Efficient Verification of Phased Dicke States

Zihao Li,1, 2 Yun-Guang Han,1, 2 Hao-Feng Sun,1, 2 Jiangwei Shang,3 and Huangjun Zhu1, 2, 4, 5, ∗

1 Department of Physics and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China
2 State Key Laboratory of Surface Physics, Fudan University, Shanghai 200433, China
3 Key Laboratory of Advanced Optoelectronic Quantum Architecture and Measurement of Ministry of Education, School of Physics, Beijing Institute of Technology, Beijing 100081, China
4 Institute for Nano electronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China
5 Collaborative Innovation Center of Advanced Microstructures, Nanjing 210093, China
(Dated: April 16, 2020)

Dicke states are typical examples of quantum states with genuine multipartite entanglement. They are valuable resources in many quantum information processing tasks, including multiparty quantum communication and quantum metrology. Phased Dicke states are a generalization of Dicke states and include antisymmetric basis states as a special example. These states are useful in atomic and molecular physics besides quantum information processing. Here we propose practical and efficient protocols for verifying all phased Dicke states, including W states and qudit Dicke states. Our protocols are based on adaptive local projective measurements with classical communication, which are easy to implement in practice. The number of tests required increases only linearly with the number n of parties, which is exponentially more efficient than traditional tomographic approaches. In the case of W states, the number of tests can be further reduced to O(√n). Moreover, we construct an optimal protocol for any antisymmetric basis state; the number of tests required decreases (rather than increases) monotonically with n. This is the only optimal protocol known for multipartite nonstabilizer states.

I. INTRODUCTION

Quantum states with genuine multipartite entanglement (GME) play crucial roles in quantum information processing and foundational studies [1–2]. Dicke states [3, 4] are one of the most important multipartite quantum states other than stabilizer states. They are useful in many quantum information processing tasks, such as multiparty quantum communication and quantum metrology [5–11]. Phased Dicke states are a generalization of Dicke states constructed by introducing phase changes and they are equally useful in the above research areas [12–13]. Besides the usual Dicke states, antisymmetric basis states are a prominent example of phased Dicke states [14–16]; they are usually used to represent the fermions, and play a paramount role in atomic and molecular physics. By now numerous experiments have been performed to prepare and engineer Dicke states [9–11, 17–19], phased Dicke states [13–20], and antisymmetric basis states [21–22] in various platforms.

In practice, it is usually extremely difficult to prepare quantum states with GME perfectly, and the success probability decays rapidly with the number of particles. Therefore, it is crucial to verify these states with high precision efficiently using limited resources. For the convenience of applications, it is also desirable to achieve this task using only local operations and classical communication (LOCC). Unfortunately, traditional tomographic approaches are notoriously inefficient and are too resource consuming for systems with more than 10 qubits [19]. Although direct fidelity estimation [23] can improve the efficiency significantly, it is still not satisfactory except for some special states, like stabilizer states. Recently, an alternative approach known as quantum state verification [24–30] has attracted increasing attention because of its potential to achieve a much higher efficiency. So far efficient verification protocols based on LOCC have been constructed for bipartite pure states [31–33], stabilizer states (including graph states) [28, 30, 31–34], hypergraph states [35], weighted graph states [36], and qudit Dicke states [37]. On the other hand, efficient protocols are still not available for many other important quantum states, including Dicke states in particular. In addition, it is extremely difficult to construct optimal verification protocols, especially for nonstabilizer states. So far optimal protocols under LOCC are known only for maximally entangled states [24–25, 38], two-qubit pure states [32], and Greenberger-Horne-Zeilinger (GHZ) states [39]. Any progress on this topic is of interest to both theoretical studies and practical applications.

In this work, we construct highly efficient and practical verification protocols for all phased Dicke states, including W states and qudit Dicke states. Our protocols only require adaptive local projective measurements and are thus easy to realize with current technologies. The number of tests required increases only linearly with the number n of parties, which is exponentially more efficient than traditional approaches, including tomography and direct fidelity estimation. In the case of W states, the number of tests can be further reduced to O(√n), which is quadratically fewer compared with the best verification protocol known in the literature [37]. For the three-qubit W state, one of our protocols is almost optimal under LOCC; in addition, the protocol is useful for fidelity esti-
mation because the verification operator is homogeneous \cite{30}. Moreover, we construct an optimal verification protocol for any antisymmetric basis state; the number of tests required decreases monotonically with $n$. This is the only optimal protocol known for multipartite nonstabilizer states. For quantum states with GME, such optimal protocols are known previously only for GHZ states \cite{39}, which are stabilizer states and have Schmidt decomposition. In the course of study, we introduce several tools for improving the efficiency of a given verification protocol, which are useful to studying quantum verification in general.

II. PURE STATE VERIFICATION

A. Basic framework

Before presenting our main results, let us take a brief review on the basic framework of pure state verification \cite{28,30}. Suppose there is a quantum device that is expected to produce the pure target state $|\Psi\rangle \in \mathcal{H}$. However, some errors may occur when the device is working, and it actually produces the states $\sigma_1, \sigma_2, \ldots, \sigma_N$ in $N$ runs. Let $\epsilon_j := 1 - \langle \Psi | \sigma_j | \Psi \rangle$ denote the infidelity between $\sigma_j$ and the target state, and $\bar{\epsilon} := \sum_j \epsilon_j / N$ denote the average infidelity. Our aim is to verify whether these states are sufficiently close to the target state on average, that is, whether the average infidelity $\bar{\epsilon}$ is smaller than some threshold $\epsilon$.

To achieve this task, for each state $\sigma_j$ the verifier performs a test and accepts the states produced if and only if (iff) all tests are passed. Each test is specified by a two-outcome measurement $\{E_l, \mathbb{1} - E_l\}$, which is chosen randomly with probability $p_l$ from a set of accessible measurements. Here the test operator $E_l$ corresponds to passing the test and satisfies the condition $E_l |\Psi\rangle = |\Psi\rangle$, so that the target state can always pass the test. If the infidelity of $\sigma_j$ satisfies $\epsilon_j \geq \bar{\epsilon}$ for some threshold $\bar{\epsilon} \geq 0$, then the maximum probability that $\sigma_j$ can pass each test on average is given by \cite{28,30}

$$\max_{\langle \Psi | \sigma | \Psi \rangle \leq 1 - \bar{\epsilon}} \text{tr}(\Omega \sigma) = 1 - \ln \frac{\delta}{1 - \nu(\Omega) \epsilon} = 1 - \nu(\Omega) \bar{\epsilon},$$

where $\Omega := \sum_l p_l E_l$ is called the verification operator or a strategy, $\lambda_2(\Omega)$ denotes the second largest eigenvalue of $\Omega$, and $\nu(\Omega) := 1 - \lambda_2(\Omega)$ is the spectral gap from the maximum eigenvalue. The probability of passing all $N$ tests is at most $\prod_j [1 - \nu(\Omega) \epsilon_j] \leq [1 - \nu(\Omega) \bar{\epsilon}]^N$. To ensure the condition $\bar{\epsilon} < \epsilon$ with significance level $\delta$, it suffices to take \cite{28,30}

$$N = \left\lceil \frac{\ln \delta}{\ln [1 - \nu(\Omega) \bar{\epsilon}]} \right\rceil \approx \frac{\ln \delta}{\nu(\Omega) \bar{\epsilon}},$$

where the approximation is applicable when $\nu(\Omega) \bar{\epsilon} \ll 1$. According to this equation, the efficiency of a verification strategy $\Omega$ is mainly determined by its spectral gap $\nu(\Omega)$.

B. Optimization of test probabilities

To optimize the verification efficiency, we need to maximize the spectral gap of the verification operator for the target state $|\Psi\rangle$ or minimize the second largest eigenvalue. Suppose the set of test operators $\{E_l\}$ for $|\Psi\rangle$ is fixed, then we need to optimize the probabilities for performing individual tests. Given a general verification operator of the form $\Omega = \sum_l p_l E_l$, the second largest eigenvalue of $\Omega$ reads

$$\lambda_2(\Omega) = \|\Omega\| = \left\| \sum_l p_l E_l \right\|,$$

where $\| \cdot \|$ denotes the operator norm and

$$\bar{\Omega} := \Omega - |\Psi\rangle \langle \Psi|, \quad E_l := E_l - |\Psi\rangle \langle \Psi|. \quad (4)$$

Note that $\lambda_2(\Omega)$ is convex in $\{p_l\}$, so that $\nu(\Omega)$ is concave in $\{p_l\}$. In addition, the minimum of $\lambda_2(\Omega)$ over $\{p_l\}$ can be computed via semidefinite programming,

$$\min_{f} \quad \frac{f}{\nu}$$

subject to $\sum_l p_l E_l \leq f \mathbb{1}, \quad p_l \geq 0,$

$$\sum_l p_l = 1.$$ (5)

The minimum in Eq. (5) can be derived analytically when $\Omega$ consists of two projective tests thanks to the following lemma, which is proved in Appendix A.

Lemma 1. Suppose $\Omega = p E_1 + (1 - p) E_2$, where $0 \leq p \leq 1$ and $P_1, P_2$ are test projectors for $|\Psi\rangle$ with ranks at least 2. Then $\lambda_2(\Omega) \geq (1 + \sqrt{q}) / 2$ and $\nu(\Omega) \leq (1 - \sqrt{q}) / 2$, where

$$q := \| P_1 \bar{P}_2 \bar{P}_1 \| = \max_{\phi \in \text{supp}(\bar{P}_1)} \langle \phi | P_2 | \phi \rangle. \quad (6)$$

If $q < 1$, then the upper bound for $\nu(\Omega)$ is saturated iff $p = 1 / 2$.

Note that any test projector based on LOCC has rank at least 2 if $|\Psi\rangle$ is entangled. Previously, Lemma 1 is known in the special case in which $P_1$ and $P_2$ are orthogonal \cite{35}.

C. Symmetrization of verification operators

Here we consider another recipe for improving the verification efficiency by employing the symmetry of the target state $|\Psi\rangle$; similar ideas have already found applications in verifying bipartite pure states \cite{28,32,33}. Suppose $\Omega$ is a verification operator for $|\Psi\rangle$, so that $\Omega \geq |\Psi\rangle \langle \Psi|$, and $\| \Omega - |\Psi\rangle \langle \Psi| \| \leq \lambda_2(\Omega)$. Let $U$ be a unitary operator that leaves $|\Psi\rangle$ invariant up to a phase factor, that is, $U |\Psi\rangle \langle U^\dagger = |\Psi\rangle \langle \Psi|$ or, equivalently, $U |\Psi\rangle = e^{i \phi} |\Psi\rangle$.
where $\phi$ is a phase (a real number). Then $U\Omega U^\dagger$ is also a valid verification operator for $|\Psi\rangle$. Moreover, $U\Omega U^\dagger$ and $\Omega$ have the same spectral gap, that is,\
\[ \nu(U\Omega U^\dagger) = \nu(\Omega). \tag{7} \]

Let $G$ be the group generated by product unitaries and permutations that leave $|\Psi\rangle/|\Psi\rangle$ invariant. Then $U\Omega U^\dagger$ can be realized by LOCC (is separable) iff $\Omega$ can be realized by LOCC (is separable) for any $U \in G$. Let $S$ be a subset of $G$ and define\
\[ \Omega^S := \int_S U\Omega U^\dagger dU, \tag{8} \]
where the integral is taken with respect to the normalized probability measure induced from the Haar measure (see Chapter 11 in Ref. [40] for example) on $G$. The measure reduces to the normalized Haar measure on $S$ when $S$ is a group and reduces to the counting measure (see page 27 in Ref. [41] for example) when $S$ is finite. The verification operator $\Omega$ is called $S$-invariant if $\Omega^S = \Omega$.

If the verification strategy $\Omega$ consists of $m$ distinct tests and has the form $\Omega = \sum_j p_j E_j$, then\
\[ \Omega^S = \sum_j p_j E^S_j, \tag{9} \]
where\
\[ E^S_j := \int_S UE_j U^\dagger dU. \tag{10} \]

If $S$ is a finite set with cardinality $|S|$, then the above equation reduces to\
\[ E^S_j = \frac{1}{|S|} \sum_{U \in S} UE_j U^\dagger. \tag{11} \]

If each test operator $E_j$ is a projector, then each $E^S_j$ can be realized by at most $|S|$ distinct projective tests. Therefore, $\Omega^S$ can be realized by at most $m|S|$ distinct projective tests.

**Proposition 1.** Suppose $S \subseteq H \leq G$. Then\
\[ \nu(\Omega) \leq \nu(\Omega^S) \leq \nu(\Omega^H) \leq \nu(\Omega^G). \tag{12} \]

Here the notation $S \subseteq H$ means $S$ is a subset of $H$; by contrast, the notation $H \leq G$ means $H$ is a subgroup of $G$. Proposition 1 shows that symmetrization is an effective way for improving the verification efficiency.

**Proof.** The inequality $\nu(\Omega) \leq \nu(\Omega^S)$ follows from Eq. (7) and the fact that $\nu(\Omega)$ is concave in $\Omega$. The inequality $\nu(\Omega^S) \leq \nu(\Omega^H)$ follows from the inequality $\nu(\Omega) \leq \nu(\Omega^S)$ and the fact that $\Omega^H = (\Omega^S)^H$ given that $S$ is a subset of the group $H$. The inequality $\nu(\Omega^H) \leq \nu(\Omega^G)$ follows from the inequality $\nu(\Omega^S) \leq \nu(\Omega^H)$.

The following proposition is useful to reducing the number of distinct tests when constructing a verification strategy based on the symmetrization procedure. It is a corollary of Eq. (14) below.

**Proposition 2.** Suppose $S \leq H \leq G$; in addition, $S$ and $H$ have the same number of irreducible components. Then $\Omega^S = \Omega^H$ and $\nu(\Omega^S) = \nu(\Omega^H)$.

Suppose $S$ is a subgroup of $G$ and has $r$ inequivalent irreducible components with dimensions $d_j$ and multiplicities $m_j$, respectively (here we view $S$ as a representation of itself). Then the Hilbert space $\mathcal{H}$ decomposes into\
\[ \mathcal{H} = \bigoplus_{j=1}^r \mathcal{H}_j \otimes \mathcal{C}^{m_j}, \tag{13} \]
where $\mathcal{H}_j$ has dimension $d_j$ and carries the $j$th irreducible representation, and $\mathcal{C}^{m_j}$ denotes the multiplicity space. Let $Q_j$ be the projector onto $\mathcal{H}_j \otimes \mathcal{C}^{m_j}$, then\
\[ \Omega^S = \sum_{j=1}^r \frac{1}{d_j} [\mathbb{1}_{\mathcal{H}_j} \otimes \text{tr}_{\mathcal{H}_j}(Q_j \Omega)] Q_j, \tag{14} \]
where $\text{tr}_{\mathcal{H}_j}$ means the partial trace over $\mathcal{H}_j$ (cf. the appendix of Ref. [42]). If all irreducible components of $S$ are inequivalent, that is, $m_j = 1$ for $j = 1, 2, \ldots, r$, then Eq. (14) reduces to\
\[ \Omega^S = \sum_{j=1}^r \frac{\text{tr}(Q_j \Omega)}{d_j} Q_j, \tag{15} \]
where $Q_j$ is the projector onto the $j$th irreducible component. In this case, all $S$-invariant verification operators commute with each other.

### III. Verification of Qudit Dicke States

In this section we construct an efficient protocol for verifying general qudit Dicke states [3]. Previously, efficient protocols are known only for qubit Dicke states [37].

#### A. Dicke states

Up to a local unitary transformation, each $n$-qudit Dicke state can be labeled by a sequence of ordered positive integers that sum up to $n$. Let\
\[ k := (k_0, k_1, \ldots, k_r), \tag{16} \]
where $k_0, k_1, \ldots, k_r$ are positive integers that satisfy the conditions $\sum_{j=0}^r k_j = n$ and $k_0 \geq k_1 \geq \cdots \geq k_r \geq 1$. Denote by $B(k)$ the set of all sequences of $n$ symbols in which $k_i$ symbols are equal to $i$ for $i = 0, 1, \ldots, r$. Then
the \( n \)-partite Dicke state corresponding to the sequence \( \mathbf{k} \) has the form
\[
|D(\mathbf{k})\rangle = \frac{1}{\sqrt{m}} \sum_{u \in B(\mathbf{k})} |u\rangle,
\]
where \( m := |B(\mathbf{k})| = n!/(\prod_{j=0}^{s} k_j)! \). For example, the Dicke state corresponding to the sequence \( \mathbf{k} = (1,1,1) \) reads
\[
|D(\mathbf{k})\rangle = \frac{1}{\sqrt{6}} (|012\rangle + |021\rangle + |102\rangle + |120\rangle + |201\rangle + |210\rangle).
\]
(18)

To avoid trivial cases, we assume that \( n \geq 3 \) and \( k_0 < n \) in the rest of this paper unless it is stated otherwise.

