Self-testing of multipartite Greenberger-Horne-Zeilinger states of arbitrary local dimension with arbitrary number of measurements per party

Shubhayan Sarkar and Remigiusz Augusiak
Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotnikow 32/46, 02-668 Warsaw, Poland

(Received 21 December 2021; accepted 17 February 2022; published 7 March 2022)

Device-independent certification schemes have gained a lot of interest lately, not only for their applications in quantum information tasks, but also their implications towards foundations of quantum theory. The strongest form of device-independent certification, known as self-testing, often requires for a Bell inequality to be maximally violated by specific quantum states and measurements. In this work, using the techniques developed recently [S. Sarkar *et al.*, npj Quantum Inf. **7**, 151 (2021)], we provide a self-testing scheme for the multipartite Greenberger-Horne-Zeilinger states of arbitrary local dimension that does not rely on self-testing results for qubit states and that exploits the minimal number of two measurements per party. This makes our results interesting as far as practical implementation of device-independent certification methods is concerned. Our self-testing statement relies on maximal violation of a Bell inequality proposed recently [R. Augusiak *et al.*, New J. Phys. **21**, 113001 (2019)].

DOI: 10.1103/PhysRevA.105.032416

I. INTRODUCTION

Quantum theory has presented us with numerous counterintuitive predictions, most of which have been verified by experiments until date. Many of them have been shown to have no classical analog. One such prediction of quantum theory is the existence of certain correlations that arise by performing local measurements on a joint entangled quantum state, which violate assumptions which any classical theory must abide. Such correlations are termed Bell nonlocal or simply nonlocal and are detected by violating Bell inequalities [1,2]. Interestingly, nonlocal correlations constitute a powerful resource for numerous applications, in particular within the device-independent framework in which one does not need to make any assumptions on the devices used to perform a given task except that they follow the rules of quantum theory. A prominent example of such applications is the device-independent quantum cryptography [3] (see also Ref. [4]).

Another such application that has gained a lot of interest within the quantum community is device-independent certification. It is actually an umbrella term encompassing a few tasks whose general aim is to make nontrivial statements about the underlying quantum system based only on the observed nonlocal correlations. This last fact makes device-independent (DI) certification schemes interesting from the practical point of view as they require much less information about the underlying system to deduce its relevant properties. For instance, Bell nonlocality has been shown to enable DI certification of quantum system's dimension [5], that a given state is entangled [6] or even the amount of entanglement present in it [7]. It allows to certify that the outcomes of quantum measurements are truly random [8,9].

The most fascinating and at the same time most complete form of device-independent certification is self-testing. Introduced in [10], it aims to harness the observed quantum correlations to provide almost full characterization of the underlying joint quantum state as well as the measurements performed on it; here, almost refers to the fact that, being based on the obtained statistical data, such certification can only be made up to certain undetectable degrees of freedom such as invariance under the action of local unitary transformation or adding an extra system that gives no contribution to the observed nonlocality. Within recent years there has been a substantial effort to propose self-testing schemes for various quantum states and/or measurements (see, e.g., Refs. [11–24]). However, most of them have been designed for bipartite entangled systems, whereas the multipartite scenario remains highly unexplored, in particular when quantum systems of arbitrary local dimension are concerned. The existing multipartite methods are devised for N-partite Greenberger-Horne-Zeilinger (GHZ) states [20–22], the stabilizer states [19,23] or stabilizer subspaces [25], and the Dicke states [26,27], all of them being nevertheless locally qubits. To the best of our knowledge, the only known self-testing scheme for multipartite states of local dimensions higher than two concerns the so-called Schmidt states including the well-known N qudit the Greenberger-Horne-Zeilinger (GHZ) state [27]

$$|\mathrm{GHZ}_{N,d}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle^{\otimes N} \tag{1}$$

with N and d being arbitrary integers such that $N, d \geqslant 2$. However, this scheme, being an adaptation of the results of Ref. [24] to the multiparty scenario, relies on application of many self-testing schemes for the two-qubit states, and requires the parties to perform three or four measurements in order to certify the state. It is thus a vital problem in the domain of DI certification whether it is possible to design schemes that require less effort to be practically implemented.

The main aim of our work is to provide a self-testing strategy for the N-partite GHZ states of local dimension d, which is based on maximal violation of a Bell inequality involving an arbitrary number of truly d-outcome measurements. Moreover, in the simplest case, our scheme requires measuring only two observables at each site, which is in fact the minimal number of measurements necessary to observe quantum nonlocality and thus to make nontrivial self-testing statements. On the other hand, we generalize some previous results in a few ways: (i) first, our results generalize the recent self-testing statement for the two-qudit maximally entangled states [17] to an arbitrary number of parties as well as an arbitrary number of measurements; (ii) it also generalizes the results of Ref. [15] derived for the chained Bell inequalities to an arbitrary number of parties and an arbitrary local dimension.

II. PRELIMINARIES

Before getting to results, let us first describe the scenario and introduce the relevant notions.

A. Multipartite Bell scenario

We consider here the multipartite Bell scenario comprising N spatially separated parties, denoted A_i $(i = 1, \dots, N)$, and one preparation device distributing among them an N-partite state ρ_N that acts on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ with each $\mathcal{H}_i$ being a finite-dimensional Hilbert space representing the physical system of party A_i. On their shares of the state the observers perform measurements and register the obtained outcomes. We consider here a general scenario in which each party A_i can freely choose to perform one of m measurements, each having d outcomes, where both m and d are arbitrary. The measurements are denoted M_{i,x_i} with $x_i = 1, \dots, m$ labeling the measurement choices of party A_i, whereas the outcomes are denoted a_i with $a_i = 0, \dots, d-1$.

The correlations observed by the parties are encoded into a vector of joint probability distributions,

$$\vec{p} = \{p(a_1, \dots, a_N|x_1, \dots, x_N)\} \in \mathbb{R}^{(md)^N}, \tag{2}$$

where $p(a_1, \dots, a_N|x_1, \dots, x_N) \equiv p(\boldsymbol{a}|\boldsymbol{x})$ denotes the joint probability of obtaining a_i by the party A_i after performing the measurement x_i and is given by the well-known Born's formula

$$p(a_1, \dots, a_N|x_1, \dots, x_N) = \mathrm{Tr}\left[\rho_N\left(M_{1,x_1}^{a_1} \otimes \cdots \otimes M_{N,x_N}^{a_N}\right)\right], \tag{3}$$

where $M_{i,x_i}^{a_i}$ are the measurement operators corresponding to the outcome a_i of the measurement x_i; recall that these are positive semidefinite and satisfy $\sum_{a_i} M_{i,x_i}^{a_i} = \mathbb{1}$ for all x_i and i. The set of joint probability distributions achievable using quantum states and quantum measurements is usually referred to as the set of quantum correlations or simply the quantum set; we denoted it by $\mathcal{Q}_{N,m,d}$.

Let us consider a certain subset of the set of quantum correlations $\mathcal{Q}_{m,d,N}$ which can be represented using local-realistic descriptions of the underlying system, commonly referred to as the set of classical or local correlations, denoted $\mathcal{L}_{m,d,N}$. Precisely, the latter contains those correlations that admit the following representation:

$$p(a_1, \dots, a_N|x_1, \dots, x_N) = \sum_{\lambda} \mu(\lambda) \prod_{i=1}^{N} p(a_i|x_i, \lambda), \tag{4}$$

where λ is a random variable distributed according to a distribution $\mu(\lambda)$ and $p(a_i|x_i, \lambda) \in \{0, 1\}$ for every x_i, a_i, and i. Similarly to $\mathcal{Q}_{N,m,d}$, the set $\mathcal{L}_{N,m,d}$ is convex; in fact, it is a polytope for any choice of N, m, and d.

B. Bell inequalities

As it was first observed by Bell in 1964 [1], in the scenario with two parties, each performing two 2-outcome measurements the local set $\mathcal{L}_{2,2,2}$ is a proper subset of $\mathcal{Q}_{2,2,2}$. To this end, he considered certain inequalities that are linear in $p(\boldsymbol{a}|\boldsymbol{x})$ that constrain the set of local correlations. These are typically termed Bell inequalities and their general form reads as

$$\mathcal{I} := \vec{t} \cdot \vec{p} \leqslant \beta_L, \tag{5}$$

where

$$\vec{t} = \{t_{a_1,\dots,a_N,x_1,\dots,x_N}\} \tag{6}$$

is a vector consisting of real numbers $\vec{t} \in \mathbb{R}^{(md)^N}$. The number appearing on the right-hand side of (5) is the maximal value of the Bell expression $\mathcal{I}$ over all classical strategies $\beta_L = \max_{\vec{p}\in\mathcal{L}_{m,d,N}} \mathcal{I}$, and is typically referred to as the classical or local bound. Analogously, by $\beta_Q = \sup_{\vec{p}\in\mathcal{Q}_{m,d,N}} \mathcal{I}$ one denotes the maximal value of $\mathcal{I}$ achievable by quantum correlations and refers to it as the quantum or the Tsirelson bound; the quantum set is in general not closed [28,29], which explains the supremum in the definition of β_Q.

Importantly, violation of (5) by some $\vec{p}$ implies that the latter is nonlocal. Moreover, if $\vec{p}$ violates a Bell inequality maximally or, in other words, achieves the maximal quantum value β_Q, then it necessarily lies at the boundary of the corresponding quantum set $\mathcal{Q}_{N,m,d}$.

In what follows, it will be more convenient for us to express Bell inequalities in terms of correlators instead of probabilities. Due to the fact that here we deal with quantum measurements with an arbitrary number of outcomes, we will use generalized expectation values, which are in general complex numbers defined as the multidimensional Fourier transform of $p(\boldsymbol{a}|\boldsymbol{x})$ (see, e.g., Refs. [30,31]):

$$\left\langle A_{1,x_1}^{k_1} \dots A_{N,x_N}^{k_N} \right\rangle = \sum_{a_1,\dots,a_N=0}^{d-1} \omega^{\boldsymbol{a}\cdot\boldsymbol{k}} p(\boldsymbol{a}|\boldsymbol{x}), \tag{7}$$

where ω is the dth root of unity $\omega = \exp(2\pi \mathbb{i}/d)$ and $\boldsymbol{k}$ is an N-component vector composed of $k_i = 0, \dots, d-1$ for all i, and, finally, $\boldsymbol{a} \cdot \boldsymbol{k} = a_1 k_1 + \cdots + a_N k_N$ stands for the standard scalar product of two real vectors.

Crucially, if the measurements performed by the observers are projective, the expectation values (7) can be represented as

$$\left\langle A_{1,x_1}^{k_1} \dots A_{N,x_N}^{k_N} \right\rangle = \mathrm{Tr}\left[\left(A_{1,x_1}^{k_1} \otimes \cdots \otimes A_{N,x_N}^{k_N}\right)\rho_N\right], \tag{8}$$

where now A_{i,x_i} are unitary operators defined as one-dimensional Fourier transforms of the measurement operators $M_{x_i}^{a}$,

$$A_{i,x_i}^{k_i} = \sum_{a_i=0}^{d-1} \omega^{a_i k_i} M_{i,x_i}^{a_i}, \tag{9}$$

for $k_i = 0, 1, \ldots, d-1$ and $i = 1, \ldots, N$. Due to the fact that for projective measurements the operators $M_{i,x_i}^{a_i}$ are pairwise orthogonal for any x_i and i, it is not difficult to realize that all $A_{i,x_i}^{k_i}$ are unitary operators with eigenvalues ω^i for $i = 0, \ldots, d-1$. Moreover, $A_{i,x_i}^{k_i}$ is simply the k_ith power of A_{i,x_i}; in what follows we refer to A_{i,x_i} as quantum observables.

In fact, as discussed below, since we are concerned with self-testing we can safely restrict our attention to projective measurements; on the same basis we can also assume that the shared state is pure.

C. Self-testing

Let us finally define the task of self-testing. To this end, we consider again the Bell experiment described above, assuming this time that the functioning of all the devices involved is unknown. That is, the parties have no knowledge about the shared state ρ_N as well as the corresponding Hilbert space, and they do not know the measurements their devices perform; in fact these can be treated as black boxes which when supplied with an input $x_i = 1, \ldots, m$ return one of possible outputs $a_i = 0, \ldots, d-1$. Yet, the measuring devices are assumed to behave according to the rules of quantum theory. Now, due to the fact that the local Hilbert spaces are uncharacterized we can make here the standard assumption that the shared state is pure, that is, $\rho_N = |\psi_N\rangle\langle\psi_N|$ for some $|\psi_N\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ and that the measurements are projective.

Now, based on the observed correlations represented by $\vec{p}$ or, equivalently, by the expectation values (7), the parties aim at making nontrivial statements about the state ρ_N and/or the measurements A_{i,x_i} performed on it. This general task is usually referred to as device-independent certification. Its strongest form is self-testing in which the parties use the observed correlations to certify that the shared state $|\psi_N\rangle$ as well as the measurements performed on it are equivalent, up to some well-understood equivalences, to some known state $|\tilde{\psi}_N\rangle \in (\mathbb{C}^d)^{\otimes N}$ and known observables $\tilde{A}_{i,x_i}$ acting on $\mathbb{C}^d$. To be more precise, let us formulate the following definition.

