = J$. If $[J]$ is of type SP then k is even. If $[J]$ is of type CP then k is odd.

We conclude with a geometric observation that relates the cycle order to the number of lines of mirror symmetry of a necklace diagram. A proof sketch is in the Appendix.

Proposition 12. Let L be the number of lines of mirror symmetry of an n-bit necklace diagram $[I]$. If $L = 0$, then the cycle order of $[I]$ is n. If $L > 0$, then the cycle order of $[I]$ is n/L.

B. C_n- and not D_n-invariant states

In this section we characterize those states that are C_n invariant and are *not* D_n invariant. The proof of Theorem 2 is in the Appendix.

Proposition 13. Let $|\psi\rangle$ be C_n invariant so that we have

$$\epsilon^k|\psi\rangle = t_\epsilon^k|\psi\rangle$$

for all k. The state $|\psi\rangle$ is D_n invariant if and only if

$$\tau|\psi\rangle = t_\tau|\psi\rangle$$

for some t_τ.

Proof. This follows from the fact that all elements of D_n can be written in the form $\tau^a \epsilon^k$ for some $a = 0, 1$ and some integer k.

Theorem 2. Let $|\psi\rangle$ be a C_n-invariant state with homomorphism $t : C_n \to U(1)$ determined by $\epsilon|\psi\rangle = t_\epsilon|\psi\rangle$. The state $|\psi\rangle$ is D_n invariant, with homomorphism $s : D_n \to U(1)$ determined by $\sigma|\psi\rangle = s_\sigma|\psi\rangle$ for all $\sigma \in D_n$ if and only if all four of the following hold:

(i) $t_\epsilon = \pm 1$

(ii) if there is an I of type SP with $c_{[I]} \neq 0$, then $s_\tau = 1$

(iii) if there is an I of type CP with $c_{[I]} \neq 0$, then $s_\tau = s_\epsilon$

(iv) if there is an I of chiral type with $c_{[I]} \neq 0$, then $c_J = s_\tau c_{\tau J}$ for all $J \in [I]$

C. D_n- and not S_n-invariant states

The following Proposition characterizes those states that are D_n invariant and are *not* S_n invariant. The proof is in the Appendix.

Proposition 14. Suppose $|\psi\rangle$ is D_n invariant. Then $|\psi\rangle$ is S_n invariant if and only if both of the following hold:

(i) $t_\epsilon = t_\tau = 1$

(ii) $C_{[I]} = C_{[J]}$ for all I, J with wt$I$ = wt$J$

D. Local unitary equivalence

The full characterization of local unitary equivalence classes for C_n-invariant and D_n-invariant states (that are not S_n invariant) awaits future work. The fact that there is only one local unitary class for the case of $A_3 = C_3$ (Theorem 1) suggests that the general case will be subtle. We record here a preliminary result for local unitary classes of the generalized Dicke states for C_n-invariant and D_n-invariant states, *whether or not* they are also S_n invariant.

We show in [8] that the Dicke states $|D_n^w\rangle$ [Eq. (10)] for S_n-invariant states belong to $\lfloor n/2 \rfloor$ distinct local unitary classes, one for each weight $w = 0, 1, 2, \ldots, \lfloor n/2 \rfloor$. The Dicke state $|D_n^w\rangle$ is local unitary equivalent to the Dicke state $|D_n^{n-w}\rangle$ via the operator $X^{\otimes n}$. The same proof, mutatis mutandis, can be used for the subgroups C_n and D_n. We give a sketch of the proof in the Appendix.

Proposition 15. Let $|D_t^{[I]}\rangle, |D_t^{[J]}\rangle$ be generalized Dicke states (see Table II) for $G = C_n$ or $G = D_n$. If wt$J \neq$ wt$I$ and wt$J \neq n -$ wt$I$, then the states $|D_t^{[I]}\rangle$ to $|D_t^{[J]}\rangle$ belong to distinct local unitary classes.

V. APPLICATIONS

This section provides evidence, both established and conjectural, that it is reasonable to expect to find resource states for quantum information protocols among the G-invariant states for $G \subset S_n$.

A. Quantum codes

In the Introduction we describe a 4-qubit code that uses the logical qubit states

$$|0_L\rangle = |M_4\rangle$$
$$|1_L\rangle = |\overline{M}_4\rangle$$

where $|\overline{M}_4\rangle = (12)|M_4\rangle$. Owing to the local unitary invariance of these states, that is,

$$U^{\otimes 4}|M_4\rangle = |M_4\rangle$$
$$U^{\otimes 4}|\overline{M}_4\rangle = |\overline{M}_4\rangle$$

for all one-qubit unitary operators U [12], this code is unaffected by noise evolutions of the form $U^{\otimes 4}$. Here is a construction in a G-invariant state framework that generalizes this example. Let $|\psi\rangle$ be a G-invariant state for some group of permutations G. The S_n orbit $\{\sigma|\psi\rangle : \sigma \in S_n\}$ of $|\psi\rangle$ may contain a set of orthogonal states. (For example, for the six-qubit C_n-invariant state

$$|\psi\rangle = \sum_{k=0}^{5} e^{2\pi ik/6}\epsilon^k|000001\rangle,$$

where ϵ is the six-cycle $\epsilon = (123456)$, the state $(12)(34)(56)|\psi\rangle$ is orthogonal to $|\psi\rangle$, but $(12)|\psi\rangle$ is not.) We leave it to future work to study properties of codes that use orthogonal sets of codewords in S_n orbits of G-invariant states.