When \( r = 1 \), \( |D(\mathbf{k})\rangle \) is a familiar qubit Dicke state. If in addition \( k_1 = 1 \), then the Dicke state reduces to a \( W \) state \[11\],
\[
|W_n\rangle = \frac{1}{\sqrt{n}} \sum_{u \in B_n^1} |u\rangle,
\]
where \( B_n^1 \) is the set of strings in \( \{0,1\}^n \) with Hamming weight 1. In particular, the three-qubit \( W \) state (\( n=3 \)) reads
\[
|W_3\rangle = \frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle).
\]
(20)

Denote by \( S \) the group of all permutations of the \( n \) parties (realized as unitary transformations); denote by \( H \) the group of all unitary transformations of the form \( U^\otimes n \), where \( U \) is diagonal in the computational basis; let \( G = SH = HS \). The Dicke state \( |D(\mathbf{k})\rangle \) is invariant under any permutation of the \( n \) parties and is thus invariant under the action of \( S \). In addition, it is invariant (up to an overall phase factor) under any unitary transformation in \( H \) or \( G \). These observations are instructive to constructing efficient protocols for verifying the state \( |D(\mathbf{k})\rangle \). Given any verification operator \( \Omega \) for \( |D(\mathbf{k})\rangle \), we can construct potentially more efficient verification operators \( \Omega^H \), \( \Omega^S \), \( \Omega^G \) according to Eq. \[8\] and Proposition \[14\].

B. Efficient verification of qudit Dicke states

To construct an efficient protocol for verifying the Dicke state \( |D(\mathbf{k})\rangle \) defined in Eq. \[17\], it is convenient to introduce some additional notations. Let
\[
\mathbf{k}_{s} := (k_0,\ldots,k_s + 1,\ldots,k_{t} - 1,\ldots,k_r),
\]
(21)
\[
\mathbf{k}_{st} := (k_0,\ldots,k_s - 1,\ldots,k_{t} - 1,\ldots,k_r),
\]
(22)
\[
\mathbf{k}_{ss} := (k_0,\ldots,k_s - 2,\ldots,k_{t}) \quad \text{for } k_s \geq 2.
\]
(23)
Here we assume that \( 0 \leq s, t \leq r \) and \( s \neq t \) in Eq. \[21\], \( 0 \leq s < t \leq r \) in Eq. \[22\], and \( 0 \leq s \leq r \) in Eq. \[23\]. Now the sets \( B(\mathbf{k}_{s}), B(\mathbf{k}_{st}), \) and \( B(\mathbf{k}_{ss}) \) can be defined in the same way as \( B(\mathbf{k}) \).

Our verification protocol consists of \( \binom{n}{2} \) distinct tests performed with uniform probabilities. Each test is associated with a pair of parties among the \( n \) parties and is based on adaptive local projective measurements. To be specific, the test \( P_{s,t,j} \) associated with parties \( i \) and \( j \) is illustrated in Fig. \[1\] and realized as follows. All \( n-2 \) parties other than parties \( i \) and \( j \) perform the generalized Pauli-Z measurement, and send the outcome \( u \) to parties \( i \) and \( j \). Conditioned on this outcome, parties \( i \) and \( j \) then perform suitable projective measurements. The outcomes corresponding to passing the test are marked by \( \checkmark \).

1. \( u \in B(\mathbf{k}_{s}) \) with \( 0 \leq s \leq g \). In this case, the normalized reduced state of parties \( i \) and \( j \) reads \( |s\rangle_i |s\rangle_j \) (if the target Dicke state is measured). Then the two parties both perform \( Z \) measurement, and the test is passed if they both obtain outcome \( s \).

2. \( u \in B(\mathbf{k}_{st}) \) with \( 0 \leq s < t \leq r \). In this case, the normalized reduced state of parties \( i \) and \( j \) reads \( \frac{1}{\sqrt{2}} (|s\rangle_i |t\rangle_j + |t\rangle_i |s\rangle_j) \). Then the two parties both perform the projective measurement

FIG. 1. Schematic view of the test \( P_{s,t,j} \) used to verify the Dicke state \( |D(\mathbf{k})\rangle \). All \( n-2 \) parties other than parties \( i \) and \( j \) first perform the generalized Pauli-Z measurement, and send the outcome \( u \) to parties \( i \) and \( j \). Conditioned on this outcome, parties \( i \) and \( j \) then perform suitable projective measurements. The outcomes corresponding to passing the test are marked by \( \checkmark \).
TABLE I. The efficiencies of various verification strategies for the $n$-qubit $W$ state, three-qubit $W$ state, $n$-partite Dicke states, phased Dicke states, and antisymmetric basis state. Here $\nu(\Omega)$ denotes the spectral gap of each strategy, and $N(\epsilon, \delta, \Omega)$ denotes the number of tests required to verify the target state within infidelity $\epsilon$ and significance level $\delta$. In addition, the coefficients $a$ and $b$ read $a = \sqrt{\pi/2} \tanh(\pi/2) \approx 1.15$ and $b = \sqrt{\pi/2} \coth(\pi/2) \approx 1.37$.

| Strategy | $\nu(\Omega)$ | $N(\epsilon, \delta, \Omega)$ |
|----------|---------------|-----------------------------|
| $\Omega_W$ ($n \gg 1$, $n$ is odd) | $b/(4\sqrt{n})$ | $4\sqrt{n}(be)^{-1} \ln \delta^{-1}$ |
| $\Omega_W$ ($n \gg 1$, $n$ is even) | $a/(4\sqrt{n})$ | $4\sqrt{n}(ae)^{-1} \ln \delta^{-1}$ |
| $\Omega_W^\phi$ ($n \gg 1$, $n$ is odd) | $b/\sqrt{n}$ | $\sqrt{n}(be)^{-1} \ln \delta^{-1}$ |
| $\Omega_W^\phi$ ($n \gg 1$, $n$ is even) | $a/\sqrt{n}$ | $\sqrt{n}(ae)^{-1} \ln \delta^{-1}$ |
| $\Omega_1$ ($n = 3$) | 0.305 | 3.28$e^{-1} \ln \delta^{-1}$ |
| $\Omega_1$ ($n = 3$) | 5/8 | $(8/5)e^{-1} \ln \delta^{-1}$ |
| $\Omega_k$ and $\Omega_k^\phi$ ($k = (2, 1)$) | 1/3 | $3e^{-1} \ln \delta^{-1}$ |
| $\Omega_k$ and $\Omega_k^\phi$ ($k \neq (2, 1)$) | 1/$(n - 1)$ | $(n - 1)e^{-1} \ln \delta^{-1}$ |
| $\Omega_{AS}$ | 1/$(n - 1)$ | $(n - 1)e^{-1} \ln \delta^{-1}$ |
| $\Omega_{AS}^\phi$ | $n/$(n + 1) | $(n + 1)n^{-1}e^{-1} \ln \delta^{-1}$ |

\[ \{T_{s,t}^+, T_{s,t}^-, I - T_{s,t}^+ - T_{s,t}^-\} \], where $I$ is the identity operator for one qubit and

\[ T_{s,t}^+ = \frac{1}{2}(|s\rangle + |t\rangle)(|s\rangle + |t\rangle), \tag{24} \]

\[ T_{s,t}^- = \frac{1}{2}(|s\rangle - |t\rangle)(|s\rangle - |t\rangle). \tag{25} \]

The test is passed if they both obtain the first outcome (corresponding to $T_{s,t}^+$) or if they both obtain the second outcome (corresponding to $T_{s,t}^-$).

3. Other cases.

The state cannot be the target state $|D(k)\rangle$, so the test is not passed.

The resulting test projector reads

\[ P_{ij} = \sum_{s=0}^g \tilde{Z}_{ij}(k_{s,t}) \otimes (|s\rangle \langle s|)^{\otimes 2}_{i,j} \]

\[ + \sum_{s<t} \tilde{Z}_{ij}(k_{s,t}) \otimes (T_{s,t}^+)^{\otimes 2} + (T_{s,t}^-)^{\otimes 2}_{i,j}, \tag{26} \]

where

\[ \tilde{Z}_{ij}(k_{s,t}) = \sum_{u \in B(k_{s,t})} |u\rangle \langle u|, \tag{27} \]

\[ \tilde{Z}_{ij}(k_{s,t}) = \sum_{u \in B(k_{s,t})} |u\rangle \langle u|. \tag{28} \]

Here the subscripts $i, j$ and the overbar indicate that the operators $\tilde{Z}_{ij}(k_{s,t})$ and $\tilde{Z}_{ij}(k_{s,t})$ act on the $n - 2$ parties other than $i$ and $j$. By contrast, the subscripts $i, j$ in $[|s\rangle \langle s|)^{\otimes 2}_{i,j}$ and $[(T_{s,t}^+)^{\otimes 2} + (T_{s,t}^-)^{\otimes 2}_{i,j}$ indicate that these operators act on parties $i$ and $j$. We perform each test with probability $1/(\binom{n}{2})$, and the resulting verification operator reads

\[ \Omega_k = \left(\frac{n}{2}\right)^{-1} \sum_{i<j} P_{i,j}. \tag{29} \]

The efficiency of this protocol is guaranteed by the following theorem, which is proved in Appendix B. The result is summarized in Table I and illustrated in Fig. 2.

Here it is worth pointing out that the spectral gap of $\Omega_k$ is closely related to the spectrum of the transposition graph [43, 44], which is of interest to some researchers beyond quantum information science.

**Theorem 3.** The spectral gap of $\Omega_k$ reads

\[ \nu(\Omega_k) = \begin{cases} 
1/2 & \text{k = (1, 1, 1)}, \\
1/3 & \text{k = (2, 1),} \\
1/(n - 1) & n \geq 4.
\end{cases} \tag{30} \]

To verify the Dicke state $|D(k)\rangle$ within infidelity $\epsilon$ and...
significance level $\delta$, the number of tests required reads

$$N(\epsilon, \delta, \Omega_k) \approx \begin{cases} 2e^{-1} \ln \delta^{-1} & k = (1, 1, 1), \\ 3e^{-1} \ln \delta^{-1} & k = (2, 1), \\ (n-1)e^{-1} \ln \delta^{-1} & n \geq 4. \end{cases}$$

(31)

By construction $\Omega_k$ is invariant under any permutation of the $n$ parties; actually we have $\Omega_k = P_{T2}^G$, where $S$ is the group of all permutations of the $n$ parties. Therefore, $\Omega_k^S = \Omega_k$ and $\Omega_k^G = \Omega_k^H$, where $G = HS$, and $H$ is the group of all diagonal unitary operators of the form $U^\otimes n$. As shown in Appendix C, the spectral gap of $\Omega_k^G$ reads

$$\nu(\Omega_k^G) = \frac{1}{n-1}, \quad n \geq 3.$$  \hspace{1cm} (32)

So we have $\nu(\Omega_k^G) = \nu(\Omega_k)$ whenever $n \geq 4$, although $\Omega_k^G \neq \Omega_k$ in general; the symmetrization procedure discussed in Sec. [1] does not help in this case.

IV. EFFICIENT VERIFICATION OF W STATES

In this section we present two more efficient protocols for verifying the $n$-qubit $W$ state defined in Eq. (19). These protocols can reduce the number of tests quadratically with respect to the number of qubits.

A. Efficient protocol based on two distinct tests

The first protocol consists of only two distinct tests. In the first test, called the standard test, all parties perform the Pauli-Z measurements, and the test is passed if only one of the $n$ outcomes is 1. The test projector reads

$$P_1 = \sum_{u \in B_1^1} |u\rangle \langle u|,$$  \hspace{1cm} (33)

where $B_1^1$ is the set of strings in $\{0, 1\}^n$ with Hamming weight 1. In the other test, each of the first $n-1$ parties performs $X$ measurements; denote the outcome by 0(1) if the measurement result is +1 (-1). The $n-1$ outcomes are labeled by a string $x \in \{0, 1\}^{n-1}$ of $n-1$ bits, which corresponds to the product state

$$|\alpha_x\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{y \in \{0, 1\}^{n-1}} (-1)^{x \cdot y} |y\rangle.$$  \hspace{1cm} (34)

The reduced state of party $n$ reads

$$|\beta_x\rangle = \frac{|1\rangle + (n-1 - 2 |x|) |0\rangle}{\sqrt{1 + (n-1 - 2 |x|)^2}},$$  \hspace{1cm} (35)

where $|x|$ denotes the Hamming weight of $x$. Then party $n$ performs the two-outcome projective measurement $\{|\beta_x\rangle \langle \beta_x|, I - |\beta_x\rangle \langle \beta_x|\}$, and the test is passed if the first outcome (corresponding to $|\beta_x\rangle \langle \beta_x|$) is obtained. The resulting test projector reads

$$P_2 = \sum_{x \in \{0, 1\}^{n-1}} |\alpha_x\rangle \langle \alpha_x| \otimes |\beta_x\rangle \langle \beta_x|.$$  \hspace{1cm} (36)

If we perform the two tests $P_1$ and $P_2$ with probability $p$ and $1-p$, respectively, then the verification operator reads

$$\Omega_{W_n} = pP_1 + (1-p)P_2.$$  \hspace{1cm} (37)

According to Lemma [1] the spectral gap $\nu(\Omega_{W_n})$ is maximized when $p = 1/2$, in which case $\Omega_{W_n} = (P_1 + P_2)/2$ and $\nu(\Omega_{W_n}) = (1-\sqrt{q})/2$, where

$$q = \|P_1 P_2 P_1\| = \begin{cases} \frac{2}{n-1} & n = 3, \\ 1 - h(n-3) & n \geq 4, \end{cases}$$  \hspace{1cm} (38)

with

$$h(n) := \frac{1}{2^n} \sum_{j=0}^{n} \binom{n}{j} \frac{(n-j)^2}{(n-2j)^2}.$$  \hspace{1cm} (39)

Here the second equality in Eq. (38) is derived in Appendix D. Therefore, we have $\nu(\Omega_{W_n}) = (1/2) - (1/\sqrt{10})$ for $n = 3$, and

$$\nu(\Omega_{W_n}) = \frac{1 - \sqrt{1 - h(n-3)}}{2} \geq \frac{h(n-3)}{4}$$  \hspace{1cm} (40)

for $n \geq 4$.

The dependence of $\nu(\Omega_{W_n})$ on $n$ is illustrated in Fig. 2. The function $\sqrt{n} h(n)$ has the following properties as proved in Appendix E.

**Proposition 4.** $\sqrt{n} h(n)$ is strictly monotonically increasing in $n$ for odd $n$ and even $n$, respectively, assuming $n \geq 0$.

**Proposition 5.** When $n \rightarrow +\infty$, $\sqrt{n} h(n)$ converges for odd $n$ and even $n$, respectively,

$$\lim_{n \rightarrow +\infty} \sqrt{2n+1} h(2n+1) = \sqrt{\frac{\pi}{2}} \tanh \left( \frac{\pi}{2} \right) \approx 1.15,$$  \hspace{1cm} (41)

$$\lim_{n \rightarrow +\infty} \sqrt{2n} h(2n) = \sqrt{\frac{\pi}{2}} \coth \left( \frac{\pi}{2} \right) \approx 1.37.$$  \hspace{1cm} (42)

Here we assume that $n$ is an integer when taking the limits.

