Two local observables are sufficient to characterize maximally entangled states of N qubits

Fengli Yan,[1,*] Ting Gao,[2,†] and Eric Chitambar[3,‡]

[1]*College of Physics Science and Information Engineering and Hebei Advanced Thin Films Laboratory,*
Hebei Normal University, Shijiazhuang 050016, China

[2]*College of Mathematics and Information Science, Hebei Normal University, Shijiazhuang 050016, China*

[3]*Center for Quantum Information and Quantum Control (CQIQC), Department of Electrical and Computer Engineering and*
Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada

Maximally entangled states (MES) represent a valuable resource in quantum information processing. In N-qubit systems the MES are N-GHZ states [i.e., the collection of $|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|00\cdots0\rangle + |11\cdots1\rangle)$] and its local unitary (LU) equivalences. While it is well known that such states are uniquely stabilized by N commuting observables, in this article we consider the minimum number of noncommuting observables needed to characterize an N-qubit MES as the unique common eigenstate. Here, we prove, rather surprisingly, that in this general case any N-GHZ state can be uniquely stabilized by only two observables. Thus, for the task of MES certification, only two correlated measurements are required with each party observing the spin of his or her system along one of two directions.

PACS number(s): 03.67.Mn, 03.65.Ta, 03.65.Ud, 03.67.Dd

I. INTRODUCTION

From both a theoretical and practical perspective, maximally entangled states (MES) play an important role in quantum information science. While there may be different ways to consider some state more entangled than another, one can work from an axiomatic perspective to define "maximally" entangled states in the multipartite setting. This is the approach taken by Gisin and Bechmann-Pasquinucci who identify N-GHZ states as maximally entangled in N-qubit systems [1]. Here an N-GHZ state has the form $\sqrt{\frac{1}{2}}(|00\cdots0\rangle + |11\cdots1\rangle)$ for some local choice of basis which, in three-qubit form, is the well-known Greenberger-Horne-Zeilinger state. One justification for considering these states as maximally entangled is that they maximally violate the Bell-Klyshko inequalities [2], a generalization of the Bell inequalities to more than two parties. Chen advanced the work of [1] by proving N-GHZ states to be the unique family of states which demonstrate such a maximal violation [3]. In this article, we adopt the perspective of these works and regard N-GHZ states as *the* maximally entangled multiqubit states.

At the same time, MES have been recognized as key ingredients in quantum information processing (QIP). The pioneering bipartite tasks of quantum key distribution (QKD) [4,5], teleportation [6], superdense coding [7], and quantum direct communication [8] all utilize the Einstein-Podolsky-Rosen (EPR) state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to achieve their powerful nonclassical effects. Multipartite generalizations of these procedures have been developed [9–12], as well as novel schemes such as quantum secret sharing [9,13], which like their bipartite ancestors, involve manipulations and measurements on MES. The general attraction of MES for information processing is dual since they not only allow for complete correlation between measurements on subsystems, but their purity also ensures these correlations to exist exclusively within the system (i.e., no external eavesdropper can be correlated with any of the subsystems).

Since the use of MES is critical to the success of the aforementioned QIP schemes, it is important for the parties to verify that they indeed are encoding their information in MES and not other types of states. One method of doing this is to prepare sufficiently more MES than needed for the given QIP task. From this larger population, a random subset of states is checked to be MES, and if this inspection passes, the remaining states are certified to also be MES with arbitrarily high probability. The task of verifying channel security then reduces to whether N parties can determine if some collection of mutually shared states are all MES. In the bipartite case, Ekert first proposed using Bell inequalities to ascertain whether two parties hold EPR states [5]. While Bell inequalities involve the expectation values of four different observables, Bennett *et al.* later observed that only two local observables were necessary to detect the possession of EPR pairs [14]. Specifically, the state $|\Psi^+\rangle$ is the unique $+1$ eigenstate of the local spin measurements $\sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z$, where σ_X and σ_Z are Pauli matrices. Consequently, repeating these measurements on some sample of states can detect the presence of a potential eavesdropper and ensure the protocol's overall safety.

