Decomposition of a symmetric multipartite observable

You Zhou, Chenghao Guo, and Xiongfeng Ma*
Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

(Received 23 February 2019; published 16 May 2019)

Production and verification of multipartite quantum state are an essential step in quantum information processing. In this work, we propose an efficient method to decompose symmetric multipartite observables, which are invariant under permutations between parties, with only $(N+1)(N+2)/2$ local measurement settings, where N is the number of qubits. We apply the decomposition technique to evaluate the fidelity between an unknown prepared state and any target permutation invariant state. In addition, for some typical permutation invariant states, such as the Dicke state with a constant number of excitations, m, we derive a tight linear bound on the number of local measurement settings, $m(2m+3)N+1$. Meanwhile, for the Greenberger-Horne-Zeilinger state, the W state, and the Dicke state, we prove a linear lower bound, $\Theta(N)$. Hence, for these particular states, our decomposition technique is optimal.

DOI: 10.1103/PhysRevA.99.052324

I. INTRODUCTION

Quantum states with genuine multipartite entanglement, such as the GHZ state [1], the Dicke state (including the W state) [2,3], and the general graph (stabilizer) state [4,5], are essential ingredients for many quantum information processing tasks, such as multipartite quantum key distribution [6], quantum secret sharing [7,8], quantum error correction [5,9], measurement-based quantum computing [10], and quantum metrology [11,12]. In practice, due to the noise caused by the uncontrolled interaction between the system and the environment, the prepared state unavoidably deviates from the target one. Hence, it is necessary to quantify such deviation, which acts as a calibration for the experimental system and provides the basis of further information processing.

A straightforward method to benchmark the system is quantum state tomography [13,14]. In reality, due to the tensor product structure of the Hilbert space, the required resources scale exponentially with the number of system parties (say, qubits) in tomography. In the last decade, the qubit number under manipulation increases significantly in various experiment systems, such as those based on ion-trap [15], superconducting [16], and linear optics [17]. Thus, it is impractical to directly conduct tomography for state-of-the-art multipartite quantum systems. Fortunately, the required resources can be dramatically reduced if one possesses some preknowledge about the prepared state and takes advantage of symmetries. In this spirit, several efficient tomography methods were put forward for various types of quantum states, such as the low-rank state [18,19], the matrix product state [20–22], and the permutation invariant (PI) state [23,24]. The insight underlying this simplification is that one only needs the parameters of the ansatz states there, such as the tensor network state and the PI state, whose number only increases polynomially with the number of qubits N.

In practical quantum information tasks, instead of gaining all the information about the density matrix, one only needs to guarantee that the prepared state holds sufficiently high fidelity with the target state. If focusing on fidelity evaluation instead of a full tomography, one can further reduce the measurement efforts. Sometimes, one only needs to detect or witness entanglement for multipartite systems. Since quantum states with high symmetries are widely used in information processing, these tasks generally involve symmetric observables, which are invariant under permutations of parties. In addition, multipartite measurement is normally very challenging in practice. Instead, it is often broken down to local measurements [25,26]. Take an N-qubit system, for example, to measure the fidelity between a prepared state ρ and the GHZ state, $\mathrm{Tr}(\rho|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|)$; one cannot measure it directly with $|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|$. Instead, $\langle|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|\rangle$ is broken down to a set of local measurements $\{A^{\otimes N}\}$, whose number determines the complexity of fidelity evaluation. Note that from a local measurement setting (LMS) $A^{\otimes N}$, not only the expectation value $\langle A^{\otimes N}\rangle$, but also the full statistics can be obtained. For instance, one can get the probability of any specific measurement result, say an N-bit string, from the Pauli Z measurement, $\sigma_Z^{\otimes N}$.

In this work, we focus on estimating the fidelity with PI states. The PI state set $\mathcal{S}_{\mathrm{PI}}$ contains all the states which are invariant under any subsystem permutation,

$$\rho^{\mathrm{PI}} = P(\pi)\rho^{\mathrm{PI}}P(\pi),\ \forall\pi, \tag{1}$$

where $P(\pi)$ is the permutation operation of the element π in the symmetry group S_N. It is worth mentioning another related state set, the symmetric state set $\mathcal{S}_S$, which contains all the pure states satisfying

$$|\psi_s\rangle = P(\pi)|\psi_s\rangle,\ \forall\pi \tag{2}$$

and their convex combination. It is not hard to see that $\mathcal{S}_S \subset \mathcal{S}_{\mathrm{PI}}$ [27].

By decomposing a symmetric observable, we construct a set of $(N+1)(N+2)/2$ LMSs to evaluate the fidelity

*xma@tsinghua.edu.cn

 ©2019 American Physical Society

between a prepared state and any target PI state. To do this, we first give a general theorem which constructs a set of product-state basis for the symmetric subspace of the N-qudit Hilbert space. Then, based on this theorem, one can find a set of product operators as the basis for the symmetric subspace of the N-partite operator space, which contains all PI states. Thus, any PI state can be decomposed as the linear combination of these basis operators. As a result, by measuring all the basis operators with local measurements, one can finally evaluate the fidelity with respect to any target PI state by only postprocessing the measurement results. By observing that several product operators can be measured with the same LMS, we finally reduce the number of LMSs to $(N+1)(N+2)/2$.

Moreover, based on this general decomposition, we can further reduce the number of LMSs for some typical PI states, such as the GHZ state, the W state, and the Dicke state, with a constant number of excitations. Define measurement complexity as the minimal number of LMSs to decompose a state and we systemically study their measurement complexities. To give an upper bound of the measurement complexity, we show an explicit decomposition of the state by finding a smaller subspace of the symmetric subspace which contains the state and constructing the basis of it with fewer LMSs. To give a lower bound, we find some subspace where the projection of the target state shows some specific form and prove that one needs enough LMSs to reestablish the same form. Combing the upper and the lower bounds, we finally show that their measurement complexities all scale as $\Theta(N)$.

The paper is organized as follows. In Sec. II, we construct a set of product-state bases for the symmetric subspace. In Sec. III, we propose a method based on the previous theorem, with $(N+1)(N+2)/2$ LMSs, to evaluate the fidelity between an unknown state and any target PI state. In Sec. V, we further reduce the number of LMSs in fidelity evaluation for some special PI states, GHZ, W, and Dicke. We finally conclude in Sec. VI with further discussions.

II. PRODUCT-STATE BASIS FOR SYMMETRIC SUBSPACE

In this section, we construct a set of linearly independent vectors (states) in the product form, which can span the symmetric subspace. This construction will help us to find LMSs for decomposition of symmetric operators and fidelity evaluation of the PI state in the following sections.

First, let us briefly review the symmetric subspace of an N-qudit Hilbert space $\mathcal{H}_d^{\otimes N}$, denoted $\mathrm{Sym}_N(\mathcal{H}_d)$. Given an element π in the symmetric group S_N with N letters, the corresponding permutation operator defined on $\mathcal{H}_d^{\otimes N}$ is

$$P_d(\pi) = \sum_{i_1,\ldots,i_N\in[d]} |i_{\pi^{-1}(1)},\ldots,i_{\pi^{-1}(N)}\rangle\langle i_1,\ldots,i_N|, \tag{3}$$

where $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ is the local basis for each qudit and $[d]=\{0,1,\ldots,d-1\}$. The symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)\subseteq\mathcal{H}_d^{\otimes N}$ contains all the pure states which are invariant under permutation,

$$\mathrm{Sym}_N(\mathcal{H}_d) = \left\{|\Psi\rangle\in\mathcal{H}_d^{\otimes N} : P_d(\pi)|\Psi\rangle = |\Psi\rangle, \quad \forall\pi\in S_N\right\}. \tag{4}$$

In the qubit case with $d=2$, we denote the permutation operator $P(\pi)$ for simplicity.

It is known that the dimension of $\mathrm{Sym}_N(\mathcal{H}_d)$ is given by [28]

$$D_S = \binom{N+d-1}{N} = \frac{(N+d-1)!}{N!(d-1)!}, \tag{5}$$

and there is a set of orthogonal (unnormalized) bases of $\mathrm{Sym}_N(\mathcal{H}_d)$,

$$\left\{|\Psi_{\vec{i}}\rangle = \sum_{\pi}|0\rangle^{\otimes i_0}|1\rangle^{\otimes i_1}\ldots|d-1\rangle^{\otimes i_{d-1}}\middle| i_k\in\mathbb{Z}^+, \sum_{k=0}^{d-1} i_k = N\right\}, \tag{6}$$

where $\mathbb{Z}^+$ denotes the nonnegative integer set and $\vec{i}=(i_0,i_1,\ldots,i_{d-1})$ is a d-dimensional vector. Here, $\sum_\pi$ represents the summation over all permutations of N qudits that yield different expressions. We keep this notation throughout the paper.