The above two propositions imply the following inequalities:

$$\frac{1}{2} \leq \sqrt{n} h(n) \leq \sqrt{\frac{\pi}{2}} \tanh \left( \frac{\pi}{2} \right), \quad n \geq 1 \text{ is odd},$$  \hspace{1cm} (43)

$$\frac{3\sqrt{2}}{5} \leq \sqrt{n} h(n) \leq \sqrt{\frac{\pi}{2}} \coth \left( \frac{\pi}{2} \right), \quad n \geq 2 \text{ is even}.$$  \hspace{1cm} (44)
By virtue of these results, we can derive lower and upper bounds for the spectrally gap, namely,

\[
\frac{1}{\sqrt{4n}} < \nu(\Omega_{W_n}) \leq \begin{cases} 
\frac{3/(8\sqrt{n})}{n \geq 3, n \neq 5}, \\
1/(2\sqrt{n}) \quad n = 5;
\end{cases}
\quad (45)
\]

these bounds can be improved when the parity of \(n\) is given; see Appendix \(F\) for more details. As a consequence of Eq. (45), the number of tests required to verify \(|W_n\rangle\) within fidelity \(\epsilon\) and significance level \(\delta\) satisfies

\[
N(\epsilon, \delta, \Omega_{W_n}) \leq \left\lfloor \frac{4\sqrt{n}}{\epsilon} \ln \delta^{-1} \right\rfloor.
\quad (46)
\]

In addition, \(\nu(\Omega_{W_n})\) admits the following limits

\[
\lim_{n \to +\infty} \sqrt{2n + 1} \nu(\Omega_{W_{2n+1}}) = \frac{\sqrt{2\pi}}{8} \coth \left( \frac{\pi}{2} \right) \approx 0.342, \quad (47)
\]

\[
\lim_{n \to +\infty} \sqrt{2n} \nu(\Omega_{W_n}) = \frac{\sqrt{2\pi}}{8} \tanh \left( \frac{\pi}{2} \right) \approx 0.287, \quad (48)
\]

as proved in Appendix \(C\). When \(n \gg 1\), we have

\[
\nu(\Omega_{W_n}) \approx \begin{cases} 
\frac{\sqrt{2\pi}}{8\sqrt{n}} \coth \left( \frac{\pi}{2} \right) \approx \frac{0.342}{\sqrt{n}} \quad n \text{ is odd,} \\
\frac{\sqrt{2\pi}}{8\sqrt{n}} \tanh \left( \frac{\pi}{2} \right) \approx \frac{0.287}{\sqrt{n}} \quad n \text{ is even;}
\end{cases}
\quad (49)
\]

\[
N(\epsilon, \delta, \Omega_{W_n}) \approx \begin{cases} 
2.93 \sqrt{\ln \delta^{-1}} \ln \delta^{-1} \quad n \text{ is odd,} \\
3.48 \sqrt{\ln \delta^{-1}} \ln \delta^{-1} \quad n \text{ is even.}
\end{cases}
\quad (50)
\]

These results are summarized in Table \(I\) and illustrated in Fig. \(2\). Compared with the protocol in Ref. \(37\) which achieves \(\nu = 1/(n-1)\) with \(\binom{n}{2}\) distinct tests when \(n \geq 4\) (cf. Sec. \(III\)), the current protocol achieves a much better scaling behavior in \(n\) and a higher efficiency whenever \(n \geq 15\), although only two distinct tests are required.

### B. Higher efficiency from symmetrization

The efficiency of the above protocol can be improved by applying the symmetrization procedure described in Sec. \(III\). Let \(G\) be the group generated by all permutations of the \(n\) qubits and diagonal unitary operators of the form \(U^{\otimes n}\). Consider the symmetrized verification operator

\[
\Omega_{W_n}^G = pP_1^G + (1-p)P_2^G = pP_1 + (1-p)P_2^G, \quad (51)
\]

Note that \(P_1^G = P_1\) is a projector, but \(P_2^G\) is not a projector. So Lemma \(I\) is not applicable, and here the optimal choice of \(p\) is not \(1/2\) in contrast to Eq. \(37\). Denote by \(\mathcal{H}_1\) the support of \(P_1\) and \(\mathcal{H}_2\) the orthogonal complement of \(\mathcal{H}_1\). Then \(\mathcal{H}_1\) and \(\mathcal{H}_2\) are invariant subspaces of \(G\). In addition, \(G\) has two inequivalent irreducible components in \(\mathcal{H}_1\): one component is spanned by \(|W_n\rangle\) and is one dimensional; the other component consists of all vectors in \(\mathcal{H}_1\) that are orthogonal to \(|W_n\rangle\). Each irreducible component in \(\mathcal{H}_2\) is not equivalent to any irreducible component in \(\mathcal{H}_1\). Consequently, \(P_2^G\) is block diagonal with respect to \(\mathcal{H}_1\) and \(\mathcal{H}_2\); in addition, \(P_1^G P_2\) is proportional to a projector. Let \(R\) be the subgroup of \(G\) generated by \(\text{diag}(1, e^{2\pi i/(n+1)})^n\) and a cyclic permutation of order \(n\); note that \(R\) has order \(n(n+1)\). By virtue of Proposition \(2\) it is not difficult to verify that \(\Omega_{W_n}^G = \Omega_{W_n}^G\), given that \(P_1\) is invariant under all permutations, while \(P_2\) is invariant under permutations of the first \(n-1\) parties. Therefore, the strategy \(\Omega_{W_n}^G\) can be realized using \(n^2 + n + 1\) distinct projective tests.

As derived in Appendix \(H\) we have

\[
\text{tr}(P_1 P_2^G P_1) = \text{tr}(P_1 P_2) - n - (n-2)h(n-1), \quad (52)
\]

where \(h(n)\) is defined in Eq. \(39\). It follows that

\[
\|P_1 P_2^G P_1\| = \frac{(n-2)[1-h(n-1)]}{n-1} \leq 1 - h(n-1). \quad (53)
\]

Let

\[
p = \frac{1 - \|P_1 P_2^G P_1\|}{2 - \|P_1 P_2^G P_1\|} = 1 + (n-2)h(n-1), \quad (54)
\]

then we have

\[
\lambda_2(\Omega_{W_n}^G) = 1 - p = \frac{n-1}{n + (n-2)h(n-1)}, \quad (55)
\]

\[
\nu(\Omega_{W_n}^G) = p = 1 + (n-2)h(n-1) > \frac{1}{\sqrt{n} + 1}, \quad (56)
\]

as shown in Appendix \(H\). In addition, by virtue of Proposition \(5\) as well as Eqs. \(43\) and \(44\), we can deduce the following limits,

\[
\lim_{n \to +\infty} \sqrt{2n + 1} \nu(\Omega_{W_{2n+1}}^G) = \frac{\sqrt{\pi}}{2} \coth \left( \frac{\pi}{2} \right) \approx 1.37, \quad (57)
\]

\[
\lim_{n \to +\infty} \sqrt{2n} \nu(\Omega_{W_n}^G) = \frac{\sqrt{\pi}}{2} \tanh \left( \frac{\pi}{2} \right) \approx 1.15. \quad (58)
\]

Numerical calculation shows that a good approximation of \(\nu(\Omega_{W_n}^G)\) can be expressed as follows,

\[
\nu(\Omega_{W_n}^G) \approx \begin{cases} 
\frac{1.37}{\sqrt{\pi} + 1.37} \quad n \text{ is odd,} \\
\frac{1.15}{\sqrt{\pi} + 1.11} \quad n \text{ is even;}
\end{cases}
\quad (59)
\]

When \(n \gg 1\), we have \(\nu(\Omega_{W_n}^G) \approx 4\nu(\Omega_{W_n})\), so the symmetrization procedure can improve the efficiency by about four times.

A comparison of the strategies \(\Omega_k\), \(\Omega_{W_n}\), and \(\Omega_{W_n}^G\) indicates that \(\Omega_{W_n}^G\) has the largest spectral gap and thus the highest efficiency for all \(n \geq 3\) [cf. Eqs. \(30\), \(45\), and \(56\)], as illustrated in Fig. \(2\). The strategy \(\Omega_{W_n}^G\) requires only two distinct tests, which is much fewer than the number \(O(n^2)\) of distinct tests required by the other two strategies. On the other hand, the strategies \(\Omega_{W_n}\) and \(\Omega_{W_n}^G\) only apply to \(W\) states, while the strategy \(\Omega_k\) applies to all qudit (including qubit) Dicke states.
V. NEARLY OPTIMAL VERIFICATION OF THE THREE-QUBIT $W$ STATE

In this section we construct a nearly optimal protocol for verifying the three-qubit $W$ state $|W_3\rangle$ shared by Alice, Bob, and Charlie. Before presenting this protocol, it is instructive to set an upper bound for the spectral gap of any verification operator based on LOCC.

According to Ref. [32], for a normalized two-qubit entangled pure state $s_0|00\rangle + s_1|11\rangle$ with Schmidt coefficients $s_0, s_1$ ($0 < s_0, s_1 < 1$ and $s_0^2 + s_1^2 = 1$), the maximum spectral gap of any verification operator based on LOCC or separable measurements is $1/(1 + s_0 s_1)$. With respect to the partition between Alice and the other two parties, $|W_3\rangle$ can be regarded as a two-qubit state in a proper subspace and has two Schmidt coefficients equal to $\sqrt{1/3}$ and $\sqrt{2/3}$, respectively. Therefore, the spectral gap of any verification operator based on LOCC or separable measurements is upper bounded by

$$\frac{1}{1 + \sqrt{2/9}} = \frac{9 - 3\sqrt{2}}{7} \approx 0.6796.$$  

If each test of the verification strategy can be realized by LOCC with one-way communication, then the upper bound can be reduced to $2/3$ according to Refs. [32, 33].

A. Nearly Optimal Verification Protocol

To start with, we construct an efficient protocol using three distinct tests. In the first test, all three parties perform $Z$ measurements, and the test is passed if only one of the three outcomes is 1. The test projector reads

$$P_1 = |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100|,$$  

which is a special case of the projector defined in Eq. (33). The other two tests are based on adaptive local projective measurements. The second test $P_2$ is defined in Eq. (36) with $n = 3$ and has the form

$$P_2 = X^+ X^+ \otimes |\gamma_+\rangle\langle \gamma_+| + X^- X^- \otimes |\gamma_-\rangle\langle \gamma_-| + (X^+ X^- + X^- X^+ ) \otimes |1\rangle\langle 1|,$$  

where $|\gamma_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $X^\pm = |\pm\rangle\langle \pm|$ and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are eigenstates of the operator $X$. For the third test, Alice performs $Z$ measurement and sends her outcome to Bob and Charlie. If the outcome of Alice is 1, so that the normalized reduced state of Bob and Charlie is $|00\rangle$ (if $|W_3\rangle$ is measured), then both Bob and Charlie perform $Z$ measurement, and the test is passed if their outcomes are both 0. If the outcome of Alice is 0, so that the normalized reduced state reads $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ (if $|W_3\rangle$ is measured), then both Bob and Charlie perform $X$ measurement, and the test is passed if their outcomes coincide. The resulting test projector reads

$$P_3 = |100\rangle\langle 100| + |0\rangle\langle 0| \otimes (X^+ X^+ + X^- X^-).$$  

Note that the three test projectors $P_1$, $P_2$, and $P_3$ have ranks 3, 4, and 3, respectively.

If we perform the three tests $P_1$, $P_2$, and $P_3$ with probabilities $p_1$, $p_2$, and $1 - p_1 - p_2$, respectively, then the verification operator is given by

$$\Omega_{\text{I}} = p_1 P_1 + p_2 P_2 + (1 - p_1 - p_2) P_3.$$  

Note that this strategy can be realized by using local projective measurements with one-way communication. Numerical calculation shows that $\lambda_2(\Omega_{\text{I}}) \geq 0.695$, and the lower bound is saturated when $p_1 \approx 0.246$ and $p_2 \approx 0.444$, in which case we have $\nu(\Omega_{\text{I}}) \approx 0.305$.

The efficiency of the above protocol can be improved by applying the symmetrization procedure described in Ref. [31]. Let $G$ be the group generated by the six permutations and diagonal unitary operators of the form $U \otimes \gamma$. Then $G$ has six irreducible components, all of which are inequivalent. Let

$$|\tau_0\rangle := |000\rangle, \quad |\tau_1\rangle := |111\rangle,$$  

$$|\tau_2\rangle := (|001\rangle - |010\rangle)/\sqrt{2},$$  

$$|\tau_3\rangle := (|001\rangle + |010\rangle - 2|100\rangle)/\sqrt{6},$$  

$$|\tau_4\rangle := (|011\rangle + |101\rangle + |110\rangle)/\sqrt{3},$$  

$$|\tau_5\rangle := (|011\rangle - |101\rangle)/\sqrt{2},$$  

$$|\tau_6\rangle := (|011\rangle + |101\rangle - 2|110\rangle)/\sqrt{6}.$$  

Then four one-dimensional irreducible components of $G$ are spanned by $|W_3\rangle$, $|\tau_0\rangle$, $|\tau_1\rangle$, $|\tau_4\rangle$, respectively. One two-dimensional component is spanned by $|\tau_2\rangle$ and $|\tau_3\rangle$, and the other two-dimensional component is spanned by $|\tau_5\rangle$ and $|\tau_6\rangle$. Given any verification operator $\Omega$ for $|W_3\rangle$, then $\Omega^G$ has the form

$$\Omega^G = |W_3\rangle\langle W_3| + \mu_0|\tau_0\rangle\langle \tau_0| + \mu_1|\tau_1\rangle\langle \tau_1| + \mu_2|\tau_2\rangle\langle \tau_2| + \mu_3|\tau_3\rangle\langle \tau_3| + \mu_4|\tau_4\rangle\langle \tau_4| + \mu_5|\tau_5\rangle\langle \tau_5| + \mu_6|\tau_6\rangle\langle \tau_6|,$$  

according to Eq. (15), where $0 \leq \mu_0, \mu_1, \mu_2, \mu_3, \mu_4 \leq 1$. On the other hand, any verification operator of this form is $G$-invariant.

Let $K$ be the subgroup of $G$ that is generated by six permutations and $U_{n/2} = \text{diag}(1, 1, i)$; note that $K$ has order 24. Then $K$ has the same number of irreducible components as $G$, so $\Omega^K = \Omega^G$ for any verification operator of $|W_3\rangle$ according to Proposition 2. In addition, if $\Omega$ can be realized by $m$ distinct projective tests, then $\Omega^K$ can be realized by at most $24m$ distinct projective tests.

Consider the verification operator

$$\Omega_{\text{II}} := \Omega_1^K = p_1 P_1 + p_2 P_2 + (1 - p_1 - p_2) P_3^K;$$  

note that $P_1^K = P_1$. Each test operator $P_j^K$ for $j = 1, 2, 3$ has the form in Eq. (60) with at most five distinct eigenvalues. The parameter vectors $\mu = (\mu_0, \mu_1, \mu_2, \mu_3, \mu_4)$
associated with the three test operators are respectively given by

\[ \mu = (0, 0, 1, 0, 0) \quad \text{for} \quad P_1^K, \]
\[ \mu = \frac{1}{5} (6, 9, 3, 8, 8) \quad \text{for} \quad P_2^K, \]
\[ \mu = \frac{1}{6} (3, 0, 3, 1, 1) \quad \text{for} \quad P_3^K. \]  

Therefore, the second largest eigenvalue of \( \Omega_{II} \) reads

\[ \lambda_2(\Omega_{II}) = \max_{p_1, p_2 \geq 9 \atop p_1 + p_2 \leq 10} \left\{ \frac{5 - 5p_1 - p_2}{10}, \frac{5 - 5p_1 + 11p_2}{30} \right\} \]
\[ \frac{5 + 5p_1 - 3p_2}{10} \geq \frac{3}{5}. \]  

The bound is saturated iff \( p_1 = 1/8 \) and \( p_2 = 5/8 \), in which case we have

\[ \Omega_{II} = |W_3\rangle\langle W_3| + \frac{3}{8} (\mathbb{1} - |W_3\rangle\langle W_3|), \]  

and

\[ \nu(\Omega_{II}) = \frac{5}{8}, \quad N(\epsilon, \delta, \Omega_{II}) \approx \frac{8}{5\epsilon} \ln \delta^{-1}. \]  

Compared with the protocol in Ref. [37] which achieves \( \nu = 1/3 \) (cf. Sec. IIIC), this protocol has a much higher efficiency. In addition, the spectral gap is only 8.04% smaller than the upper bound \( \nu(\Omega) \leq (9 - 3\sqrt{2})/7 \) for strategies based on LOCC or separable measurements. Accordingly, the number of tests required by the strategy \( \Omega_{II} \) is only 8.74% more than the optimal strategy based on separable measurements.

**B. Additional applications**

The strategy \( \Omega_{II} \) is homogeneous and so can be applied to fidelity estimation [30]. Note that the passing probability of any state \( \rho \) is related to its fidelity with the target state \( |W_3\rangle \) as follows, \( \text{tr}(\rho \Omega_{II}) = \frac{5}{8} (W_3|\rho|W_3) + \frac{3}{8} \), which implies that

\[ F = (W_3|\rho|W_3) = \frac{8}{5} \text{tr}(\rho \Omega_{II}) - \frac{3}{5}. \]  

According to Ref. [30], the standard deviation of this estimation is given by \( \Delta F = \sqrt{(1 - F)(F + 3/5)/N} \), where \( N \) is the number of tests performed.