Definition. Consider a Bell experiment consisting of N parties, each performing m d-outcome measurements represented by observables A_{i,x_i} on their shares of a joint state $|\psi_N\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$, where $\mathcal{H}_i$ denotes the Hilbert space of the ith party. We say that the observed correlations self-test the reference state $|\tilde{\psi}_N\rangle \in (\mathbb{C}^d)^{\otimes N}$ and observables $\tilde{A}_{i,x_i}$ acting on $\mathbb{C}^d$ if one can deduce from them that (i) each local Hilbert space decomposes as $\mathcal{H}_i = \mathbb{C}^d \otimes \mathcal{H}_i''$ for some finite-dimensional $\mathcal{H}_i''$, and (ii) there exist local unitary operations $U_i : \mathcal{H}_i \to \mathcal{H}_i$ such that

$$U_1 \otimes \cdots \otimes U_N |\psi_N\rangle = |\tilde{\psi}_N\rangle \otimes |\mathrm{aux}_N\rangle \tag{10}$$

for some auxiliary state $|\mathrm{aux}_N\rangle \in \mathcal{H}_1'' \otimes \cdots \otimes \mathcal{H}_N''$ and

$$U_i\, A_{i,x_i}\, U_i^\dagger = \tilde{A}_{i,x_i} \otimes \mathbb{1}_i'', \tag{11}$$

where $\mathbb{1}_i''$ is an identity acting on $\mathcal{H}_i''$.

Notice that in our case the reference state $|\tilde{\psi}_N\rangle$ is the GHZ state (1), whereas the reference observables $\tilde{A}_{i,x_i}$ are provided explicitly below in Eqs. (15)–(17).

A necessary condition to derive a self-testing statement based on the observed correlations $\vec{p}$ is that they violate some Bell inequality maximally. Hence, the first task is to identify a Bell inequality that is maximally violated by the multipartite GHZ state of arbitrary dimension with arbitrary number of measurements per party. Quite recently, a Bell inequality meeting this requirement was derived in [30]. In the correlator picture it can be stated in the following form:

$$\langle \hat{\mathcal{I}}_{N,m,d} \rangle \leqslant \beta_L, \tag{12}$$

where $\hat{\mathcal{I}}_{N,m,d}$ is the Bell operator given by

$$\hat{\mathcal{I}}_{N,m,d} := \sum_{\alpha_1,\ldots,\alpha_{N-1}=1}^{m} \sum_{k=1}^{d-1} \left(a_k A_{1,\alpha_1}^k \otimes \bigotimes_{i=2}^{N} A_{i,\alpha_{i-1}+\alpha_i-1}^{(-1)^{i-1}k} + a_k^* A_{1,\alpha_1+1}^k \otimes \bigotimes_{i=2}^{N} A_{i,\alpha_{i-1}+\alpha_i-1}^{(-1)^{i-1}k} \right), \tag{13}$$

where the complex coefficients a_k are given by

$$a_k = \frac{\omega^{(2k-d)/4m}}{2\cos(\pi/2m)}, \tag{14}$$

and we assume the convention that $A_{i,m+1} = \omega A_{i,1}$ and $\alpha_N = 1$.

The maximal quantum value of this inequality is known to be $\beta_Q = m^{N-1}(d-1)$. At the same time, the local bound β_L has been computed numerically only for some cases in [30]; yet, it was shown that $\beta_L < \beta_Q$ for all finite N and d. The maximal quantum value can be achieved by the N-partite GHZ state of local dimension d defined in Eq. (1) and the following measurements:

$$\mathcal{O}_{1,x} = U_x F_d\, \Omega_d F_d^\dagger U_x^\dagger, \quad \mathcal{O}_{2,x} = V_x F_d^\dagger \Omega_d F_d V_x^\dagger \tag{15}$$

for the first two parties, and

$$\mathcal{O}_{\mathrm{odd},x} = W_x F_d\, \Omega_d F_d^\dagger W_x^\dagger \tag{16}$$

and

$$\mathcal{O}_{\mathrm{ev},x} = W_x^\dagger F_d^\dagger \Omega_d F_d W_x \tag{17}$$

for all other parties A_i with $i = 3, \ldots, N$ numbered by odd and even numbers, respectively. Here

$$F_d = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{ij} |i\rangle\langle j|, \quad \Omega_d = \mathrm{diag}[1, \omega, \ldots, \omega^{d-1}] \tag{18}$$

with $\omega = \exp(2\pi \mathbb{i}/d)$. Then, the unitary operations U_x, V_x, and W_x are defined as

$$U_x = \sum_{j=0}^{d-1} \omega^{-j\alpha_M(x)} |j\rangle\langle j|, \quad V_x = \sum_{j=0}^{d-1} \omega^{j\beta_M(x)} |j\rangle\langle j|, \tag{19}$$

and

$$W_x = \sum_{j=0}^{d-1} \omega^{-j\gamma_M(x)} |j\rangle\langle j|, \tag{20}$$

where

$$\gamma_m(x) = \frac{1}{m}\left(x - \frac{1}{2}\right), \quad \zeta_m(x) = \frac{x}{m}, \quad \theta_m(x) = \frac{x-1}{m}. \tag{21}$$

It is worth noticing that the above observables are by the very definition unitary and that their eigenvalues are ω^i, with $i = 0, \ldots, d-1$, and thus they perfectly match our scenario. Moreover, for the particular case $N = m = 2$, they reproduce the well-known Collins-Gisin-Linden-Massar-Popescu (CGLMP) measurements [32,33].

In the next section, we prove that the above-mentioned state and the measurements are the only realizations up to the freedom of local unitaries and some auxiliary system which can saturate the quantum bound of the inequality (12).

III. RESULTS

We are now ready to present our main result, that is, the self-testing statement for the GHZ state (1) of arbitrary local dimension and the corresponding measurements (15), (16), and (17). The key ingredient in establishing this result is a sum-of-squares decomposition of the Bell operator $\hat{\mathcal{I}}_{N,m,d}$ provided in Ref. [30]. Indeed, for any choice of the local observables A_{i,x_i} acting on $\mathcal{H}_i$ one has

$$\beta_Q \mathbb{1} - \hat{\mathcal{I}}_{N,m,d} = \frac{1}{2}\sum_{\alpha_1,\ldots\alpha_N=1}^{m}\sum_{k=1}^{d-1}\left(P^{(k)}_{\alpha_1,\ldots,\alpha_N}\right)^{\dagger} P^{(k)}_{\alpha_1,\ldots,\alpha_N} + \frac{m^{N-2}}{2}\sum_{\alpha=1}^{m-2}\sum_{k=1}^{d-1}\left(R^{(k)}_{\alpha}\right)^{\dagger} R^{(k)}_{\alpha}, \tag{22}$$

where

$$P^{(k)}_{\alpha_1,\ldots,\alpha_N} = \mathbb{1} - \left(a_k A^k_{1,\alpha_1} + a_k^* A^k_{1,\alpha_1+1}\right) \otimes \bigotimes_{i=2}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1} \tag{23}$$

and

$$R^{(k)}_{\alpha} = \mu^*_{\alpha,k} A^k_{1,2} + \nu^*_{\alpha,k} A^k_{1,\alpha+2} + \tau_{\alpha,k} A^k_{1,\alpha+3} \tag{24}$$

for $\alpha = 1, \ldots, m-2$ and $k = 1, \ldots, d-1$, and $\mathbb{1}$. The coefficients $\mu_{\alpha,k}$, $\nu_{\alpha,k}$, and $\tau_{\alpha,k}$ are given by

$$\mu_{\alpha,k} = \frac{\omega^{(\alpha+1)(d-2k)/2m}}{2\cos(\pi/2m)} \frac{\sin(\pi/m)}{\sqrt{\sin(\pi\alpha/m)\sin[\pi(\alpha+1)/m]}},$$
$$\nu_{\alpha,k} = -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)} \frac{\sqrt{\sin[\pi(\alpha+1)/m]}}{\sqrt{\sin(\pi\alpha/m)}},$$
$$\tau_{\alpha,k} = \frac{1}{2\cos(\pi/2m)} \frac{\sqrt{\sin(\pi\alpha/m)}}{\sqrt{\sin[\pi(\alpha+1)/m]}} \tag{25}$$

for all k and $\alpha = 1, 2, \ldots, m-3$. For $\alpha = m-2$, we have

$$\mu_{m-2,k} = -\frac{\omega^{-k}\omega^{-(d-2k)/2m}}{2\cos(\pi/2m)\sqrt{2\cos(\pi/m)}},$$
$$\nu_{m-2,k} = -\frac{\omega^{(d-2k)/2m}}{2\cos(\pi/2m)\sqrt{2\cos(\pi/m)}},$$
$$\tau_{m-2,k} = \frac{\sqrt{2\cos(\pi/m)}}{2\cos(\pi/2m)}. \tag{26}$$

Before stating our main result, let us introduce two unitary observables with eigenvalues ω^i. The first one is the d-dimensional generalization of σ_z-Pauli matrix given by

$$Z_d = \sum_{i=0}^{d-1}\omega^i |i\rangle\langle i|, \tag{27}$$

whereas the second one is defined as

$$T_{d,m} = \sum_{i=0}^{d-1}\omega^{i+\frac{1}{m}}|i\rangle\langle i| - \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right) \times \sum_{i,j=0}^{d-1}(-1)^{\delta_{i,0}+\delta_{j,0}}\omega^{\frac{i+j}{2}-\frac{d-2}{2m}}|i\rangle\langle j|, \tag{28}$$

where hollow $\mathbb{i}$ denotes the imaginary unit, $\delta_{i,j}$ is the Kronecker delta such that $\delta_{i,j} = 1$ for $i = j$ and $\delta_{i,j} = 0$ otherwise. Note that for $m = d = 2$, $T_{2,2} = -\sigma_x$, which is another Pauli matrix.

Now, we can state our main theorem.

Theorem. Assume that the Bell inequality (12) is maximally violated by some state $|\psi_N\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ and unitary observables A_{i,α_i} for $i \in \{1, 2, \ldots, N\}$ and $\alpha_i \in \{1, 2, \ldots, m\}$. Then, each local Hilbert space decomposes as $\mathcal{H}_i = \mathbb{C}^d \otimes \mathcal{H}_i''$ for some finite-dimensional Hilbert spaces $\mathcal{H}_i''$, and there exist local unitary transformations $U_i : \mathcal{H}_i \to \mathcal{H}_i$ such that

$$U_i A_{i,\alpha_i} U_i^{\dagger} = \mathcal{O}_{i,\alpha_i} \otimes \mathbb{1}_i'', \tag{29}$$

where $\mathcal{O}_{i,\alpha_i}$ are the $d \times d$ observables defined in Eqs. (15)–(17), and $\mathbb{1}_i''$ are the identity matrices acting on $\mathcal{H}_i''$ for all i's, and, finally,

$$U_1 \otimes \cdots \otimes U_N |\psi_N\rangle = |\mathrm{GHZ}_{N,d}\rangle \otimes |\mathrm{aux}_N\rangle, \tag{30}$$

for some $|\mathrm{aux}_N\rangle \in \mathcal{H}_1'' \otimes \cdots \otimes \mathcal{H}_N''$.

Proof. The proof is highly technical and makes use of several lemmas that are proven in the Appendix.

The proof is divided into three major steps. In the first one we concentrate on the first party and characterize its Hilbert space as well as the observables measured by them; in fact, we show that in $\mathcal{H}_1$ one can identify a qudit Hilbert space $\mathbb{C}^d$ and prove the existence of a unitary operation that brings all $A_{1,x}$ to the ideal measurements (15). Then, we extend the above observations to the remaining parties. In the third part of the proof we focus on the state $|\psi_N\rangle$, and exploiting the explicit form of the observables that have just been characterized, we show that up to some additional degrees of freedom it is unitarily equivalent to the N-qudit GHZ state.

The Hilbert space structure and characterization of observables. We begin by noting that without any loss of generality we can assume here that the local reduced states ρ_i of $|\psi_N\rangle$ are full rank; in other words, we assume that the dimensions of A_{i,x_i} and the corresponding ρ_i are equal.

Let us now show that maximal violation of the Bell inequality (12) allows one to identify a qudit in each local Hilbert space in the sense that $\mathcal{H}_i = \mathbb{C}^d \otimes \mathcal{H}_i''$ for any i, and, simultaneously, to obtain the form of $A_{i,2}$ and $A_{i,3}$ for any $i = 2, \ldots, N$.

We concentrate on the first party A_1, the proof for the other A_i's follow exactly the same lines. The departure point for our considerations are certain relations for the observables A_{i,x_i} and the state $|\psi_N\rangle$ that are induced by the sum-of-squares decomposition (34). Precisely, this decomposition implies that any $|\psi_N\rangle$ and A_{i,x_i} maximally violating the Bell inequality (12) must necessarily satisfy

$$P^{(k)}_{\alpha_1,\dots,\alpha_N}|\psi_N\rangle = 0 \tag{31}$$

for any configuration of the indices α_i, which through (23) implies that

$$\overline{A}^{(k)}_{1,\alpha_1} \otimes \bigotimes_{i=2}^{N} A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1}|\psi_N\rangle = |\psi_N\rangle \tag{32}$$

for all k and α_i, where we have denoted

$$\overline{A}^{(k)}_{1,\alpha} = a_k A^k_{1,\alpha} + a_k^* A^k_{1,\alpha+1}. \tag{33}$$

Since A_{i,α_i} are unitary for all i and α_i, we then straightforwardly conclude that the operators acting on the first party's Hilbert space must satisfy the following relations:

$$\overline{A}^{(k)}_{1,\alpha}\overline{A}^{(d-k)}_{1,\alpha} = \mathbb{1}_{A_1} \quad \text{and} \quad \overline{A}^{(k)}_{1,\alpha} = \left[\overline{A}^{(1)}_{1,\alpha}\right]^k \tag{34}$$

for any $k = 1,\dots,d-1$ and $\alpha = 1,\dots,m$. By noting that $a_{d-k} = a_k^*$, one further obtains

$$\overline{A}^{(d-k)}_{1,\alpha} = \overline{A}^{(k)\dagger}_{1,\alpha} \tag{35}$$

for all k and α, and therefore the relations (34) imply that the combinations of observables (33) are also quantum observables, i.e., are unitary and their spectra are from $\{1, \omega, \dots, \omega^{d-1}\}$.