Using stabilizer formalism [15], this idea can be generalized to check the safety of multipartite MES. The set of commuting product Pauli operators having $|\mathrm{GHZ}_N\rangle$ as the *unique* common $+1$ eigenstate forms an Abelian group. Letting $\{P_i\}_{i=1}^k$ denote a minimal set of generators for this group and I the identity, the projector onto their common $+1$ eigenspace is given by $\frac{1}{2^k}\Pi_{i=1}^k(I + P_i)$. The dimension of this space is given by $\mathrm{tr}[\frac{1}{2^k}\Pi_{i=1}^k(I + P_i)] = \frac{2^N}{2^k}$, which means that at least N commuting local spin measurements are needed to determine whether the parties share $|\mathrm{GHZ}_N\rangle$. In fact, the observables $\sigma_X^{\otimes N}, \sigma_Z \otimes \sigma_Z \otimes I^{\otimes(N-2)}, \sigma_Z \otimes I \otimes \sigma_Z \otimes I^{\otimes(N-3)}, \ldots, \sigma_Z \otimes I^{\otimes(N-2)} \otimes \sigma_Z$ suffice. Nevertheless, a natural question is whether fewer than N measurements are sufficient to certify the possession of $|\mathrm{GHZ}_N\rangle$ if we do not require the measurements to commute. In this article, we find

———————
*flyan@hebtu.edu.cn
†gaoting@hebtu.edu.cn
‡e.chitambar@utoronto.ca

that remarkably for any N, only two different observables are needed.

II. MAIN RESULT AND PROOF

For a more precise statement of our results, let unit vectors $\vec{v}_l$ and $\vec{w}_l$ describe two arbitrary directions in which party l measures the "spin" of his or her system via observables $A_l = \vec{v}_l \cdot \vec{\sigma}$ and $B_l = \vec{w}_l \cdot \vec{\sigma}$, respectively. Then we consider the common $+1$ eigenspace of operators $A := \bigotimes_{l=1}^N A_l$ and $B =: \bigotimes_{l=1}^N B_l$. It is found that for any N-GHZ state $|\psi\rangle$, there exists vectors $\vec{v}_l$ and $\vec{w}_l$ such that $|\psi\rangle$ is the unique $+1$ eigenstate of the two operators just given. We also investigate the converse: for any two observables of the form $\bigotimes_{l=1}^N A_l$ and $\bigotimes_{l=1}^N B_l$, under what conditions do they possess a one-dimensional eigenspace. Note that since each B_l has eigenvalues of ± 1, local unitary operators can be applied, and without loss of generality we can assume $B = \sigma_Z^{\otimes N}$. With a perhaps slight abuse of language, we say that a state is *stabilized* by some operator if it is a $+1$ eigenstate. Our results are summarized as follows:

Theorem 1. For observables $A = \bigotimes_{l=1}^N A_l$, $B = \sigma_Z^{\otimes N}$ with $A_l = (\sin\theta_l \cos\phi_l, \sin\theta_l \sin\phi_l, \cos\theta_l) \cdot \vec{\sigma}$,

(i) if there exists no bit string $\vec{m}$ with $m_l \in \{0,1\}$ such that $\sin\{[\sum_{l=1}^N (-1)^{m_l}\theta_l]/2\} = 0$, then A and B have no common eigenstates,

(ii) if there exists exactly one bit string $\vec{m}$ such that $m_1 = 0$ and $\sin\{[\sum_{l=1}^N (-1)^{m_l}\theta_l]/2\} = 0$, then some N-GHZ state is the unique common $+1$ eigenstate of A and B; moreover, to every N-GHZ state $|\psi\rangle$ there exists θ_l and ϕ_l such that $|\psi\rangle$ is uniquely stabilized by A and B, and

(iii) if there exists more than one one bit string $\vec{m}$ such that $m_1 = 0$ and $\sin\{[\sum_{l=1}^N (-1)^{m_l}\theta_l]/2\} = 0$, then the common $+1$ eigenstates of A and B are given by the solution to Eq. (4).

In statements (ii) and (iii), the condition $m_1 = 0$ is added just to avoid trivial redundancies. Since $-\sin x = \sin(-x)$, a string $\vec{m}$ will solve $\sin\{[\sum_{l=1}^N (-1)^{m_l}\theta_l]/2\} = 0$ if its complement string having components $1 - m_l$ is also a solution.