Besides fidelity estimation, our protocol in Eq. (70) is also useful for state verification in the adversarial scenario, in which case the state to be verified is prepared by a potentially malicious adversary [29, 30]. If there is no restriction on the accessible measurements, the optimal strategy for verifying \( |\Psi\rangle \) in the adversarial scenario can be chosen to be homogeneous,

\[ \Omega = |\Psi\rangle\langle\Psi| + \lambda_2(\Omega)(\mathbb{1} - |\Psi\rangle\langle\Psi|). \]  

According to Refs. [29, 30], in the high-precision limit \( \epsilon, \delta \to 0 \), the minimal number of tests required to verify \( |\Psi\rangle \) reads (assuming \( \lambda_2(\Omega) > 0 \)),

\[ N \approx \frac{\ln \lambda_2(\Omega)}{\lambda_2(\Omega)^{-1}} - \ln \delta^{-1}. \]  

This number is minimized when \( \lambda_2(\Omega) = 1/e \), which yields \( N \approx e^{-1} \ln \delta^{-1} \). Since our verification strategy \( \Omega_{II} \) for \( |W_3\rangle \) is homogeneous with \( \lambda_2(\Omega_{II}) = 3/8 \), it can be applied to the adversarial scenario directly. For high-precision state verification, the number of tests required reads \( N \approx 2.7188e^{-1} \ln \delta^{-1} \), which is only about 0.02% more than the optimal strategy. When \( \epsilon, \delta \) are small but not infinitesimal (say \( \epsilon, \delta \leq 0.01 \)), our strategy is still nearly optimal.

**VI. VERIFICATION OF PHASED DICKE STATES**

In this section we consider the verification of phased Dicke states [12, 13], which have the form

\[ |\Psi\rangle = \frac{1}{\sqrt{m}} \sum_{u \in B(k)} e^{i\phi(u)}|u\rangle, \]  

where \( m = |B(k)| = n!/(\prod_{j=0}^{k-1} k_j! \) and the phase \( \phi(u) \) is a real-valued function of the sequence \( u \).

Similar to the verification protocol for Dicke states, our protocol for \( |D_\phi(k)\rangle \) consists of \( \binom{n}{2} \) distinct tests based on adaptive local projective measurements. Each test is associated with a pair of parties among the \( n \) parties. The test \( P_{i,j}^\phi \) associated with parties \( i \) and \( j \) is realized as follows as illustrated in Fig. 3. All \( n - 2 \) parties other than the parties \( i \) and \( j \) perform the generalized Pauli-Z measurements, and their outcomes are labeled by a sequence \( u \) of \( n - 2 \) symbols, which corresponds to the product state \( |u\rangle \). The measurements of parties \( i \) and \( j \) depend on the outcome \( u \), and we need to distinguish three cases. Recall that \( k_s \) and \( k_a \) are defined in Eqs. (22) and (23), respectively. Suppose \( k_0, k_1, \ldots, k_g \geq 2 \) and \( k_{g+1} = k_{g+2} = \cdots k_r = 1 \), where \( -1 \leq g \leq r \).

1. \( u \in B(k_s) \) with \( 0 \leq s \leq g \).

In this case, the normalized reduced state of parties \( i \) and \( j \) reads \( |s\rangle_i |s\rangle_j \) up to an irrelevant phase factor (if the target phased Dicke state is measured). Then the two parties both perform Z measurement, and the test is passed if they both obtain outcome \( s \).

2. \( u \in B(k_a) \) with \( 0 \leq s < t \leq r \).

In this case, the normalized reduced state of parties \( i \) and \( j \) reads,

\[ \frac{1}{\sqrt{2}} |s\rangle_i |t\rangle_j + e^{i\theta(i, j, u)} |t\rangle_i |s\rangle_j, \]  

\[ \theta(i, j, u) := \phi(v(j, i, u)) - \phi(v(i, j, u)). \]
Here \( v(i, j, u), v(j, i, u) \in B(k) \) are defined as follows,

\[
v_i(i, j, u) = s, \quad v_j(i, j, u) = t, \quad v_{ij}(i, j, u) = u, \quad \text{(78)}
\]

\[
v_i(j, i, u) = t, \quad v_j(j, i, u) = s, \quad v_{ij}(j, i, u) = u, \quad \text{(79)}
\]

where \( v_{ij}(i, j, u) \) means the subsequence of \( v(i, j, u) \) without the \( i \)th and \( j \)th components, and \( v_{ij}(j, i, u) \) is defined in the same way. Note that the parameters \( s \) and \( t \) are determined by \( u \). Then parties \( i \) and \( j \) perform projective measurements \( \{\Gamma_{i,j,u}^+, \Gamma_{i,j,u}^-, I - \Gamma_{i,j,u}^+ - \Gamma_{i,j,u}^-\} \) and \( \{\Gamma_{j,i,u}^+, \Gamma_{j,i,u}^-, I - \Gamma_{j,i,u}^+ - \Gamma_{j,i,u}^-\} \), respectively, where

\[
\Gamma_{i,j,u}^+ = \frac{1}{2} [(s + e^{\theta(i,j,u)/2}) |s\rangle + e^{-i\theta(i,j,u)/2} |t\rangle], \quad \text{(80)}
\]

\[
\Gamma_{i,j,u}^- = \frac{1}{2} [(s - e^{i\theta(i,j,u)/2}) |s\rangle - e^{-i\theta(i,j,u)/2} |t\rangle], \quad \text{(81)}
\]

and \( \Gamma_{i,j,u}^\pm \) are defined in a similar way with \( \theta(i, j, u) \) replaced by \( \theta(j, i, u) = -\theta(i, j, u) \). The test is passed if they both obtain the first outcome (corresponding to \( \Gamma^+ \)) or if they both obtain the second outcome (corresponding to \( \Gamma^- \)).

3. Other cases.

The state cannot be the target state \( |D_0(k)\rangle \), so the test is not passed.

The resulting test projector reads

\[
P_{i,j}^{\phi} = \sum_{s=0}^{2^n} Z_{i,j}(k_{ss}) \otimes [(|s\rangle \langle s|)^{\otimes 2}]_{i,j} + \sum_{s<t} \sum_{u \in B(k_{ss})} |u\rangle \langle u| \otimes (\Gamma_{i,j,u}^+ \otimes \Gamma_{j,i,u}^+ + \Gamma_{i,j,u}^- \otimes \Gamma_{j,i,u}^-)_{i,j}, \quad \text{(82)}
\]

where \( Z_{i,j}(k_{ss}) \) is the projector defined in Eq. (27). Each test is performed with probability \( 1/\binom{n}{2} \), and the resulting verification operator reads

\[
\Omega_{i,j}^{\phi} = \binom{n}{2}^{-1} \sum_{i<j} P_{i,j}^{\phi}. \quad \text{(83)}
\]

The efficiency of this protocol is guaranteed by the following theorem, which is proved in Appendix 1.

**Theorem 6.** The spectral gap of \( \Omega^{\phi} \) is the same as that of \( \Omega_k \) in Eq. (30), namely,

\[
\nu(\Omega^{\phi}) = \nu(\Omega_k) = \begin{cases} 1/2 & k = (1, 1, 1), \\ 1/3 & k = (2, 1), \\ 1/(n-1) & n \geq 4. \\ \end{cases} \quad \text{(84)}
\]

To verify the phased Dicke state \( |D_0(k)\rangle \) within infidelity \( \epsilon \) and significance level \( \delta \), the number of tests required reads

\[
N(\epsilon, \delta, \Omega^{\phi}) \approx \begin{cases} 2\epsilon^{-1} \ln \delta^{-1} & k = (1, 1, 1), \\ 3\epsilon^{-1} \ln \delta^{-1} & k = (2, 1), \\ (n-1)\epsilon^{-1} \ln \delta^{-1} & n \geq 4. \end{cases} \quad \text{(85)}
\]

VII. OPTIMAL VERIFICATION OF ANTISYMMETRIC BASIS STATES

Finally, we consider the verification of the \( n \)-partite antisymmetric basis state, also known as the Slater determinant state \( |\text{AS}_n\rangle \). It has the following form

\[
|\text{AS}_n\rangle = \frac{1}{\sqrt{n!}} \sum_{j_1, j_2, \ldots, j_n} \tilde{\epsilon}_{j_1, j_2, \ldots, j_n} |j_1 - 1\rangle \otimes \cdots \otimes |j_n - 1\rangle, \quad \text{(86)}
\]

where \( j_1, j_2, \ldots, j_n \in \{1, 2, \ldots, n\} \) and \( \tilde{\epsilon}_{j_1, j_2, \ldots, j_n} \) is the Levi-Civita symbol. Note that \( |\text{AS}_n\rangle \) can be regarded as a bipartite maximally entangled state of Schmidt rank \( n \) between one party and the other parties. So the spectral gap of any verification operator based on LOCC or separable measurements is upper bounded by \( n/(n+1) \) according to known results on the verification of maximally entangled states [24, 25, 38]. Here we shall show
that this upper bound can be saturated for any antisymmetric basis state with \( n \geq 2 \). When \( n = 2 \), the state \( |\text{AS}_2\rangle \) is a singlet and can be verified using protocols for bipartite pure states proposed in Refs. \([24, 25, 31–33, 38]\).

Here we focus on the multipartite case with \( n \geq 3 \).

### A. Efficient verification protocol

Note that the antisymmetric basis state \( |\text{AS}_n\rangle \) in Eq. (86) is a special case of phased Dicke states in Eq. (75) with \( k = (1, 1, \ldots, 1) \) and \( \phi(u) = 1 \) \((-1)\) if \( u \) is an even (odd) permutation of \( 0, 1, 2, \ldots, n - 1 \). Therefore, \( |\text{AS}_n\rangle \) can be verified using the strategy presented in Eq. (83) tailored to this specific case. Here we shall construct a variant protocol that also consists of \( \binom{n}{2} \) distinct tests, and each test is associated with a pair of parties. In the test \( P_{ij}^{\text{AS}} \) associated with parties \( i \) and \( j \), all \( n - 2 \) parties other than parties \( i \) and \( j \) perform the generalized Pauli-Z measurements, and their outcomes are labeled by a sequence \( u \) of \( n - 2 \) symbols, which corresponds to the product state \( |u\rangle \). The measurements of parties \( i \) and \( j \) depend on the outcome \( u \), and we need to distinguish two cases.

1. \( u \in B(\mathbf{k}_{st}) \) with \( 0 \leq s < t \leq n - 1 \).
   In this case, the normalized reduced state of parties \( i \) and \( j \) reads \( \frac{1}{\sqrt{2}}(|s\rangle_{i}|t\rangle_{j} - |t\rangle_{i}|s\rangle_{j}) \). Then the two parties both perform the projective measurement \( \{T_{s,t}^{+}, T_{s,t}^{-}, I - T_{s,t}^{+} - T_{s,t}^{-}\} \), where \( T_{s,t}^{+} \) and \( T_{s,t}^{-} \) are projectors defined in Eqs. (24) and (25). The test is passed if one of them obtains the first outcome (corresponding to \( T_{s,t}^{+} \)) and the other one obtains the second outcome (corresponding to \( T_{s,t}^{-} \)).

2. Other cases.
   The state cannot be the target state \( |\text{AS}_n\rangle \), so the test is not passed.

The resulting test projector reads

\[
P_{ij}^{\text{AS}} = \sum_{s < t} \tilde{Z}_{i,j}(\mathbf{k}_{st}) \otimes (T_{s,t}^{+} \otimes T_{s,t}^{-} + T_{s,t}^{-} \otimes T_{s,t}^{+})_{i,j},
\]

where \( \tilde{Z}_{i,j}(\mathbf{k}_{st}) \) is defined in Eq. (28) and acts on the tensor product space of all parties other than \( i \) and \( j \).

We perform each test with probability \( 1/\binom{n}{2} \), and the resulting verification operator reads

\[
\Omega_{\text{AS}_n} = \left(\frac{n}{2}\right)^{-1} \sum_{i<j} P_{ij}^{\text{AS}}.
\]

The efficiency of this protocol is guaranteed by the following theorem, which is proved in Appendix [3]

**Theorem 7.** The spectral gap of \( \Omega_{\text{AS}_n} \) with \( n \geq 3 \) reads

\[
\nu(\Omega_{\text{AS}_n}) = \frac{1}{n - 1}.
\]

To verify the antisymmetric basis state \( |\text{AS}_n\rangle \) within infidelity \( \epsilon \) and significance level \( \delta \), the number of tests required reads

\[
N(\epsilon, \delta, \Omega_{\text{AS}_n}) \approx \frac{n - 1}{\epsilon} \ln \delta^{-1}.
\]

Incidentally, the measurement \( \{T_{s,t}^{+}, T_{s,t}^{-}, I - T_{s,t}^{+} - T_{s,t}^{-}\} \) employed in the above verification protocol can be replaced by the alternative \( \{T_{s,t}^{+}, T_{s,t}^{-}, I - T_{s,t}^{+} - T_{s,t}^{-}\} \), where

\[
T_{s,t}^{+} = \frac{1}{2} (|s\rangle + |t\rangle)(|s\rangle - |t\rangle),
\]

\[
T_{s,t}^{-} = \frac{1}{2} (|s\rangle - |t\rangle)(|s\rangle + |t\rangle).
\]

Accordingly, the test projector \( P_{ij}^{\text{AS}} \) is replaced by

\[
P_{ij}^{\text{AS}} = \sum_{s < t} \tilde{Z}_{i,j}(\mathbf{k}_{st}) \otimes (\tilde{T}_{s,t}^{+} \otimes \tilde{T}_{s,t}^{-} + \tilde{T}_{s,t}^{-} \otimes \tilde{T}_{s,t}^{+})_{i,j},
\]

and the resulting verification operator \( \tilde{\Omega}_{\text{AS}_n} \) is given by Eq. (88) with \( P_{ij}^{\text{AS}} \) replaced by \( \tilde{P}_{ij}^{\text{AS}} \). This verification strategy is a special case of the strategy presented in Sec. VI (tailored to the antisymmetric basis state). According to Theorems [6] and [7] we have

\[
\nu(\tilde{\Omega}_{\text{AS}_n}) = \frac{1}{n - 1} = \nu(\Omega_{\text{AS}_n}).
\]

Therefore, the two strategies \( \Omega_{\text{AS}_n} \) and \( \tilde{\Omega}_{\text{AS}_n} \) are equally efficient.
B. Optimal verification protocol based on symmetrization

Let $\tilde{H}$ be the group of all unitary transformations of the form $U^{\otimes n}$ with $U \in U(C^n)$ (here $U$ is not required to be diagonal), let $S$ be the group of all permutations of the $n$ particles, and let $G = H S$. Then the projector onto the antisymmetric basis state $|\text{AS}_n\rangle$ is invariant under $G$. Therefore, we can construct a symmetrized strategy $\Omega^G_{\text{AS}_n}$ according to Sec. II C. Similar to $\Omega_k$, by construction $\Omega^G_{\text{AS}_n}$ is invariant under $S$, so we have $\Omega^S_{\text{AS}_n} = \Omega_{\text{AS}_n}$ and $\Omega^G_{\text{AS}_n} = \Omega^G_{\text{AS}_n}$. For the convenience of practical applications, the group $U(C^n)$ used to construct $\tilde{H}$ can also be replaced by a unitary $t$-design with $t = n$ [42, 46].

To determine $\Omega^G_{\text{AS}_n}$, note that $\tilde{H}$ is a representation of $U(C^n)$ and $S$ is a representation of the symmetric group $\mathcal{S}_n$ of $n$ letters. Accordingly, $\tilde{G}$ is a representation of $U(C^n) \times \mathcal{S}_n$. By Schur-Weyl duality [47, 48], all the irreducible components of $\tilde{G}$ in $(C^n)^{\otimes n}$ are multiplicity free, and each irreducible component is labeled by a partition of $n$. Meanwhile, $(C^n)^{\otimes n}$ has the following decomposition

$$
(C^n)^{\otimes n} = \bigoplus_{\mu \vdash n} \mathcal{H}_\mu = \bigoplus_{\mu \vdash n} W_\mu \otimes S_\mu,
$$

where the notation $\mu \vdash n$ means $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ is a partition of $n$, which means $\mu_j$ are nonnegative integers arranged in decreasing order and sum up to $n$. Here $W_\mu$ carries the irreducible representation of the unitary group $U(C^n)$, while $S_\mu$ carries the irreducible representation of the symmetric group $\mathcal{S}_n$. Let $D_\mu = \dim(W_\mu)$ and $d_\mu = \dim(S_\mu)$; let $P_\mu$ be the projector onto $\mathcal{H}_\mu$; then we have $\text{tr}(P_\mu) = \dim(\mathcal{H}_\mu) = d_\mu D_\mu$. The following theorem is proved in Appendix [K].