Additionally, we have another set of relations arising from the sum-of-squares (SOS) decomposition (22) given by

$$R^{(k)}_{\alpha}|\psi_N\rangle = 0 \tag{36}$$

which due to the fact that the single-site reduced density matrices of the state $|\psi_N\rangle$ are full rank, are equivalent to

$$R^{(k)}_{\alpha} = 0 \tag{37}$$

for all $k = 1,\dots,d-1$ and $\alpha = 1,\dots,m-2$. The relations (34) and (37) are key factors in proving our self-testing statement. In fact, these relations give rise to Lemma 1 presented in the Appendix that says that the unitary observables $A^n_{1,\alpha}$ are traceless for $\alpha = 2, 3$ and for any $n \neq d$ which is a divisor of d, that is,

$$\mathrm{Tr}(A^n_{1,\alpha}) = 0 \quad (\alpha = 2, 3). \tag{38}$$

Now, denoting by $\lambda_{i,\alpha}$ the multiplicities of the eigenvalues ω^i $(i = 1,\dots,d-1)$ of the two observables $A_{1,2}$ and $A_{1,3}$, Eq. (38) implies that

$$\sum_{i=0}^{d-1}\lambda_{i,\alpha}\omega^{ni} = 0 \quad (\alpha = 2, 3), \tag{39}$$

where n is a divisor of d such that $n \neq d$. By virtue of Fact 1 stated in the Appendix, Eq. (39) allows us to conclude that the multiplicities $\lambda_{i,\alpha}$ are all equal or, equivalently, $\lambda_{0,\alpha} = \dots = \lambda_{d-1,\alpha}$. As a consequence, we have that $\mathrm{Tr}(A^n_{1,\alpha}) = 0$ for all $n = 1, 2, \dots, d-1$ and $\alpha = 2, 3$. Moreover, by employing the relation (37) the latter fact can be directly extended to any observable $A_{1,\alpha}$ measured by the first party. Precisely, taking trace of Eq. (37) and using the explicit form of $R^{(n)}_{\alpha}$, one arrives at

$$\mu^*_{\alpha,n}\mathrm{Tr}\left(A^n_{1,2}\right) + \nu^*_{\alpha,n}\mathrm{Tr}\left(A^n_{1,\alpha+2}\right) + \tau_{\alpha,n}\mathrm{Tr}\left(A^n_{1,\alpha+3}\right) = 0, \tag{40}$$

which for $\alpha = 1$ implies that $\mathrm{Tr}(A^n_{1,4}) = 0$. Analogously, for $\alpha = 2$ it gives $\mathrm{Tr}(A^n_{1,5}) = 0$. Continuing this procedure recursively for any α until $\alpha = m-2$, we conclude that $\mathrm{Tr}(A^n_{1,\alpha}) = 0$ for all n and α.

The fact that the multiplicities of the eigenvalues of all the observables measured by the first party are equal means that the dimension of a Hilbert space these observables act on is a multiple of d or, equivalently, that $\mathcal{H}_1 = \mathbb{C}^d \otimes \mathcal{H}''_1$ for some finite-dimensional Hilbert space $\mathcal{H}''_1$. Moreover, as shown in Lemma 2 in the Appendix, there exists a unitary $V_1 : \mathcal{H}_1 \to \mathcal{H}_1$ such that $V_1 A_{1,2} V_1^\dagger = Z_d \otimes \mathbb{1}''_1$ and $V_1 A_{1,3} V_1^\dagger = T_{d,m} \otimes \mathbb{1}''_1$ where Z_d and $T_{d,m}$ are quantum observables defined in (28) and $\mathbb{1}''_1$ is an identity acting on $\mathcal{H}''_1$.

We then show in Lemma 3 in the Appendix that the observables $A_{1,2}$ and $A_{1,3}$ are unitarily equivalent to the optimal measurements (15). In fact, one can check that for the unitary matrix $W_1 : \mathbb{C}^d \to \mathbb{C}^d$ given explicitly by

$$W_1 = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{3i}{2m}+ij+\frac{j}{2}}|i\rangle\langle j|, \tag{41}$$

the following relations hold true:

$$W_1\, Z_d\, W_1^\dagger = \mathcal{O}_{1,2}, \quad W_1\, T_{d,m}\, W_1^\dagger = \mathcal{O}_{1,3}. \tag{42}$$

As a consequence, there exist a local unitary transformation $U_1 : \mathcal{H}_1 \to \mathcal{H}_1$ such that

$$U_1\, A_{1,\alpha}\, U_1^\dagger = \mathcal{O}_{1,\alpha} \otimes \mathbb{1}''_1 \quad (\alpha = 2, 3). \tag{43}$$

To find the other measurements of the first party, we exploit the relation (37). Plugging the obtained observables into (37) for $\alpha = 1$, we have

$$U_1\, A_{1,4}\, U_1^\dagger = -\frac{1}{\tau_{1,1}}(\mu^*_{1,1}\,\mathcal{O}_{1,2} + \nu^*_{1,1}\,\mathcal{O}_{1,3}) \otimes \mathbb{1}''_1 \tag{44}$$

for all n. A key observation here is that the ideal observables (15), (16), and (17) also satisfy the relations (37). This directly implies that

$$U_1\, A_{1,4}\, U_1^\dagger = \mathcal{O}_{1,4} \otimes \mathbb{1}''_1. \tag{45}$$

Again, after exploiting (37) for $\alpha = 2$,

$$U_1\, A_{1,5}\, U_1^\dagger = -\frac{1}{\tau_{1,2}}(\mu^*_{1,2}\mathcal{O}_{1,2} + \nu^*_{1,2}\mathcal{O}_{1,4}) \otimes \mathbb{1}''_1, \tag{46}$$

and using the relation (37) for the ideal observables one has

$$U_1\, A_{1,5}\, U_1^\dagger = \mathcal{O}_{1,5} \otimes \mathbb{1}''_1. \tag{47}$$

Applying this reasoning recursively for $\alpha = 3,\dots,m-2$, we conclude that

$$U_1 A_{1,\alpha} U_1^\dagger = \mathcal{O}_{1,\alpha} \otimes \mathbb{1}''_1 \tag{48}$$

for all $\alpha = 1,\dots,m$. This is explicitly shown in Lemma 4 in the Appendix.

Observables of all the other parties. Following a similar strategy, we now show that for all the other parties the observables are equivalent to the optimal measurements (15), (16), and (17) up to some unitary transformation. To this end, we first find complementary SOS decompositions of the same Bell operator $\hat{\mathcal{I}}_{N,m,d}$ (13),

$$\beta_Q\mathbb{1} - \hat{\mathcal{I}}_{N,m,d} = \frac{1}{2}\sum_{\alpha_1,\ldots,\alpha_N=1,2}\sum_{k=1}^{d-1}\left(P^{(k)}_{n,\alpha_1,\ldots,\alpha_N}\right)^\dagger P^{(k)}_{n,\alpha_1,\ldots,\alpha_N} + \frac{m^{N-2}}{2}\sum_{\alpha=1}^{m-2}\sum_{k=1}^{d-1}\left(R^{(k)}_{n,\alpha}\right)^\dagger R^{(k)}_{n,\alpha}, \tag{49}$$

where

$$P^{(k)}_{n,\alpha_1,\ldots\alpha_N} = \mathbb{1} - A^{(k)}_{1,\alpha_1}\otimes\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1}\otimes\bigotimes_{\substack{i=2\\i\neq n}}^{N}A^{(-1)^{i-1}k}_{i,\alpha_{i-1}+\alpha_i-1} \tag{50}$$

with $n = 2,\ldots,N$ and for odd n,

$$\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} = a_kA^k_{n,\alpha_{n-1}+\alpha_n-1} + a^*_kA^k_{n,\alpha_{n-1}+\alpha_n}, \tag{51}$$

whereas for even n,

$$\overline{A}^{(k)}_{n,\alpha_{n-1}+\alpha_n-1} = a_kA^{-k}_{n,\alpha_{n-1}+\alpha_n-1} + a^*_kA^{-k}_{n,\alpha_{n-1}+\alpha_n-2}. \tag{52}$$

As before, in the above expressions we use the convention that $A_{n,\alpha+m} = \omega A_{n,\alpha}$ and $A_{n,0} = \omega^{-1}A_{n,m}$ for all n, α. Further, for odd n,

$$R^{(k)}_{n,\alpha} = \mu^*_{\alpha,k}A^k_{n,2} + \nu^*_{\alpha,k}A^k_{n,\alpha+2} + \tau_{\alpha,k}A^k_{n,\alpha+3}, \tag{53}$$

whereas for even n,

$$R^{(k)}_{n,\alpha} = \mu_{\alpha,k}A^{-k}_{n,2} + \nu_{\alpha,k}A^{-k}_{n,\alpha+2} + \tau_{\alpha,k}A^{-k}_{n,\alpha+3}. \tag{54}$$

As in the previous case, the above SOS decompositions imply that the state $|\psi_N\rangle$ as well as the observables A_{i,x_i} which maximally violate the Bell inequality (12) satisfy

$$P^{(k)}_{n,\alpha_1,\ldots,\alpha_N}|\psi_N\rangle = 0. \tag{55}$$

As concluded before using (32), we proceed in the similar way to obtain the relations for the observables of all the parties,

$$\overline{A}_{n,\alpha}\overline{A}^\dagger_{1,\alpha} = \mathbb{1} \quad\text{and}\quad \overline{A}^{(k)}_{n,\alpha} = \left[\overline{A}^{(1)}_{n,\alpha}\right]^k \tag{56}$$

for any α and any $n = 2,\ldots,N-1$. Also, using the fact that $a_{d-k} = a^*_k$ we have $\overline{A}^{(d-k)}_{n,\alpha} = \overline{A}^{(k)\dagger}_{n,\alpha}$ for any $k = 1,\ldots,d-1$ and $\alpha = 1,\ldots,m$. Furthermore, we have

$$R^{(k)}_{n,\alpha} = 0 \tag{57}$$

for all $k = 1,\ldots,d-1$ and $\alpha = 1,2,\ldots,m-2$. Note that for any observable $A_{n,\alpha}$ we obtained exactly the same relations as those derived previously for $A_{1,\alpha}$ given in Eq. (34). Consequently, we can straightforwardly conclude that for each party A_n the corresponding Hilbert space decomposes as $\mathcal{H}_n = \mathbb{C}^d\otimes\mathcal{H}''_n$ for some finite-dimensional $\mathcal{H}''_n$ and, moreover, that there exists a unitary operation $V_n : \mathcal{H}_n \to \mathcal{H}_n$ such that

$$V_n A_{n,2} V_n^\dagger = Z_d\otimes\mathbb{1}''_n, \quad V_n A_{n,3} V_n^\dagger = T_{d,m}\otimes\mathbb{1}''_n, \tag{58}$$

where $\mathbb{1}''_i$ is the identity matrix acting on $\mathcal{H}''_n$ for any n. In Lemma 3 of the Appendix, we show that the obtained Z_d and $T_{d,m}$ are equivalent to the ideal measurements (15), (16), and (17) up to local unitary transformations, that is,

$$\mathcal{O}_{2,2} = W_2 Z_d W_2^\dagger, \quad \mathcal{O}_{2,3} = W_2 T_{d,m} W_2^\dagger \tag{59}$$

for the second party A_2,

$$\mathcal{O}_{\text{odd},2} = W_{\text{odd}} Z_d W^\dagger_{\text{odd}}, \quad \mathcal{O}_{\text{odd},3} = W_{\text{odd}}T_{d,m}W^\dagger_{\text{odd}} \tag{60}$$

for all the parties numbered by odd numbers, and

$$\mathcal{O}_{\text{ev},2} = W_{\text{ev}} Z_d W^\dagger_{\text{ev}}, \quad \mathcal{O}_{\text{ev},3} = W_{\text{ev}} T_{d,m} W^\dagger_{\text{ev}} \tag{61}$$

for the "even" parties. The unitary operators are given by

$$W_2 = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{2i}{m}+ij+\frac{j}{2}}|d-1-i\rangle\langle j|,$$

$$W_{\text{odd}} = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{i}{m}+ij+\frac{j}{2}}|i\rangle\langle j|,$$

$$W_{\text{ev}} = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{i}{m}+ij+\frac{j}{2}}|d-1-i\rangle\langle j|. \tag{62}$$

As a result, we conclude that there exist local unitary transformations $U_i : \mathbb{C}^d\otimes\mathcal{H}''_i \to \mathbb{C}^d\otimes\mathcal{H}''_i$ such that

$$U_i A_{i,\alpha_i} U_i^\dagger = \mathcal{O}_{i,\alpha_i}\otimes\mathbb{1}''_i \tag{63}$$

for $\alpha_i = 2, 3$. As concluded for the first party, exploiting the relations (53) and (54) one infers that (63) holds true for all $\alpha_i = 1,\ldots,m$. This is explicitly shown in Lemma 4 in the Appendix. This concludes the part of the proof devoted to finding all the observables that violate the Bell inequality (12) maximally.