B. Hypergraph states with GHZ-like local unitary stabilizers

The Greenberger-Horne-Zeilinger (GHZ) state of n qubits,

$$\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}),$$

is an important resource in quantum information theory. In [15] (see Prop. 5.5) we construct hypergraph state $|\psi\rangle$ consisting of n "essential" qubits together with an auxiliary core of an arbitrary number m of qubits in such a way that $|\psi\rangle$ is invariant under permutations of the auxiliary qubits. Briefly, $|\psi\rangle$ is constructed by starting with the uniform superposition

$H^{\otimes(m+n)}|0\rangle^{\otimes(m+n)}$ of all the computational basis states and then applying, for each essential qubit k, the operator

$$C_k = \mathbb{1} - 2(|1\rangle\langle 1|)^{\otimes(m+1)}$$

to the m auxiliary qubits together with the kth essential qubit:

$$|\psi\rangle = \left(\prod_{k=1}^{n} C_k\right) H^{\otimes(m+n)}|0\rangle^{\otimes(m+n)}.$$

The state $|\psi\rangle$ shares entanglement properties with the n-qubit GHZ state in the sense that the local unitary stabilizer group of $|\psi\rangle$ is isomorphic to the local unitary stabilizer group of the GHZ state, where the essential qubits of $|\psi\rangle$ correspond to the qubits of the GHZ state. Results await future investigation, but we expect that the "GHZ-like" state $|\psi\rangle$ will serve as a useful version of a GHZ state, for example, in a setting where there is a possibility of the loss of some qubits. We conjecture that protocols for the GHZ state that are based on the local unitary stabilizer group will adapt to $|\psi\rangle$. An example is a verification protocol (Pappa *et al.* [16]), based on applying random local unitary stabilizers, which verifies (or disqualifies) possibly untrusted GHZ states whose qubits are distributed among parties who may or may not be trusted.

C. Further applications

Burchardt *et al.* [10] describe how G-invariant states (called "Dicke-like" states in their paper) can be used for parallel teleportation protocols, secret sharing schemes, and quantum chemistry applications to molecules with a high degree of spatial symmetry. The authors demonstrate how entanglement in Dicke-like states, as measured by concurrence, can be concentrated between selected subsets of parties while at the same time suppressing correlations between other pairs of parties. The authors conjecture that this property will be useful for protocols where variable strength of entanglement interactions between certain parties is desired.

VI. CONCLUSION

We have characterized multiqubit states that are invariant under the alternating, cyclic, and dihedral subgroups of the group of permutations of the qubits and have described applications to quantum technology that exploit these symmetries.

Directions for continued work on the classification of states that are invariant under subgroups of S_n include the following: Can we characterize the configurations of Bloch sphere points that have the same G symmetrizations? Could we use such a characterization to prove things about local unitary classes of G-invariant states (like we can for S_n-invariant states)?

Towards applications, what performance properties are possessed by codes that are invariant under proper subgroups of S_n? How can the loss tolerance of the "GHZ-like" state (described in the previous section) enhance entanglement verification protocols?

Finally, as we have done for symmetric states [9], it will be natural to extend this work to mixed states.

APPENDIX: PROOFS OF PROPOSITIONS

Proof of Proposition 2. By the properties of group actions we have $t_e = 1$, where e is the identity permutation, and $t_{\sigma\tau} = t_\sigma t_\tau$ for all σ, τ in S_n. In particular, we may write any permutation σ as a product

$$\sigma = \tau_1 \tau_2 \cdots \tau_k$$

of transpositions τ_j. Thus it suffices to show that $t_\tau = 1$ for any transposition τ in order to prove the proposition. The case $n = 1$ is trivial, so now assume that $n \geqslant 3$. Let $\tau = (k\ell)$ be a transposition. Write $|\psi\rangle = \sum_I c_I |I\rangle$ in the standard basis and choose a multi-index $I_0 = i_1 i_2 \cdots i_n$ such that $i_k = i_\ell$ and $c_{I_0} \neq 0$. (Start by choosing any J such that $c_J \neq 0$. By the pigeonhole principle, there must be two indices a, b such that $j_a = j_b$. Apply a permutation σ that takes a, b to k, ℓ, and let $I_0 = \sigma J$.) Now we have

$$\sigma|\psi\rangle = c_{I_0}|I_0\rangle + \sum_{J \neq I_0} t_\tau c_J |\tau J\rangle.$$

But this last expression must equal $|\psi\rangle = c_{I_0}|I_0\rangle + \sum_{J \neq I_0} c_J |J\rangle$, so it must be that $t_\tau = 1$.

Proof of Proposition 3. First, observe that the requirement that t is constant on stabilizers of strings I with nonzero coefficients c_I guarantees that the expression t_g does not depend on which $g \in G$ is chosen in the expression t_g, as long as $gL_{[I]} = J$. Indeed, suppose that $gL = hL$. Then $g^{-1}hL = L$, so $t_g^{-1}t_h = t_e = 1$, so $t_g = t_h$.