Proof. Let $\Pi_{A\cap B}$ be the projector onto the common $+1$ eigenspace of A and B, and choose $|\Psi\rangle_{SE}$ to be any purification of it in some larger Hilbert space. Here, S refers to the N-qubit system, and E refers to the environment or perhaps an eavesdropper. Thus, we assume $(A \otimes I_E)|\Psi\rangle_{SE} = (B \otimes I_E)|\Psi\rangle_{SE} = |\Psi\rangle_{SE}$. We seek the conditions for $\Pi_{A\cap B}$ being a one-dimensional projector, which is equivalent to $|\Psi\rangle_{SE}$ being a product state: $|\psi\rangle_S |e_0\rangle_E$. In this case, $|\Psi\rangle_{SE}$ is perfectly secure from leaking any information to an eavesdropper.

We begin by defining two sets $\mathcal{S}_0 = \{\vec{j} \in \mathbb{Z}_2^N : \oplus_{l=1}^N j_l = 0\}$ and $\mathcal{S}_1 = \{\vec{j} \in \mathbb{Z}_2^N : \oplus_{l=1}^N j_l = 1\}$. The bitwise inner product between two N-bit strings will be denoted by $\vec{j} \cdot \vec{k} = \sum_{l=1}^N j_l k_l$.

Any state stabilized by $\sigma_Z^{\otimes N} \otimes I_E$ is of the form,

$$|\Psi\rangle = \sum_{\vec{i} \in \mathcal{S}_0} |\vec{i}\rangle |e_{\vec{i}}\rangle, \tag{1}$$

where $|e_{\vec{i}}\rangle$ are states of the environment and $|\vec{i}\rangle = \bigotimes_{l=1}^N |i_l\rangle_l$ with $i_l \in \{0,1\}$. Since $A_l = \begin{pmatrix} \cos\theta_l & e^{-i\phi_l}\sin\theta_l \\ e^{i\phi_l}\sin\theta_l & -\cos\theta_l \end{pmatrix}$, the action $A_l|i_l\rangle$ can be conveniently expressed as $(\cos\theta_l)^{\bar{i}_l}(e^{-i\phi_l}\sin\theta_l)^{i_l}|0\rangle_l +$

$(e^{i\phi_l}\sin\theta_l)^{\bar{i}_l}(-\cos\theta_l)^{i_l}|1\rangle_l$ where $\bar{i}_l = 1 - i_l$. Then the equality $(\bigotimes_{l=1}^N A_l \otimes I_E)|\Psi\rangle = |\Psi\rangle$ becomes

$$|\Psi\rangle = \sum_{\vec{i} \in \mathcal{S}_0} \bigotimes_{l=1}^N [(\cos\theta_l)^{\bar{i}_l}(e^{-i\phi_l}\sin\theta_l)^{i_l}|0\rangle_l$$
$$+ (e^{i\phi_l}\sin\theta_l)^{\bar{i}_l}(-\cos\theta_l)^{i_l}|1\rangle_l] |e_{\vec{i}}\rangle$$
$$= \sum_{\vec{i} \in \mathcal{S}_0} |\vec{i}\rangle |e_{\vec{i}}\rangle. \tag{2}$$

Contracting by $\langle\vec{j}|$ gives

$$|e_{\vec{j}}\rangle = \sum_{\vec{i} \in \mathcal{S}_0} \prod_{l=1}^N [(\cos\theta_l)^{\bar{i}_l}(e^{-i\phi_l}\sin\theta_l)^{i_l}]^{\bar{j}_l}$$
$$\times [(e^{i\phi_l}\sin\theta_l)^{\bar{i}_l}(-\cos\theta_l)^{i_l}]^{j_l} |e_{\vec{i}}\rangle. \tag{3}$$