The state. Finally, using the derived optimal measurements and the relations (34) we now show that the state which maximally violates the Bell inequality (12) is, up to local unitary transformations and some additional irrelevant degrees of freedom, the N-partite GHZ state (1) of local dimension d.

To this aim, we exploit the fact that each local Hilbert space is $\mathcal{H}_n = \mathbb{C}^d\otimes\mathcal{H}''_n$, and therefore the state can be decomposed as

$$|\psi_N\rangle = \sum_{i_1,\ldots,i_N=0}^{d-1}|i_1,\ldots,i_N\rangle|\psi_{i_1,\ldots,i_N}\rangle, \tag{64}$$

where $|\psi_{i_1,\ldots,i_N}\rangle$ are some, in general, unnormalized vectors from $\mathcal{H}''_1\otimes\cdots\otimes\mathcal{H}''_N$.

Now, considering the relations (34) for $k = 1$ and different values of α_i's we demonstrate that $|\psi_{i_1,\ldots,i_N}\rangle = 0$ whenever there is a pair of indices $i_k \neq i_l$ for some $k \neq l$. Moreover, all components with $i_1 = \cdots = i_N$ turn out to be equal. We thus find that the only state which maximally violates the Bell inequality (12) is given by

$$U_1\otimes\cdots\otimes U_N|\psi_N\rangle = |\text{GHZ}_{N,d}\rangle\otimes|\text{aux}_N\rangle, \tag{65}$$

where $|\text{aux}_N\rangle \in \mathcal{H}''_1\otimes\cdots\otimes\mathcal{H}''_N$. A more detailed explanation of this part of the proof can be found in Lemma 5 in the Appendix. This completes the proof of our self-testing statement. ■

IV. CONCLUSIONS

We proposed a self-testing statement for quantum states shared among arbitrary number of parties and of arbitrary local dimension that utilizes a truly d-outcome Bell inequality.

Contrary to the previous approach to self-testing of the GHZ states of Ref. [27], which is a generalization of the results of Ref. [24], our method does not rely on self-testing results for two-dimensional systems. Moreover, it allows for a device-independent certification of the GHZ states based on only two observables per observer, which is in fact the minimal number of observables allowing to observe quantum nonlocality and thus to make nontrivial self-testing statements. This lowers the experimental effort necessary to implement our scheme. Let us also notice that our self-testing method generalizes some previous results in a couple of ways. On one hand, we generalize the self-testing statement for two-qudit maximally entangled states derived in Ref. [17] to an arbitrary number of observers as well as an arbitrary number of measurements. On the other hand, we generalize the self-testing statement based on the chained Bell inequalities given in Ref. [15] to quantum systems of an arbitrary local dimension as well as an arbitrary number of parties.

Our considerations provoke some further questions. First, as far as the possibility of experimental implementations of our results is concerned, it would be interesting to study how robust is our self-testing statement to noises and experimental imperfections and how its robustness scales with the number of parties N. Deriving analytically such robust statements for any d and N is certainly a hard task, hence, we leave it for future publications. Let us notice, nevertheless, that for the particular case of $N = m = 2$ and $d = 3$, the robustness of a self-testing statement for various two-qutrit entangled states based on violation of the Bell inequality (12) and its variants was investigated in Refs. [17,34] by using the numerical approach of Ref. [35]. Another route for future research would be to explore whether our self-testing scheme can be used for device-independent certification of randomness. In fact, it was shown in Ref. [17] that in the bipartite case the maximal violation of the Bell inequality (12) certifies $\log_2 d$ bits of local randomness which by using the results of this work can be generalized to the GHZ states. It would be interesting to see whether our self-testing statement allows for certification of more randomness from these states by taking into account measurements performed by groups of parties, not only a single one as in Ref. [17]. Finally, it would be interesting to see whether our scheme can be further generalized to obtain self-testing methods for other genuinely entangled multipartite states; in fact, no general scheme allowing to self-test any multipartite genuinely entangled state is known.

ACKNOWLEDGMENT

This work is supported by the Foundation for Polish Science through the First Team project (First TEAM/2017-4/31) co-financed by the European Union under the European Regional Development Fund.

APPENDIX: PROOF OF LEMMAS REQUIRED FOR SELF-TESTING

Before proceeding towards the lemmas, let us recall a fact proven in [17].

Fact 1. Consider a real polynomial

$$W(x) = \sum_{i=0}^{d-1} \lambda_i x^i \tag{A1}$$

with rational coefficients $\lambda_i \in \mathbb{Q}$. Assume that ω^n with $\omega = \mathrm{e}^{2\pi \mathrm{i}/d}$ is a root of $W(x)$ for any n being a proper divisor of d, i.e., $n \neq d$ such that $d/n \in \mathbb{N}$. Then, $\lambda_0 = \lambda_1 = \cdots = \lambda_{d-1}$.

Below we state and prove all lemmas used in the proof of our main result. Some of the proofs are long and technical and therefore we divided them into steps marked as observations.

Lemma 1. Consider two unitary observables $A_{1,\alpha}$ such that $\alpha = 2, 3$ acting on a finite-dimensional Hilbert space whose eigenvalues are ω^l ($l \in \{0, \dots, d-1\}$). If they satisfy the conditions (34), then for any $n \neq d$ which is a divisor of d,

$$\mathrm{Tr}\big(A_{1,\alpha}^n\big) = 0 \quad (\alpha = 2, 3). \tag{A2}$$

Proof. First, we substitute the explicit forms of $\overline{A}_{1,2}$ and a_k into both relations in (34) for $\alpha = 2$, which after some algebra gives us two sets of equations for $k = 1, \dots, d-1$:

$$\omega^{\frac{2k-d}{2m}} A_{1,2}^k A_{1,3}^{-k} + \omega^{-\frac{2k-d}{2m}} A_{1,3}^k A_{1,2}^{-k} = 2\cos\left(\frac{\pi}{m}\right)\mathbb{1} \tag{A3}$$

and

$$\omega^{k/m} A_{1,2}^{2k} + \omega^{-k/m} A_{1,3}^{2k} = A_{1,2}^k A_{1,3}^k + A_{1,3}^k A_{1,2}^k. \tag{A4}$$

Multiplying then Eq. (A4) by $A_{1,2}^{-k}$ and taking trace on both sides, one obtains

$$\omega^{k/m}\mathrm{Tr}\big(A_{1,2}^k\big) + \omega^{-k/m}\mathrm{Tr}\big(A_{1,3}^{2k} A_{1,2}^{-k}\big) = 2\,\mathrm{Tr}\big(A_{1,3}^k\big). \tag{A5}$$

On the other hand, multiplying Eq. (A3) by $A_{1,3}^k$ and taking the trace on both sides, we get

$$\omega^{\frac{2k-d}{2m}}\,\mathrm{Tr}\big(A_{1,2}^k\big) + \omega^{-\frac{2k-d}{2m}}\,\mathrm{Tr}\big(A_{1,3}^{2k} A_{1,2}^{-k}\big) = 2\,\cos\left(\frac{\pi}{m}\right)\mathrm{Tr}\big(A_{1,3}^k\big). \tag{A6}$$

Then, one eliminates the term $\mathrm{Tr}(A_{1,3}^{2k}A_{1,2}^{-k})$ from (A5) and (A6) to arrive at

$$\mathrm{Tr}\big(A_{1,2}^{k}\big) = 2\omega^{-k/m}\frac{1-\cos(\pi/m)\omega^{-d/2m}}{1-\omega^{-d/m}}\mathrm{Tr}\big(A_{1,3}^{k}\big) \tag{A7}$$

which can be further simplified to

$$\mathrm{Tr}\big(A_{1,2}^{k}\big) = \omega^{-k/m}\mathrm{Tr}\big(A_{1,3}^{k}\big) \quad \left(k=1,\dots,\left\lfloor\frac{d}{2}\right\rfloor\right). \tag{A8}$$

We have thus established a relation between traces of powers of the observables $A_{1,2}$ and $A_{1,3}$. It is thus enough to prove that they vanish for one of these observables. To this end, we prove the following observation.

Observation 1.1. The following identities hold true for any non-negative integer $t\in\mathbb{N}\cup\{0\}$ and $x=1,\dots,\lfloor d/2\rfloor$:

$$\mathrm{Tr}\big(A_{1,2}^{x}\big) = \omega^{\frac{2tx}{m}}\,\mathrm{Tr}\big(A_{1,2}^{(2t+1)x}A_{1,3}^{-2tx}\big). \tag{A9}$$

Proof. We prove this relation using mathematical induction. First, let us notice that it is trivially satisfied for $t=0$. Now, let us suppose that (A9) holds true for $t=s-1$,

$$\mathrm{Tr}\big(A_{1,2}^{x}\big) = \omega^{\frac{2(s-1)x}{m}}\,\mathrm{Tr}\big(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\big) \tag{A10}$$

for $x=1,\dots,\lfloor d/2\rfloor$. We will prove that the relation (A9) holds also true for $t=s$. For this purpose, let us look at the right-hand side of Eq. (A9) for $t=s$ and consider (A3) for $k=2sx$, multiply it by $A_{1,2}^{x}$, and take the trace on both sides. This gives

$$\omega^{\frac{4sx-d}{2m}}\mathrm{Tr}\big(A_{1,2}^{(2s+1)x}A_{1,3}^{-2sx}\big) + \omega^{\frac{d-4sx}{2m}}\mathrm{Tr}\big(A_{1,3}^{2sx}A_{1,2}^{(-2s+1)x}\big) = \cos\Big(\frac{\pi}{m}\Big)\mathrm{Tr}\big(A_{1,2}^{x}\big). \tag{A11}$$

We consider again Eq. (A3) for $k=(2s-1)x$, multiply it by $A_{1,3}^{x}$, and then take the trace on both sides, which results in

$$\omega^{\frac{2(2s-1)x-d}{2m}}\mathrm{Tr}\big(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\big) + \omega^{\frac{d-2(2s-1)x}{2m}}\mathrm{Tr}\big(A_{1,3}^{2sx}A_{1,2}^{(-2s+1)x}\big) = \cos\Big(\frac{\pi}{m}\Big)\mathrm{Tr}\big(A_{1,3}^{x}\big), \tag{A12}$$

which after employing Eq. (A8) for $k=x$ simplifies to

$$\omega^{\frac{4(s-1)x-d}{2m}}\mathrm{Tr}\big(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\big) + \omega^{\frac{d-4sx}{2m}}\mathrm{Tr}\big(A_{1,3}^{2sx}A_{1,2}^{(-2s+1)x}\big) = \cos\Big(\frac{\pi}{m}\Big)\mathrm{Tr}\big(A_{1,2}^{x}\big). \tag{A13}$$

Note that the above expression is valid only for $x=1,\dots,\lfloor d/2\rfloor$. After subtracting Eq. (A13) from Eq. (A11) we arrive at

$$\mathrm{Tr}\big(A_{1,2}^{(2s+1)x}A_{1,3}^{-2sx}\big) = \omega^{-\frac{2x}{m}}\big(A_{1,2}^{(2s-1)x}A_{1,3}^{-2(s-1)x}\big), \tag{A14}$$

which together with Eq. (A10) gives

$$\mathrm{Tr}\big(A_{1,2}^{(2s+1)x}A_{1,3}^{-2sx}\big) = \omega^{-\frac{2sx}{m}}\mathrm{Tr}\big(A_{1,2}^{x}\big). \tag{A15}$$

This completes the proof of Observation 1.1. ■

We are now in a position to prove Eq. (A2). Let n be a divisor of d, that is, $d/n\in\mathbb{N}$. Note that any divisor of d (except d itself) is always smaller or equal to $d/2$. There are two possibilities of d/n being even or odd. Whenever d/n is even, that is, there exists some integer t such that $n=d/2t$, we substitute $x=n=d/2t$ in Eq. (A9), which gives

$$\mathrm{Tr}\big(A_{1,2}^{n}\big) = \omega^{d/m}\,\mathrm{Tr}\big(A_{1,2}^{d+n}A_{1,3}^{-d}\big). \tag{A16}$$

Using the fact that $A_{1,\alpha}^{d}=\mathbb{1}$, the above relation simplifies to

$$\mathrm{Tr}\big(A_{1,2}^{n}\big) = \omega^{d/m}\mathrm{Tr}\big(A_{1,2}^{n}\big). \tag{A17}$$

As a consequence, for any $m\geqslant 2$, we have that for any n such that d/n is even, $\mathrm{Tr}(A_{1,2}^{n})=0$. Using then Eq. (A8) one can similarly conclude that $\mathrm{Tr}(A_{1,3}^{n})=0$.