Now, let $h \in G$. We have

$$\begin{aligned}
h|\psi\rangle &= \sum_{[I]} c_{[I]} \sum_{J \in [I]} t_g^{-1}|J\rangle \\
&= h\left(\sum_{[I]} c_{[I]} \sum_{J \in [I]} t_{(h^{-1}g)}^{-1}|h^{-1}J\rangle\right) \\
&= \sum_{[I]} c_{[I]} \sum_{J \in [I]} t_{(h^{-1}g)}^{-1}|J\rangle \\
&= \sum_{[I]} c_{[I]} \sum_{J \in [I]} t_h t_g^{-1}|J\rangle \\
&= t_h|\psi\rangle.
\end{aligned}$$

Proof of Proposition 4. We have

$$\begin{aligned}
\sigma|\psi\rangle &= \sigma \sum_{\pi \in G} t_\pi^{-1}|\phi_{\pi^{-1}(1)}\rangle \cdots |\phi_{\pi^{-1}(n)}\rangle \\
&= \sum_{\pi \in G} t_\pi^{-1}|\phi_{\pi^{-1}\sigma^{-1}(1)}\rangle \cdots |\phi_{\pi^{-1}\sigma^{-1}(n)}\rangle \\
&= \sum_{\pi \in G} t_\pi^{-1}|\phi_{(\sigma\pi)^{-1}(1)}\rangle \cdots |\phi_{(\sigma\pi)^{-1}(n)}\rangle \\
&= \sum_{\xi \in G} t_{\sigma^{-1}\xi}^{-1}|\phi_{\xi^{-1}(1)}\rangle \cdots |\phi_{\xi^{-1}(n)}\rangle \quad (\xi = \sigma\pi)
\end{aligned}$$

$$= t_\sigma \sum_{\xi \in G} t_\xi^{-1} |\phi_{\xi^{-1}(1)}\rangle \cdots |\phi_{\xi^{-1}(n)}\rangle$$

$$= t_\sigma |\psi\rangle.$$

Proof of Corollary 3. The first statement follows from $\sigma^3 = 1$. From $\tau^2 = 1$, we have $t_\tau = \pm 1$ for $\tau = (ab)(cd)$ with a, b, c, d distinct. From the equation

$$(ab)(cd) = (dca)(abc)$$

we have $t_\tau = \omega^k$ for some k. It follows that $t_\tau = 1$.

Now let $n \geqslant 3$ and suppose that $|\psi\rangle$ is A_n invariant but not S_3 invariant. By Corollary 2, there is a 3-cycle (abc) such that $t_{(abc)} \neq 1$. Let u, v, w be three distinct values in $\{1, 2, \ldots, n\}$. We have the following equations in S_n:

$$(vuw) = (uv)(cw)(bv)(au)(abc)(au)(bv)(cw)(uv), \quad \text{(A1)}$$

$$(uvw) = (cw)(bv)(au)(abc)(au)(bv)(cw). \quad \text{(A2)}$$

Consider the three equations

$$a = u, b = v, c = w. \quad \text{(A3)}$$

We consider four cases:

(i) If none of the equations (A3) hold, then (A1) is an equation in A_n. By Corollary 2, it follows that $t_{(uvw)} = t_{(abc)}^*$.

(ii) If exactly 1 of Eqs. (A3) holds, then (A2) is an equation in A_n. By Corollary 2, it follows that $t_{(uvw)} = t_{(abc)}$.

(iii) If exactly two of Eqs. (A3) hold, then Eq. (A1) is an equation in A_n. By Corollary 2, it follows that $t_{(uvw)} = t_{(abc)}^*$.

(iv) If all three of Eqs. (A3) hold, then we have $(uvw) = (abc)$, and so $t_{(uvw)} = t_{(abc)}$.

Proof of Proposition 5. Let $n \geqslant 5$ and suppose that $|\psi\rangle$ is A_n invariant and not S_n invariant. Let $|\psi\rangle = \sum_I c_I |I\rangle$ be the expansion of $|\psi\rangle$ in the computational basis. Choose I such that $c_I \neq 0$. Because $n \geqslant 5$, there must be three positions u, v, w such that $i_u = i_v = i_w$. By Corollary 2, there must be some 3-cycle (abc) such that $t_{(abc)} \neq 1$. By the discussion immediately preceding the statement of the Proposition, we have $t_{(uvw)} = t_{(abc)}$ or $t_{(uvw)} = t_{(abc)}^*$. In both cases, $t_{(uvw)} \neq 1$. Now $(uvw)I = I$, but $t_{(uvw)}I \neq I$. Thus we must have $c_I = 0$, contradicting our assumption. It follows that the state $|\psi\rangle$ cannot exist.

Another Proof of Proposition 5. Observe that the first two cases listed in the proof of Corollary 3 both lead to contradictions. In place of (A1) and (A2), consider the following equations:

$$(uvw) = (uv)(cw)(bu)(av)(abc)(av)(bu)(cw)(uv), \quad \text{(A4)}$$

$$(vuw) = (cw)(bu)(av)(abc)(av)(bu)(cw), \quad \text{(A5)}$$

that interchange the 3-cycles (uvw), (uwv) on the left. In the first case [none of the equations in (A3) hold], apply (A4) to conclude that $t_{(uvw)} = t_{(abc)}$. But this contradicts the conclusion in the proof to Corollary 3 that $t_{(uvw)} = t_{(abc)}^*$ (because $t_{(abc)} = \omega$, ω^* is not real). Similarly, in the second case [exactly one of the equations in (A3) holds], apply (A5) to conclude that $t_{(uvw)} = t_{(abc)}^*$. This is again a contradiction to the conclusion in Corollary 3 that we have $t_{(uvw)} = t_{(abc)}$. Now we have ruled out the possibility of the first two cases, so it
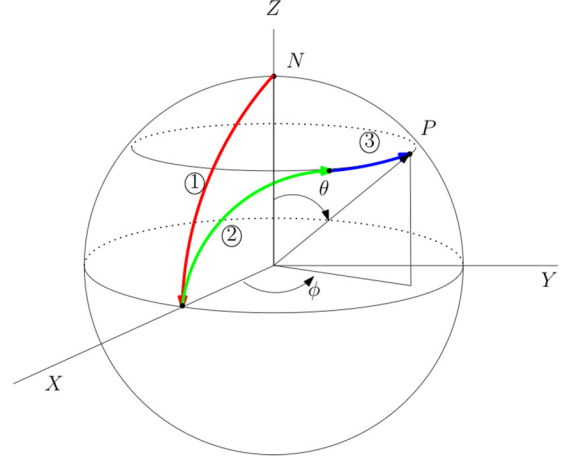

FIG. 4. Moving N to P with rotations ① $= R_{\frac{\pi}{2}, Y}$, ② $= R_{-\frac{\pi}{2}, (\cos(\frac{\pi}{2}-\theta), \sin(\frac{\pi}{2}-\theta), 0)}$, and ③ $= R_{\phi-(\frac{\pi}{2}-\theta), Z}$.

must be that exactly two or three of Eqs. (A3) hold. This in turn implies that $n = 3$ or $n = 4$.