Here we allow for $\vec{j}$ to be any string with obviously $|e_{\vec{j}}\rangle = 0$ for $\vec{j} \in \mathcal{S}_1$. The system's state will be unentangled from the environment if there exists complex scalars $c_{\vec{i}}$ and some state $|e_0\rangle$ such that $|e_{\vec{i}}\rangle = c_{\vec{i}}|e_0\rangle$ for all $\vec{i} \in \mathcal{S}_0$. Substituting this into the previous equation gives the system of 2^{N-1} linear equations,

$$c_{\vec{j}} = \sum_{\vec{i} \in \mathcal{S}_0} \prod_{l=1}^N [(\cos\theta_l)^{\bar{i}_l}(e^{-i\phi_l}\sin\theta_l)^{i_l}]^{\bar{j}_l}$$
$$\times [(e^{i\phi_l}\sin\theta_l)^{\bar{i}_l}(-\cos\theta_l)^{i_l}]^{j_l} c_{\vec{i}}, \quad \forall\vec{j} \in \mathcal{S}_0. \tag{4}$$

Thus, there exists a unique solution to this if the state $|\psi\rangle = \sum_{\vec{i} \in \mathcal{S}_0} c_{\vec{i}}|\vec{i}\rangle$ is uniquely stabilized by both A and B. On the other hand, if there are multiple solutions, then $\dim(\Pi_{A\cap B}) > 1$, and if there is no solution, then $\Pi_{A\cap B} = \emptyset$.

At this point, we have essentially answered the question of whether two given observables uniquely stabilize a state since (4) can be efficiently solved. However, by further analysis, we can better understand its solution set and obtain the converse result of part (ii) in Theorem 1.

Taking $|e'_{\vec{i}}\rangle = \prod_{l=1}^N (-1)^{i_l/2} e^{-i\phi_l i_l} |e_{\vec{i}}\rangle$, $e^{i\beta(\vec{j})} = \prod_{l=1}^N (-1)^{j_l/2} e^{i\phi_l j_l}$ and using the identity $i_l \oplus j_l = i_l + j_l - 2i_l j_l$, Eq. (3) simplifies to

$$|e_{\vec{j}}\rangle = e^{i\beta(\vec{j})} \sum_{\vec{i} \in \mathcal{S}_0} \prod_{l=1}^N \cos\theta_l[(-1)^{-1/2}\tan\theta_l]^{i_l \oplus j_l}|e'_{\vec{i}}\rangle \tag{5}$$

where we take the convention $0^0 = 1$. Now for $\vec{j} \in \mathcal{S}_1$, the LHS becomes zero and we are left with the system of 2^{N-1} vector equations,

$$\sum_{\vec{i} \in \mathcal{S}_0} \prod_{l=1}^N \cos\theta_l[(-1)^{-1/2}\tan\theta_l]^{i_l \oplus j_l}|e'_{\vec{i}}\rangle = 0. \tag{6}$$

We can encode all this information in the following way. For any $\vec{m} \in \mathbb{Z}_2^N$, define the function $f_{\vec{m}} : \mathcal{S}_1 \to \{-1, +1\}$ by $f_{\vec{m}}(\vec{v}) := (-1)^{\vec{m}\cdot\vec{v}}$. Observe that if $\vec{m} \neq \vec{n}$, then $f_{\vec{m}} \neq f_{\vec{n}}$. Indeed, there must exist some component k such that one and only one m_k or n_k is zero, and hence $(-1)^{\vec{m}\cdot\vec{e}_k} \neq (-1)^{\vec{n}\cdot\vec{e}_k}$ with $\vec{e}_k$ being the kth unit vector. At the same time, for every $\vec{m}$ its complement $\vec{n}$ is the only vector such that $f_{\vec{m}} = -f_{\vec{n}}$

$(n_l = 1 - m_l)$. Thus while there are 2^N different bit vectors $\vec{m}$, there are 2^{N-1} linearly independent functions $(-1)^{\vec{m}\cdot\vec{v}}$ generated by the $\vec{m} \in \mathbb{Z}_2^N$. Consequently, all possible 2^{N-1} linearly independent combinations formed by adding or subtracting the equations in (6) are contained in the equations,

$$\sum_{\substack{\vec{i}\in\mathcal{S}_0 \\ \vec{j}\in\mathcal{S}_1}} \prod_{l=1}^N (-1)^{m_l j_l} \cos\theta_l [(-1)^{-1/2}\tan\theta_l]^{i_l\oplus j_l}|e'_{\vec{i}}\rangle = 0, \quad (7)$$

for any choice of $m_l \in \{0,1\}$.