Now, for any divisor n of d such that d/n is odd, we choose $x=n=d/(2t+1)$ in Eq. (A9), which leads us to

$$\mathrm{Tr}\big(A_{1,2}^{n}\big) = \omega^{d/m}\omega^{-n/m}\,\mathrm{Tr}\big(A_{1,3}^{n}\big). \tag{A18}$$

Comparing the above expression with Eq. (A8), one directly concludes that $\mathrm{Tr}(A_{1,\alpha})=0$ for any n such that d/n is odd and $n\leqslant d/2$. Thus, we have shown that for any n which is a divisor of d, $\mathrm{Tr}(A_{1,\alpha}^{n})=0$ for $\alpha=2,3$. This completes the proof. ■

Lemma 2. Let us consider two unitary operators $A_{1,2}$ and $A_{1,3}$ acting on $\mathbb{C}^d\otimes\mathcal{H}_1''$ with eigenvalues ω^l for $l=0,1,\dots,d-1$ satisfying the conditions (34). Then, there exists a unitary $V_1:\mathcal{H}_1\to\mathcal{H}_1$ such that $V_1\,A_{1,2}\,V_1^{\dagger}=Z_d\otimes\mathbb{1}_1''$ and $V_1\,A_{1,3}\,V_1^{\dagger}=T_{d,m}\otimes\mathbb{1}_1''$ where $Z_d, T_{d,m}$ are defined in (28).

Proof. We begin by proving the following relation for $A_{1,2}$ and $A_{1,3}$:

$$A_{1,3}^{k} = -(k-1)\omega^{\frac{k}{m}}A_{1,2}^{k} + \omega^{\frac{k-1}{m}}\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t} \tag{A19}$$

for $k = 1, \dots, d$. To this end, we use the mathematical induction. First, it is not difficult to see that for $k = 1$, the relation (A19) is trivially satisfied as both its sides equal $A_{1,3}$. Assuming then that (A19) holds true for k, we will prove that it $k \to k+1$. With this aim, we consider (34) for $\alpha_1 = 2$ and rewrite it as

$$\overline{A}_{1,2}^{(k+1)} = \overline{A}_{1,2}^{(k)}\overline{A}_{1,2}^{(1)} \quad (k = 1, \dots, d-1). \tag{A20}$$

Plugging in the explicit form of $\overline{A}_{1,2}^{(k)}$ we arrive at

$$A_{1,3}^{k+1} = -\omega^{\frac{k+1}{m}}A_{1,2}^{k+1} + \omega^{\frac{k}{m}}A_{1,2}^{k}A_{1,3} + \omega^{\frac{1}{m}}A_{1,3}^{k}A_{1,2}, \tag{A21}$$

which after substituting $A_{1,3}^k$ from Eq. (A19) into it gives

$$\begin{aligned} A_{1,3}^{k+1} &= -\omega^{\frac{k+1}{m}}A_{1,2}^{k+1} + \omega^{\frac{k}{m}}A_{1,2}^{k}A_{1,3} - \omega^{\frac{1}{m}}A_{1,2}\left[(k-1)\omega^{\frac{k}{m}}A_{1,2}^{k} - \omega^{\frac{k-1}{m}}\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}\right] \\ &= -k\omega^{\frac{k+1}{m}}A_{1,2}^{k+1} + \omega^{\frac{k}{m}}\sum_{t=0}^{k}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-t}. \end{aligned} \tag{A22}$$

Now, from the fact that the multiplicities of all the eigenvalues of $A_{1,\alpha}$ are equal, we conclude that there exists a unitary operation $V_1' : \mathcal{H}_1 \to \mathcal{H}_1$ such that $V_1' A_{1,2} V_1'^{\dagger} = Z_d \otimes \mathbb{1}_1''$. Moreover, we can always write $V_1' A_{1,3} V_1'^{\dagger}$ in the following way:

$$V_1' A_{1,3} V_1'^{\dagger} = \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes F_{ij}, \tag{A23}$$

where F_{ij} are some matrices acting on $\mathcal{H}_1''$. In order to make our further considerations simpler and easier to follow we drop the unitary V_1 acting on the observables for now and bring it back at the end of the proof; analogously, we write $\mathbb{1}$ instead of $\mathbb{1}_1''$.

Our aim now is to determine F_{ij} using relations (A19). First, we calculate F_{ii} and then proceed to F_{ij} for $i \neq j$. Equation (A19) for $k = d-1$ gives us

$$A_{1,3}^{\dagger} = -(d-2)\omega^{\frac{d-1}{m}}A_{1,2}^{\dagger} + \omega^{\frac{d-2}{m}}\sum_{t=0}^{d-2}A_{1,2}^{t}A_{1,3}A_{1,2}^{d-t-2}. \tag{A24}$$

Taking then $A_{1,2} = Z_d \otimes \mathbb{1}_1''$ and $A_{1,3}$ as given in Eq. (A23), the above expression (A24) can be rewritten as

$$\sum_{i,j=0}^{d-1} |j\rangle\langle i| \otimes F_{ij}^{\dagger} = -(d-2)\omega^{\frac{d-1}{m}}\sum_{i=0}^{d-1}\omega^{-i}|i\rangle\langle i| \otimes \mathbb{1} + \omega^{\frac{d-2}{m}}\sum_{i,j=0}^{d-1}\sum_{t=0}^{d-2}\omega^{-2j+t(i-j)}|i\rangle\langle j| \otimes F_{ij}. \tag{A25}$$

We can now project the first subsystem onto $|i\rangle\langle i|$ to obtain the following relation:

$$F_{ii}^{\dagger} = -(d-2)\omega^{\frac{d-1}{m}}\omega^{-i}\mathbb{1} + (d-1)\omega^{\frac{d-2}{m}}\omega^{-2i}F_{ii}. \tag{A26}$$

Taking the Hermitian conjugation of the above equation,

$$F_{ii} = -(d-2)\omega^{-\frac{d-1}{m}}\omega^{i}\,\mathbb{1} + (d-1)\omega^{-\frac{d-2}{m}}\omega^{2i}F_{ii}^{\dagger}, \tag{A27}$$

and substituting $F_{ii}^{\dagger}$ from Eq. (A26) into it, we obtain

$$F_{ii} = -(d-2)\omega^{-\frac{d-1}{m}}\omega^{i}\,\mathbb{1} - (d-2)(d-1)\omega^{\frac{1}{m}+i}\mathbb{1} + (d-1)^2F_{ii}, \tag{A28}$$

which after some manipulations can be stated as

$$\begin{aligned} F_{ii} &= \frac{1}{d}\omega^{i+\frac{1}{m}}\left(d-1+\omega^{-\frac{d}{m}}\right)\mathbb{1} \\ &= \omega^{i+\frac{1}{m}}\left[1 - \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{-\frac{d}{2m}}\right]\mathbb{1}. \end{aligned} \tag{A29}$$

Now we focus on determining the matrices F_{ij} for $i \neq j$. Our derivation is based on a sequence of observations. First, taking the $|j\rangle\langle i|$ elements of Eq. (A25) for $i \neq j$, one finds the equation

$$F_{ji}^{\dagger} = \omega^{\frac{d-2}{m}}\omega^{-2j}\sum_{t=0}^{d-2}\omega^{t(i-j)}F_{ij}, \tag{A30}$$

which after taking into account that

$$\sum_{t=0}^{d-2}\omega^{t(i-j)} = -\omega^{-(i-j)} \quad (i \neq j) \tag{A31}$$

reduces to

$$F_{ij} = -\omega^{-\frac{d-2}{m}}\omega^{i+j}F_{ji}^{\dagger}. \tag{A32}$$

Note that (A24) only relates the symmetric elements of $A_{1,3}$ in the form (A32). To find the explicit form of F_{ij}, we need to consider equations similar to Eq. (A25), however, with higher-order terms in F_{ij}. To this end, let us prove the following observation.

Observation 2.1. The following conditions hold true for any $k = 1, \dots, d-1$ and $m \geqslant 2$:

$$\omega^{-\frac{1}{m}}\sum_{i,j=0}^{d-1}|i\rangle\langle j| \otimes \left[\sum_{\substack{l=0\\ l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{lj} + k\omega^{(k-1)i}F_{ii}F_{ij}\right] - (k-1)\sum_{i,j=0}^{d-1}\omega^{ki}|i\rangle\langle j| \otimes F_{ij}$$

$$= -k\omega^{\frac{1}{m}}\sum_{i=0}^{d-1}\omega^{(k+1)i}|i\rangle\langle i| \otimes \mathbb{1} + \sum_{i,j=0}^{d-1}|i\rangle\langle j| \otimes \sum_{t=0}^{k}\omega^{kj+t(i-j)}F_{ij}. \tag{A33}$$

Proof. Let us consider a trivial relation $A_{1,3}^{k+1} = A_{1,3}^{k}A_{1,3}$ and substitute in it $A_{1,3}^{k+1}$ and $A_{1,3}^{k}$ using Eq. (A19). This leads us to

$$-k\omega^{\frac{1}{m}}A_{1,2}^{k+1} + \sum_{t=0}^{k}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-t} = -(k-1)A_{1,2}^{k}A_{1,3} + \omega^{-\frac{1}{m}}\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}A_{1,3}. \tag{A34}$$

We now evaluate the sum appearing on the right-hand side by substituting the explicit forms of $A_{1,2}$ and $A_{1,3}$:

$$\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}A_{1,3} = \sum_{i,j=0}^{d-1}|i\rangle\langle j| \otimes \sum_{l=0}^{d-1}\sum_{t=0}^{k-1}\omega^{l(k-1)}\omega^{t(i-l)}F_{il}F_{lj}. \tag{A35}$$

Splitting the sum over l into two parts, $l = i$ and $l \neq i$, and using the fact that

$$\sum_{t=0}^{k-1}\omega^{t(i-l)} = \frac{1-\omega^{k(i-l)}}{1-\omega^{i-l}}, \tag{A36}$$

we obtain

$$\sum_{t=0}^{k-1}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-1-t}A_{1,3} = \sum_{i,j=0}^{d-1}|i\rangle\langle j| \otimes \left[\sum_{\substack{l=0\\ l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{lj} + k\omega^{(k-1)i}F_{ii}F_{ij}\right]. \tag{A37}$$

Then, using similar arguments, the sum on the left-hand side of Eq. (A34) can be expressed as

$$\sum_{t=0}^{k}A_{1,2}^{t}A_{1,3}A_{1,2}^{k-t} = \sum_{i,j=0}^{d-1}\omega^{kj}\sum_{t=0}^{k}\omega^{t(i-j)}|i\rangle\langle j| \otimes F_{ij}. \tag{A38}$$

Plugging Eqs. (A37) and (A38) into Eq. (A34) one arrives at (A33) which completes the proof of Observation 2.1. ■

Equipped with the relation (A33) we can now proceed with the characterization of F_{ij}. Precisely, the diagonal terms (A33) can be used to prove the following observation.

Observation 2.2. The following conditions hold true for any pair $i \neq j$:

$$F_{ij}F_{ij}^{\dagger} = \frac{4}{d^2}\sin^2\left(\frac{\pi}{m}\right)\mathbb{1}. \tag{A39}$$

Proof. Let us first consider Eq. (A33) and project the first subsystem onto $|i\rangle\langle i|$ which, after simple algebra, gives

$$\sum_{\substack{l=0\\ l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{li} = k\omega^{ki}\left[2\omega^{\frac{1}{m}}F_{ii} - \omega^{-i}F_{ii}^{2} - \omega^{i+\frac{2}{m}}\mathbb{1}\right]. \tag{A40}$$

This after substituting F_{ii} from Eq. (A29) simplifies to

$$\sum_{\substack{l=0\\l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{li}=-\frac{k}{d^2}\omega^{i(k+1)+\frac{2}{m}}(1-\omega^{-d/m})^2\mathbb{1}, \tag{A41}$$

which, after a few manipulations, can be rewritten as

$$\sum_{\substack{l=0\\l\neq i}}^{d-1}\left(\frac{1-\omega^{k(l-i)}}{1-\omega^{i-l}}\right)F_{il}F_{li}\omega^{-\left(i+l+\frac{2}{m}\right)}\omega^{\frac{d}{m}}=\frac{k}{d^2}\omega^{\frac{d}{m}}(1-\omega^{-\frac{d}{m}})^2\mathbb{1}. \tag{A42}$$

Then, after taking into account Eq. (A32), changing the index l to j, and simplifying the right-hand side, we have

$$\sum_{\substack{j=0\\j\neq i}}^{d-1}\left(\frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}}\right)F_{ij}F_{ij}^{\dagger}=\frac{4k}{d^2}\sin^2\left(\frac{\pi}{m}\right)\mathbb{1}, \tag{A43}$$

for $i,k=0,\dots,d-1$. We then multiply the above expression by ω^{kn} with $k=0,\dots,d-1$ and $n=1,\dots,d-1$, and then sum the resulting relation over all k's, which yields

$$-\sum_{\substack{j=0\\j\neq i}}^{d-1}\frac{1}{1-\omega^{i-j}}F_{ij}F_{ij}^{\dagger}\sum_{k=0}^{d-1}\omega^{k(j-i+n)}=\frac{4}{d^2}\sin^2\left(\frac{\pi}{m}\right)\sum_{k=0}^{d-1}k\omega^{kn}\mathbb{1}. \tag{A44}$$

Exploiting the following identities

$$\sum_{k=0}^{d-1}\omega^{kn}=0,\quad \sum_{k=0}^{d-1}k\omega^{kn}=\frac{d}{\omega^n-1}, \tag{A45}$$

and

$$\sum_{k=0}^{d-1}\omega^{k(j-i+n)}=\delta_{j,i-n\mod d} \tag{A46}$$

that are satisfied for any $n=1,\dots,d-1$, we arrive at the following relation:

$$F_{i(i-n\mod d)}F_{i(i-n\mod d)}^{\dagger}=\frac{4}{d^2}\sin^2\left(\frac{\pi}{m}\right)\mathbb{1}. \tag{A47}$$

Note that for any $i=0,\dots,d-1$ there exist $n=1,\dots,d-1$ such that $i-n\mod d$ is any number from $\{0,\dots,d-1\}$ and is different than i. This completes the proof of Observation 2.2. ■

While (A39) tell us a lot about the matrices F_{ij}, it is still not enough to determine their explicit form. To complete the characterization we consider a unitary operation $\widetilde{V}:\mathcal{H}_1\to\mathcal{H}_1$ of the form

$$\widetilde{V}=\sum_{i=0}^{d-1}|i\rangle\langle i|\otimes\widetilde{V}_i, \tag{A48}$$

where $\widetilde{V}_i:\mathcal{H}_1''\to\mathcal{H}_1''$ are unitary operations defined as

$$\widetilde{V}_0=\mathbb{1},\quad \widetilde{V}_i=-\frac{d\mathbb{i}}{2\sin(\pi/m)}\omega^{-\frac{i}{2}+\frac{d-2}{2m}}F_{0i} \tag{A49}$$

for $i=1,\dots,d-1$. Importantly, $\widetilde{V}$ commutes with Z_d and thus preserves the form of $A_{1,2}$.