Proof of Theorem 1

We begin with a Lemma about rotations of the unit sphere. We will write $(a, b, c) = (\theta, \phi)_{\text{spherical}}$ to denote the point on the unit sphere with rectangular coordinates (a, b, c) and spherical coordinates (θ, ϕ), that is, $a = \cos \phi \sin \theta$, $b = \sin \phi \sin \theta$, $c = \cos \theta$. We will write $R_{\theta, (a,b,c)}$ to denote the rotation of the sphere by θ radians about the axis determined by the point (a, b, c) on the sphere. We will also write $R_{\theta, Z}$, $R_{\theta, Y}$ to denote the rotations $R_{\theta, (0,0,1)}$, $R_{\theta, (0,1,0)}$, respectively.

Lemma 2. Let (θ, ϕ) be the spherical coordinates of a point P on the sphere, so that

$$P = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta).$$

Let $N = (0, 0, 1)$ and let

$$R = R_{\phi-(\frac{\pi}{2}-\theta), Z} \circ R_{-\frac{\pi}{2}, (\cos(\frac{\pi}{2}-\theta), \sin(\frac{\pi}{2}-\theta), 0)} \circ R_{\frac{\pi}{2}, Y}. \quad \text{(A6)}$$

Then we have

$$R(N) = P.$$

See Fig. 4 .

Proof. We have

$R(N)$

$$= \left(R_{\phi-(\frac{\pi}{2}-\theta), Z} \circ R_{-\frac{\pi}{2}, (\cos(\frac{\pi}{2}-\theta), \sin(\frac{\pi}{2}-\theta), 0)} \circ R_{\frac{\pi}{2}, Y} \right)(N)$$

$$= \left(R_{\phi-(\frac{\pi}{2}-\theta), Z} \circ R_{-\frac{\pi}{2}, (\cos(\frac{\pi}{2}-\theta), \sin(\frac{\pi}{2}-\theta), 0)} \right)(1, 0, 0)$$

$$= R_{\phi-(\frac{\pi}{2}-\theta), Z} \left(\theta, \frac{\pi}{2} - \theta \right)_{\text{spherical}}$$

$$= (\theta, \phi)_{\text{spherical}}$$

$$= P.$$

This proves the Lemma.

Lemma 3. Let $U = e^{i\pi/4(\alpha X + \beta Y)}$, where α, β are real and $\alpha^2 + \beta^2 = 1$, and let $\xi = \alpha + i\beta$. We claim that

$$U^{\otimes 3} |M_3(a, b)\rangle = |M_3(a', b')\rangle,$$

where (a', b') is given by

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & e^{i(\pi/2-\xi-\pi/3)} \\ e^{i(\pi/2+\xi+\pi/3)} & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \quad (A7)$$

Proof of Lemma 3. We have

$$U = \exp[i\pi/4(\alpha X + \beta Y)] = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -e^{-i\phi} \\ e^{i\phi} & 1 \end{bmatrix},$$

where $e^{i\xi} = \alpha + i\beta$, and where $\phi = \xi + \pi/2$. Thus U is the rotation $R_{-\pi/2,(\alpha,\beta,0)}$ of the Bloch sphere (see [17], Exercise 4.6). Using

$$|M_3(a,b)\rangle = \frac{1}{\sqrt{3}}(0, a\omega^2, a\omega, b\omega, a, b\omega^2, b, 0)^T,$$

it is straightforward to check that

$$U^{\otimes 3}|M_3(a,b)\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \omega e^{-i\phi} \\ -\omega^2 e^{i\phi} & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}.$$

Using $\omega = e^{2\pi i/3}$ and $\phi = \xi + \pi/2$, we obtain Eq. (A7).

Lemma 4. Let $U = e^{-i\frac{u}{2}Z}$, where u is a real number. We have

$$U^{\otimes 3}|M_3(a,b)\rangle = |M_3(a',b')\rangle,$$

where (a', b') is given by

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} e^{-iu/2} & 0 \\ 0 & e^{iu/2} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \quad (A8)$$

Proof of Theorem 1. We will exhibit an LU transformation that takes $|M_3(1,0)\rangle$ to $|M_3(a,b)\rangle$ for any (a,b). Let θ, ϕ be spherical coordinates for the point on the Bloch sphere that represents the one-qubit state $a|0\rangle + b|1\rangle$, that is, we have

$$a|0\rangle + b|1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle.$$

Let $U = U_3 U_2 U_1$, where U_1, U_2, U_3 are given by

$$U_3 = \exp\left[\frac{-i}{2}\left(\phi + \theta - \frac{\pi}{2}\right)Z\right], \quad (A9)$$

$$U_2 = \exp\left[i\frac{\pi}{4}\left(\cos\left(\frac{\pi}{6} - \theta\right)X + \sin\left(\frac{\pi}{6} - \theta\right)Y\right)\right], \quad (A10)$$

$$U_1 = \exp\left[-i\frac{\pi}{4}\left(\cos\left(\frac{\pi}{6}\right)X + \sin\left(\frac{\pi}{6}\right)Y\right)\right]. \quad (A11)$$