Meanwhile, the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$ can be spanned by the symmetric product states,

$$\mathrm{Sym}_N(\mathcal{H}_d) = \mathrm{span}\{|\phi\rangle^{\otimes N} : |\phi\rangle\in\mathcal{H}_d\}. \tag{7}$$

For a finite N, it is not hard to see that the symmetric product states, $|\phi\rangle^{\otimes N}$, are linearly dependent. In the following, we construct a product-state basis for the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$, by selecting $\binom{N+d-1}{N}$ linearly independent product states, as shown in Theorem II.

Define a $d\times(N+1)$ matrix with complex elements $a_{k,j}$ satisfying

$$\begin{aligned} &a_{0,j} = 1,\\ &a_{k,j}\neq a_{k,j'}, \quad \forall 1\leqslant k\leqslant d-1, \end{aligned} \tag{8}$$

for all $0\leqslant j\neq j'\leqslant N$. That is, all the elements in the zeroth row are 1; and for the other rows, the elements are different for different columns.

Theorem 1. The following state set $\mathcal{B}$ contains $\binom{N+d-1}{N}$ linearly independent vectors which are (unnormalized) symmetric product states, and they can span the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$,

$$\mathcal{B} = \left\{|\Phi_{\vec{j}}\rangle = (a_{0,j_0}|0\rangle + a_{1,j_1}|1\rangle + \ldots + a_{d-1,j_{d-1}}|d-1\rangle)^{\otimes N}|j_k\in\mathbb{Z}^+, \quad \sum_{k=0}^{d-1} j_k = N\right\}, \tag{9}$$

where the coefficients a_{k,j_k} are selected from any matrix satisfying Eq. (8).

In the following, we call the vectors in $\mathcal{B}$ a set of bases of $\mathrm{Sym}_N(\mathcal{H}_d)$, even though they might not be orthogonal with each other. The complete proof of Theorem 1 is shown in Appendix A, which is based on induction. Here, we present the qubit case of Theorem 1 in Corollary 1 and provide a simple proof.

Corollary 1. The following state set $\mathcal{B}$ contains $N+1$ linearly independent vectors which are (unnormalized) symmetric product states, and they can span the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_2)$,

$$\mathcal{B} = \{|\Phi_j\rangle = (|0\rangle + a_j|1\rangle)^{\otimes N} | 0 \leqslant j \leqslant N\}, \tag{10}$$

where a_i are complex numbers and $a_j \neq a_{j'}$ for $j \neq j'$.

Proof. The state set $\mathcal{B}$ only contains symmetric product states in $\mathrm{Sym}_N(\mathcal{H}_2)$. From Eq. (5), the dimension of $\mathrm{Sym}_N(\mathbb{C}^2)$ is $N+1$, which equals the cardinality of $\mathcal{B}$. Therefore, we only need to prove that the states in $\mathcal{B}$ are linearly independent.

In this qubit case, the orthogonal basis, given in Eq. (6),

$$\left\{|\Psi_i\rangle = \sum_{\pi} |0\rangle^{\otimes N-i}|1\rangle^{\otimes i}, 0 \leqslant i \leqslant N\right\}, \tag{11}$$

contains all the Dicke states. If one expands $|\Phi_j\rangle$ of Eq. (10) in this $\{|\Psi_i\rangle\}$ basis, the coefficients are $(1, a_j, a_j^2, \ldots, a_j^N)^T$. The matrix formed by the coefficients $(|\Phi_0\rangle, |\Phi_1\rangle, \ldots, |\Phi_N\rangle)$ is a Vandermonde matrix which is nonsingular. Consequently, $|\Phi_k\rangle$ are linearly independent and form a basis of $\mathrm{Sym}_N(\mathcal{H}_2)$.

III. SYMMETRIC OBSERVABLE DECOMPOSITION AND FIDELITY EVALUATION

In this section, we propose a method to decompose a symmetric observable and apply it to evaluate the fidelity between a prepared state ρ and any target PI state using $(N+1)(N+2)/2$ LMSs. Here, we only focus on the N-qubit scenario, but the method can be generalized to the N-qudit case. As shown in Eq. (1), a PI state is defined on the density matrix level. That is, ρ^{PI} is invariant under any permutation operation among qubits. Due to this permutation invariant property, we only need to consider the case where the local operators in LMS are the same for all qubits [23], that is, in the form of $A^{\otimes N}$, where A is a qubit Hermitian operator. Generally, one needs a set of LMSs $\{A_i^{\otimes N}\}$ to evaluate the fidelity. Also, the target state is normally pure. We have the following theorem.

Theorem 2. For any N-qubit target PI state $|\Psi^{\mathrm{PI}}\rangle$, the fidelity between a prepared state ρ and $|\Psi^{\mathrm{PI}}\rangle$,

$$F = \langle\Psi^{\mathrm{PI}}|\rho|\Psi^{\mathrm{PI}}\rangle, \tag{12}$$

can be evaluated with $(N+1)(N+2)/2$ LMSs.

Denote the projector formed by the PI state, $|\Psi^{\mathrm{PI}}\rangle\langle\Psi^{\mathrm{PI}}|$, to be Ψ^{PI}. In order to measure the fidelity F in Eq. (12), one should decompose the projector Ψ^{PI} into local measurements. In the following, we introduce the symmetric subspace of N-qubit Hermitian operators where Ψ^{PI} is located. Then, by constructing a set of tensor-product bases of this symmetric subspace, we can accordingly decompose Ψ^{PI}.

Proof. Let us first define the symmetric subspace of N-qubit Hermitian operators. Denote the N-qubit Pauli group G_N, whose element, called the N-qubit Pauli operator, is a tensor product of single-qubit Pauli operators and identity $G_1 = \{\mathbb{I}, \sigma_X, \sigma_Y, \sigma_Z\}$. An N-qubit Hermitian operator M can be written as the linear combination of the Pauli operators in G_N. Since the operators we consider here are Hermitian, their coefficients must be real. Thus, the operator space F_{G_N} is isomorphic to $(\mathbb{R}^4)^{\otimes N}$, with $\mathbb{R}$ denoting the real domain. Then the corresponding symmetric subspace, $\mathrm{Sym}_N(G_1)$, is defined as

$$\mathrm{Sym}_N(G_1) = \{M \in F_{G_N} : P(\pi)MP(\pi) = M, \forall\pi \in S_N\}. \tag{13}$$

By the definition in Eq. (1), any PI state $\rho^{\mathrm{PI}} \in \mathrm{Sym}_N(G_1)$.

Since $\mathrm{Sym}_N(G_1)$ is isomorphic to $\mathrm{Sym}_N(\mathbb{R}^4)$, the dimension of $\mathrm{Sym}_N(G_1)$ is $\binom{N+3}{3}$ according to Eq. (5). Meanwhile, the results shown in Sec. II can be directly applied to the operator space here.

(1) Similarly to the orthogonal basis shown in Eq. (6), the following Hermitian operators form an orthogonal basis (in the sense of the Hilbert-Schmidt inner product) of $\mathrm{Sym}_N(G_1)$,

$$M_{i,j,k} = \sum_{\pi} \mathbb{I}^{\otimes i} \otimes \sigma_X^{\otimes j} \otimes \sigma_Y^{\otimes k} \otimes \sigma_Z^{\otimes(N-i-j-k)}, \tag{14}$$

where $\sigma_X^{\otimes j}$ denotes that there are totally j qubits with σ_X on them, similar to $\mathbb{I}^{\otimes i}, \sigma_Y^{\otimes k}, \sigma_Z^{\otimes(N-i-j-k)}$.

(2) Similarly to Eq. (7), product operators can also span the symmetric subspace,

$$\mathrm{Sym}_N(G_1) = \mathrm{span}\{A^{\otimes N} : A = a\mathbb{I} + b\sigma_X + c\sigma_Y + d\sigma_Z\}, \tag{15}$$

where $a, b, c, d \in \mathbb{R}$.