Theorem 8. For $n \geq 3$ we have

$$
\Omega^G_{\text{AS}_n} = \sum_{\mu \vdash n} \frac{d_\mu}{D_\mu} P_\mu,
$$

$$
\beta(\Omega^G_{\text{AS}_n}) = \frac{1}{n + 1}, \quad \nu(\Omega^G_{\text{AS}_n}) = \frac{n}{n + 1}.
$$

To verify the antisymmetric basis state $|\text{AS}_n\rangle$ within infidelity $\epsilon$ and significance level $\delta$, the number of tests required reads

$$
N(\epsilon, \delta, \Omega^G_{\text{AS}_n}) \approx \frac{n + 1}{n\epsilon} \ln \delta^{-1}.
$$

Equation Eq. (97) in Theorem 8 follows from Eq. (96) and Lemma 2 below, which imply that the second largest eigenvalue of $\Omega^G_{\text{AS}_n}$ is $d_\mu/D_\mu$ with $\mu = (2, 1, \ldots, 1)$. In this case, we have $d_\mu = n - 1$ and $D_\mu = n^2 - 1$, which yields Eq. (97). Theorem 8 implies that our protocol associated with the verification operator $\Omega^G_{\text{AS}_n}$ is optimal for verifying the antisymmetric basis state $|\text{AS}_n\rangle$ under LOCC. This is the only optimal protocol known for multipartite nonstabilizer states. For quantum states with GME, it is extremely difficult to construct optimal verification protocols under LOCC, and such optimal protocols are known previously only for GHZ states [39].

A partition $\mu \vdash n$ is majorized by another partition $\mu' \vdash n$, denoted by $\mu \prec \mu'$, if

$$
\sum_{j=1}^{k} \mu_j \leq \sum_{j=1}^{k} \mu'_j \quad \forall k = 1, 2, \ldots, n.
$$

Note that the inequality is saturated when $k = n$. The following lemma as proved in Appendix K is very instructive to understanding the spectrum and spectral gap of the verification operator $\Omega^G_{\text{AS}_n}$.

Lemma 2. Suppose $\mu, \mu' \vdash n$ and $\mu \prec \mu'$; then

$$
\frac{D_\mu}{d_\mu} \leq \frac{D_{\mu'}}{d_{\mu'}}.
$$

C. Efficient certification of GME

According to Ref. [2], a quantum state $\rho$ is genuinely multipartite entangled (GME) if its fidelity with some multipartite entangled state $|\Psi\rangle$ is larger than $C_\Psi$, where $C_\Psi$ is the square of the maximum of the Schmidt coefficients of $|\Psi\rangle$ with respect to all bipartitions. Note that $C_\Psi$ equals $1/n$ when $|\Psi\rangle$ is the antisymmetric basis state $|\text{AS}_n\rangle$. Thus a state $\rho$ is GME if $\text{tr}(\rho|\text{AS}_n\rangle\langle\text{AS}_n|) > 1/n$. Given a verification strategy $\Omega$ for $|\text{AS}_n\rangle$, to certify the GME of the antisymmetric basis state with significance level $\delta$, the number of tests is determined by Eq. (2) with $\epsilon = (n - 1)/n$. If $\Omega$ is the optimal local strategy with $\nu(\Omega) = n/(n + 1)$ (the strategy $\Omega^G_{\text{AS}_n}$ constructed in Sec. VII B for example), then this number reads

$$
N_E = \left\lfloor \frac{\ln \delta}{\ln 2 - \ln(n + 1)} \right\rfloor,
$$

which decreases monotonically with $n$. We have $N_E = 1$ when $n \geq 25^{-1} - 1$, so the GME of the antisymmetric basis state can be certified with any given significance level using only one test when the number $n$ of particles is large enough. Previously, single-copy certification of GME is known only for GHZ states [39] and qudit stabilizer states [30]. The current result is of special interest because it may shed light on the certification of GME of other nonstabilizer states.

VIII. SUMMARY

We proposed several efficient protocols for verifying general phased Dicke states, including $W$ states and qudit Dicke states. Our protocols require only adaptive local projective measurements and can be realized with
current technologies. To verify an $n$-qudit phased Dicke state within infidelity $\epsilon$, the number of tests required is only $O(n^2/\epsilon)$, which is exponentially more efficient than previous approaches based on quantum state tomography and direct fidelity estimation. In addition, this number can be further reduced to $O(\sqrt{n}/\epsilon)$ for $W$ states. One of our protocols for the three-qubit $W$ state is nearly optimal for both nonadversarial and adversarial scenario, and it can also be applied to fidelity estimation. Moreover, we constructed an optimal protocol for verifying the antisymmetric basis state; the number of tests required decreases monotonically with the number $n$ of particles. By virtue of this protocol, the GME of the antisymmetric basis state can be certified with any given significance level using only one test when $n$ is sufficiently large. In this way, our work provides powerful tools for characterizing and verifying various phased Dicke states. In the course of study, we introduced several methods for improving the efficiency of a given verification strategy, which are useful to studying quantum verification in general. In addition, our work highlights the significance of graph theory and representation theory in studying quantum verification, which is of interest to many researchers beyond quantum information science.

**ACKNOWLEDGMENT**

ZL thanks Jiahao Li for helpful discussion on the proof of Proposition 5. HZ is grateful to Prof. Eiichi Bannai for stimulating discussion on the spectrum of the transposition graph. This work is supported by the National Natural Science Foundation of China (Grant No. 11875110) and Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX04). JS acknowledges support by the Beijing Institute of Technology Research Fund Program for Young Scholars and the National Natural Science Foundation of China (Grant No. 11805010).

**Appendix A: Proof of Lemma 7**

**Proof.** Note that $|\Psi\rangle$ is an eigenstate of $P_0$ and $P_2$ with eigenvalue 1 by assumption. Without loss of generality, we can assume that $P_1$ has rank $l+1$ and $P_2$ has rank $h+1$ with $h \leq l$. Then we can find two sets of orthonormal states $(|\phi_j\rangle)_{j=1}^{l}$ and $(|\varphi_k\rangle)_{k=1}^{h}$ such that

$$
P_1 = |\Psi\rangle\langle\Psi| + \sum_{j=1}^{l} |\phi_j\rangle\langle\phi_j|, \quad P_2 = |\Psi\rangle\langle\Psi| + \sum_{k=1}^{h} |\varphi_k\rangle\langle\varphi_k|, \quad |\langle\phi_j|\varphi_k\rangle|^2 = q_k \delta_{jk},$$

(A1)

where the overlaps $q_k$ are arranged in decreasing order, that is, $1 \geq q_1 \geq q_2 \geq \cdots q_h \geq 0$. As a consequence, we have

$$
\bar{P}_1 = \sum_{j=1}^{l} |\phi_j\rangle\langle\phi_j|, \quad \bar{P}_2 = \sum_{k=1}^{h} |\varphi_k\rangle\langle\varphi_k|,
$$

(A2)

$$
q := \|\bar{P}_1 \bar{P}_2 \bar{P}_1\| = \left( \sum_{j=1}^{l} |\phi_j\rangle\langle\phi_j| \right) \left( \sum_{k=1}^{h} |\varphi_k\rangle\langle\varphi_k| \right) \left( \sum_{j=1}^{l} |\phi_j\rangle\langle\phi_j| \right) = \left( \sum_{j=1}^{h} q_j |\varphi_k\rangle\langle\varphi_k| \right) = q_1.
$$

(A3)

$$
\max_{|\phi\rangle \in \text{supp}(P_2)} \langle\phi| P_2 |\phi\rangle = \max_{\sum_{j=1}^{l} |c_j|^2 = 1} \sum_{j,k=1}^{l} c_j^* c_k |\langle\phi_j| P_2 |\varphi_k\rangle| = \max_{\sum_{j=1}^{h} |c_j|^2 = 1} \sum_{j=1}^{h} q_j |c_j|^2 = q_1 = \|\bar{P}_1 \bar{P}_2 \bar{P}_1\| = q.
$$

(A4)

In addition, the verification operator $\Omega$ can be expressed as follows,

$$
\Omega = pP_1 + (1-p)P_2 = |\Psi\rangle\langle\Psi| + \sum_{j=1}^{h} \left[ p|\phi_j\rangle\langle\phi_j| + (1-p)|\varphi_j\rangle\langle\varphi_j| \right] + p \sum_{k=h+1}^{l} |\varphi_k\rangle\langle\varphi_k|.
$$

(A5)

So the second largest eigenvalue of $\Omega$ reads

$$
\lambda_2(\Omega) = \|\Omega - |\Psi\rangle\langle\Psi|\| = \max_{1 \leq j \leq h} \| p|\phi_j\rangle\langle\phi_j| + (1-p)|\varphi_j\rangle\langle\varphi_j| \| = \max_{1 \leq j \leq h} \frac{1}{2} \left[ 1 + \sqrt{(2p-1)^2 + 4p(1-p)q_j} \right] = \frac{1}{2} \left[ 1 + \sqrt{(2p-1)^2 + 4p(1-p)q} \right] = \frac{1}{2} \left[ 1 + \sqrt{4(1-q)p^2 - 4(1-q)p + 1} \right] \geq \frac{1}{2} \left( 1 + \sqrt{q} \right).
$$

(A6)

If $q < 1$, then the lower bound is saturated iff $p = 1/2$, in which case we have $\Omega = (P_1 + P_2)/2$. Therefore, the spectral gap satisfies $\nu(\Omega) \leq (1 - \sqrt{q})/2$, and the upper bound is saturated iff $p = 1/2$, which confirms Lemma 7. □
Appendix B: Proof of Theorem 3

Proof. The verification operator $\Omega_k$ can be expressed as

$$\Omega_k = \left(\frac{n}{2}\right)^{-1} \sum_{i<j} \sum_{s=0}^{g} \mathbb{Z}_{i,j}(k_{ss}) \otimes \left(\left|\langle s| \langle \rangle\right| \otimes \left|\langle \rangle \langle s\rangle\right|\right)_{i,j} + \left(\frac{n}{2}\right)^{-1} \sum_{i<j} \sum_{s<t} \mathbb{Z}_{i,j}(k_{st}) \otimes \left(\left|\langle s| \langle \rangle\right| \otimes \left|\langle \rangle \langle s\rangle\right|\right)_{i,j}$$

$$= \frac{1}{n(n-1)} \left(\sum_{s=0}^{r} k_s^2 - n\right) \mathcal{Z}(k) + \frac{2}{n(n-1)} \sum_{i<j} \sum_{s<t} \mathbb{Z}_{i,j}(k_{st}) \otimes \left(\left|\langle s| \langle \rangle\right| \otimes \left|\langle \rangle \langle s\rangle\right|\right)_{i,j}$$

$$= \frac{1}{n(n-1)} \left[ M_1 + \sum_{s=t} M(s,t) \right]. \tag{B1}$$

Here $|\psi_{s,t}^+\rangle = \frac{1}{\sqrt{2}}(|\langle s|\rangle + |\langle t|\rangle)$, $|\phi_{s,t}^+\rangle = \frac{1}{\sqrt{2}}(|\langle s|\rangle - |\langle t|\rangle)$, $\mathcal{Z}(k) = \sum_{u,v \in B(k)} |u\rangle \langle u|$, and

$$M_1 := \left(\sum_{s=0}^{r} k_s^2 - n + \sum_{s=0}^{r} k_s k_t \right) \mathcal{Z}(k) + \sum_{u,v \in B(k)} |u\rangle \langle v|,$$

$$M(s,t) := \frac{k_s(k_s + 1)}{2} \sum_{u \in B(k_s')} |u\rangle \langle u| + \frac{k_t(k_t + 1)}{2} \sum_{v \in B(k_t')} |v\rangle \langle v| + \sum_{u,v \in B(k')} \left( |u\rangle \langle v| + |v\rangle \langle u| \right), \tag{B3}$$

where the notation $u \sim v$ means $u_j \neq v_j$ for exactly two values of $j$. The coefficient matrix $(A_{uv})$ for $u,v \in B(k)$ happens to be the adjacency matrix $A(k)$ of the transposition graph $G(k)$ explained in Appendix E. Note that $M_1$ and all $M(s,t)$ (with $s,t = 0,1,\ldots,r$ and $s < t$) are hermitian and have mutually orthogonal supports, so all of them are positive semidefinite given that $\Omega_k$ is positive semidefinite by construction.

According to Lemma 3 in Appendix E, the maximum eigenvalue of $A(k)$ is $d = (n^2 - \sum_{s=0}^{r} k_s^2)/2$ with multiplicity 1, and the second largest eigenvalue of $A(k)$ is equal to $d - n$. Therefore, the two largest eigenvalues of $M_1$ read

$$\lambda_1(M_1) = n(n-1), \quad \lambda_2(M_1) = n(n-1) - n = n(n-2). \tag{B4}$$

In addition, direct calculations show that $M(s,t)$ has an eigenstate

$$|\Theta_{s,t}\rangle = \frac{1}{\sqrt{k_s(k_s + 1) + k_t(k_t + 1)}} \left[ \sqrt{k_s(k_s + 1)} |D(k_s')\rangle + \sqrt{k_t(k_t + 1)} |D(k_t')\rangle \right]$$

$$= \frac{\prod_{j=0}^{s-1} k_j!}{k_s k_t (k_s + 1) (k_t + 1) (n_l)!} \left[ k_s(k_s + 1) \sum_{u \in B(k_s')} |u\rangle + k_t(k_t + 1) \sum_{u \in B(k_t')} |u\rangle \right], \tag{B5}$$

with eigenvalue

$$\lambda_1(M(s,t)) = \frac{k_s(k_s + 1)}{2} + \frac{k_t(k_t + 1)}{2}. \tag{B6}$$

According to the Perron-Frobenius theorem (see Chapter 8 in Ref. 49 for example), this is the largest eigenvalue of $M(s,t)$, given that $M(s,t)$ is irreducible in the subspace spanned by $|u\rangle$ with $u \in B(k_s') \cup B(k_t')$, that is, the graph corresponding to the third term of $M(s,t)$ in Eq. (B3) is connected. In conjunction with Eqs. (B1) and (B4), we can deduce the second largest eigenvalue and spectral gap of $\Omega_k$, with the result

$$\lambda_2(\Omega_k) = \max \left\{ \frac{\lambda_2(M_1)}{n(n-1)}, \max_{s < t} \frac{\lambda_1(M(s,t))}{n(n-1)} \right\} = \max \left\{ \frac{n-2}{n-1} \frac{k_0(k_0 + 1) + k_1(k_1 + 1)}{2(n-1)} \right\}, \tag{B7}$$

$$\nu(\Omega_k) = 1 - \lambda_2(\Omega_k) = \min \left\{ \frac{1}{n-1}, 1 - \frac{k_0(k_0 + 1) + k_1(k_1 + 1)}{2(n-1)} \right\}. \tag{B8}$$

When $n \geq 4$, the above equations reduce to

$$\lambda_2(\Omega_k) = \frac{n-2}{n-1}, \quad \nu(\Omega_k) = \frac{1}{n-1}, \tag{B9}$$

which confirms Eq. (30). When $n = 3$, Eq. (30) can be verified directly by virtue of Eq. (B8).

Equation (B11) follows from Eqs. (2) and (30). This observation completes the proof of Theorem 3. \qed
Appendix C: Determination of $\Omega_k^G$ and proof of Eq. (32)

Denote by $H$ the group of all unitary transformations of the form $U^{\otimes n}$, where $U$ is diagonal in the computational basis. According to Eqs. (8) and (B1), we have

$$\Omega_k^G = \Omega_k^H = \frac{M_1^H + \sum_{s<t} M_{(s,t)}^H}{n(n-1)},$$

where

$$M_1^H = M_1, \quad M_{(s,t)}^H = \frac{k_s(k_s + 1)}{2} \sum_{u \in B(k_s^2)} |u\rangle\langle u| + \frac{k_t(k_t + 1)}{2} \sum_{v \in B(k_t^2)} |v\rangle\langle v|.$$  (C2)

Equation (C2) follows from Eqs. (B2) and (B3) as well as the fact that $(|u\rangle\langle v|)^H = |u\rangle\langle v|$ if $u$ and $v$ can be turned into each other by a permutation, while $(|u\rangle\langle v|)^H = 0$ otherwise.