We next use the facts that $(-1)^{m_l j_l} = (-1)^{m_l i_l}(-1)^{m_l(i_l\oplus j_l)}$, and that for a fixed $\vec{i}$, $\{i_l \oplus j_l : j_l \in \mathcal{S}_1\} = \mathcal{S}_1$ since $\bigoplus_{l=1}^N i_l = 0$. Hence,

$$\sum_{\vec{j}\in\mathcal{S}_1} \prod_{l=1}^N \cos((-1)^{m_l}\theta_l)[(-1)^{-1/2}\tan((-1)^{m_l}\theta_l)]^{j_l}$$
$$\times \sum_{\vec{i}\in\mathcal{S}_0} (-1)^{\vec{m}\cdot\vec{i}}|e'_{\vec{i}}\rangle = 0. \quad (8)$$

By mathematical induction, it is not difficult to prove that

$$\sum_{\vec{j}\in\mathcal{S}_1} \prod_{l=1}^N \cos\theta_l[(-1)^{-1/2}\tan\theta_l]^{j_l} = (-1)^{-1/2}\sin\Sigma_{l=1}^N\theta_l,$$
$$(9)$$
$$\sum_{\vec{j}\in\mathcal{S}_0} \prod_{l=1}^N \cos\theta_l[(-1)^{-1/2}\tan\theta_l]^{j_l} = \cos\Sigma_{l=1}^N\theta_l.$$

Then from Eq. (8) we have

$$\sin\left(\Sigma_{l=1}^N(-1)^{m_l}\theta_l\right)\sum_{\vec{i}\in\mathcal{S}_0}(-1)^{\vec{m}\cdot\vec{i}}|e'_{\vec{i}}\rangle = 0 \quad (10)$$

for every $\vec{m} \in \mathbb{Z}_2^N$. Let $\mathcal{M}$ denote the set of all binary vectors $\vec{m} \in \mathcal{M}$ such that $\sin(\Sigma_{l=1}^N(-1)^{m_l}\theta_l) = 0$. Consequently, $\sum_{\vec{i}\in\mathcal{S}_0}(-1)^{\vec{m}\cdot\vec{i}}|e'_{\vec{i}}\rangle = 0$ for every $\vec{m} \in \mathcal{M}^c := \mathbb{Z}_2^N \setminus \mathcal{M}$. Multiplying both sides by $(-1)^{\vec{m}\cdot\vec{h}}$ with $\vec{h} \in \mathcal{S}_0$ and summing over $\mathcal{M}^c$ gives

$$0 = \sum_{\vec{m}\in\mathcal{M}^c}\sum_{\vec{i}\in\mathcal{S}_0}(-1)^{\vec{m}\cdot(\vec{h}+\vec{i})}|e'_{\vec{i}}\rangle$$
$$= \sum_{\vec{i}\in\mathcal{S}_0}\left[\sum_{\vec{m}\in\mathbb{Z}_2^N}(-1)^{\vec{m}\cdot(\vec{h}+\vec{i})}|e'_{\vec{i}}\rangle - \sum_{\vec{m}\in\mathcal{M}}(-1)^{\vec{m}\cdot(\vec{h}+\vec{i})}|e'_{\vec{i}}\rangle\right]$$
$$= 2^N\left(|e'_{\vec{h}}\rangle - \frac{1}{2}\sum_{\vec{m}\in\mathcal{M}}(-1)^{\vec{m}\cdot\vec{h}}|E(\vec{m})\rangle\right), \quad (11)$$

where $|E(\vec{m})\rangle = 2^{-(N-1)}\sum_{\vec{i}\in\mathcal{S}_0}(-1)^{\vec{m}\cdot\vec{i}}|e'_{\vec{i}}\rangle$. Here, in passing from the second to the third equation, we have used the general fact that $\sum_{\vec{m}\in\mathbb{Z}_2^N}(-1)^{\vec{m}\cdot\vec{v}} = 0$ unless v_l is even for all l, in which case it equals 2^N. From (11) we immediately see that $\mathcal{M} \neq \emptyset$ or else $|e'_{\vec{h}}\rangle = 0$ for all $\vec{h} \in \mathcal{S}_0$. This proves statement (i) of the theorem.