(3) Similarly to the proof of Theorem 1, with the previous two steps, we only need to select $\binom{N+3}{3}$ linearly independent operators $\{A^{\otimes N}\}$ to act as the product-form basis of $\mathrm{Sym}_N(G_1)$. According to Theorem 1, we can construct a basis set for $\mathrm{Sym}_N(G_1)$ with product operators, where the local bases are $\{\mathbb{I}, \sigma_X, \sigma_Y, \sigma_Z\}$. To be specific,

$$\mathcal{B}_o = \left\{(a_{1,j_1}\mathbb{I} + a_{2,j_2}\sigma_X + a_{3,j_3}\sigma_Y + a_{0,j_0}\sigma_Z)^{\otimes N} \,\middle|\, \sum_{k=0}^{3} j_k = N\right\}, \tag{16}$$

where the subscript "o" denotes an operator set, and the coefficients a_{k,j_k} with $0 \leqslant k \leqslant 3$ and $0 \leqslant j_k \leqslant N$ are real numbers satisfying Eq. (8).

After step 3, we further reduce the number $\binom{N+3}{3}$ down to $\binom{N+2}{2}$ due to the fact that some of the product operators can be measured by the same LMS. Since $a_{0,j_0} = 1$ for any j_0, the operator set in Eq. (16) can also be written as

$$\mathcal{B}_o = \{(a_i\mathbb{I} + b_j\sigma_X + c_k\sigma_Y + \sigma_Z)^{\otimes N} | 0 \leqslant i, j, k \leqslant N,\ i + j + k \leqslant N\}, \tag{17}$$

where, for simplicity of notation, let $a_i = a_{1,i}$, $b_j = a_{2,j}$, and $c_k = a_{3,k}$.

On account of Observation 1, below, product operators in $\mathcal{B}_o$ with different a_i but the same b_j and c_k can be obtained via the same LMS $(b_j\sigma_X + c_k\sigma_Y + \sigma_Z)^{\otimes N}$. Therefore, the total number of LMSs required is the number of different parameter sets (b_j, c_k), which equals the number of solutions for $j + k \leqslant N$, i.e., $\binom{N+2}{2} = (N+1)(N+2)/2$.

Consequently, one can utilize $(N+1)(N+2)/2$ LMSs to obtain the expectation values of all the basis operators in $\mathcal{B}_o$ of symmetric subspace $\mathrm{Sym}_N(G_1)$. Since any PI state $\Psi^{\mathrm{PI}} \in \mathrm{Sym}_N(G_1)$, we can decompose any Ψ^{PI} in this basis and finally obtain the fidelity in Eq. (12).

Observation 1. The expectation value of the product operator $(a\mathbb{I} + b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N}$ can be obtained via the LMS $(b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N}$.

Proof.

$$(a\mathbb{I} + b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N} = \sum_{i=0}^{N} a^i \sum_{\pi} \mathbb{I}^{\otimes i} \otimes (b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N-i}. \tag{18}$$

Note that each term in Eq. (18) can be directly obtained from the LMS, $(b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N}$.

Some remarks on and discussion of Theorem 2 are listed as follows.

(1) We show how to efficiently decompose a general PI state in a set of product-form basis in Appendix B, which is useful in practical implementation. And we remark that this decomposition is suitable for general symmetric operators, which may be useful for other related problems. In fact, on account of Theorem 1, it is possible to choose other sets of product-form bases. Thus, we also discuss how to choose a basis which is more robust to noise there.

(2) Theorem 2 can be directly extended to the qudit case, by considering the generalized local Pauli basis for qudits.

(3) Our method can evaluate the fidelity between an unknown prepared state and any PI state with the same $\binom{N+2}{2}$ LMSs, by postprocessing only the measurement results.

(4) The basis operators in $\mathcal{B}_o$ of Eq. (16) span the symmetric subspace $\mathrm{Sym}_N(G_1)$, which contains all the PI states, $\rho^{\mathrm{PI}} \in \mathrm{Sym}_N(G_1)$. From the proof of Theorem 2, the expectation values of all these operators in $\mathcal{B}_o$ can be measured with $\binom{N+2}{2}$ LMSs. As a result, in addition to the fidelity evaluation in Eq. (12), one can also gain more detailed information on a generic PI state ρ^{PI} with these measurements. This is related to permutation invariant tomography [23], where one can extract the permutation invariant component of a state with $\binom{N+2}{2}$ LMSs. Note that our basis constructed in Eq. (16) is more explicit and different, compared to the one shown in Ref. [23].

We show in the following that our decomposition method can further help to reduce the number of LMSs for some special PI states. To be specific, it is known that for the GHZ state and the W state, one only needs $N+1$ and $2N-1$ LMSs to decompose them, respectively [29], compared with $\binom{N+2}{2}$ for a general PI state. In the following sections, we define a quantity called the *measurement complexity* which quantifies the minimal number of LMSs to decompose a state and systemically study the measurement complexities for the GHZ state, the W state, and the Dicke state.

TABLE I. Measurement complexity of some typical PI states. For these states, the measurement complexity is linear, $\Theta(N)$.

State	Upper bound	Lower bound
W	$2N-1$ [29]	$N-1$
Dicke	$m(2m+3)N+1$	$N-2m+1$
GHZ	$N+1$ [29]	$\lceil \frac{N+1}{2} \rceil$

IV. COMPLEXITY UPPER BOUND OF THE DICKE STATE

In the previous section, we have obtained a method to decompose any PI state, and in the following we focus on reducing the number of LMSs for some specific PI states. Certain PI states are typical for quantum information processing and have been extensively studied, including the GHZ state, the W state, and the Dicke state. In this section and the next section, the numbers of LMSs required for these states are discussed.

First, let us give the definition of the *measurement complexity* of PI states, strictly speaking, symmetric-measurement complexity, since the LMSs utilized here are in the symmetric form. For simplicity, we use the term measurement complexity without confusion.

Definition 1. For an N-qubit PI state ρ, measurement complexity $C_S(\rho)$ is the minimal number of LMSs to decompose it,

$$C_S(\rho) = \min n_A, \quad s.t., \rho = \sum_{i=1}^{n_A} \sum_{j=1}^{N} \alpha_{ij} \sum_{\pi} \mathbb{I}^{\otimes j} A_i^{\otimes N-j}, \tag{19}$$

where $A_i = b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z$ and $\alpha_{ij}, b_i, c_i, d_i \in \mathbb{R}$.

Here we allow $\sum_\pi \mathbb{I}^{\otimes j} A_i^{\otimes N-j}$ to appear in the summation in Eq. (19), since its expectation value can be inferred from the LMS $A_i^{\otimes N}$. Note that we do not need to introduce $\mathbb{I}$ into A_i, like $(a_i\mathbb{I} + b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z)^{\otimes N}$, since any operator $\sum_\pi \mathbb{I}^{\otimes j}(a_i\mathbb{I} + A_i)^{\otimes N-j}$ can be written as a combination of $\sum_\pi \mathbb{I}^{\otimes j} A_i^{\otimes N-j}$.

A summary of the results is reported in Table I. It is noteworthy that the measurement complexities for these states all increase linearly with the number of qubits, $\Theta(N)$, whereas the measurement complexity of a general PI state grows quadratically with N, as stated in Theorem 2.

In this section, we focus on finding the upper bound of the measurement complexity. To find the upper bound, one needs to give a specific decomposition of the state. Note that one can use $N+1$ and $2N-1$ LMSs to decompose the GHZ and the W state, respectively, which are listed as the upper bounds in Table I.

In the following, we give an explicit decomposition of the Dicke state $|D_{N,m}\rangle$ of N qubits with m excitations [2],

$$|D_{N,m}\rangle = \frac{1}{\sqrt{\binom{N}{m}}} \sum_{\pi} |0\rangle^{\otimes N-m} |1\rangle^{\otimes m}, \tag{20}$$

using $m(2m+3)N+1$ LMSs. Note that as $m=1$, it is the W state [3],

$$|W_N\rangle = \frac{1}{\sqrt{N}}(|10\ldots01\rangle + |01\ldots0\rangle + \ldots + |00\ldots1\rangle). \tag{21}$$

To do so, we characterize a subspace of the symmetric subspace that contains the state, then construct a basis set for that subspace with some LMSs. Consequently, one obtains an upper bound of the measurement complexity of $|D_{N,m}\rangle$, which is summarized in the following theorem.

Theorem 3. The measurement complexity of the Dicke state $|D_{N,m}\rangle$ is upper bounded by

$$C_S(D_{N,m}) \leqslant m(2m+3)N+1. \tag{22}$$

Proof. The density matrix of $|D_{N,m}\rangle$ can be explicitly written as

$$\begin{aligned} D_{N,m} &= \frac{1}{\binom{N}{m}}\sum_{t=0}^{m}\Theta_t, \\ \Theta_t &\equiv \sum_{\pi}(|1\rangle\langle 1|)^{\otimes m-t}\otimes(|0\rangle\langle 1|)^{\otimes t}\otimes(|1\rangle\langle 0|)^{\otimes t} \\ &\quad\otimes(|0\rangle\langle 0|)^{\otimes N-m-t}, \end{aligned} \tag{23}$$

where we denote each term in the summation Θ_t, and Θ_0 is the diagonal term. It is clear that Θ_0 can be obtained by the Z-basis measurement $\sigma_Z^{\otimes N}$. Thus in the following we focus on Θ_t with $1\leqslant t\leqslant m$, which are the off-diagonal terms.