Applying Lemmas 3 and 4, we have that U acts as the rotation (A6),

$$R = R_{\phi-(\frac{\pi}{2}-\theta),Z} \circ R_{-\frac{\pi}{2},(\cos(\frac{\pi}{2}-\theta),\sin(\frac{\pi}{2}-\theta),0)} \circ R_{\frac{\pi}{2},Y}.$$

Thus, by Lemma 2 we have

$$U^{\otimes 3}|M_3(1,0)\rangle = |M_3(a,b)\rangle,$$

as desired. Now if we are given $|M_3(a',b')\rangle$, use the same construction to choose a unitary V such that

$$V^{\otimes 3}|M_3(1,0)\rangle = |M_3(a',b')\rangle.$$

Now we have the LU equivalence

$$(VU^\dagger)^{\otimes 3}|M_3(a,b)\rangle = |M_3(a',b')\rangle.$$

Finally, we show that $\overline{|M_3(a,b)\rangle}$ is LU equivalent to $|M_3(1,0)\rangle$. Given a, b, construct an LU operator U as above

such that $U|M_3(1,0)\rangle = |M_3(\overline{a},\overline{b})\rangle$. Then apply the LU operator

$$W = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & \omega^2 \end{bmatrix}$$

to obtain the LU equivalence

$$WU|M_3(1,0)\rangle = \overline{|M_3(a,b)\rangle}.$$

Proof of Proposition 9.
Let $G = A_3$, and let $|\psi\rangle = \mathrm{GSym}_t(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle)$ be A_3 invariant but not S_3 invariant and not zero. By Lemma 1 we must have $t_{(123)} \neq 1$. Without loss of generality, suppose that $t_{(123)} = \omega^2 = e^{4\pi i/3}$. If $|\phi_1\rangle = |\phi_2\rangle = |\phi_3\rangle$ (or possibly differing by a global phase factor) then we have

$$|\psi\rangle = \mathrm{GSym}_t(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle) \propto (1 + \omega + \omega^2)|\phi_1\rangle^{\otimes 3} = 0.$$

Conversely, suppose that $|\psi\rangle = 0$. Let

$$|\phi_1\rangle = a|0\rangle + b|1\rangle$$
$$|\phi_2\rangle = c|0\rangle + d|1\rangle$$
$$|\phi_3\rangle = e|0\rangle + f|1\rangle$$

so that we have

$$|\psi\rangle = \mathrm{GSym}_t(a|0\rangle + b|1\rangle, c|0\rangle + d|1\rangle, e|0\rangle + f|1\rangle)$$
$$\propto |M_3(bce + \omega acf + \omega^2 ade, bde + \omega bcf + \omega^2 adf)\rangle.$$

Choosing a unitary operator U so that $U|\phi_1\rangle = |0\rangle$ allows us to set $a = 1$ and $b = 0$ in the above expressions, and we may work with the LU equivalent state $|\psi'\rangle = U^{\otimes 3}|\psi\rangle$ of the form

$$|\psi'\rangle = \mathrm{GSym}_t(|0\rangle, c|0\rangle + d|1\rangle, e|0\rangle + f|1\rangle)$$
$$\propto |M_3(cf + \omega de, \omega df)\rangle.$$

The assumption that $|\psi'\rangle = 0$ implies that $df = 0$. If $d = 0$, then we have $|\psi'\rangle \propto |M_3(cf, 0)\rangle$. Since $c \neq 0$ (otherwise, $|\phi_2\rangle = c|0\rangle + d|1\rangle = 0$ would not be a state), so we have $f = 0$. This implies $|\phi_1\rangle = |\phi_2\rangle = |\phi_3\rangle = |0\rangle$ up to phase. A similar argument works for the case $f = 0$. This completes the proof.

Proof of Proposition 10.
Let $G = A_4$ and let $|\psi\rangle = \mathrm{GSym}_t(|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle)$ be A_4 invariant but not S_4 invariant and not zero. By Lemma 1 we must have $t_{(123)} \neq 1$. Without loss of generality, suppose that $t_{(123)} = \omega = e^{2\pi i/3}$. By Proposition 8 we know that $|\psi\rangle = |M_4\rangle$ or its conjugate, or zero. By the $U(2)^{\otimes 4}$ invariance of $|M_4\rangle$ and its conjugate [12], we may choose a unitary operator U such that $U|\phi_1\rangle = |0\rangle$, so that we have

$$|\psi\rangle = U^{\otimes 4}|\psi\rangle$$
$$= \mathrm{GSym}_t(U|\phi_1\rangle, U|\phi_2\rangle, U|\phi_3\rangle, U|\phi_4\rangle)$$
$$= \mathrm{GSym}_t(|0\rangle, a|0\rangle + b|1\rangle, c|0\rangle + d|1\rangle, e|0\rangle + f|1\rangle).$$

A straightforward calculation yields

$$|\psi\rangle \propto (adf + \omega bde + \omega^2 bcf)|M_4\rangle. \quad (A12)$$