We then have

$$\widetilde{V}A_{1,3}\widetilde{V}^{\dagger}=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\tilde{F}_{ij}, \tag{A50}$$

where we denoted $\tilde{F}_{ij}=\widetilde{V}_iF_{ij}\widetilde{V}_j^{\dagger}$. For a remark, all the algebraic relations for F_{ij} obtained so far hold true for $\tilde{F}_{ij}$, and $\tilde{F}_{ii}=F_{ii}$. Now, we see that

$$\tilde{F}_{0j}=\widetilde{V}_0F_{0j}\widetilde{V}_j^{\dagger}=\frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{\frac{j}{2}+\frac{2-d}{2m}}\mathbb{1}, \tag{A51}$$

where we employed Eq. (A39) for $i=0$. Now, using Eq. (A32) we obtain that $\tilde{F}_{j0}=\tilde{F}_{0j}$.

In the remaining part of the proof of Lemma 2, we focus on the elements F_{ij} for $i, j \neq 0$ and $i \neq j$. To do so, we exploit the off-diagonal elements of (A43).

Observation 2.3. The following conditions hold true:

$$\sum_{\substack{i=1\\i\neq j}}^{d-1}\left(\frac{1-\omega^{ki}}{1-\omega^{i}}\right)\omega^{\frac{i}{2}}F_{ij}=\frac{1}{d}(1-\omega^{-\frac{d}{m}})\omega^{\frac{j}{2}+\frac{1}{m}}\left(k+\frac{1-\omega^{kj}}{1-\omega^{j}}\omega^{j}\right)\mathbb{1}, \tag{A52}$$

for $k, j = 1, \dots, d-1$.

Proof. Taking the inner product with $\langle i|\cdot|j\rangle$ (where $i \neq j$) on the both sides of (A33) we obtain

$$-(k-1)\omega^{ki}F_{ij}+\omega^{-\frac{1}{m}}\sum_{\substack{l=0\\l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{lj}+k\omega^{(k-1)i}\omega^{-\frac{1}{m}}F_{ii}F_{ij}=\frac{\omega^{(k+1)i}-\omega^{(k+1)j}}{\omega^{i}-\omega^{j}}F_{ij}. \tag{A53}$$

Rearranging some terms and using F_{ii} from (A29), we have

$$\sum_{\substack{l=0\\l\neq i}}^{d-1}\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}F_{il}F_{lj}=\omega^{\frac{1}{m}}\left\{\frac{\omega^{(k+1)i}-\omega^{(k+1)j}}{\omega^{i}-\omega^{j}}+\left[\frac{k}{d}(1-\omega^{-d/m})-1\right]\omega^{ki}\right\}F_{ij}. \tag{A54}$$

Next, we set $i = 0$ and obtain

$$\sum_{l=1}^{d-1}\frac{1-\omega^{kl}}{1-\omega^{l}}F_{0l}F_{lj}=\omega^{\frac{1}{m}}\left[\frac{1-\omega^{(k+1)j}}{1-\omega^{j}}+\frac{k}{d}(1-\omega^{-d/m})-1\right]F_{0j}. \tag{A55}$$

Substituting F_{0j} from (A51),

$$\sum_{l=1}^{d-1}\frac{1-\omega^{kl}}{1-\omega^{l}}\omega^{\frac{l}{2}}F_{lj}=\omega^{\frac{j}{2}+\frac{1}{m}}\left[\frac{1-\omega^{(k+1)j}}{1-\omega^{j}}+\frac{k}{d}(1-\omega^{-d/m})-1\right]\mathbb{1}. \tag{A56}$$

Taking the term corresponding to $l = j$ out of the sum and expressing F_{jj} with the aid of Eq. (A29) we arrive at the desired formula Eq. (A52), which completes the proof of Observation 2.3. ■

We can finally determine the form of F_{ij} for $i \neq j$ and $i, j \neq 0$. To this end, we multiply Eq. (A52) by ω^{-kn} with $n = 1, \dots, d-1$ such that $n \neq j$ and then sum both sides of the resulting formula over $k = 0, \dots, d-1$, obtaining

$$\sum_{\substack{i=1\\i\neq j}}^{d-1}\frac{\omega^{i/2}}{1-\omega^{i}}F_{ij}\sum_{k=0}^{d-1}(\omega^{-kn}-\omega^{k(i-n)})=\frac{1}{d}(1-\omega^{-d/m})\omega^{\frac{j}{2}+\frac{1}{m}}\left[\sum_{k=0}^{d-1}k\omega^{-kn}+\frac{\omega^{j}}{1-\omega^{j}}\sum_{k=0}^{d-1}(\omega^{-kn}-\omega^{k(j-n)})\right]\mathbb{1}. \tag{A57}$$

Notice that in the above equation the first sum over k on the left-hand side as well as the last two sums on the right-hand side simply vanish for $n \neq j$. Now, exploiting Eq. (A45) as well as the fact that

$$\sum_{k=0}^{d-1}\omega^{k(n-i)}=d\delta_{n,i}, \tag{A58}$$

and the identity

$$\sum_{k=0}^{d-1}k\omega^{kn}=\frac{d}{\omega^{n}-1},\qquad n=1,\dots,d-1 \tag{A59}$$

proven in [17], we obtain

$$-\frac{\omega^{n/2}}{1-\omega^{n}}F_{nj}=\frac{1}{d^{2}}(1-\omega^{-d/m})\frac{\omega^{\frac{j}{2}+\frac{1}{m}}}{\omega^{-n}-1}\mathbb{1}, \tag{A60}$$

which after simple algebra leads us to

$$\begin{aligned}F_{ij}&=-\frac{1}{d}\left(1-\omega^{-d/m}\right)\omega^{\frac{i+j}{2}+\frac{1}{m}}\mathbb{1}\\&=-\frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{\frac{i+j}{2}+\frac{2-d}{2m}}\mathbb{1}\end{aligned} \tag{A61}$$

for $i,j=1,\ldots,d-1$ such that $i\neq j$. Finally, taking into account Eqs. (A23), (A29), (A51), and (A61) we conclude that there exists a unitary operation $V_1=\widetilde{V}V_1'$ such that $V_1 A_{1,2} V_1^{\dagger}=Z_d\otimes\mathbb{1}$ and

$$V_1 A_{1,3} V_1^{\dagger}=T_{d,m}\otimes\mathbb{1} \tag{A62}$$

with $T_{d,m}$ given by

$$T_{d,m}=\sum_{i=0}^{d-1}\omega^{i+\frac{1}{m}}|i\rangle\langle i|-\frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\sum_{i,j=0}^{d-1}(-1)^{\delta_{i,0}+\delta_{j,0}}\omega^{\frac{i+j}{2}-\frac{d-2}{2m}}|i\rangle\langle j|. \tag{A63}$$

This completes the characterization of $A_{1,2}$ and $A_{1,3}$. ■

Lemma 3. The following unitary operators acting on $\mathbb{C}^d$,

$$W_1=\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{3i}{2m}+ij+\frac{j}{2}}|i\rangle\langle j|,$$

$$W_2=\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{2i}{m}+ij+\frac{j}{2}}|d-1-i\rangle\langle j|,$$

$$W_{\text{odd}}=\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{i}{m}+ij+\frac{j}{2}}|i\rangle\langle j|,$$

$$W_{\text{ev}}=\frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{-\frac{i}{m}+ij+\frac{j}{2}}|d-1-i\rangle\langle j| \tag{A64}$$

transform $Z_d, T_{d,m}$ defined in Eq. (28) to the ideal measurements given in Eqs. (15)–(17) in the following way:

$$\mathcal{O}_{i,2}=W_i Z_d W_i^{\dagger},\quad \mathcal{O}_{i,3}=W_i T_{d,m} W_i^{\dagger}, \tag{A65}$$

where $W_i=W_{\text{odd/ev}}$ for odd and even numbered party i, respectively.

Proof. Let us first notice that the ideal observables from (15)–(17) can be written in the matrix form as

$$\mathcal{O}_{1,x}=\sum_{i=0}^{d-2}\omega^{\gamma_m(\alpha)}|i\rangle\langle i+1|+\omega^{(1-d)\gamma_m(\alpha)}|d-1\rangle\langle 0|,$$

$$\mathcal{O}_{2,x}=\sum_{i=0}^{d-2}\omega^{\zeta_m(\alpha)}|i+1\rangle\langle i|+\omega^{(1-d)\zeta_m(\alpha)}|0\rangle\langle d-1| \tag{A66}$$

for the first two parties, and

$$\mathcal{O}_{\text{odd},x}=\sum_{i=0}^{d-2}\omega^{\theta_m(\alpha)}|i\rangle\langle i+1|+\omega^{(1-d)\theta_m(\alpha)}|d-1\rangle\langle 0|,$$

$$\mathcal{O}_{\text{ev},x}=\sum_{i=0}^{d-2}\omega^{\theta_m(\alpha)}|i+1\rangle\langle i|+\omega^{(1-d)\theta_m(\alpha)}|0\rangle\langle d-1| \tag{A67}$$

for the remaining parties. This allows us to find their eigendecompositions

$$\mathcal{O}_{n,x}=\sum_{r=0}^{d-1}\omega^{r}|r\rangle\langle r|_{n,x} \tag{A68}$$

with $x=2,3$ and $n=1,\ldots,N$, where the eigenvectors are defined as

$$|r\rangle_{1,x}=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\omega^{[r-\gamma_m(x)]q}|q\rangle,$$

$$|r\rangle_{2,x}=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\omega^{-[r-\zeta_m(x)]q}|q\rangle,$$

$$|r\rangle_{n_{\text{odd}},x} = \frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\omega^{[r-\theta_m(x)]q}|q\rangle,$$

$$|r\rangle_{n_{\text{ev}},x} = \frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\omega^{-[r-\theta_m(x)]q}|q\rangle, \tag{A69}$$

where $\gamma_m(x)$, $\zeta_m(x)$, and $\theta_m(x)$ are given in Eq. (21) and $\{|q\rangle\}$ is the computational basis of $\mathbb{C}^d$. It should be noticed here that by the very construction the vectors $|r\rangle_{i,x}$ are mutually orthogonal for any choice of i and x.

Let us now consider the spectral decompositions of Z_d and $T_{d,m}$:

$$Z_d = \sum_{q=0}^{d-1}\omega^q|q\rangle\langle q|, \quad T_{d,m} = \sum_{r=0}^{d-1}\omega^r|r\rangle\langle r|_T. \tag{A70}$$

We know that the following spectral decomposition holds, where $|q\rangle$ form the computational basis in $\mathbb{C}^d$, whereas $|r\rangle_T$ are the eigenvectors of $T_{d,m}$ given by

$$|r\rangle_T = \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{-\frac{d}{2m}}\sum_{q=0}^{d-1}(-1)^{\delta_{q,0}}\frac{\omega^{-\frac{q}{2}}}{1-\omega^{r-q-\frac{1}{m}}}|q\rangle. \tag{A71}$$

For completeness, let us now verify that $|r\rangle_T$ are the eigenvectors of $T_{d,m}$:

$$T_{d,m}|r\rangle_T = \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{-\frac{d}{2m}}\sum_{q=0}^{d-1}(-1)^{\delta_{q,0}}\omega^{\frac{q}{2}+\frac{1}{m}}\left[\frac{1}{1-\omega^{r-q-\frac{1}{2}}} - \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{-\frac{d}{2m}}\sum_{k=0}^{d-1}\frac{1}{1-\omega^{r-k-\frac{1}{m}}}\right]|q\rangle. \tag{A72}$$

Using the formula for the sum of a geometric sequence we have the following relation:

$$\sum_{l=0}^{d-1}\omega^{(r-k-\frac{1}{m})l} = \frac{1-\omega^{-\frac{d}{m}}}{1-\omega^{r-k-\frac{1}{m}}}$$

$$= 2\,\mathbb{i}\sin\left(\frac{\pi}{m}\right)\frac{\omega^{-\frac{d}{2m}}}{1-\omega^{r-k-\frac{1}{m}}}, \tag{A73}$$

which can later be used to write

$$\sum_{k=0}^{d-1}\frac{1}{1-\omega^{r-k-\frac{1}{m}}} = \frac{\omega^{d/2m}}{2\mathbb{i}\,\sin(\pi/m)}\sum_{l=0}^{d-1}\sum_{k=0}^{d-1}\omega^{(r-k-\frac{1}{m})l}. \tag{A74}$$

Noting that the sum over k is nonzero iff $l=0$, we obtain

$$\sum_{k=0}^{d-1}\frac{1}{1-\omega^{r-k-\frac{1}{2}}} = \frac{d\omega^{d/2m}}{2\,\mathbb{i}\sin(\pi/m)}. \tag{A75}$$

Substituting the above relation (A75) into Eq. (A72), we finally have

$$T_{d,m}|r\rangle_T = \frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{-d/2m}\sum_{q=0}^{d-1}(-1)^{\delta_{q,0}}\omega^{\frac{q}{2}+\frac{1}{m}}\left(\frac{1}{1-\omega^{r-q-\frac{1}{m}}}-1\right)|q\rangle$$

$$= \omega^r|r\rangle_T. \tag{A76}$$

Thus, the vectors $|r\rangle_T$ are the eigenvectors of $T_{d,m}$.