With the relations $|1\rangle\langle 1| = (\mathbb{I}-\sigma_Z)/2$, $|0\rangle\langle 0| = (\mathbb{I}+\sigma_Z)/2$, $|0\rangle\langle 1| = (\sigma_X + i\sigma_Y)/2$, and $|1\rangle\langle 0| = (\sigma_X - i\sigma_Y)/2$, Θ_t can be written in the form

$$\Theta_t = \sum_{\pi}\left(\frac{\mathbb{I}-\sigma_Z}{2}\right)^{\otimes m-t}\otimes\chi_t\otimes\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes N-m-t}, \tag{24}$$

where χ_t is given by

$$\begin{aligned} \chi_t &= \sum_{\pi}(|0\rangle\langle 1|)^{\otimes t}\otimes(|1\rangle\langle 0|)^{\otimes t} \\ &= \sum_{\pi}\left(\frac{\sigma_X+i\sigma_Y}{2}\right)^{\otimes t}\otimes\left(\frac{\sigma_X-i\sigma_Y}{2}\right)^{\otimes t} \\ &= \sum_{l=0}^{2t}\sum_{\pi}\alpha_{t,l}\sigma_X^{\otimes l}\sigma_Y^{\otimes(2t-l)}, \end{aligned} \tag{25}$$

where $\alpha_{t,l}$ are the corresponding coefficients, whose values do not affect the following analysis.

Based on the single-qubit operators appearing in Θ_t, we utilize a new orthogonal one-qubit basis $G_1' = \{\frac{\mathbb{I}-\sigma_Z}{2}, \sigma_X, \sigma_Y, \frac{\mathbb{I}+\sigma_Z}{2}\}$ to act as the local basis, and clearly one has $\mathrm{Sym}_N(G_1') = \mathrm{Sym}_N(G_1)$. Similarly to Eq. (14), the corresponding new orthogonal basis of the symmetric subspace is

$$\begin{aligned} M'_{i,j,k} &= \sum_{\pi}\left(\frac{\mathbb{I}-\sigma_Z}{2}\right)^{\otimes i}\otimes\sigma_X^{\otimes j}\otimes\sigma_Y^{\otimes k} \\ &\quad\otimes\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes(N-i-j-k)}. \end{aligned} \tag{26}$$

As a result, Θ_t lies in the subspace

$$V_t = \mathrm{span}\{M'_{i,j,k}|i+j+k=m+t\}. \tag{27}$$

In fact, V_t is isomorphic to $\mathrm{Sym}_{(m+t)}(\mathbb{R}^3)$, in the sense that

$$\begin{aligned} &\sum_{\pi}\left(a\left(\frac{\mathbb{I}-\sigma_Z}{2}\right)+b\sigma_X+c\sigma_Y\right)^{\otimes(m+t)}\otimes\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes(N-m-t)} \\ &\quad= \sum_{i+j+k=m+t} a^i b^j c^k M'_{i,j,k}. \end{aligned} \tag{28}$$

Thus, according to Theorem 1, for any two real number sets $\{b_0, b_1, \ldots, b_{m+t}\}$ and $\{c_0, c_1, \ldots, c_{m+t}\}$,

$$\begin{aligned} &\left\{A_{j,k}^{(t)} = \sum_{\pi}\left(\frac{\mathbb{I}-\sigma_Z}{2}+b_j\sigma_X+c_k\sigma_Y\right)^{\otimes(m+t)}\right. \\ &\qquad\left.\otimes\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes(N-m-t)}\middle| j+k\leqslant m+t\right\} \end{aligned} \tag{29}$$

is a basis set of V_t.

Consequently, by constructing $A_{j,k}^{(t)}$ for all j,k, each Θ_t in the V_t subspace can be decomposed. Then after decomposing all Θ_t, the decomposition of $D_{N,m}$ can be obtained. In the following, we show how to construct $A_{j,k}^{(t)}$ with LMSs.

Since $1\leqslant t\leqslant m$, the parameters b_j, c_k which determine the basis operator $A_{j,k}^{(t)}$ of each subspace V_t in Eq. (29) are extended to $\{b_0, b_1, \ldots, b_{2m}\}$ and $\{c_0, c_1, \ldots, c_{2m}\}$. That is, we construct $A_{j,k}^{(t)}$ of different t by using the same sets of b_j and c_k, which can help us save the number of LMSs.

Denote $T_{j,k} = \frac{\mathbb{I}-\sigma_Z}{2} + b_j\sigma_X + c_k\sigma_Y$ for simplicity, and the basis operator $A_{j,k}^{(t)}$ of the V_t space in Eq. (29) shows that

$$A_{j,k}^{(t)} = \sum_{\pi} T_{j,k}^{\otimes(m+t)}\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes(N-m-t)}. \tag{30}$$

$A_{j,k}^{(t)}$ is a symmetric operator, generated by the single-qubit operators $T_{j,k}$ and $(\mathbb{I}+\sigma_Z)/2$. Thus, according to Theorem 1, for specific j,k, one can construct $A_{j,k}^{(t)}$ by the following $N+1$ product basis for any t,

$$\left\{\left(\tan\theta_k T_{i,j} + \frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes N}\right\}, \tag{31}$$

where $0\leqslant k\leqslant N$, $0\leqslant\theta_k<\pi$, and $\theta_k\neq\theta_{k'}$ with $k\neq k'$. For example, $\theta_k = \frac{k\pi}{N+1}$. As a result, after constructing $A_{j,k}^{(t)}$, we can decompose Θ_t, as well as $D_{N,m}$.

Finally, let us count the total number of LMSs. For each $T_{j,k}$, we need $N+1$ LMSs. And there are $\binom{2m+2}{2} = (m+1)(2m+1)$ different $T_{j,k}$'s. Thus there is a total of $(m+1)(2m+1)(N+1)$ LMSs. In fact, one can reduce the number of LMSs with more careful analysis. There is one setting, $(\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes N}$, with $\theta_k = 0$ shared by all $T_{j,k}$, which is equivalent to the $\sigma_Z^{\otimes N}$ setting. In addition, if we choose $b_0 = c_0 = 0$, $T_{0,0}$ only needs the same setting $\sigma_Z^{\otimes N}$. As a result, the final number of LMSs is

$$((m+1)(2m+1)-1)N+1 = m(2m+3)N+1. \tag{32}$$

Some remarks are as follows. First, our construction is general and suitable for any Dicke state $|D_{N,m}\rangle$. We expect

that the number of LMSs could be reduced further with more elaborate analysis. Specifically, one may find a smaller subspace compared with V_t that contains Θ_t. Second, as $m = 1$, our upper bound is $5N + 1$, which is larger than the previous result, $2N - 1$, for the W state. Thus, it is also expected that for certain Dicke states, such as $|D_{N,2}\rangle$, the number of LMSs can also be reduced. And we leave them for further work.

V. LOWER BOUND ON THE MEASUREMENT COMPLEXITY

In this section, we bound the measurement complexity of the GHZ state, the W state, and the Dicke state from below. The corresponding results are listed in the third column in Table I.

Before formally discussing the lower bound of the measurement complexity for a specific state, here we explain the high-level idea of how to bound it from below. On the one hand, we find a subspace in which the projection of the state has a certain form; on the other hand, on account of the product form of the LMS, we show that the projection result can only be reconstructed with a high enough number of LMSs.

First, let us study the measurement complexity of the N-qubit GHZ state [1],

$$|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \tag{33}$$

In Ref. [29], the authors decompose $|\mathrm{GHZ}_N\rangle$ into $N + 1$ LMSs. In the following theorem, we provide a lower bound for the measurement complexity of the GHZ state which also grows linearly. It means that one should make use of $\Theta(N)$ LMSs to evaluate the fidelity with the GHZ state.