Note that $M_1$ and all $M_{(s,t)}^H$ (with $s, t = 0, 1, \ldots, r$ and $s < t$) are positive semidefinite and have mutually orthogonal supports. The largest eigenvalue of $M_{(s,t)}^H$ reads $\lambda_1(M_{(s,t)}^H) = k_s(k_s + 1)/2$. In conjunction with Eqs. (C1), (C2), and (B4), we can deduce the second largest eigenvalue and the spectral gap of $\Omega_k^G$, with the result

$$\lambda_2(\Omega_k^G) = \max \left\{ \frac{\lambda_2(M_{(s,t)}^H)}{n(n-1)}, \max_{s<t} \frac{\lambda_1(M_{(s,t)}^H)}{n(n-1)} \right\} = \max \left\{ \frac{n - 2}{n-1}, \frac{k_0(k_0 + 1)}{2n(n-1)} \right\} = \frac{n - 2}{n-1}, \quad \nu(\Omega_k^G) = \frac{1}{n-1},$$

which confirms Eq. (32).

Appendix D: Proof of Eq. (38)

Proof. Note that each ket $|\zeta\rangle$ in the support of the test projector $P_1$ in Eq. (33) has the following form

$$|\zeta\rangle = a_1|10\ldots00\rangle + a_2|01\ldots00\rangle + \cdots + a_n|00\ldots01\rangle,$$

where $a_1, a_2, \ldots, a_n$ are complex numbers that satisfy the normalization condition $\sum_{j=1}^n |a_j|^2 = 1$. In conjunction with Lemma 1 and Eqs. (34)-(36), we can deduce that

$$q = \|ar{P}_1 P_2 P_1\| = \max_{\langle W_0 | \zeta \rangle = 0} \frac{\langle \zeta | P_2 | \zeta \rangle}{\langle \zeta | P_1 | \zeta \rangle} = \frac{1}{2^{n-1}} \max_{\sum_{j=0}^{n-1} a_j = 0, \sum_{j=1}^{n-1} |a_j|^2 = 1} \sum_{x \in \{0, 1\}^{n-1}} |a_n + (n - 1 - 2|x|) \sum_{j=1}^{n-1} (-1)^{x_j} a_j|^2$$

$$= \frac{1}{2^{n-1}} \sum_{j=0}^{n-1} \sum_{|x| = k} a_n + (n - 1 - 2k) \sum_{j=1}^{n-1} (-1)^{x_j} a_j$$

$$= \left| \frac{4k(n-1-k)(n-1-2k)}{(n-1)(n-2)} \left( \begin{array}{c} n-1 \n \end{array} \right) \right| + \left( \begin{array}{c} n-1 \n \end{array} \right) \left\{ 1 + (n - 1 - 2k) \left[ 1 - \frac{2}{n-1} - \frac{8k(n-1-k)}{(n-1)(n-2)} \right] \right\} |a_n|^2,$$  (D3)
for $k = 0, 1, \ldots, n - 1$, where $a^*_j$ denotes the complex conjugate of $a_j$. The last equality in Eq. (D3) follows from the following equations,

$$
\sum_{|x|=k} \sum_{j=1}^{n-1} (-1)^x a_j = \frac{n-1-2k}{n-1} \binom{n-1}{k} \sum_{j=1}^{n-1} a_j = -\frac{n-1-2k}{n-1} \binom{n-1}{k} a_n, \quad (D4)
$$

$$
\sum_{|x|=k} \sum_{j=1}^{n-1} (-1)^x a_j^2 = \left( \frac{n-1}{k} \right) \left[ \sum_{j=1}^{n-1} |a_j|^2 + \frac{(n-1)(n-2) - 4k(n-1-k)}{(n-1)(n-2)} \sum_{i,j=1}^{n-1, n-1} a_i a_j^* \right] = \left( \frac{n-1}{k} \right) \left[ \frac{4k(n-1-k)}{(n-1)(n-2)} + \frac{(n-1)(n-2) - 8k(n-1-k)}{(n-1)(n-2)} |a_n|^2 \right]. \quad (D5)
$$

In deriving the second equality in Eq. (D5), we have employed the following facts

$$
\sum_{j=1}^{n-1} |a_j|^2 = 1 - |a_n|^2, \quad \sum_{i,j=1}^{n-1, n-1} a_i a_j^* = \left[ \sum_{i=1}^{n-1} a_i \right]^2 - \sum_{j=1}^{n-1} |a_j|^2 = |1 - |a_n|^2 - (1 - |a_n|^2)| = 2|a_n|^2 - 1. \quad (D6)
$$

Now by plugging Eq. (D3) into Eq. (D2) we obtain

$$
q = c_1(n) + \max_{\sum_{j} |a_j|^2=1} c_2(n) |a_n|^2, \quad (D7)
$$

where the coefficients $c_1(n)$ and $c_2(n)$ read

$$
c_1(n) := \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{n-1}{k} \frac{4k(n-1-k)(n-1-2k)^2}{[n-1](n-2)[1+(n-1-2k)^2]} = \frac{1}{2^{n-3}} \sum_{k=0}^{n-3} \binom{n-3}{k} \frac{(n-1)(n-2k)^2}{[n-1][1+(n-1-2k)^2]} = 1 - h(n-3), \quad (D8)
$$

$$
c_2(n) := \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{n-1}{k} \frac{2(n-1-k)(n-1-2k)}{[n-1][1+(n-1-2k)^2]} = \frac{1}{2^{n-1}} \sum_{k=0}^{n-1} \binom{n-1}{k} \frac{(n-1-k)(n-1-2k)}{[n-1][1+(n-1-2k)^2]} - 2c_1(n) \quad (D9)
$$

and $h(n)$ is defined in Eq. (39).

If $n = 3$, then $c_1(n) = 0$ and $c_2(n) = \frac{3}{5} > 0$, so the maximum in Eq. (D7) is attained when $a_1 = a_2 = -\frac{1}{\sqrt{6}}$ and $a_3 = \sqrt{\frac{2}{3}}$, in which case we have

$$
q = c_1(3) + \frac{2}{3} c_2(3) = \frac{2}{5}, \quad (D10)
$$

which confirms Eq. (38) in the case $n = 3$.

If $n = 4, 5$, then $c_2(n) < 0$ by direct calculation. If $n \geq 6$, then

$$
c_2(n) = \frac{2}{n-1} h(n-1) + 2h(n-3) - \frac{n+1}{n-1} \frac{1}{n-1} + 1 - \frac{n+1}{n-1} = -\frac{1}{n-1} < 0, \quad (D11)
$$

where the first inequality follows from the fact that $h(n) < 1/2$ for $n \geq 3$, which is easy to prove. Therefore, $c_2(n) < 0$ for $n \geq 4$. In this case, the maximum in Eq. (D7) is attained when $a_1 = -a_2 = \frac{1}{\sqrt{2}}$ and $a_j = 0$ for $j = 3, 4, \ldots, n$, which yields

$$
q = c_1(n) = 1 - h(n-3) \quad (D12)
$$

and confirms Eq. (38).
Appendix E: Proofs of Propositions 4 and 5

Proof of Proposition 4. To prove Proposition 4, it suffices to prove that $\sqrt{n+2} h(n+2) > \sqrt{n} h(n)$ for each integer $n \geq 0$. When $n = 0$, the inequality is obvious; when $n \geq 1$, the inequality can be proved as follows,

$$\frac{2^{n+2}}{\sqrt{n}} \left[ \sqrt{n+2} h(n+2) - \sqrt{n} h(n) \right] = \sqrt{n+2} \sum_{j=0}^{n+2} \frac{(n+2)_j}{n+2 - (n+2)j^2} - \sum_{j=0}^{n} \frac{4^n}{1 + (n+2)j^2} \geq 0.$$  

(E1)

Here the first inequality holds because $\frac{2^{n+2}}{n} > \frac{2^{n+2}}{n+1}$, and the last inequality holds because

$$\frac{n+2}{n} \left( \frac{n+2}{j+1} - 4 \binom{n}{j} \right) = \left[ \frac{(n+2)^2}{(j+1)(n+1-j)} - 4 \right] \binom{n}{j} \geq 0, \quad j = 0, 1, \ldots, n. \quad (E2)$$

Therefore, $\sqrt{n} h(n)$ is strictly monotonically increasing in $n$ for odd $n$ and even $n$, respectively. \qed

Proof of Proposition 5. First, Eq. (42) in Proposition 5 can be derived as follows,

$$\lim_{n \to \infty} \sqrt{2n} h(2n) = \lim_{n \to \infty} \sqrt{2n} \sum_{j=0}^{\infty} \frac{\binom{n}{j}}{1 + (2n - 2j)^2} = \sqrt{2n} \left[ \lim_{n \to \infty} \sqrt{2n} \binom{2n}{n} \right] \left[ \lim_{n \to \infty} \sum_{j=0}^{n} \frac{\binom{2n}{n} \binom{2n}{j}}{1 + (2n - 2j)^2} \right] = \frac{\sqrt{2}}{\pi} \left[ \lim_{n \to \infty} \sum_{j=0}^{\infty} \frac{1}{1 + (2n - 2j)^2} \right] = \frac{\sqrt{2}}{\pi} \left[ 1 + \frac{\pi}{2} \coth \left( \frac{\pi}{2} \right) - 1 \right] = \frac{\sqrt{2}}{\pi} \coth \left( \frac{\pi}{2} \right) \approx 1.37, \quad (E3)$$

where the third equality follows from Eqs. (E4) and (E5) below, and the fifth equality is a corollary of Eq. (E6) below.

$$\lim_{n \to \infty} \frac{\sqrt{2n} h(2n)}{2^{2n}} \binom{2n}{n} = \lim_{n \to \infty} \frac{\sqrt{2n} h(2n)!}{2^{2n} n!} = \frac{\sqrt{2}}{\pi}; \quad (E4)$$

$$\lim_{n \to \infty} \frac{\sum_{j=0}^{n} \binom{2n}{n}^{-1} \binom{2n}{j}}{1 + (2n - 2j)^2} = \lim_{n \to \infty} \frac{1}{2n} \sum_{j=0}^{2n} \frac{1}{1 + (2n - 2j)^2}; \quad (E5)$$

$$\lim_{n \to \infty} \sum_{k=1}^{n} \left( \frac{1}{1 + 2k^2} - \frac{1}{1 + 4k^2} \right) = \frac{1}{2} \lim_{n \to \infty} \sum_{k=1}^{n} \left( \frac{1}{i/2 - k} + \frac{1}{i/2 + k} \right) = \frac{1}{4} \left[ \pi \cot \left( \frac{\pi}{2} \right) + 2i \right] = \frac{\pi}{4} \coth \left( \frac{\pi}{2} \right) - 1. \quad (E6)$$

The second equality in Eq. (E4) follows from the Wallis formula [see Eq. (1) in Ref. [50] for example] or the Stirling formula; the second equality in Eq. (E6) follows from Theorem 6.12 in Ref. [51].

To prove Eq. (E5), note that the left-hand side in Eq. (E5) cannot be larger than the right-hand side thanks to the inequality $(\binom{n}{j}) \leq (\binom{n}{n/2})$. To complete the proof, it suffices to prove the opposite inequality, which can be derived as follows.

$$\lim_{n \to \infty} \sum_{j=0}^{n} \frac{1}{1 + (2n - 2j)^2} - \lim_{n \to \infty} \sum_{j=0}^{n} \frac{(2n)^{-1} \binom{2n}{j}}{1 + (2n - 2j)^2} = 2 \lim_{n \to \infty} \sum_{k=1}^{n} \frac{1 - (2n)^{-1} \binom{2n}{n+k}}{1 + 4k^2} = 2 \lim_{n \to \infty} \sum_{k=1}^{\lfloor n/2 \rfloor} \frac{1 - (2n)^{-1} \binom{2n}{n+k}}{1 + 4k^2} \leq 2 \lim_{n \to \infty} \frac{\sum_{k=1}^{\lfloor n/2 \rfloor} k^2}{n(1 + 4k^2)} + 2 \lim_{n \to \infty} \frac{\sum_{k=1}^{\lfloor n/2 \rfloor} 1}{1 + 4k^2} \leq 2 \lim_{n \to \infty} \frac{\left( \frac{n^2}{4} \right)}{4n} + 2 \lim_{n \to \infty} \frac{n}{4n^{4/3}} = 0, \quad (E7)$$

The equality in Eq. (E7) follows from Theorem 6.12 in Ref. [51].
The second equality in Eq. (E10) follows from the Wallis formula \([\text{cf. Eq. (E4)}]\); the second and third equalities in where the first inequality is a consequence of the following equation,

\[
\lim_{n \to \infty} \sqrt{2n + 1} h(2n + 1) = \lim_{n \to \infty} \frac{\sqrt{2n + 1}}{2n+1} \sum_{j=0}^{2n+1} \frac{\binom{2n+1}{j}}{1 + (2n + 1 - 2j)^2} = \sqrt{\frac{2}{\pi}} \lim_{n \to \infty} \sum_{j=0}^{2n+1} \frac{1}{1 + (2n + 1 - 2j)^2} = \sqrt{\frac{2}{\pi}} \sum_{k=0}^{n} \frac{2}{1 + (2k+1)^2}
\]

where the third equality follows from Eqs. (E10) and (E11) below, and the fifth equality is a corollary of Eq. (E12) below.

\[
\lim_{n \to \infty} \sqrt{\frac{2n+1}{2n+1}} \binom{2n+1}{n} = \lim_{n \to \infty} \sqrt{\frac{2n}{2n(n+1)}} \left[ \lim_{n \to \infty} \sqrt{\frac{2n+1}{2n}} \frac{2n+1}{2(n+1)} \right] = \frac{\sqrt{2}}{\pi}
\]

(E9)

The second equality in Eq. (E10) follows from the Wallis formula [cf. Eq. (E4)]; the second and third equalities in Eq. (E12) follow from Eq. (E9) above and Theorem 6.12 in Ref. [51], respectively; Eq. (E11) can be proved in a similar way as Eq. (E5), given the following equation,

\[
\binom{2n+1}{n} = \frac{n!(n+1)!}{(n+1+k)!n!} \geq \left( 1 - \frac{k^2 + k}{n+1} \right)^k \geq 1 - \frac{k^2}{n}, \; k \in \{0, 1, \ldots, n\}.
\]

(E13)

\[\square\]

Appendix F: Bounds for \(\nu(\Omega_{W_n})\) and proof of Eq. (45)

To derive lower bounds for \(\nu(\Omega_{W_n})\), we shall consider two cases depending on the parity of the qubit number \(n\).

1. \(n\) is an odd integer.

Direct calculation based on Eqs. (38)-(40) shows that \(\sqrt{n} \nu(\Omega_{W_n}) > 3/10\) for \(3 \leq n \leq 33\). When \(n \geq 35\), we have

\[
\sqrt{n} \nu(\Omega_{W_n}) > \frac{1}{4} \sqrt{n-3} h(n-3) \geq \frac{1}{4} \sqrt{32} h(32) > \frac{3}{10}.
\]

(F1)

where the first inequality follows from Eq. (40), and the second inequality follows from Proposition 4. Therefore, \(\sqrt{n} \nu(\Omega_{W_n}) > 3/10\) when \(n\) is odd and \(n \geq 3\), which implies the lower bound in Eq. (45).

2. \(n\) is an even integer.

Direct calculation based on Eqs. (39) and (40) shows that \(\sqrt{n} \nu(\Omega_{W_n}) > 1/4\) for \(4 \leq n \leq 42\). When \(n \geq 44\), we have

\[
\sqrt{n} \nu(\Omega_{W_n}) > \frac{1}{4} \sqrt{n-3} h(n-3) \geq \frac{1}{4} \sqrt{44} h(41) > \frac{1}{4}.
\]

(F2)
In conclusion, the lower bound in Eq. (45) holds for any integer $n$ that satisfies $n \geq 3$.

To derive upper bounds for $\nu(\Omega_{W_n})$, we also consider two cases depending on the parity of the qubit number $n$.

1. $n$ is an odd integer.