Let us now show that the unitary operations (A64) transform Z_d and $T_{d,m}$ to the optimal measurements $\mathcal{O}_{i,2}$ and $\mathcal{O}_{i,3}$ for any $i = 1,\ldots,N$. To this aim, it is sufficient to show that they transform the eigenvectors of one observable to the eigenvectors of another observable up to a complex number. Let us first consider W_1. The action of its Hermitian conjugation on the eigenvectors of $\mathcal{O}_{1,2}$, $|r\rangle_{1,2}$, given explicitly in Eq. (A69), can be expressed as

$$W_1^\dagger|r\rangle_{1,2} = \frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j)q}\omega^{-\frac{j}{2}}|j\rangle. \tag{A77}$$

Using the fact that

$$\sum_{q=0}^{d-1}\omega^{(r-j)q}=d\delta_{r,j}, \tag{A78}$$

the above simplifies to

$$W_1^{\dagger}|r\rangle_{1,2}=\omega^{\delta_{r,0}-\frac{r}{2}}|r\rangle. \tag{A79}$$

Since $|r\rangle$ are the eigenvectors of Z_d we thus obtain that $W_1^{\dagger}\mathcal{O}_{1,2}W_1=Z_d$.

Let us now determine the action of $W_1^{\dagger}$ on the eigenvectors of $\mathcal{O}_{1,3}$. Using Eqs. (A64) and (A69) one obtains

$$W_1^{\dagger}|r\rangle_{1,3}=\frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j-\frac{1}{m})q}\omega^{-\frac{j}{2}}|j\rangle. \tag{A80}$$

Taking into account Eqs. (A73) and (A71) we then have

$$\begin{aligned}W_1^{\dagger}|r\rangle_{1,3}&=\frac{2\mathbb{i}}{d}\sin\left(\frac{\pi}{m}\right)\omega^{-\frac{d}{2m}}\sum_{j=0}^{d-1}(-1)^{\delta_{j,0}}\frac{\omega^{-\frac{j}{2}}}{1-\omega^{r-j-\frac{1}{m}}}|j\rangle\\&=|r\rangle_{T_{d,m}}.\end{aligned} \tag{A81}$$

Let us then consider W_2 given by the second formula in (A64) and apply $W_2^{\dagger}$ to the eigenvectors of $\mathcal{O}_{2,2}$. This leads us to

$$W_2^{\dagger}|r\rangle_{2,2}=\frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j)q+(d-1)(\frac{2}{m}-r)-\frac{j}{2}}|j\rangle, \tag{A82}$$

and, after employing Eq. (A78), to

$$W_2^{\dagger}|r\rangle_{2,2}=(-1)^{\delta_{r,0}}\omega^{(d-1)(\frac{2}{m}-r)-\frac{j}{2}}|r\rangle. \tag{A83}$$

Thus, up to some phases, $W_2^{\dagger}$ maps the eigenvectors of $\mathcal{O}_{2,2}$ to those of Z_d; in other words, $W_2^{\dagger}\mathcal{O}_{2,2}W_2=Z_d$. Analogously, we can write

$$W_2^{\dagger}|r\rangle_{2,3}=\frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j-\frac{1}{m})q+(d-1)(\frac{2}{m}-r)-\frac{j}{2}}|j\rangle,$$

which after carrying out the sum over q using Eq. (A73) simplifies to

$$W_2^{\dagger}|r\rangle_{2,3}=\omega^{(d-1)(\frac{2}{m}-r)}|r\rangle_T. \tag{A84}$$

Next, we look at $W_{\rm odd}$ defined through the third formula in Eq. (A64). The action of $W_2^{\dagger}$ on the eigenvectors of the second observable $\mathcal{O}_{\rm odd,2}$ of each odd party is given by

$$W_{\rm odd}^{\dagger}|r\rangle_{n_{\rm odd},2}=\frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j)q}\omega^{-\frac{j}{2}}|j\rangle, \tag{A85}$$

which by using Eq. (A78) can be rewritten as

$$W_{\rm odd}^{\dagger}|r\rangle_{\rm odd,2}=(-1)^{\delta_{r,0}}\omega^{-r/2}|r\rangle. \tag{A86}$$

Similarly, we have for $\mathcal{O}_{\rm odd,3}$,

$$W_{\rm odd}^{\dagger}|r\rangle_{\rm odd,3}=\frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j-\frac{1}{m})q}\omega^{-\frac{j}{2}}|j\rangle,$$

which by virtue of Eq. (A73) simplifies to

$$W_{\rm odd}^{\dagger}|r\rangle_{\rm odd,3}=|r\rangle_T. \tag{A87}$$

Let us finally consider $W_{\rm ev}$ given by the fourth equation of (A64). We have

$$W_{\rm ev}^{\dagger}|r\rangle_{\rm ev,2}=\frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j)q+(d-1)(\frac{2}{m}-r)-\frac{j}{2}}|j\rangle, \tag{A88}$$

which after performing the summation over q simplifies to

$$W_{\mathrm{ev}}^{\dagger}|r\rangle_{\mathrm{ev},2} = (-1)^{\delta_{r,0}}\omega^{(d-1)(\frac{2}{m}-r)-\frac{r}{2}}|r\rangle. \quad \text{(A89)}$$

Consequently, $W_{\mathrm{ev}}^{\dagger}\,\mathcal{O}_{\mathrm{ev},2}\,W_{\mathrm{ev}} = Z_d$.

Then, for the third observable $\mathcal{O}_{\mathrm{ev},3}$ we have

$$W_{\mathrm{ev}}^{\dagger}|r\rangle_{\mathrm{ev},3} = \frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{\delta_{j,0}}\omega^{(r-j-\frac{1}{m})q+(d-1)(\frac{2}{m}-r)-\frac{j}{2}}|j\rangle, \quad \text{(A90)}$$

which by using Eq. (A73) reduces to

$$W_{\mathrm{ev}}^{\dagger}|r\rangle_{\mathrm{ev},3} = \omega^{(d-1)(\frac{2}{m}-r)}|r\rangle_T, \quad \text{(A91)}$$

implying that $W_{\mathrm{ev}}^{\dagger}\,\mathcal{O}_{\mathrm{ev},3}\,W_{\mathrm{ev}} = T_{d,m}$. This completes the proof. ■

Lemma 4. Assume that the observables $A_{n,2}$ and $A_{n,3}$ are of the form

$$U_i A_{i,\alpha} U_i^{\dagger} = \mathcal{O}_{i,\alpha}\otimes \mathbb{1}_i'' \quad (\alpha = 2, 3) \quad \text{(A92)}$$

for any $i = 1, \dots, N$, where $\mathcal{O}_{i,\alpha}$ are the optimal observables given in Eqs. (15)–(17). If the observables A_{i,α_i} for all i, α_i satisfy the relations (37) and (57), then

$$U_i A_{i,\alpha_i} U_i^{\dagger} = \mathcal{O}_{i,\alpha_i}\otimes \mathbb{1}_i'' \quad \text{(A93)}$$

for all i, α_i.

Proof. Now, we can show that the measurements A_{i,α_i} for all α_i and i are equivalent to the optimal measurements (A66) and (A67). To this end, we consider the relations (37) and (57), which for $k = 1$ give

$$R_{n,\alpha}^{(1)} = \mu_{\alpha,1}^{*}A_{n,2} + \nu_{\alpha,1}^{*}A_{n,\alpha+2} + \tau_{\alpha,1}A_{n,\alpha+3} = 0 \quad \text{(A94)}$$

for odd n, and

$$R_{n,\alpha}^{(1)} = \mu_{\alpha,k}A_{n,2}^{-1} + \nu_{\alpha,1}A_{n,\alpha+2}^{-1} + \tau_{\alpha,1}A_{n,\alpha+3}^{-1} = 0 \quad \text{(A95)}$$

for even n, where the coefficients $\mu_{\alpha,1},\ \nu_{\alpha,1}$, and $\tau_{\alpha,1}$ are given in Eqs. (25) and (26). A key observation here is that the ideal observables $\mathcal{O}_{n,\alpha}$ are known to maximally violate the above Bell inequality and thus satisfy the relations (A94) and (A95). Next, we choose $\alpha = 1$ and we observe from (A94) and (A95) that, for all n,

$$A_{n,4} = -\frac{1}{\tau_{1,1}}(\mu_{1,1}^{*}A_{n,2} + \nu_{1,1}^{*}A_{n,3}), \quad \text{(A96)}$$

where we used the fact that $A_{i,\alpha}^{-1} = A_{i,\alpha}^{\dagger}$. We showed in Lemma 3 that $A_{n,2}$ and $A_{n,3}$ are unitarily equivalent to the optimal measurements $\mathcal{O}_{n,2}\otimes\mathbb{1}_n''$ and $\mathcal{O}_{n,3}\otimes\mathbb{1}_n''$ given in Eqs. (A66) and (A67). As a consequence, $A_{n,4}$ is equivalent to $\mathcal{O}_{n,4}\otimes\mathbb{1}_n''$ up to a unitary transformation. Similarly, we can put $\alpha = 2$ in (A94) and (A95) and conclude that, for all n,

$$A_{n,5} = -\frac{1}{\tau_{2,1}}(\mu_{2,1}^{*}A_{n,2} + \nu_{2,1}^{*}A_{n,4}). \quad \text{(A97)}$$

This implies that $A_{n,5}$ is equivalent to $\mathcal{O}_{n,5}\otimes\mathbb{1}_n''$ up to some unitary transformation. We continue in a similar manner, and conclude that there exist local unitary transformations $U_i : \mathcal{H}_i \to \mathcal{H}_i$ such that

$$\forall\, i, \alpha, \quad U_i\, A_{i,\alpha}\, U_i^{\dagger} = \mathcal{O}_{i,\alpha}\otimes\mathbb{1}_i'', \quad \text{(A98)}$$

which completes the proof. ■

Lemma 5. Assume that A_{i,α_i} are of the form (29) with $\mathcal{O}_{i,\alpha_i}$ defined in Eqs. (15)–(17). If these observables and some state $|\psi_N\rangle$ satisfy the relation (34), then there exist local unitary transformations $U_i : \mathcal{H}_i \to \mathcal{H}_i$ such that

$$U_1\otimes\cdots\otimes U_N|\psi_N\rangle = |\mathrm{GHZ}_{N,d}\rangle\otimes|\mathrm{aux}_N\rangle$$

for some $|\mathrm{aux}_N\rangle \in \mathcal{H}_1''\otimes\cdots\otimes\mathcal{H}_N''$.

Proof. Let us first consider the operator $\overline{A}_{1,\alpha}^{(1)}$ defined in Eq. (33). Using (29) we can state it as

$$\begin{aligned} U_1\overline{A}_{1,\alpha}^{(1)}U_1^{\dagger} &= a_1\mathcal{O}_{1,\alpha} + a_1^{*}\mathcal{O}_{1,\alpha+1} \\ &= \left[\sum_{i=0}^{d-2}\omega^{\gamma_m(\alpha)}(a_1 + a_1^{*}\omega^{\frac{1}{m}})|i\rangle\langle i+1| + \omega^{(1-d)\gamma_2(\alpha)}(a_1 + a_1^{*}\omega^{-\frac{d-1}{m}})|d-1\rangle\langle 0|\right]\otimes\mathbb{1}_n''. \end{aligned} \quad \text{(A99)}$$

Using the fact that $a_1 + a_1^*\omega^{1/m} = \omega^{1/2m}$ and $a_1 + a_1^*\omega^{-(d-1)/m} = \omega^{-(d-1)/2m}$, we get

$$U_1\overline{A}_{1,\alpha}^{(1)}U_1^\dagger = \left[\sum_{i=0}^{d-2}\omega^{\zeta_m(\alpha)}|i\rangle\langle i+1| + \omega^{-(d-1)\zeta_m(\alpha)}|d-1\rangle\langle 0|\right]\otimes \mathbb{1}_n'', \tag{A100}$$

where we used the fact that $\gamma_m(x) + 1/2m = \zeta_m(x)$ [cf. Eq. (21)]. For ease of calculation, we first look at how each of the measurements from (32) act on any vector from $\mathbb{C}^d \otimes \mathcal{H}_1''$ of the form $|j\rangle|\phi\rangle$, where $|j\rangle$ is an element of the computational basis of $\mathbb{C}^d$ whereas $|\phi\rangle$ is an arbitrary vector from $\mathcal{H}_1''$,

$$\begin{aligned} U_1\overline{A}_{1,\alpha}^{(1)}U_1^\dagger|j\rangle|\phi\rangle &= \omega^{(1-d\delta_{j,0})(\alpha/m)}|j-1\rangle|\phi\rangle,\\ U_2A_{2,\alpha}^{-1}U_2^\dagger|j\rangle|\phi\rangle &= \omega^{-(1-d\delta_{j,0})(\alpha/m)}|j-1\rangle|\phi\rangle,\\ U_{n_{\rm odd}}A_{n_{\rm odd},\alpha}U_{n_{odd}}^\dagger|j\rangle|\phi\rangle &= \omega^{(1-d\delta_{j,0})\theta_m(\alpha)}|j-1\rangle|\phi\rangle,\\ U_{n_{\rm ev}}A_{n_{\rm ev},\alpha}^{-1}U_{n_{ev}}^\dagger|j\rangle|\phi\rangle &= \omega^{-(1-d\delta_{j,0})\theta_m(\alpha)}|j-1\rangle|\phi\rangle, \end{aligned}\tag{A101}$$

where $|-1\rangle \equiv |d-1\rangle$.