If three of the $|\phi_i\rangle$ are equal up to phase, say (without loss of generality), $|\phi_1\rangle = |\phi_2\rangle = |\phi_3\rangle$, then we have $b = d = 0$. Thus by (A12), we have $|\psi\rangle = 0$. Conversely, if $|\psi\rangle = 0$ then we must have
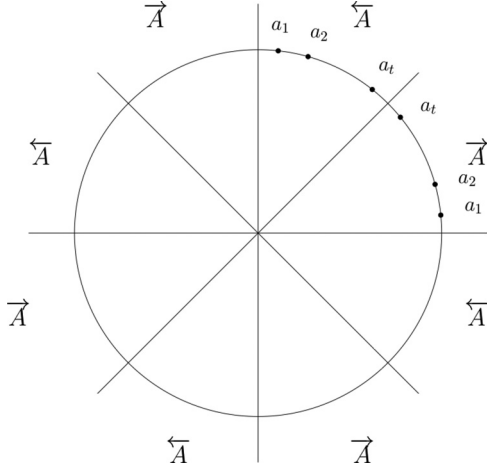
$$adf + \omega bde + \omega^2 bcf = 0.$$

FIG. 5. The cycle order of a necklace diagram is determined by the number of lines of mirror symmetry.

The solutions to this polynomial in the six state coefficients a, b, c, d, e, f is a set of measure zero in $\mathbb{C}^6$.

Proof of Proposition 11. Suppose J is of type SP. Let K be a self-palindromic string in $[J]$, that is, such that $\tau K = K$, and choose ℓ so that $\epsilon^\ell K = J$. Then we have

$$\tau \epsilon^k J = J$$

$$\tau \epsilon^k \epsilon^\ell K = \epsilon^\ell K \quad \text{(substituting } J = \epsilon^\ell K)$$

$$\tau \epsilon^{k+\ell} \tau K = \epsilon^\ell K \quad \text{(using } \tau K = K)$$

$$\epsilon^{-k-\ell} K = \epsilon^\ell K \quad \text{(using } \tau \epsilon \tau = \epsilon^{-1})$$

$$\epsilon^{-k-2\ell} K = K.$$

We must have $m | (k + 2\ell)$, so k is even. Now suppose J is of type CP. Choose $K \in [J]$ such that $\tau K = \epsilon K$. A similar derivation to the one above leads to

$$\epsilon^{-k-2\ell-1} K = K$$

so that $m | (k + 2\ell + 1)$, and therefore k must be odd.

Proof sketch for Proposition 12. In place of a formal proof, we illustrate the case for $L = 4$. The lines of symmetry partition the set of vertices into $2L$ subsets of equal size, say $t = \frac{n}{2L}$, as in Fig. 5. Let $\overrightarrow{A}$ denote the bit string $\overrightarrow{A} = (a_1 a_2 \cdots a_{t-1} a_t)$ in one of the regions between the lines of symmetry, and let $\overleftarrow{A} = (a_t a_{t-1} \cdots a_2 a_1)$ be the reversed bit string. By reflection symmetry, the class of the necklace diagram is $[\underbrace{\overrightarrow{A}\,\overleftarrow{A} \cdots \overrightarrow{A}\,\overleftarrow{A}}_{L \text{ pairs}}]$, and it is clear that the cycle order of the necklace diagram is $2t = n/L$.

Proof of Theorem 2. We begin with the "only if" direction, that is, we suppose $|\psi\rangle$ is D_n invariant, and we will show that properties (i)–(iv) must hold. Note that if $|\psi\rangle$ is D_n invariant with $\sigma |\psi\rangle = s_\sigma |\psi\rangle$ for all $\sigma \in D_n$, then we must have $s_\epsilon = t_\epsilon$ and $s_\tau = \pm 1$.

(i) The equation $\tau \epsilon \tau = \epsilon^{-1}$ in D_n implies that $s_\tau s_\epsilon s_\tau = s_\epsilon^{-1}$, so we have $s_\epsilon^2 = s_\tau^2 = 1$, so $s_\epsilon = t_\epsilon = \pm 1$.

(ii) Suppose there is an I of type SP such that $c_{[I]} \neq 0$. There is a string $J \in [I]$ such that $\tau J = J$, so we must have $s_\tau = 1$.

(iii) Suppose there is an I of type CP such that $c_{[I]} \neq 0$. There is a string $J \in [I]$ such that $\tau J = \epsilon J$, so we must have $s_\tau = s_\epsilon$.

(iv) The equation $c_J = s_\tau c_{\tau J}$ must hold for all J by (7). In particular, it must hold for any such J of chiral type.

Now we prove the "if" direction. Suppose that conditions (i)–(iv) hold. We will show that $|\psi\rangle$ is D_n invariant by showing that $|\psi\rangle$ has the Dicke form

$$|\psi\rangle = \sum_{[I]} d_{[I]} \sum_{J \in [I]} s_g^{-1} |J\rangle \quad \text{(where } gL_{[I]} = J) \quad \text{(A13)}$$

for a homomorphism $s : D_n \to U(1)$ with the property that s is constant on D_n orbits $[I]$ for which $d_{[I]} \neq 0$. Note that $[I]$ denotes the D_n orbit of I in (A13). For I of type SP or CP, the D_n orbit and C_n orbit of I are the same. For I of chiral type, the D_n orbit of I is the union

$$[I]_{D_n} = [I]_{C_n} \cup [\tau I_{C_n}] \quad \text{(A14)}$$

of disjoint C_n orbits.