Direct calculation based on Eqs. (38)-(40) shows that $\sqrt{n}\nu(\Omega_{W_n}) < 3/8$ for $3 \leq n \leq 45$ with $n \neq 5$ and $\sqrt{n}\nu(\Omega_{W_n}) < 0.411 < 1/2$ when $n = 5$. When $n \geq 47$, we have

$$\sqrt{n}\nu(\Omega_{W_n}) = \sqrt{n-3}h(n-3)\frac{1 - \sqrt{1 - h(n-3)}}{2h(n-3)} < \sqrt{\frac{\pi}{2}}\coth\left(\frac{\pi}{2}\right) \times 1.034 \times 0.265 < \frac{3}{8},$$

where the first inequality follows from Eq. (44) and the following equations,

$$\frac{\sqrt{n}}{n-3} \leq \frac{\sqrt{47}}{47-3} < 1.034,$$

$$h(n-3) \leq \frac{1}{\sqrt{n-3}} \times \sqrt{\frac{\pi}{2}} \coth\left(\frac{\pi}{2}\right) \leq \sqrt{\frac{\pi}{2(47-3)}} \coth\left(\frac{\pi}{2}\right) < 0.207,$$

$$1 - \frac{\sqrt{1 - h(n-3)}}{2h(n-3)} < 1 - \frac{\sqrt{1 - 0.207}}{2 \times 0.207} < 0.265.$$  \hfill (F3)

The first inequality in Eq. (F5) follows from Eq. (44); the first inequality in Eq. (F6) follows from Eq. (F5) and the fact that the real-valued function $(1 - \sqrt{1-x})/(2x)$ is monotonically increasing in $x$ when $0 < x \leq 1$. Therefore, $\sqrt{n}\nu(\Omega_{W_n}) < 3/8$ when $n$ is odd and $n \geq 3, n \neq 5$, which implies the upper bound in Eq. (45).

2. $n$ is an even integer.

Direct calculation based on Eqs. (39) and (40) shows that $\sqrt{n}\nu(\Omega_{W_n}) < 0.31$ for $4 \leq n \leq 52$. When $n \geq 54$, we have

$$\sqrt{n}\nu(\Omega_{W_n}) = \sqrt{n-3}h(n-3)\frac{1 - \sqrt{1 - h(n-3)}}{2h(n-3)} < \sqrt{\frac{\pi}{2}}\tanh\left(\frac{\pi}{2}\right) \times 1.03 \times 0.261 < 0.31,$$

where the first inequality follows from Eq. (43) and the following equations,

$$\frac{\sqrt{n}}{n-3} \leq \frac{\sqrt{54}}{54-3} < 1.03,$$

$$h(n-3) \leq \sqrt{\frac{2\pi}{(n-3)}} \tanh\left(\frac{\pi}{2}\right) \leq \sqrt{\frac{2\pi}{2(54-3)}} \tanh\left(\frac{\pi}{2}\right) < 0.161,$$

$$1 - \frac{\sqrt{1 - h(n-3)}}{2h(n-3)} < 1 - \frac{\sqrt{1 - 0.161}}{2 \times 0.161} < 0.261.$$  \hfill (F7)

The first inequality in Eq. (F9) follows from Eq. (43); the first inequality in Eq. (F10) follows from Eq. (F9) and the fact that the real-valued function $(1 - \sqrt{1-x})/(2x)$ is monotonically increasing in $x$ when $0 < x \leq 1$. Therefore, $\sqrt{n}\nu(\Omega_{W_n}) < 0.31$ when $n$ is even and $n \geq 4$, which implies the upper bound in Eq. (45) again.

In conclusion, Eq. (45) holds for any integer $n$ that satisfies $n \geq 3$.

Appendix G: Proofs of Eqs. (47) and (48)

Proof. Equation (47) can be proved as follows,

$$\lim_{n \to +\infty} \sqrt{2n + 1}\nu(\Omega_{W_{2n+1}}) = \lim_{n \to +\infty} \sqrt{2n + 1} - \frac{1 - \sqrt{1 - h(2n-2)}}{2} = \left[ \lim_{n \to +\infty} \sqrt{2n - 2} h(2n-2) \right] \left[ \lim_{n \to +\infty} \sqrt{\frac{2n+1}{2n-2}} - \frac{1 - \sqrt{1 - h(2n-2)}}{2h(2n-2)} \right] = \frac{1}{4} \sqrt{\frac{\pi}{2}} \coth\left(\frac{\pi}{2}\right) \approx 0.342.$$  \hfill (G1)
Here the first equality follows from Eq. (40); the third one follows from Eq. (42) and the fact that $\lim_{n \to +\infty} h(n) = 0$. Equation (48) can be proved as follows,

$$\lim_{n \to +\infty} \sqrt{2n}n(\Omega_{W_n}) = \lim_{n \to +\infty} \sqrt{2n} \frac{1 - \sqrt{1 - h(2n - 3)}}{2}$$

$$= \left[ \lim_{n \to +\infty} \sqrt{2n - 3} h(2n - 3) \right] \left( \lim_{n \to +\infty} \sqrt{\frac{2n}{2n - 3}} \right) \left[ \lim_{n \to +\infty} \frac{1 - \sqrt{1 - h(2n - 3)}}{2h(2n - 3)} \right] = \frac{1}{4} \sqrt{\frac{\pi}{2}} \tanh \left( \frac{\pi}{2} \right) \approx 0.287. \quad (G2)$$

The first equality follows from Eq. (40); the third one follows from Eq. (41) and the fact that $\lim_{n \to +\infty} h(n) = 0$. □

**Appendix H: Proofs of Eqs. (52), (55), and (56)**

*Proof of Eq. (52).* The equality $\text{tr}(P_1 P_2^G) = \text{tr}(P_1 P_2)$ in Eq. (52) follows from the fact that $P_1$ is invariant under the action of $G$, that is, $P_1^G = P_1$. The second equality in Eq. (52) can be derived from Eqs. (33) and (36) as follows,

$$\text{tr}(P_1 P_2) = \langle 00 \ldots 01 | P_2 | 00 \ldots 01 \rangle + \sum_{u \in B^1_{n-1}} (\langle u \otimes 0 | P_2 (| u \otimes | 0 \rangle)

$$

$$= h(n - 1) + (n - 1)\left[ 1 - h(n - 1) \right] = n - 1 - (n - 2)h(n - 1), \quad (H1)$$

where $B^1_{n-1}$ is the set of strings in $\{0, 1\}^{n-1}$ with Hamming weight 1. Here the second equality follows from the following equations,

$$\langle 00 \ldots 01 | P_2 | 00 \ldots 01 \rangle = \sum_{x \in \{0, 1\}^{n-1}} |\langle 00 \ldots 0 | \alpha_x \rangle|^2 \cdot |\langle 1 | \beta_x \rangle|^2 = \frac{1}{2^{n-1}} \sum_{x \in \{0, 1\}^{n-1}} \frac{1}{1 + (n - 1 - 2|x|)^2}$$

$$= \frac{1}{2^{n-1}} \sum_{j=0}^{n-1} \binom{n-1}{j} \frac{1}{1 + (n - 1 - 2j)^2} = h(n - 1), \quad (H2)$$

$$\langle u \otimes 0 | P_2 (| u \otimes | 0 \rangle = \sum_{x \in \{0, 1\}^{n-1}} |\langle u | \alpha_x \rangle|^2 \cdot |\langle 0 | \beta_x \rangle|^2 = \frac{1}{2^{n-1}} \sum_{x \in \{0, 1\}^{n-1}} \left[ \frac{1}{1 + (n - 1 - 2|x|)^2} \right]$$

$$= 1 - \frac{1}{2^{n-1}} \sum_{j=0}^{n-1} \binom{n-1}{j} \frac{1}{1 + (n - 1 - 2j)^2} = 1 - h(n - 1), \quad u \in B^1_{n-1}. \quad (H3)$$

□

*Proof of Eq. (55).* Note that $\Omega_{W_n}^G$ can be expressed as follows,

$$\Omega_{W_n}^G = pP_1 + (1 - p)P_2^G = pP_1 + (1 - p)P_1 P_2^G P_1 + (1 - p)(1 - P_1) P_2^G (1 - P_1), \quad (H4)$$

given that $P_1$ and $P_2^G$ commute with each other. Therefore,

$$\lambda_2(\Omega_{W_n}^G) = \max \{ p + (1 - p)\| P_1 P_2^G P_1 \|, (1 - p)\| (1 - P_1) P_2^G (1 - P_1) \| \} = 1 - p = \frac{n - 1}{n + (n - 2)h(n - 1)}. \quad (H5)$$

Here the second equality follows from the equality $p + (1 - p)\| P_1 P_2^G P_1 \| = 1 - p$ [cf. Eq. (54)] and the inequality $(1 - p)\| (1 - P_1) P_2^G (1 - P_1) \| \leq 1 - p$. □

*Proof of Eq. (56).* The equalities in Eq. (56) follow from Eq. (55).

When $3 \leq n \leq 40$, the lower bound in Eq. (56) can be verified directly by virtue of Eq. (39). When $n \geq 41$, the lower bound follows from the following equation

$$\sqrt{n} + (n - 2)\sqrt{\bar{n}}h(n - 1) + 1 > \sqrt{n} + n - 1 > n. \quad (H6)$$

Here the first inequality is a consequence of the inequalities $\sqrt{n}h(n - 1) > \sqrt{n - 1}h(n - 1) > 1$, the second of which follows from Proposition 4 and the assumption $n \geq 41$, given that $\sqrt{40}h(40) > \sqrt{41}h(41) > 1$. This observation completes the proof of Eq. (56). □
Appendix I: Proof of Theorem 6

Proof. In analogy to \( \Omega_k \) (cf. Appendix B), the verification operator \( \Omega_k^\phi \) can be expressed as

\[
\Omega_k^\phi = \left( \frac{n}{2} \right)^{-1} \sum_{i<j} \sum_{s=0}^r \tilde{Z}_{i,j}(k_{ss}) \otimes \left[ (|s\rangle\langle s|)^{\otimes 2} \right]_{i,j} + \left( \frac{n}{2} \right)^{-1} \sum_{i<j} \sum_{s<t} \sum_{u \in B(k_{st})} |u\rangle\langle u| \otimes (\Gamma_{i,j,u}^+ \otimes \Gamma_{j,i,u}^- + \Gamma_{i,j,u}^- \otimes \Gamma_{j,i,u}^+))_{i,j}
\]

\[
= \frac{1}{n(n-1)} \left( \sum_{s=0}^r k_s^2 - n \right) Z(k) + \frac{2}{n(n-1)} \sum_{i<j} \sum_{s<t} \tilde{Z}_{i,j}(k_{st}) \otimes \left[ (|\varphi_{s,t}^+\rangle\langle \varphi_{s,t}^+|)_{i,j} + \frac{1}{2} (|st\rangle\langle st| + |ts\rangle\langle ts|)_{i,j} \right]
\]

\[
+ \frac{1}{n(n-1)} \sum_{i<j} \sum_{s<t} \sum_{u \in B(k_{st})} |u\rangle\langle u| \otimes \left[ e^{i\phi(v(i,j,u))} |st\rangle\langle st|(e^{-i\phi(v(i,j,u))} + e^{i\phi(v(j,i,u))}) |ts\rangle\langle ts| e^{-i\phi(v(i,j,u))} \right]_{i,j}
\]

\[
= \frac{1}{n(n-1)} \left[ M'_1 + \sum_{s,t} M(s,t) \right]. \quad (11)
\]

Here \( |\varphi_{s,t}^+\rangle = \frac{1}{\sqrt{2}}(|s\rangle|t\rangle + |t\rangle|s\rangle) \), \( Z(k) = \sum_{u \in B(k)} |u\rangle\langle u| \), \( \tilde{Z}_{i,j}(k_{st}) \) is defined in Eq. 28, \( v(i,j,u) \) and \( v(j,i,u) \) are defined in Eqs. 78 and 79, \( M(s,t) \) is defined in Eq. (B3), and

\[
M'_1 := \left( \sum_{s=0}^r k_s^2 - n + \sum_{s \leq t} k_s k_t \right) Z(k) + \sum_{u,v \in B(k)} \sum_{u \sim v} \left( e^{i\phi(u)} |u\rangle \langle v| e^{-i\phi(u)} \right)
\]

\[
= \frac{1}{2} \left( n^2 - 2n + \sum_{s=0}^r k_s^2 \right) Z(k) + \sum_{u,v \in B(k)} \sum_{u \sim v} A_{uv} \left( e^{i\phi(u)} |u\rangle \langle v| e^{-i\phi(v)} \right), \quad (12)
\]

where the notation \( u \sim v \) means \( u_j \neq v_j \) for exactly two values of \( j \). The coefficient matrix \( A_{uv} \) for \( u,v \in B(k) \) happens to be the adjacency matrix \( A(k) \) of the transposition graph \( G(k) \) (cf. Appendix L).

Note that \( M'_1 \) can be turned into \( M_1 \) in Eq. (B2) by a diagonal unitary transformation; similarly, \( \Omega_k^\phi \) can be turned into \( \Omega_k \) by a diagonal unitary transformation (cf. Appendix B). Therefore, \( \Omega_k^\phi \) and \( \Omega_k \) have the same spectrum and the same spectral gap. Thanks to Eqs. (B8) and (B9), we have

\[
\nu(\Omega_k^\phi) = \nu(\Omega_k) = \min \left\{ \frac{1}{n-1}, 1 - \frac{k_0(k_0 + 1) + k_1(k_1 + 1)}{2n(n-1)} \right\} = \begin{cases} 1/2 & \text{for } k = (1,1,1), \\ 1/3 & \text{for } k = (2,1), \\ 1/(n-1) & \text{for } n \geq 4. \\ \end{cases} \quad (13)
\]

This result confirms Eq. (84) and implies Eq. (85) in view of Eq. (2) (cf. Theorem 3). \( \square \)

Appendix J: Proof of Theorem 7

Proof. The verification operator \( \Omega_{AS,n} \) can be expressed as

\[
\Omega_{AS,n} = \left( \frac{n}{2} \right)^{-1} \sum_{i<j} \sum_{s<t} \tilde{Z}_{i,j}(k_{st}) \otimes \left( T^+_{s,t} \otimes T^-_{s,t} + T^-_{s,t} \otimes T^+_{s,t} \right)_{i,j}
\]

\[
= \frac{2}{n(n-1)} \sum_{i<j} \tilde{Z}_{i,j}(k_{st}) \otimes \left[ (|\psi_{s,t}^+\rangle\langle \psi_{s,t}^+|)_{i,j} + (|\psi_{s,t}^-\rangle\langle \psi_{s,t}^-|)_{i,j} \right]
\]

\[
= \frac{1}{n(n-1)} \left[ M^{AS}_1 + \sum_{s<t} \sum_{u \in B(k'_s)} \sum_{v \in B(k'_t)} X_{s,t}^{u,v} \right]. \quad (J1)
\]

Here \( |\psi_{s,t}^+\rangle = \frac{1}{\sqrt{2}}(|s\rangle|t\rangle - |t\rangle|s\rangle) \), \( |\psi_{s,t}^-\rangle = \frac{1}{\sqrt{2}}(|s\rangle|s\rangle - |t\rangle|t\rangle) \),

\[
M^{AS}_1 := \frac{n(n-1)}{2} Z(k) - \sum_{u,v \in B(k)} |u\rangle\langle v| = \frac{n(n-1)}{2} Z(k) - \sum_{u,v \in B(k)} A_{uv} |u\rangle\langle v|, \quad (J2)
\]

\[
X_{s,t}^{u,v} := |u\rangle\langle u| + |v\rangle\langle v| - |u\rangle\langle v| - |v\rangle\langle u|, \quad (J3)
\]
and the notation \( u \sim v \) means \( u_j \neq v_j \) for exactly two values of \( j \). In addition, the coefficient matrix \( (A_{uv}) \) for \( u, v \in B(k) \) happens to be the adjacency matrix \( A(k) \) of the transposition graph \( G(k) \) [43]. Note that \( M_1^{AS} \) and all \( X_{s,t}^{u,v} \) [with \( s < t \), \( u \in B(k^s) \), \( v \in B(k^t) \), and \( u \sim v \)] are hermitian and have mutually orthogonal supports, so all of them are positive semidefinite given that \( \Omega_{AS} \) is positive semidefinite by construction.

According to Lemma 3 in Appendix [4], the smallest eigenvalue of \( A(k) \) is equal to \(-n(n-1)/2\) with multiplicity 1, and the second smallest eigenvalue of \( A(k) \) is \( n - n(n-1)/2 \). Therefore, the two largest eigenvalues of \( M_1^{AS} \) read

\[
\lambda_1(M_1^{AS}) = n(n-1), \quad \lambda_2(M_1^{AS}) = n(n-1) - n = n(n-2).
\] (J4)

In addition, direct calculations show that the maximum eigenvalue of \( X_{s,t}^{u,v} \) is 2. In conjunction with Eqs. (J1) and (J4), we can deduce the second largest eigenvalue and spectral gap of \( \Omega_{AS} \), with the result (assuming \( n \geq 3 \))

\[
\lambda_2(\Omega_{AS}) = \max \{ \frac{\lambda_2(M_1^{AS})}{n(n-1)}, \frac{\max \lambda_1(X_{s,t}^{u,v})}{n(n-1)} \} = \frac{n-2}{n-1},
\] (J5)

\[
\nu(\Omega_{AS}) = 1 - \lambda_2(\Omega_{AS}) = \frac{1}{n-1},
\] (J6)

which confirms Eq. (89).