Theorem 4. The measurement complexity of the N-qubit GHZ state $|\mathrm{GHZ}_N\rangle$ is lower-bounded by

$$C_S(|\mathrm{GHZ}_N\rangle) \geqslant \left\lceil \frac{N+1}{2} \right\rceil. \tag{34}$$

Proof. The density matrix of the GHZ state can be written in the form [29]

$$\mathrm{GHZ}_N = \frac{1}{2}\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes N} + \frac{1}{2}\left(\frac{\mathbb{I}-\sigma_Z}{2}\right)^{\otimes N} + \frac{1}{2^N}\sum_{\text{even } k=0}^{N}(-1)^{k/2}\sum_{\pi}\sigma_Y^{\otimes k}\sigma_X^{\otimes(N-k)}, \tag{35}$$

where the first two terms account for the diagonal elements, and the last one for the off-diagonal elements.

Denote the set of LMSs used to decompose the GHZ state as

$$\mathcal{A} = \left\{A_i^{\otimes N} = (b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z)^{\otimes N} \middle| i = 1, 2, \ldots, n_A\right\}, \tag{36}$$

and the final operator constructed from $\mathcal{A}$ shown in Eq. (19) as O,

$$O = \sum_{i=1}^{n_A}\sum_{j=1}^{N}\alpha_{ij}\sum_{\pi}\mathbb{I}^{\otimes j}A_i^{\otimes N-j}. \tag{37}$$

It is assumed that $O = \mathrm{GHZ}_N$.

Then consider the projection onto the subspace,

$$\mathrm{span}\{M_{0,N-k,k} | 0 \leqslant k \leqslant N, \text{even } k\}, \tag{38}$$

where $M_{i,j,k}$ is the orthogonal basis defined in (14). For the GHZ state, we write the projection results on all the basis operators $M_{0,N-k,k}$ in Eq. (38) in vector form as

$$v_{\mathrm{GHZ}} = \frac{1}{2^N}(1, -1, 1, \ldots, (-1)^{\lfloor N/2\rfloor}). \tag{39}$$

For O, it is not hard to see that only the following terms in the summation of Eq. (37) have nonzero projection on this subspace,

$$\sum_{i=1}^{n_A}\alpha_{i0}A_i^{\otimes N}, \tag{40}$$

and the projection result shows

$$v_O = \sum_{i=1}^{n_A}\alpha_{i0}\left(b_i^N, b_i^{N-2}c_i^2, \ldots, b_i^{N-2\lfloor N/2\rfloor}c_i^{2\lfloor N/2\rfloor}\right). \tag{41}$$

Since $O = \mathrm{GHZ}_N$, the projection results should also be equal, i.e., $v_{\mathrm{GHZ}} = v_O$. In the following, we show that if $v_G = v_O$, the number of LMSs $n_A \geqslant \lceil \frac{N+1}{2} \rceil$.

Here we focus on the case where $b_i \neq 0$ and $c_i \neq 0$ and leave the proof of the general case to Appendix C. Define $\beta_i = (c_i/b_i)^2$ and it is clear that $\beta_i > 0$; then v_O shows

$$v_O = \sum_{i=1}^{n_A}\alpha_i\left(1, \beta_i \ldots, \beta_i^{\lfloor N/2\rfloor}\right), \tag{42}$$

where $\alpha_i = \alpha_{i0}b_i^N$.

We construct the function

$$g(x) = \sum_{i=1}^{n_A}\alpha_i\beta_i^x, \tag{43}$$

which is the linear combination of n_A exponential functions. Since $v_O = v_G$, we have

$$g(0) = \frac{1}{2^N}, \quad g(1) = -\frac{1}{2^N}, \quad g(2) = \frac{1}{2^N}, \ldots, \ g(\lfloor N/2\rfloor) = (-1)^{\lfloor N/2\rfloor}\frac{1}{2^N}, \tag{44}$$

and it is clear that $g(x)$ changes its sign with respect to adjacent points. On account of the continuity of $g(x)$, there is at least one root of $g(x) = 0$ in each of the intervals $(0, 1), (1, 2), \ldots, (\lfloor N/2\rfloor - 1, \lfloor N/2\rfloor)$. Totally, there are at least $\lfloor N/2\rfloor$ roots.

On the other hand, it is known that $g(x)$ has $n_A - 1$ roots at most [30], as shown in Lemma 1 below. Consequently, one has $n_A - 1 \geqslant \lfloor N/2\rfloor$, i.e., $n_A \geqslant \lceil \frac{N+1}{2} \rceil$.

Lemma 1. [30] For real numbers $\{\alpha_i\}_1^n$ and $\{\beta_i\}_1^n$ with $\alpha_i \neq 0$, $\beta_i > 0$, and $\beta_i \neq \beta_j$ for $i \neq j$, the function

$$g(x) = \sum_{i=1}^{n}\alpha_i\beta_i^x \tag{45}$$

has at most $n - 1$ roots.

The proof of Lemma 1 can be found in [30].

Then we give the measurement complexity lower bounds of the Dicke state as well as the W state.

Theorem 5. The measurement complexity of the Dicke state $|D_{N,m}\rangle$ is lower-bounded by

$$C_S(|D_{N,m}\rangle) \geqslant N - 2m + 1. \tag{46}$$

As a result of Theorem 5, we also have the lower bound for the W state.

Corollary 1. The measurement complexity of the N-qubit W state $|W_N\rangle$ is lower-bounded by

$$C_S(|W_N\rangle) \geqslant N - 1. \tag{47}$$

There is a known decomposition of $|W_N\rangle$ using $2N-1$ LMSs [29], which is consistent with our lower bound. This means that one should make use of $\Theta(N)$ LMSs to evaluate the fidelity with the W state.

The proof of Theorem 5 is similar to that of Theorem 4 for the GHZ state. We find a specific subspace where the state $D_{N,m}$ has zero projection. On the other hand, we show that there should be at least $N-2m+1$ LMSs in the decomposition of $D_{N,m}$, in order to make the projection also be zero. The detailed proof is reported in Appendix D.

VI. CONCLUSION AND OUTLOOK

In this paper, by introducing a set of product bases for the symmetric subspace, we show that with $(N+1)(N+2)/2$ LMSs, one can decompose a symmetric observable and evaluate the fidelity between an unknown prepared state and any PI state. For some typical PI states, such as the GHZ state, the W state, and the Dicke state with constant number excitations, we can further reduce the measurement complexity down to the linear regime.

There are a few prospective problems that can be explored in the future. First, it is interesting to show whether the measurement complexity of Dicke states with $\Theta(N)$ excitations, such as $|D_{N,\frac{N}{2}}\rangle$, is still $\Theta(N)$. Second, besides the GHZ state, the W state, and the Dicke state, one might also reduce the measurement complexity for other PI states using similar decomposition techniques. Third, our decomposition technique focuses on the party permutation symmetry but it might also be extended to other types of symmetry, such as the permutation symmetry of eigenstates in high-dimensional systems. In addition, the observable decomposition method can be directly applied to entanglement detection, by constructing the corresponding fidelity-based entanglement witnesses [25,31], where further reduction of the measurement complexity is expected [29,32]. In fact, we find that this kind of construction can yield better witness operators considering entanglement detection under coherent noises [33].

ACKNOWLEDGMENTS

We acknowledge Q. Zhao and X. Yuan for the insightful discussions. This work was supported by National Natural Science Foundation of China Grants No. 11875173 and No. 11674193, and National Key R&D Program of China Grant No. 2017YFA0303900.

Y.Z. and C.G. contributed equally to this work.

APPENDIX A: PROOF OF THEOREM 1

Here we give the proof of Theorem 1, which constructs a set of product-state bases for the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$, that is,

$$\mathcal{B} = \{|\Phi_{\vec{j}}\rangle = (a_{0,j_0}|0\rangle + a_{1,j_1}|1\rangle + \ldots + a_{d-1,j_{d-1}}|d-1\rangle)^{\otimes N}\}, \tag{A1}$$

where $\sum_{k=0}^{d-1} j_k = N$ and the coefficients a_{k,j_k} are selected from any matrix denoted $A_{d,N}$ satisfying Eq. (8). Since $a_{0,j_0} = 1$ for any j_0, the basis set in Eq. (A1) becomes

$$\mathcal{B} = \{|\Phi_{\vec{j}}\rangle = (|0\rangle + a_{1,j_1}|1\rangle + \ldots + a_{d-1,j_{d-1}}|d-1\rangle)^{\otimes N}\}, \tag{A2}$$

and the constraint of j_k can be replaced with $\sum_{k=1}^{d-1} j_k \leqslant N$.