If $\mathcal{M}$ contains only one string $\vec{m}$ and its complement, then $|e'_{\vec{h}}\rangle = (-1)^{\vec{m}\cdot\vec{h}}|E(\vec{m})\rangle$ for all $\vec{h} \in \mathcal{S}_0$. Substituting this back

into (5) yields

$$|e_{\vec{j}}\rangle = e^{i\beta(\vec{j})}|E(\vec{m})\rangle$$
$$\times \sum_{\vec{i}\in\mathcal{S}_0}\prod_{l=1}^N(-1)^{m_l i_l}\cos\theta_l[(-1)^{-1/2}\tan\theta_l]^{i_l\oplus j_l}, \quad (12)$$

with $\vec{j} \in \mathcal{S}_0$. We simplify this expression analogous to Eq. (8) to obtain

$$|e_{\vec{j}}\rangle = e^{i\beta(\vec{j})}(-1)^{\vec{m}\cdot\vec{j}}|E(\vec{m})\rangle$$
$$\times \sum_{\vec{i}\in\mathcal{S}_0}\prod_{l=1}^N\cos((-1)^{m_l}\theta_l)[(-1)^{-1/2}\tan((-1)^{m_l}\theta_l)]^{i_l}.$$
$$(13)$$

The second identity in (9) then gives

$$|e_{\vec{j}}\rangle = e^{i\beta(\vec{j})}(-1)^{\vec{m}\cdot\vec{j}}\cos\left(\Sigma_{l=1}^N(-1)^{m_l}\theta_l\right)|E(\vec{m})\rangle. \quad (14)$$

At the same time, since $\vec{j} \in \mathcal{S}_0$, we must have $|e'_{\vec{j}}\rangle = e^{-i\beta(\vec{j})}|e_{\vec{j}}\rangle = (-1)^{\vec{m}\cdot\vec{j}}|E(\vec{m})\rangle$ which gives the additional condition that $\cos(\Sigma_{l=1}^N(-1)^{m_l}\theta_l) = 1$. Then using (14), we return to $|\Psi\rangle_{SE}$ by

$$|\Psi\rangle_{SE} = \sum_{\vec{j}\in\mathcal{S}_0}e^{i\beta(\vec{j})}(-1)^{\vec{m}\cdot\vec{j}}|\vec{j}\rangle|E(\vec{m})\rangle$$
$$= \sum_{\vec{j}\in\mathcal{S}_0}\bigotimes_{l=1}^N|\tilde{j}_l\rangle_l|E(\vec{m})\rangle \quad (15)$$

where $|\tilde{0}\rangle = |0\rangle$, $|\tilde{1}\rangle = (-1)^{(1/2+m_l)}e^{i\phi_l}|1\rangle$. From parity considerations, it is straightforward to see that under the local rotation of $|0\rangle \to (|0\rangle + |1\rangle)$ and $|1\rangle \to (|0\rangle - |1\rangle)$ by each party, the state $|GHZ_N\rangle$ transforms as

$$|00\cdots0\rangle + |11\cdots1\rangle \to (|0\rangle + |1\rangle)^{\otimes N} + (|0\rangle - |1\rangle)^{\otimes N}$$
$$= \sum_{\vec{j}\in\mathcal{S}_0}\bigotimes_{l=1}^N|j_l\rangle_l. \quad (16)$$

This proves $|\Psi\rangle_{SE}$ to be of the form $|\psi\rangle_S|e_0\rangle_E$ where $|\psi\rangle_S$ is an N-GHZ state; the two necessary and sufficient conditions are $\sin(\Sigma_{l=1}^N(-1)^{m_l}\theta_l) = 0$ and $\cos(\Sigma_{l=1}^N(-1)^{m_l}\theta_l) = 1$ which we can combine into the single equation $\sin\{[\Sigma_{l=1}^N(-1)^{m_l}\theta_l]/2\} = 0$.