Equation (90) follows from Eqs. (2) and (89).

**Appendix K: Proofs of Theorem 8 and Lemma 2**

**Proof of Theorem 8** According to Eq. (15), we have

\[
\Omega_{AS}^2 = \sum_{\mu \in \mathcal{N}} \frac{1}{d_\mu} \text{tr}(\Omega_{AS}^2 P_\mu) P_\mu = \sum_{\mu \in \mathcal{N}} \frac{1}{d_\mu} \text{tr}(\Omega_{AS} P_\mu) P_\mu.
\] (K1)

By representation theory, the projector \( P_\mu \) can be expressed as follows,

\[
P_\mu = \frac{d_\mu}{n!} \sum_{\sigma \in \mathcal{S}_n} \chi_\mu(\sigma) U_\sigma,
\] (K2)

where \( U_\sigma \) is the unitary operator corresponding to the permutation \( \sigma \), and \( \chi_\mu(\sigma) \) is the character of \( \sigma \) associated with the representation labeled by \( \mu \). Therefore,

\[
\text{tr}(\Omega_{AS} P_\mu) = \frac{1}{n(n-1)} \left[ \text{tr}(P_\mu M_1^{AS}) + \sum_{s<t} \sum_{u \in B(k^s)} \sum_{v \in B(k^t)} \chi_\mu(\tau) \langle \mu | M_1^{AS} | \mu \rangle \right] = d_\mu^2
\] (K3)

which implies Eq. (96). Here the first equality follows from Eq. (J1), and the notation \( u \sim v \) means \( u_j \neq v_j \) for exactly two values of \( j \). The second equality follows from Eqs. (K1) and (K5) below,

\[
\text{tr}(P_\mu M_1^{AS}) = \frac{n(n-1)}{2} \text{tr}[P_\mu Z(k)] - \sum_{u, v \in B(k)} A_{u,v} \langle u | P_\mu | v \rangle = \frac{n(n-1)}{2} \sum_{u \in B(k)} \langle u | P_\mu | u \rangle - \sum_{u \neq v \in B(k)} \langle \mu | P_\mu | \mu \rangle
\]

\[
= \frac{n(n-1)}{2} d_\mu^2 |B(k)| - \sum_{u, v \in B(k)} d_\mu \chi_\mu(\tau) = \frac{n(n-1)}{2} d_\mu^2 - \frac{n(n-1)}{2} d_\mu \chi_\mu(\tau),
\] (K4)

\[
\sum_{s<t} \sum_{u \sim v \in B(k^s)} \sum_{v \in B(k^t)} \langle u | P_\mu | u \rangle = 2 \sum_{s<t} \sum_{u \in B(k^s)} \langle u | P_\mu | u \rangle = n(n-1) |B(k^s)| d_\mu \chi_\mu(\tau) = \frac{n(n-1)}{2} d_\mu^2 + \frac{n(n-1)}{2} d_\mu \chi_\mu(\tau),
\] (K5)

where \( \tau \in \mathcal{S}_n \) is any transposition.
Alternatively, the trace $\tr(\Omega_{AS_n}P_\mu)$ can be derived by virtue of Eqs. (87) and (88) as follows,

$$\tr(\Omega_{AS_n}P_\mu) = \binom{n}{2}^{-1} \sum_{i<j} \tr(P_\mu P_{i,j}^{AS}) = \tr(P_\mu P_{1,2}^{AS}) = \sum_{s<t} \tr\left\{ P_\mu \left[ (T_{s,t}^+ \otimes T_{s,t}^- + T_{s,t}^- \otimes T_{s,t}^+) \otimes \bar{Z}(k_{st}) \right] \right\}$$

$$= \sum_{s<t} \tr\left\{ P_\mu U_{st}^\otimes (T_{s,t}^+ \otimes T_{s,t}^- + T_{s,t}^- \otimes T_{s,t}^+) \otimes \bar{Z}(k_{st}) \right\} \left( U_{st}^\otimes \right) = \sum_{s<t} \tr\left\{ P_\mu \left[ (|st\rangle\langle st| + |ts\rangle\langle ts|) \otimes \bar{Z}(k_{st}) \right] \right\}$$

$$= \tr[ P_\mu \bar{Z}(k) ] = \sum_{u \in B(k)} \langle u | P_\mu | u \rangle = \sum_{u \in B(k)} \sum_{\sigma \in S_n} \chi_\mu(\sigma) | u \rangle | U_\sigma | u \rangle = d_\mu^2 \mu | B(k) \rangle = d_\mu^2,$$  \hspace{1cm} (K6)

where

$$U_{st} = \frac{1}{\sqrt{2}} (|s\rangle \langle s| + |s\rangle \langle t| + |t\rangle \langle s| - |t\rangle \langle t|) + \sum_{r \neq s,t} |r\rangle \langle r|.$$  \hspace{1cm} (K7)

Equation (97) in Theorem 8 follows from Eq. (96) and Lemma 2. Equation (98) follows from Eqs. (2) and (97). □

Proof of Lemma 3. According to the well-known dimension formulas for $D_\mu$ and $d_\mu$ (see Refs. [47, 48] for example), we have

$$\frac{D_\mu}{d_\mu} = \frac{1}{n!} \prod_{j=1}^{d} \frac{(d + \mu_j - j)!}{(d - j)!} = \frac{1}{n!} \prod_{j=1}^{d} \frac{\Gamma(d + \mu_j - j + 1)}{\Gamma(d - j + 1)},$$  \hspace{1cm} (K8)

where $d = n$ is the local dimension. Note that this formula is still applicable when $d \neq n$. As an implication, we have

$$\ln \frac{D_\mu}{d_\mu} = \sum_{j=1}^{d} \ln \Gamma(d + \mu_j - j + 1) - \sum_{j=1}^{d} \ln \Gamma(d - j + 1) = \ln(n!).$$  \hspace{1cm} (K9)

Recall that the function $\ln \Gamma(x)$ is convex in $x$ for $x > 0$, we conclude that $\ln \frac{D_\mu}{d_\mu}$ is convex and thus Schur convex in $\mu$. Therefore, $\ln \frac{D_\mu}{d_\mu} \leq \ln \frac{D_{\mu'}}{d_{\mu'}}$ whenever $\mu < \mu'$, which confirms Lemma 2. □

Appendix L: The spectrum of the transposition graph

Let $k := (k_0, k_1, \ldots, k_r)$ with $k_0, \ldots, k_r$ being positive integers and $n = \sum_{j=0}^{r} k_j$. Recall that $B(k)$ is the set of all sequences of $n$ symbols in which $k_s$ symbols are equal to $s$ for $s = 0, 1, \ldots, r$. The transposition graph $G(k)$ is a regular graph whose vertices are labeled by sequences in $B(k)$. Two distinct vertices $u, v \in B(k)$ are adjacent iff $u$ and $v$ can be turned into each other by a transposition, that is, $|u_j| \neq |v_j|$ for exactly two values of $j$. The number of vertices in $G(k)$ is equal to the cardinality of $B(k)$, which reads $|B(k)| = n!/(\prod_{j=0}^{r} k_j!)$, and the degree of $G(k)$ is given by

$$d := \frac{1}{2} \left( n^2 - \sum_{s=0}^{r} k_s^2 \right).$$  \hspace{1cm} (L1)

Let $A(k)$ be the adjacency matrix of $G(k)$. The eigenvalues of $G(k)$ are defined as the eigenvalues of $A(k)$. Here we are interested in the largest and second largest eigenvalues of $G(k)$, which are crucial to the proof of Theorems 3 and 6. The lemma below follows from Eq. (4.2) in Ref. 144.

Lemma 3. The largest eigenvalue of $G(k)$ is equal to its degree $d$ and has multiplicity 1; the second largest eigenvalue of $G(k)$ is equal to $d - n$.

When $k_0 = k_1 = \cdots = k_{n-1} = 1$, the graph $G(k)$ reduces to the Cayley graph of the symmetric group. In this case we can also determine the smallest and second smallest eigenvalues of $G(k)$. To this end, note that the sequences in $B(k)$ can be divided into two groups of equal size: one group can be constructed from the sequence $(0, 1, \ldots, n - 1)$ by even permutations, and the other group can be constructed by odd permutations. In addition, $G(k)$ is a bipartite graph with respect to this partition; accordingly, the adjacency matrix $A(k)$ has a block form,

$$A = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix},$$  \hspace{1cm} (L2)
Lemma 4. Suppose $k = (k_0, k_1, \ldots, k_{n-1})$ with $k_j = 1$ for $j = 0, 1, \ldots, n - 1$. Then the smallest eigenvalue of $G(k)$ is equal to $-d$ and has multiplicity 1, where $d = n(n - 1)/2$ is the degree of $G(k)$; the second smallest eigenvalue of $G(k)$ is equal to $n - d$.

Let us take $k = (1, 1, 1)$ for example. In this case we have $n = d = 3$, and $G(k)$ is a bipartite graph with six vertices labeled by the sequences $(0, 1, 2), (1, 2, 0), (2, 0, 1), (0, 2, 1), (1, 0, 2), (2, 1, 0)$. With respect to this order, the adjacency matrix of $G(k)$ reads

$$A(k) = \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}.$$  \hspace{1cm} (L3)

Direct calculation shows that $A(k)$ has three distinct eigenvalues $3, 0, -3$, with multiplicities $1, 4, 1$, respectively, which agrees with Lemmas 3 and 4.

\begin{thebibliography}{99}
\bibitem{1} R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum Entanglement. Rev. Mod. Phys. \textbf{81}, 865 (2009).
\bibitem{2} O. Gühne and G. Tóth, Entanglement detection. \textit{Phys. Rep.} \textbf{474}, 1 (2009).
\bibitem{3} R. H. Dicke, Coherence in spontaneous radiation processes. \textit{Phys. Rev.} \textbf{93}, 99 (1954).
\bibitem{4} T.-C. Wei, and P. M. Goldbart, Geometric measure of entanglement and applications to bipartite and multipartite quantum states. \textit{Phys. Rev. A} \textbf{68}, 042307 (2003).
\bibitem{5} R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum Entanglement. \textit{Rev. Mod. Phys.} \textbf{81}, 865 (2009).
\bibitem{6} M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral, Quantum teleportation and multiparticle entanglement. \textit{Phys. Rev. A} \textbf{59}, 156 (1999).
\bibitem{7} L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schnied, and P. Treutlein, Quantum metrology with nonclassical states of atomic ensembles. \textit{Rev. Mod. Phys.} \textbf{90}, 035005 (2018).
\bibitem{8} X.-Y. Luo, Y.-Q. Zou, L.-N. Wu, Q. Liu, M.-F. Han, M. K. Tey, and L. You, Deterministic entanglement generation from driving through quantum phase transitions. \textit{Science} \textbf{355}, 620-623 (2017).
\bibitem{9} N. Kiesel, C. Schmid, G. Tóth, E. Solano, and H. Weinfurter, Experimental observation of four-photon entangled Dicke state with high fidelity. \textit{Phys. Rev. Lett.} \textbf{98}, 063604 (2007).
\bibitem{10} R. Prevedel et al. Experimental realization of Dicke states of up to six qubits for multiparity quantum networking. \textit{Phys. Rev. Lett.} \textbf{103}, 020503 (2009).
\bibitem{11} W. Wieczorek et al. Experimental entanglement of a six-photon symmetric Dicke state. \textit{Phys. Rev. Lett.} \textbf{103}, 020504 (2009).
\bibitem{12} P. Krammer, H. Kampermann, D. Bruß, R. A. Bertlmann, L. C. Kwek, and C. Macchiavello, Multiparite Entanglement Detection via Structure Factors. \textit{Phys. Rev. Lett.} \textbf{103}, 100502 (2009).
\bibitem{13} A. Chiuri, G. Vallone, N. Bruno, C. Macchiavello, D. Bruß, and P. Mataloni, Hyperentangled Mixed Phased Dicke States: Optical Design and Detection. \textit{Phys. Rev. Lett.} \textbf{105}, 250501 (2010).
\bibitem{14} K. A. Dennis and W. K. Wootters, Entanglement sharing among quantum particles with more than two orthogonal states. \textit{Phys. Rev. A} \textbf{65}, 010301(R) (2001).
\bibitem{15} P. Zanardi, Quantum entanglement in fermionic lattices. \textit{Phys. Rev. A} \textbf{65}, 042101 (2002).
\bibitem{16} S. Bravyi, Entanglement entropy of multipartite pure states. \textit{Phys. Rev. A} \textbf{67}, 012313 (2003).
\bibitem{17} Y.-Q. Zou et al. Beating the classical precision limit with spin-1 Dicke states of more than 10,000 atoms. \textit{Proc. Natl. Acad. Sci.} \textbf{115}, 6381 (2018).
\bibitem{18} D. Cruz et al. Efficient quantum algorithms for GHZ and W states, and implementation on the IBM quantum computer. \textit{Adv. Quantum Technol.} \textbf{2}, 1900015 (2019).
\bibitem{19} H. Häffner et al. Scalable multiparticle entanglement of trapped ions. \textit{Nature} \textbf{438}, 643 (2005).
\bibitem{20} A. Chiuri, C. Greganti, and P. Mataloni, Engineering a C-Phase quantum gate: optical design and experimental realization. \textit{Eur. Phys. J. D} \textbf{66}, 195 (2012).
\bibitem{21} Y. Zhang, F. S. Roux, T. Konrad, M. Agnew, J. Leach, and A. Forbes, Engineering two-photon high-dimensional states through quantum phase interference. \textit{Sci. Adv.} \textbf{2(2)}, e1501165 (2016).
\bibitem{22} D. W. Berry, M. Kieferová, A. Scherer, Y. R. Sanders, G. H. Low, N. Wiebe, C. Gidney, and R. Babbush, Improved techniques for preparing eigenstates of fermionic Hamiltonians. \textit{npj Quantum Inf.} \textbf{4}, 22 (2018).
\bibitem{23} S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements. \textit{Phys. Rev. Lett.} \textbf{106}, 230501 (2011).
\bibitem{24} M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using
\end{thebibliography}
hypothesis testing. *J. Phys. A: Math. Gen.* **39**, 14427 (2006).

[25] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing. *New J. Phys.* **11**, 043028 (2009).

[26] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Reliable quantum certification of photonic state preparations. *Nat. Commun.* **6**, 8498 (2015).

[27] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, Reliable quantum certification of photonic state preparations. *Quantum Sci. Technol.* **2**, 015004 (2017).

[28] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).

[29] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).

[30] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario. *Phys. Rev. A* **100**, 062335 (2019).

[31] Z. Li, Y.-G. Han, and H. Zhu, Efficient verification of bipartite pure states. *Phys. Rev. A* **100**, 032316 (2019).

[32] K. Wang and M. Hayashi, Optimal verification of two-qubit pure states. *Phys. Rev. A* **100**, 032315 (2019).

[33] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states. *npj Quantum Inf.* **5**, 112 (2019).

[34] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing. *Phys. Rev. Lett.* **115**, 220502 (2015).

[35] H. Zhu and M. Hayashi, Efficient verification of hypergraph states. *Phys. Rev. Appl.* **12**, 054047 (2019).

[36] M. Hayashi and Y. Takeuchi, Verifying commuting quantum computations via fidelity estimation of weighted graph states. *New J. Phys.* **21**, 093060 (2019).

[37] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient verification of Dicke states. *Phys. Rev. Appl.* **12**, 044020 (2019).

[38] H. Zhu and M. Hayashi, Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A* **99**, 052346 (2019).

[39] Z. Li, Y.-G. Han, and H. Zhu, Optimal verification of Greenberger-Horne-Zeilinger States. (2019), arXiv:1909.08979, to appear in *Phys. Rev. Appl.*

[40] P. R. Halmos, *Measure theory*. (Springer, New York, 2013).

[41] R. L. Schilling, *Measures, Integrals and Martingales*. (Cambridge University Press, Cambridge, England, 2005).

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

[43] P. J. Chase, Transposition Graphs. *SIAM. J. Comput.* **2(2)**, 128 (1973).

[44] P. Caputo, T. M. Liggett, and T. Richthammer, Proof of Aldous’ spectral gap conjecture. *J. Amer. Math. Soc.* **23(3)**, 831-851 (2010).

[45] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A* **62**, 062314 (2000).

[46] 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).

[47] H. Weyl, *The Theory of Groups and Quantum Mechanics*. (Methuen & co. ltd., London, 1931. Translated from the second (revised) German edition by H. P. Robertson).