On the other hand, as shown in Eq. (6), there is another set of orthogonal (unnormalized) bases of $\mathrm{Sym}_N(\mathcal{H}_d)$ showing [28]

$$\left\{|\Psi_{\vec{i}}\rangle = \sum_{\pi} |0\rangle^{\otimes i_0}|1\rangle^{\otimes i_1}\ldots|d-1\rangle^{\otimes i_{d-1}}\right\}, \tag{A3}$$

where $\vec{i} = (i_0, i_1, \ldots, i_{d-1})$, a d-dimensional vector, with $i_k \in \mathbb{N}$ and $\sum_{k=0}^{d-1} i_k = N$. It is the generalization of Eq. (11) from the qubit to the qudit case.

The number of vectors in $\mathcal{B}$ is $D_S = \binom{N+d-1}{d-1} = \frac{(N+d-1)!}{N!(d-1)!}$, the dimension of $\mathrm{Sym}_N(\mathcal{H}_d)$. Thus one only needs to show that the vectors in $\mathcal{B}$ are linearly independent. Here, we write $|\Phi_{\vec{j}}\rangle$ in the $\{|\Psi_{\vec{i}}\rangle\}$ basis, and the result shows

$$|\Phi_{\vec{j}}\rangle = \sum_{\vec{i}} \prod_{k=1}^{d-1} a_{k,j_k}^{i_k} |\Psi_{\vec{i}}\rangle. \tag{A4}$$

The corresponding coefficient matrix of all $\{|\Phi_{\vec{j}}\rangle\}$ shows

$$M_{\vec{i},\vec{j}}^{A_{d,n}} = \langle\Psi_{\vec{i}}|\Phi_{\vec{j}}\rangle = \prod_{k=1}^{d-1} a_{k,j_k}^{i_k}, \tag{A5}$$

where each column vector is the coefficient of $|\Phi_{\vec{j}}\rangle$. We say $A_{d,N}$ *generating* $M^{A_{d,N}}$.

In the following we show that the determinant of $M^{A_{d,N}}$ is nonzero, by utilizing the induction method on both d (the local dimension) and N (the qudit number). First, when $d=1$ or $N=1$, it is not hard to check that $\{|\Phi_{\vec{j}}\rangle\}$ are linearly independent and form a basis set.

For general d and N, we do the following row transformation on $M^{A_{d,N}}$: for the row index $\vec{i}$ satisfying $i_1 = 0$, keep these rows unchanged; for the other ones with $1 \leqslant i_1 \leqslant N$, we find the corresponding row with index $\vec{i}' = (i_0+1, i_1-1, i_2, i_3, \ldots, i_{d-1})$ and subtract $a_{1,0}$ multiplying this row $\vec{i}'$. Note that we do this transformation in order from $i_1 = N$ to $i_1 = 1$, and the resulting matrix shows

$$M'_{\vec{i},\vec{j}} = \begin{cases} \prod_{k=1}^{d-1} a_{k,j_k}^{i_k}, & i_1 = 0, \\ \prod_{k=1}^{d-1} a_{k,j_k}^{i_k} - a_{1,0}\prod_{k=1}^{d-1} a_{k,j_k}^{i_k-\delta(k-1)} & \\ = (a_{1,j_1} - a_{1,0})\prod_{k=1}^{d-1} a_{k,j_k}^{i_k-\delta(k-1)}, & 1 \leqslant i_1 \leqslant N, \end{cases} \tag{A6}$$

where the function $\delta(k-1)=1$ as $k=1$, and otherwise it equals zero.

From Eq. (A6), one can see that for the matrix elements $M_{\vec{i},\vec{j}}$ satisfying $1 \leqslant i_1 \leqslant N$ and $j_1 = 0$ equal to zero. That is, $M'_{\vec{i},\vec{j}}$ is an upper triangular block matrix, i.e.,

$$M'_{\vec{i},\vec{j}} = \begin{pmatrix} M^1_{\vec{i},\vec{j}} & M_{\neg} \\ 0 & M^2_{\vec{i},\vec{j}} \end{pmatrix}, \tag{A7}$$

where $M^1_{\vec{i},\vec{j}}$ ($M^2_{\vec{i},\vec{j}}$) is a square matrix which is located in the rows $i_1 = (>)0$ and columns $j_1 = (>)0$, and $M_{\neg}$ is the off-diagonal part. In the following, we show that the determinants of $M^1_{\vec{i},\vec{j}}$ and $M^2_{\vec{i},\vec{j}}$ are both nonzero by induction.

Since $i_1 = j_1 = 0$, $M^1_{\vec{i},\vec{j}}$ is generated by the matrix

$$A^1_{d-1,N} = \{a^1_{k,j} = a_{k+1,j} | k \in \{1,\ldots,d-2\}, \\ j \in \{0,1,\ldots,N\}\}. \tag{A8}$$

Actually, the matrix $A^1_{d-1,N}$ is related to a $d-1$ local dimension and N-fold tensor. By induction principle, we can get that $\det(M^1_{\vec{i},\vec{j}}) \neq 0$.

For the other submatrix $M^2_{\vec{i},\vec{j}}$ with $i_1, j_1 \geqslant 1$ shown in Eq. (A6), the precoefficient $(a_{1,j_1} - a_{1,0}) \neq 0$, and it remains the same in the same column. Since we only care about the nonzero property of $\det(M^2_{\vec{i},\vec{j}})$, we can eliminate these unimportant precoefficients and check the determinant of the remaining matrix,

$$M^3_{\vec{i},\vec{j}} = \prod_{k=1}^{d-1} a^{i_k-\delta(k-1)}_{k,j_k}. \tag{A9}$$

Denoting a new $i'_1 = i_1 - 1$ and $i'_k = i_k$ for $k \neq 1$, then one has $\sum_k i'_k = N-1$. In this way, it is not hard to see that $M^3_{\vec{i},\vec{j}}$ can be generated by the matrix

$$A^3_{d,N-1} = \{a^3_{k,j} | k \in \{1,\ldots,d-1\}, j \in \{0,1,\ldots,N-1\}\}, \tag{A10}$$

where

$$a^3_{k,j} = \begin{cases} a_{k,j+1}, k=1, \\ a_{k,j}, k=2,\ldots,d-1. \end{cases} \tag{A11}$$

In fact, $A^3_{d,N-1}$ is related to a d local dimension and $(N-1)$–fold tensor. Again by induction principle, we have that $\det(M^3_{\vec{i},\vec{j}}) \neq 0$, and thus $\det(M^2_{\vec{i},\vec{j}}) \neq 0$.

Consequently, $\det(M^{A_{d,n}}) = \det(M^1_{\vec{i},\vec{j}})\det(M^2_{\vec{i},\vec{j}}) \neq 0$, and $\{|\Phi_{\vec{j}}\rangle\}$ is a basis set of the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$.

APPENDIX B: DECOMPOSITION OF THE PI STATE IN THE PRODUCT-FORM BASIS

In this section, we show explicitly how to efficiently decompose a general PI state in the product-form basis. The product operators in $\mathcal{B}_o$ in Eq. (17) form a basis of the operator symmetric subspace $\mathrm{Sym}_N(G_1)$,

$$\mathcal{B}_o = \{O_{\vec{\alpha}} = (a_i\mathbb{I} + b_j\sigma_X + c_k\sigma_Y + \sigma_Z)^{\otimes N} | 0 \\ \leqslant i,j,k \leqslant N,\ i+j+k \leqslant N\}, \tag{B1}$$

where we denote the product operator $O_{\vec{\alpha}} = (a_i\mathbb{I} + b_j\sigma_X + c_k\sigma_Y + \sigma_Z)^{\otimes N}$, with $\vec{\alpha} = \{i,j,k\}$ being a three-dimensional vector as the index. In general, these linearly independent operators $O_{\vec{\alpha}}$ may be not orthogonal. Meanwhile, there is another orthogonal basis of $\mathrm{Sym}_N(G_1)$ shown in Eq. (16),

$$M_{\vec{\beta}} \doteq M_{i,j,k} = \sum_{\pi} \mathbb{I}^{\otimes i} \otimes \sigma_X^{\otimes j} \otimes \sigma_Y^{\otimes k} \otimes \sigma_Z^{\otimes(N-i-j-k)}, \tag{B2}$$

where $\vec{\beta} = \{i,j,k\}$ also denotes a three-dimensional vector as the index of $M_{i,j,k}$.

We show in the following how to express a general PI state Ψ^{PI} in the product-form basis $\{O_{\vec{\alpha}}\}$, i.e.,

$$\Psi^{\mathrm{PI}} = \sum_{\vec{\alpha}} \gamma_{\vec{\alpha}} O_{\vec{\alpha}}, \tag{B3}$$

where $\gamma_{\vec{\alpha}}$ are real coefficients that we need to figure out.