Furthermore, starting from (15), we can reverse the construction. For instance, if N is odd, then choosing $\theta_l = 2\pi/N$ for all l generates a unique solution (up to its complement) of $\vec{m} = \vec{0}$ for $\sin\{[\Sigma_{l=1}^N(-1)^{m_l}\theta_l]/2\} = 0$. As a result, the state $|\psi\rangle = \sum_{\vec{j}\in\mathcal{S}_0}\bigotimes_{l=1}^N|\tilde{j}_l\rangle_l$ is uniquely stabilized by A and B for any choice of ϕ_l. Any other N-GHZ state can be written as $\bigotimes_{i=1}^N U_i|\psi\rangle$ for local unitaries U_i, and we compute this state to be uniquely stabilized by $\bigotimes_{i=1}^N U_i A_i U_i^\dagger$ and $\bigotimes_{i=1}^N U_i B_i U_i^\dagger$. For even N, the procedure is identical with $\theta_1 = \frac{4\pi}{N+1}$ and $\theta_l = \frac{2\pi}{N+1}$ for $l > 1$. Statement (ii) of the theorem is proven.

Now suppose that $\mathcal{M}$ contains more than one $\vec{m}$ such that $m_1 = 0$ and $\sin\{[\Sigma_{l=1}^N(-1)^{m_l}\theta_l]/2\} = 0$. Then $|e'_{\vec{h}}\rangle = \frac{1}{2}\sum_{\vec{m}\in\mathcal{M}}(-1)^{\vec{m}\cdot\vec{h}}|E(\vec{m})\rangle$, and either (a) $|e'_{\vec{h}}\rangle \not\propto |e'_{\vec{j}}\rangle$ for

some $\vec{h}, \vec{j} \in \mathcal{S}_0$, or (b) $|e'_{\vec{h}}\rangle = c_{\vec{h}}|e_0\rangle$ for all $\vec{h} \in \mathcal{S}_0$ and $c_{\vec{h}}$ some complex scalar. In case (a), from Eq. (1) we see that the system and the environment are entangled which means $\dim(\Pi_{A \cap B}) > 1$. In case (b), the system is separated from the environment, and A and B will have a unique $+1$ eigenstate if Eq. (4) has a solution. In both cases, the global state is $|\Psi\rangle_{SE} = \sum_{\substack{\vec{m} \in \mathcal{M} \\ m_1=0}} |\mathrm{GHZ}_N(\vec{m})\rangle |E(\vec{m})\rangle$ where each $|\mathrm{GHZ}_N(\vec{m})\rangle$ is an N-GHZ state of the form $\frac{1}{\sqrt{2}}(|k_1 k_2 \ldots k_N\rangle + |\bar{k}_1 \bar{k}_2 \ldots \bar{k}_N\rangle)$ $k_l \in \{\tilde{0}, \tilde{1}\}$, with $\{|\tilde{0}\rangle_l, |\tilde{1}\rangle_l\}$ a local basis of party l fixed for all $\vec{m}$. This completes the proof of part (iii). ∎

In conclusion, we have considered the minimum number of spin-direction measurements required to certify the possession of maximally entangled states in N-qubit systems. Our results are especially important to QKD where a central task is verifying the purity of a quantum channel and the absence of a possible eavesdropper. Specifically we have shown that for every N-qubit maximally entangled state, only two different local measurements are needed to accomplish this certification.

Note that in our analysis, we have mainly focused on the mutual $+1$ eigenspaces of A and B. However, by considering all combinations of $\pm A$ and $\pm B$, we can learn whether the two observables share *any* unique eigenstate. A natural question for future research is the minimum number of measurements needed to test for MES in higher dimensional N-party systems.

[1] N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).

[2] D. N. Klyshko, Phys. Lett. A **172**, 399 (1993).

[3] Z. Q. Chen, Phys. Rev. Lett. **93**, 110403 (2004).

[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore* (IEEE, New York, 1984), pp. 175–179.

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] C. H. Bennett, G. Brassard, C. Crérpeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[7] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[8] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[9] K. Chen and H. K. Lo, in *Proceedings of the International Symposium on Information Theory (ISIT 2005), Adelaide, Australia* (IEEE, New York, 2005), pp. 1607–1611.

[10] A. Karlsson and M. Bourennane, Phys. Rev. A **58**, 4394 (1998).

[11] P. Agrawal and A. Pati, Phys. Rev. A **74**, 062320 (2006).

[12] T. Gao, F. L. Yan, and Z. X. Wang, J. Phys. A **38**, 5761 (2005).

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

[14] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

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