To show that $|\psi\rangle$ can be written in the form (A13), we start with $|\psi\rangle$ in C_n Dicke form:

$$|\psi\rangle = \sum_{[I]} c_{[I]} \sum_{k=0}^{n-1} t_\epsilon^{-k} |\epsilon^k L_{[I]}\rangle$$

$$= \sum_{[I]\text{SPtype}} \sum_{k=0}^{n-1} t_\epsilon^{-k} |\epsilon^k L_{[I]}\rangle$$

$$+ \sum_{[I]\text{CPtype}} \sum_{k=0}^{n-1} t_\epsilon^{-k} |\epsilon^k L_{[I]}\rangle$$

$$+ \sum_{[I]_{D_n}\text{chiraltype}}$$

$$\left(c_{[I]} \sum_{k=0}^{n-1} t_\epsilon^{-k} |\epsilon^k L_{[I]}\rangle + c_{[\tau I]} \sum_{k=0}^{n-1} t_\tau^{-1} t_\epsilon^{-k} |\tau \epsilon^k \tau L_{[I]}\rangle \right)$$

[using(A4)]

$$= \sum_{[I]\text{SPtype}} \sum_{k=0}^{n-1} t_\epsilon^{-k} |\epsilon^k L_{[I]}\rangle$$

$$+ \sum_{[I]\text{CPtype}} \sum_{k=0}^{n-1} t_\epsilon^{-k} |\epsilon^k L_{[I]}\rangle$$

$$+ \sum_{[I]_{D_n}\text{chiraltype}} c_{[I]} \sum_{k=0}^{n-1} t_\epsilon^{-k} (|\epsilon^k L_{[I]}\rangle + |\tau \epsilon^k \tau L_{[I]}\rangle)$$

[using(iv)].

By Proposition (3), all that remains to be shown is that s_τ can be assigned in a way that guarantees the following condition:

$$\text{if } \tau \epsilon^k J = J \text{ for some } c_{[J]} \neq 0, \text{ then } s_\tau s_\epsilon^k = 1. \quad \text{(A15)}$$

Because $\tau \epsilon^k$ cannot stabilize any J of chiral type, it suffices to show that (A15) holds for J of type SP or CP. We consider cases:

Suppose there is an I of type SP with $c_{[I]} \neq 0$ and a J of type CP with $c_{[J]} \neq 0$. Then by (ii) and (iii), we have $s_\tau = s_\epsilon = 1$, so (A15) holds.

Suppose there is an I of type SP with $c_{[I]} \neq 0$, but there is no J of type CP with $c_{[J]} \neq 0$. By (ii), we have $s_\tau = 1$. If the cycle order of I is odd, then $s_\epsilon = 1$ (s_ϵ is a power of $e^{e\pi i/m}$ for an odd number m, so s_ϵ cannot equal minus 1), so (A15) holds. If the cycle order of I is even, then by Proposition 11 we have that k must be even if $\tau \epsilon^k I = I$, so (A15) holds.

Finally, suppose there is an I of type CP with $c_{[I]} \neq 0$, but there is no J of type SP with $c_{[J]} \neq 0$. By (iii), we have $s_\tau = s_\epsilon$. If the cycle order of J is odd, we have $s_\epsilon = 1$. If the cycle order of I is odd, then $s_\epsilon = 1$, so (A15) holds. If the cycle order of I is even, then by Proposition 11, we have that k must be odd if $\tau \epsilon^k I = I$, so (A15) holds.

This concludes the proof of the Theorem.

Proof of Proposition 14. We begin with the "only if" direction, that is, we suppose $|\psi\rangle$ is S_n invariant with $\sigma|\psi\rangle = s_\sigma|\psi\rangle$ for all $\sigma \in S_n$. Proposition 2 states that if $|\psi\rangle$ is S_n invariant where $n \geqslant 3$, then $t_\sigma = 1$ for all $\sigma \in S_n$. So, we know that $t_\epsilon = t_\tau = 1$. Since $|\psi\rangle$ is S_n invariant, all terms of the same weight must share the same coefficient, otherwise a series of transpositions would be unable to take one term to the other while also accounting for this coefficient shift. Thus we can conclude $C_{[I]} = C_{[J]}$ for all I, J with $\text{wt}I = \text{wt}J$.

Now looking at the "if" direction, we suppose that the two statements hold to prove that $|\psi\rangle$ is S_n invariant. Let C_w be the common value of $C_{[I]}$ for all I with weight w, then

$$|\psi\rangle = \sum_{[I]} C_{[I]} \sum_{J \in [I]} t_g^{-1}|J\rangle$$
$$= \sum_{[I]} C_{[I]} \sum_{J \in [I]} |J\rangle \quad \text{[using (i)]}$$
$$= \sum_{w=0}^{n} C_w \sum_{\text{wt}J=w} |J\rangle.$$

Evidently, this is the Dicke form for an S_n-invariant state, thus completing the proof.

Proof of Proposition 15. The proof is the same as the proof for Theorem 1 in [8], with the observation that full permutational symmetry may be replaced by cyclic symmetry in places where symmetry is needed. We will not reproduce the full proof here, which requires lengthy technical preliminaries. Instead we provide a sketch of the main ideas.

Let $|D^w\rangle$ denote a generalized Dicke state $|D_t^{[I]}\rangle$ for some bit string I with $\text{wt}I = w$, for $G = S_n$, $G = C_n$, or $G = D_n$. It does not matter whether the phase homomorphism $t : G \rightarrow U(1)$ is trivial, and it does not matter what particular G-orbit class is for I. Every part of the proof depends only on the weight of I and on the fact that D^w has at least cyclic symmetry.