Our strategy is as follows. First, decompose the PI state on the orthogonal basis $\{M_{\vec{\beta}}\}$ as

$$\Psi^{\mathrm{PI}} = \sum_{\vec{\beta}} \gamma'_{\vec{\beta}} M_{\vec{\beta}}. \tag{B4}$$

Since the basis operators $M_{\vec{\beta}}$ are orthogonal, the coefficient can be efficiently obtained,

$$\gamma'_{\vec{\beta}} = c_{\vec{\beta}} \mathrm{Tr}(M_{\vec{\beta}} \Psi^{\mathrm{PI}}), \tag{B5}$$

where $c_{\vec{\beta}} = \frac{i!j!k!(N-i-j-k)!}{2^N N!}$ is the normalization constant.

Second, do the basis transformation between $M_{\vec{\beta}}$ and $O_{\vec{\alpha}}$. The elements of the basis transformation matrix can be obtained by expressing $O_{\vec{\alpha}}$ on $M_{\vec{\beta}}$, that is,

$$\Omega_{\vec{\beta},\vec{\alpha}} = c_{\vec{\beta}} \mathrm{Tr}(M_{\vec{\beta}} O_{\vec{\alpha}}). \tag{B6}$$

As a result,

$$\begin{aligned} \Psi^{\mathrm{PI}} &= \sum_{\vec{\alpha}} \gamma_{\vec{\alpha}} O_{\vec{\alpha}} \\ &= \sum_{\vec{\alpha},\vec{\beta}} \gamma_{\vec{\alpha}} \Omega_{\vec{\beta},\vec{\alpha}} M_{\vec{\beta}} \\ &= \sum_{\vec{\beta}} \gamma'_{\vec{\beta}} M_{\vec{\beta}}. \end{aligned} \tag{B7}$$

Thus, one has $\gamma'_{\vec{\beta}} = \sum_{\vec{\alpha}} \Omega_{\vec{\beta},\vec{\alpha}} \gamma_{\vec{\alpha}}$ and $\gamma_{\vec{\alpha}} = \Omega^{-1}\gamma'_{\vec{\beta}}$. Note that the inverse of the matrix Ω can be evaluated efficiently by the numerical method, since the dimension of the matrix is $\binom{N+2}{2}$. As a result, by measuring the expectation values of product operators $\langle O_{\vec{\alpha}}\rangle$, one can get the fidelity $\langle\Psi^{\mathrm{PI}}\rangle = \sum_{\vec{\alpha}} \gamma_{\vec{\alpha}} \langle O_{\vec{\alpha}}\rangle$ with respect to any PI state Ψ^{PI}, by postprocessing only the measurement results.

Moreover, as shown in Eq. (16), one can choose other possible product-form bases by changing the parameters of the local operators that satisfy Eq. (8). Different product-form bases may show different noise tolerances in practical application. For instance, there is some basis choice where two product operators are too "close" (even though they are linearly independent), such that they return almost the same result under some measurement imperfection. Thus, we suggest the following selection method, which makes the basis operators be distributed as "evenly" as possible. One

chooses the coefficients in Eq. (B1) as follows: $a_i = \tan\theta_i$ with $\theta_i = \frac{i\pi}{N+1}$, $b_j = \tan\theta_j$ with $\theta_j = \frac{j\pi}{N+1}$, and $c_k = \tan\theta_k$ with $\theta_k = \frac{k\pi}{N+1}$.

Finally, we would like to remark that the method shown above can also be applied to decompose general symmetric operators directly, which may be useful in other related problems.

APPENDIX C: PROOF OF THEOREM 4 WHEN $b_i = 0$ or $c_i = 0$ IN EQ. (41)

Here we give the proof of Theorem 4 in the case where $b_i = 0$ or $c_i = 0$ in Eq. (41). Remember that in the text, we project the operator GHZ_N and O in a specific subspace in Eq. (38), and the projection results are, respectively,

$$v_{\mathrm{GHZ}} = \frac{1}{2^N}(1, -1, 1, \ldots, (-1)^{\lfloor N/2\rfloor}), \tag{C1}$$

$$v_O = \sum_{i=1}^{n_A} \alpha_{i0}\big(b_i^N, b_i^{N-2}c_i^2, \ldots, b_i^{N-2\lfloor N/2\rfloor}c_i^{2\lfloor N/2\rfloor}\big). \tag{C2}$$

Then we define a function $g(x)$ in Eq. (43) which is a summation of several exponential functions and use the root property of it to bound the number of LMSs.

Here we consider the general case where $b_i = 0$ or $c_i = 0$. Let S denote the set of i with both b_i and c_i not equal to 0, and define $\beta_i = (c_i/b_i)^2$ only on S. Let S_b denote the set of i with $c_i = 0$, $b_i \neq 0$, and let S_c denote the set of i with $b_i = 0$, $c_i \neq 0$. Then v_O can be written as

$$\begin{aligned} v_O = &\sum_{i\in S} \alpha_i\big(1, \beta_i \ldots, \beta_i^{\lfloor N/2\rfloor}\big) + (\alpha_b, 0, \ldots, 0) \\ &+ (0, \ldots, 0, \alpha_c), \end{aligned} \tag{C3}$$

where $\alpha_i = \alpha_{i0}b_i^N$, $\alpha_b = \sum_{i\in S_b}\alpha_{i0}b_i^N$, and $\alpha_c = \sum_{i\in S_c}\alpha_{i0}b_i^{N-2\lfloor N/2\rfloor}c_i^{2\lfloor N/2\rfloor}$. It is clear that

$$n_A \geqslant |S| + |S_b| + |S_c|. \tag{C4}$$

And we define $g(x)$ of the set S as

$$g(x) = \sum_{i\in S}\alpha_i\beta_i^x. \tag{C5}$$

Since $v_O = v_G$, $g(0) = 1 - \alpha_b$, $g(1) = -1, \ldots, g(\lfloor N/2\rfloor) = (-1)^{\lfloor N/2\rfloor} - \alpha_c$. Because the continuity of $g(x)$, there is at least one root of $g(x)$ in each of the intervals $(1, 2), (2, 3), \ldots, (\lfloor N/2\rfloor - 2, \lfloor N/2\rfloor - 1)$, which means $\lfloor N/2\rfloor - 2$ roots in total. If $\alpha_b = 0$, there is at least another root in $(0, 1)$. Similarly, if $\alpha_c = 0$, there is at least another root in $(\lfloor N/2\rfloor - 1, \lfloor N/2\rfloor)$.

Therefore, the number of roots of $g(x)$ is at least

$$\begin{aligned} &\lfloor N/2\rfloor - 2 + I(\alpha_b = 0) + I(\alpha_c = 0) \\ &\quad = \lfloor N/2\rfloor - I(\alpha_b \neq 0) - I(\alpha_c \neq 0) \\ &\quad \geqslant \lfloor N/2\rfloor - |S_b| - |S_c|, \end{aligned} \tag{C6}$$

where $I(x)$ denote that function that $I(x) = 0$ or 1 when x is true or false.

Then apply Lemma 1 to $g(x)$; we get $|S| - 1 \geqslant \lfloor N/2\rfloor - |S_b| - |S_c|$. Combining this with (C4), one has $n_A \geqslant \lceil\frac{N+1}{2}\rceil$.

APPENDIX D: PROOF OF THEOREM 5

Here we give the proof of Theorem 5. As mentioned in the text, we find a subspace where $D_{N,m}$ has zero projection and, at the same time, show that one needs at least $N - 2m + 1$ LMSs to make the projection also be zero.

As in the GHZ-state case, suppose the optimal LMSs are

$$\mathcal{A} = \big\{A_i^{\otimes N} = (b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z)^{\otimes N}\big|i = 1, 2, \ldots, n_A\big\}. \tag{D1}$$

The final operator constructed from $\mathcal{A}$ is denoted O,

$$O = \sum_{i=1}^{n_A}\sum_{j=1}^{N}\alpha_{ij}\sum_{\pi}\mathbb{I}^{\otimes j}A_i^{\otimes N-j}, \tag{D2}$$

and it is assumed that $O = D_{N,m}$.