Having determined the action of the measurements on the elements of the standard basis, let us then decompose the state $|\overline{\psi}_N\rangle = U_1\otimes\cdots\otimes U_N|\psi_N\rangle$ as

$$|\overline{\psi}_N\rangle = \sum_{i_1,\dots,i_N=0}^{d-1}|i_1,\dots,i_N\rangle|\psi_{i_1,\dots,i_N}\rangle \tag{A102}$$

for some, in general unnormalized, vectors $|\psi_{i_1,\dots,i_N}\rangle \in \mathcal{H}_1''\otimes\cdots\otimes\mathcal{H}_N''$, and consider the relations (32) for $\alpha_1=\alpha_2=\cdots=\alpha_N=1$ and $k=1$. Taking into account that $\theta_m(1)=0$, this relation gives

$$\sum_{i_1,\dots,i_N=0}^{d-1}\omega^{\frac{d}{m}(\delta_{i_2,0}-\delta_{i_1,0})}\;|i_1-1\rangle\dots|i_N-1\rangle|\psi_{i_1,\dots,i_N}\rangle = \sum_{i_1,\dots,i_N=0}^{d-1}|i_1,\dots,i_N\rangle|\psi_{i_1,\dots,i_N}\rangle, \tag{A103}$$

from which we directly obtain that for all $i_1,\dots,i_N$,

$$\omega^{\frac{d}{m}(\delta_{i_2,0}-\delta_{i_1,0})}|\psi_{i_1,\dots,i_N}\rangle = |\psi_{i_1-1,\dots,i_N-1}\rangle. \tag{A104}$$

Again, considering the relations (32) for $\alpha_1=2$ and $\alpha_2=\cdots=\alpha_N=1$ with $k=1$, we have

$$\forall\; i_1,\dots,i_N,\quad \omega^{\frac{2d}{m}(\delta_{i_2,0}-\delta_{i_1,0})}|\psi_{i_1,\dots,i_N}\rangle = |\psi_{i_1-1,\dots,i_N-1}\rangle. \tag{A105}$$

Simultaneously, solving the above equations (A104) and (A105), we have the following conditions. First, when $\delta_{i_2,0}=\delta_{i_1,0}$,

$$|\psi_{i_1,i_2\dots,i_N}\rangle = |\psi_{i_1-1,i_2-1,\dots,i_N-1}\rangle \tag{A106}$$

for $i_1, i_2 = 1,2,\dots,d-1$ or $i_1=i_2=0$ and for all $i_3,i_4,\dots,i_N$. Second, when $\delta_{i_1,0}\neq\delta_{i_2,0}$,

$$|\psi_{i_1,0,i_3,\dots,i_N}\rangle = 0,\quad |\psi_{0,i_2,\dots,i_N}\rangle = 0 \tag{A107}$$

for $i_1,i_2=1,2,\dots,d-1$ and for all $i_3,i_4,\dots,i_N$. Now consider (A106) for $i_2=1$ and $i_1\neq 1$,

$$|\psi_{i_1,1\dots,i_N}\rangle = |\psi_{i_1-1,0,\dots,i_N-1}\rangle = 0. \tag{A108}$$

Again considering (A106) for $i_2=2$ and $i_1\neq 2$,

$$|\psi_{i_2,2,\dots,i_N}\rangle = |\psi_{i_1-1,1,\dots,i_N-1}\rangle = 0. \tag{A109}$$

Continuing in a similar way, we have that

$$|\psi_{i_1,i_2,\dots,i_N}\rangle = 0 \qquad \forall\; i_1,i_2,\dots,i_N\;\text{ s.t. }\; i_1\neq i_2 \tag{A110}$$

and

$$|\psi_{i_2-1,i_2-1,i_3-1,\dots,i_N-1}\rangle = |\psi_{i_2,i_2,i_3,\dots,i_N}\rangle \quad \forall\; i_2,i_3,\dots,i_N. \tag{A111}$$

Using the above conditions (A111) and (A110) and considering the relations (32) for $\alpha_1=\alpha_3=\cdots=\alpha_N=1$ and $\alpha_2=2$, we arrive at the following condition for all $i_2,\dots,i_N$:

$$\omega^{\frac{d}{m}(\delta_{i_2,0}-\delta_{i_3,0})}|\psi_{i_2,i_2,i_3\dots,i_N}\rangle = |\psi_{i_2-1,i_2-1,i_3-1,\dots,i_N-1}\rangle. \tag{A112}$$

For the case when $\delta_{i_2,0}=\delta_{i_3,0}$ we have

$$|\psi_{i_2,i_2,i_3,\dots,i_N}\rangle = |\psi_{i_2-1,i_2-1,i_3-1,\dots,i_N-1}\rangle \tag{A113}$$

for $i_2, i_3 = 1, 2, \ldots, d-1$ or $i_2 = i_3 = 0$ and for all $i_4, i_5 \ldots, i_N$. Second when $\delta_{i_2,0} \neq \delta_{i_3,0}$, using (A110) and (A116) we can conclude that

$$|\psi_{0,0,i_3,\ldots,i_N}\rangle = 0, \quad |\psi_{i_2,i_2,0,\ldots,i_N}\rangle = 0 \tag{A114}$$

for $i_2, i_3 = 1, 2, \ldots, d-1$ and for all $i_4, i_5 \ldots, i_N$. Again considering (A114) for $i_2 = 1$ and $i_3 \neq 1$,

$$|\psi_{1,1,i_3,\ldots,i_N}\rangle = |\psi_{0,0,i_3,\ldots,i_N-1}\rangle = 0. \tag{A115}$$

Again considering (A114) for $i_2 = 2$ and $i_3 \neq 2$,

$$|\psi_{2,2,i_3,\ldots,i_N}\rangle = |\psi_{1,1,i_3,\ldots,i_N-1}\rangle = 0. \tag{A116}$$

Continuing in a similar way, we have that

$$|\psi_{i_2,i_2,i_3,\ldots,i_N}\rangle = 0 \quad \forall\, i_2, i_3, \ldots, i_N \ \text{ s.t. } \ i_2 \neq i_3 \tag{A117}$$

and

$$\forall\, i_2, i_4, \ldots, i_N, \quad |\psi_{i_2-1,i_2-1,i_2-1,\ldots,i_N-1}\rangle = |\psi_{i_2,i_2,i_2,\ldots,i_N}\rangle. \tag{A118}$$

Using the above conditions (A117) and (A118), we proceed in a similar manner by again considering the relations (32) for $\alpha_1 = \alpha_2 = \alpha_4 = \cdots = \alpha_N = 1$ and $\alpha_3 = 2$ and arrive at

$$\omega^{\frac{d}{m}(\delta_{i_4,0}-\delta_{i_2,0})}|\psi_{i_2,i_2,i_2,i_4,\ldots,i_N}\rangle = |\psi_{i_2-1,i_2-1,i_2-1,i_4-1,\ldots,i_N-1}\rangle \tag{A119}$$

for all $i_2, i_4, \ldots, i_N$. For the case when $\delta_{i_2,0} = \delta_{i_4,0}$ we have

$$|\psi_{i_2,i_2,i_2,i_4,\ldots,i_N}\rangle = |\psi_{i_2-1,i_2-1,i_2-1,i_4,\ldots,i_N-1}\rangle \tag{A120}$$

for $i_2, i_4 = 1, 2, \ldots, d-1$ or $i_2 = i_4 = 0$ and for all $i_5, i_6, \ldots, i_N$. For the case when $\delta_{i_2,0} \neq \delta_{i_4,0}$ along with (A106) and (A119), we have

$$|\psi_{0,0,0,i_4,\ldots,i_N}\rangle = 0, \quad |\psi_{i_2,i_2,i_2,0,\ldots,i_N}\rangle = 0 \tag{A121}$$

for $i_2, i_4 = 1, 2, \ldots, d-1$ and for all $i_5, i_6 \ldots, i_N$. In a similar manner as concluded above, we again have that

$$|\psi_{i_2,i_2,i_2,i_4,\ldots,i_N}\rangle = 0 \qquad \forall\, i_2, i_4 \ldots, i_N \ \text{ s.t. } \ i_2 \neq i_4 \tag{A122}$$

and for all $i_2, i_5, \ldots, i_N$,

$$|\psi_{i_2-1,i_2-1,i_2-1,i_2-1\ldots,i_N-1}\rangle = |\psi_{i_2,i_2,i_2,i_2,\ldots,i_N}\rangle. \tag{A123}$$

We proceed in a similar manner, considering $N-1$ different equations with $\alpha_n = 2$ for all $n \neq N$ with the rest of coefficients as $\alpha_1 = \alpha_2 = \alpha_3 = \cdots = \alpha_N = 1$ and conclude that the only terms among $|\psi_{i_1,i_2,i_3,\ldots,i_N}\rangle$ which are nonzero are related as

$$\forall\, i, \quad |\psi_{i-1,i-1,i-1,\ldots,i-1}\rangle = |\psi_{i,i,i,\ldots,i}\rangle. \tag{A124}$$

As a consequence, with the proper normalization we can conclude that

$$U_1 \otimes \cdots \otimes U_N|\psi_N\rangle = \left(\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle^{\otimes N}\right) \otimes |\psi_{0,\ldots,0}\rangle \tag{A125}$$

which is the N-partite GHZ state of local dimension d along with some uncorrelated auxiliary state, denoted by $|\psi_{0,\ldots,0}\rangle$. This completes the proof. ■

[1] J. S. Bell, Physics Physique Fizika **1**, 195 (1964).
[2] J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966).
[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[4] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[5] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).
[6] J.-D. Bancal, N. Gisin, Y. C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).
[7] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013).
[8] R. Colbeck and R. Renner, Nat. Commun. **2**, 411 (2011).
[9] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[10] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, NJ, 1998), p. 503.
[11] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A: Math. Theor. **45**, 455304 (2012).
[12] T. H. Yang and M. Navascués, Phys. Rev. A **87**, 050102(R) (2013).

[13] C. Bamps and S. Pironio, Phys. Rev. A **91**, 052111 (2015).

[14] Y. Wang, X. Wu, and V. Scarani, New J. Phys. **18**, 025021 (2016).

[15] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, New J. Phys. **18**, 035013 (2016).

[16] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, Quantum **3**, 198 (2019).

[17] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, npj Quantum Inf. **7**, 151 (2021).

[18] L. Mančinska, J. Prakash, and C. Schafhauser, Constant-sized robust self-tests for states and measurements of unbounded dimension, arXiv:2103.01729.

[19] M. McKague, Theory Quantum Comput. Commun. Cryptogr., **6745**, 104 (2014).

[20] J. Kaniewski, Phys. Rev. Lett. **117**, 070402 (2016).

[21] J. Kaniewski, Phys. Rev. A **95**, 062323 (2017).

[22] E. Panwar, P. Pandya, and M. Wieśniak, An elegant proof of self-testing for multipartite Bell inequalities, arXiv:2202.06908.

[23] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, Phys. Rev. Lett. **124**, 020402 (2020).

[24] A. Coladangelo, K. T. Goh, and V. Scarani, Nat. Commun. **8**, 15485 (2017).

[25] O. Makuta and R. Augusiak, New J. Phys. **23**, 043042 (2021).

[26] X. Wu, Y. Cai, T.-H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, Phys. Rev. A **90**, 042339 (2014).

[27] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, New J. Phys. **20**, 083041 (2018).

[28] W. Slofstra, Forum of Mathematics **7**, e1 (2019).

[29] S. Beigi, Quantum **5**, 389 (2021).

[30] R. Augusiak, A. Salavrakos, J. Tura, and A. Acín, New J. Phys. **21**, 113001 (2019).

[31] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Phys. Rev. Lett. **119**, 040402 (2017).

[32] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).

[33] J. Barrett, A. Kent, and S. Pironio, Phys. Rev. Lett. **97**, 170409 (2006).

[34] J. Wang, S. Paeshani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. M. Bacco *et al.*, Science **360**, 285 (2018).

[35] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).