From the observation that

$$(e^{itZ})^{\otimes n}|D^w\rangle = e^{it(n-2w)}|D^w\rangle$$

we have that the group

$$\{e^{it(2w-n)}((e^{itZ})^{\otimes n} : t \in \mathbb{R}\} \tag{A16}$$

is contained in the local unitary stabilizer Stab_{D^w}. We view the local unitary group as the Lie group $U(1) \times SU(2)^n$, with Lie algebra $u(1) \oplus \bigoplus_{j=1}^{n} su(2)$, where $u(1)$ is the real vector space $u(1) = \{it : t \in \mathbb{R}\}$ and $su(2)$ is the real vector space of traceless skew-Hermitian matrices. The Lie algebra of (A16) is the real vector space

$$\{it[(2w-n) + Z^{(1)} + Z^{(2)} + \cdots + Z^{(n)}] : t \in \mathbb{R}\} \tag{A17}$$

so that (A17) is a subspace of the Lie algebra of the group Stab_{D^w}. The notation $Z^{(k)}$ denotes the Pauli Z operator acting on the kth qubit. The heart of the proof is an argument that in fact, (A17) is the entire Lie algebra of Stab_{D^w}. The idea is that if there were some stabilizer Lie algebra element $is + \sum_{k=1}^{n} M_k^{(k)}$ with M_k independent of Z, then there would also be an element in the stabilizer Lie algebra with $[M_k, Z]$ in the kth summand, and therefore the projection of the stabilizer Lie algebra in the kth position would be three dimensional. By the cyclic symmetry of D^w, it would follow that the projection of the stabilizer Lie algebra would be three dimensional in all qubits. But we have classified all possible states whose Lie algebra stabilizers have three-dimensional projections in each qubit (these states are superpositions of products of singlet states, see [18]), and these states are *not* local unitary equivalent to D^w. Thus it must be that (A17) is all of the Lie algebra of Stab_{D^w} and therefore that (A16) is all of the connected component of Stab_{D^w} that contains the identity.

Now suppose that there is some local unitary operator $U = U_1 \otimes U_2 \otimes \cdots \otimes U_n$, for some 2×2 unitary operators $U_1, U_2, \ldots, U_n$, that takes $|D^w\rangle$ to $|D^{w'}\rangle$. It follows that $\text{Stab}_{D^{w'}} = U\text{Stab}_{D^w}U^\dagger$. For each k we must have $U_k Z U_k^\dagger \propto Z$. It is a simple exercise to see that this implies $U_k = \pm I, \pm X$ and therefore $U_k Z U_k^\dagger = \pm Z$. It turns out that all of the U_k must be equal, so we have

$$U(it(2w-n) + Z^{(1)} + \cdots + Z^{(n)})U^\dagger$$
$$= it(2w-n) \pm (Z^{(1)} + \cdots + Z^{(n)}). \tag{A18}$$

In the case where the last expression (A18) is

$$it(2w-n) + (Z^{(1)} + \cdots + Z^{(n)}),$$

we conclude that $w' = w$, and in the case where the last expression (A18) is

$$it(2w-n) - (Z^{(1)} + \cdots + Z^{(n)}),$$

we conclude that $w' = n - w$. This completes the sketch of the proof.

---

[1] D. A. Meyer and N. R. Wallach, Global entanglement in multiparticle systems, J. Math. Phys. **43**, 4273 (2002).

[2] M. Aulbach, D. Markham, and M. Murao, The maximally entangled symmetric state in terms of the geometric measure, New J. Phys. **12**, 073025 (2010).

[3] M. Aulbach, D. Markham, and M. Murao, Geometric entanglement of symmetric states and the Majorana representation, in *Proceedings of TQC 2010*, Lecture Notes in Computer Science (Springer, Berlin, 2010).

[4] D. J. H. Markham, Entanglement and symmetry in permutation symmetric states, Phys. Rev. A **83**, 042332 (2011).

[5] G. Toth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, and H. Weinfurter, Permutationally Invariant Quantum Tomography, Phys. Rev. Lett. **105**, 250403 (2010).

[6] T. Bastin, S. Krins, P. Mathonet, M. Godefroid, L. Lamata, and E. Solano, Operational Families of Entanglement Classes for Symmetric *n*-Qubit States, Phys. Rev. Lett. **103**, 070503 (2009).

[7] T. Bastin, P. Mathonet, and E. Solano, Operational entanglement families of symmetric mixed *n*-qubit states, Phys. Rev. A **91**, 022310 (2015).

[8] C. D. Cenci, D. W. Lyons, L. M. Snyder, and S. N. Walck, Symmetric states: Local unitary equivalence via stabilizers, Quantum Inf. Comput. **10**, 1029 (2010).

[9] C. D. Cenci, D. W. Lyons, and S. N. Walck, Local unitary group stabilizers and entanglement for multiqubit symmetric states, edited by Dave Bacon, Miguel Martin-Delgado, and Martin Roetteler, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science Vol. 6745 (Springer, Berlin, 2014), pp. 198–207.

[10] A. Burchardt, J. Czartowski, and K. Życzkowski, Entanglement in highly symmetric multipartite quantum states, Phys. Rev. A **104**, 022426 (2021).

[11] A. Higuchi and A. Sudbery, How entangled can two couples get? Phys. Lett. A **273**, 213 (2000).

[12] D. W. Lyons, S. N. Walck, and S. A. Blanda, Classification of nonproduct states with maximum stabilizer dimension, Phys. Rev. A **77**, 022309 (2008).

[13] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. (Prentice Hall, Englewood Cliffs, NJ, 1991).

[14] J. A. Gallian, *Contemporary Abstract Algebra*, 9th ed. (Cengage Learning, Boston, MA, 2017).

[15] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, Local unitary symmetries of hypergraph states, J. Phys. A: Math. Theor. **48**, 095301 (2015).

[16] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties, Phys. Rev. Lett. **108**, 260502 (2012).

[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[18] D. W. Lyons and S. N. Walck, Multiparty quantum states stabilized by the diagonal subgroup of the local unitary group, Phys. Rev. A **78**, 042314 (2008).