As shown in Eqs. (23), (24), and (25), $D_{N,m}$ can be decomposed as

$$D_{N,m} = \frac{1}{\binom{N}{m}}\sum_{t=0}^{m}\Theta_t, \tag{D3}$$

with

$$\begin{aligned} \Theta_t &= \sum_{\pi}\left(\frac{\mathbb{I} - \sigma_Z}{2}\right)^{\otimes m-t} \otimes \chi_t \otimes \left(\frac{\mathbb{I} + \sigma_Z}{2}\right)^{\otimes N-m-t}, \\ \chi_t &= \sum_{l=0}^{2t}\sum_{\pi}\alpha_{t,l}\sigma_X^{\otimes l}\sigma_Y^{\otimes(2t-l)}. \end{aligned} \tag{D4}$$

It is not hard to see that the total number of σ_X and σ_Y operators on N qubits is at most $2m$, appearing in every terms of the decomposition in Eq. (D3). Thus $D_{N,m}$ lies in the subspace, $\mathrm{span}\{M_{i,j,k}|0 \leqslant j + k \leqslant 2m\}$, where $M_{i,j,k}$ are defined in (14).

For the constructed operator O, there should be some operator A_i satisfying $b_i \neq 0$ in the LMSs in Eq. (D1); otherwise there will be no σ_X term in O. If all the operators A_i with $b_i \neq 0$ satisfy $d_i = 0$, $O \neq D_{N,m}$, since there are terms like $\sum_{\pi}\sigma_X^{\otimes 2t}\sigma_Z^{\otimes N-2t}$ in $D_{N,m}$.

Now consider the subspace

$$V_1 = \mathrm{span}\{M_{0,j,0}|2m + 1 \leqslant j \leqslant N\}. \tag{D5}$$

Note that the projection of $D_{N,m}$ on V_1 is zero. For O, only the following terms could have nonzero projection in this subspace,

$$\sum_{i=1}^{n_A}\alpha_{i0}A_i^{\otimes N}, \tag{D6}$$

and we write the projection on $M_{0,j,0}$ in Eq. (D5) in vector form as

$$v_O = \sum_{i=1}^{n_A}\alpha_{i0}\big(b_i^{2m+1}d_i^{N-2m-1}, b_i^{2m+2}d_i^{N-2m-2}, \ldots, b_i^N\big), \tag{D7}$$

where we consider $b_i \neq 0$; otherwise it contributes nothing to the summation. On account of $O = D_{N,m}$, this projection result should also be zero, i.e., $v_O = \vec{0}$.

First, we focus on the case where all $d_i \neq 0$; denote $\beta_i = b_i/d_i$. And v_O can be written as

$$v_O = \sum_i \alpha_i \left(1, \beta_i, \ldots, \beta_i^{N-2m-1}\right)^T = \vec{0}, \tag{D8}$$

where α_i is the summation of all the corresponding coefficients sharing the same β_i,

$$\alpha_i = \sum_{i':\beta_{i'}=\beta_i} \alpha_{i'0} b_{i'}^{2m+1} d_{i'}^{N-2m-1}. \tag{D9}$$

In fact, there is at least one $\alpha_i \neq 0$. To illustrate this, let us consider another subspace,

$$V_2 = \mathrm{span}\{M_{0,j,0} | 1 \leqslant j \leqslant 2m\}. \tag{D10}$$

It is clear that the projection of $D_{N,m}$ on V_2 is nonzero. For example, the terms like $\sum_\pi \sigma_X^{\otimes 2t} \sigma_Z^{\otimes N-2t}$ are the basis of it. In the meantime, the projection of O on V_2 is

$$v'_O = \sum_i \alpha_i \left(\beta_i^{-2m}, \beta_i^{-2m+1}, \ldots, \beta_i^{-1}\right)^T. \tag{D11}$$

Consequently, there is at least one $\alpha_i \neq 0$; otherwise $v'_O = \vec{0}$, which is in contradiction to $O = D_{N,m}$.

Denote the number of different β_i as n_β. Then Eq. (D8) means that an $(N-2m) \times n_\beta$ Vandermonde matrix multiplies a nonzero vector $\{\alpha_i\}$. Due to the nonsingularity of the Vandermonde matrix, the result can be $\vec{0}$ only if $n_\beta > N - 2m$. As a result, the number of measurement settings is lower-bounded by $n_A \geqslant n_\beta > N - 2m$.

For the case where there are LMSs with $d_i = 0$, denote the set of these LMSs S; the projection in Eq. (D7) shows

$$\sum_{i\in S} \alpha_{i0} b_j^N (0, 0, \ldots, 1)^T + \sum_{i\in[n_A]\setminus S} \alpha_{i0} b_j^{2m+1} d_i^{N-2m-1} \times (1, \beta_i, \ldots, \beta_i^{N-2m-1})^T = \vec{0}. \tag{D12}$$

Denote $\sum_{i\in S} \alpha_{i0} b_j^N = \alpha'$. If $\alpha' \neq 0$, it is just adding one vector in the linear combination compared with Eq. (D8),

$$\alpha'(0, 0, \ldots, 1)^T + \sum_i \alpha_i (1, \beta_i, \ldots, \beta_i^{N-2m-1})^T = \vec{0}. \tag{D13}$$

Similarly, based on the nonsingularity of the Vandermonde matrix, $n_\beta + 1 > N - 2m$. Hence, $n_A \geqslant n_\beta + 1 > N - 2m$.

[1] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bells Theorem, Quantum Theory and Conceptions of the Universe. Fundamental Theories of Physics*, Vol. 37, edited by M. Kafatos (Springer, Dordrecht, Netherlands, 1989), p. 69.

[2] R. H. Dicke, Phys. Rev. **93**, 99 (1954).

[3] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

[4] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).

[5] D. Gottesman, arXiv:quant-ph/9705052.

[6] K. Chen and H.-K. Lo, Quantum Info. Comput. **7**, 689 (2007).

[7] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[8] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2010).

[10] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[11] D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen, Phys. Rev. A **50**, 67 (1994).

[12] V. Giovannetti, S. Lloyd, and L. Maccone, Science **306**, 1330 (2004).

[13] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).

[14] *Quantum State Estimation*, Lecture notes in Physics Vol. 649, edited by M. Paris and J. E. Rehacek (Springer, Berlin, Heidelberg, 2004).

[15] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **106**, 130506 (2011).

[16] C. Song, K. Xu, W. Liu, C.-p. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y.-A. Chen, C.-Y. Lu, S. Han, and J.-W. Pan, Phys. Rev. Lett. **119**, 180511 (2017).

[17] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **117**, 210502 (2016).

[18] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Phys. Rev. Lett. **105**, 150401 (2010).

[19] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, New J. Phys. **14**, 095022 (2012).

[20] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nat. Commun. **1**, 149 (2010).

[21] T. Baumgratz, D. Gross, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **111**, 020401 (2013).

[22] B. P. Lanyon, C. Maier, M. Holzäpfel, T. Baumgratz, C. Hempel, P. Jurcevic, I. Dhand, A. S. Buyskikh, A. J. Daley, M. Cramer, M. B. Plenio, R. Blatt, and C. F. Roos, Nat. Phys. **13**, 1158 (2017).

[23] G. Tóth, W. Wieczorek, D. Gross, R. Krischek, C. Schwemmer, and H. Weinfurter, Phys. Rev. Lett. **105**, 250403 (2010).

[24] T. Moroder, P. Hyllus, G. Tóth, C. Schwemmer, A. Niggebaum, S. Gaile, O. Gühne, and H. Weinfurter, New J. Phys. **14**, 105001 (2012).

[25] B. M. Terhal, Theoret. Comput. Sci. **287**, 313 (2002).

[26] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).

[27] For example, the Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ has eigenvalue -1 of the permutation operation between the two qubits, i.e., $P(2,1)|\Psi^-\rangle = -|\Psi^-\rangle$. Hence $|\Psi^-\rangle \notin S_S$ but $|\Psi^-\rangle \in S_{PI}$. Symmetric states possess many interesting properties. For example, there is a dichotomy for the entanglement depth of the

pure symmetric state [34,35], i.e., they are either product states or fully entangled.
[28] A. W. Harrow, arXiv:1308.6595.
[29] O. Gühne, C.-Y. Lu, W.-B. Gao, and J.-W. Pan, Phys. Rev. A **76**, 030305(R) (2007).
[30] T. Tossavainen, Austral. Math. Soc. Gazette **33**, 47 (2006).
[31] O. Gühne and G. Toth, Phys. Rep. **474**, 1 (2009).
[32] Q. Zhao, G. Wang, X. Yuan, and X. Ma, arXiv:1902.07869.
[33] Y. Zhou, C. Guo, and X. Ma (unpublished).
[34] T. Ichikawa, T. Sasaki, I. Tsutsui, and N. Yonezawa, Phys. Rev. A **78**, 052105 (2008).
[35] T.-C. Wei, Phys. Rev. A **81**, 054102 (2010).