Supplementary Information for "Self-testing quantum systems of arbitrary local dimension with minimal number of measurements"

Shubhayan Sarkar,[1] Debashis Saha,[1] Jędrzej Kaniewski,[2] and Remigiusz Augusiak[1]

[1]Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotnikow 32/46, 02-668 Warsaw, Poland
[2]Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland

SUPPLEMENTARY METHODS

Proof of self-testing

Here we provide the full proof of theorem stated in the main text. However, before diving into more detailed considerations we recall certain facts that will be used throughout the proof. First, let us recall that the explicit form of the SATWAP Bell inequality with two measurements per observer is

$$\mathcal{I}_d = \sum_{k=1}^{d-1}\left(a_k\langle A_1^k B_1^{d-k}\rangle + a_k^*\omega^k\langle A_1^k B_2^{d-k}\rangle + a_k^*\langle A_2^k B_1^{d-k}\rangle + a_k\langle A_2^k B_2^{d-k}\rangle\right) \leq \beta_{\mathrm{L}}, \tag{1}$$

where

$$a_k = \frac{1}{\sqrt{2}}\omega^{\frac{2k-d}{8}} = \frac{1-\mathbb{i}}{2}\omega^{k/4} = \frac{1-\mathbb{i}}{2}\mathrm{e}^{\frac{\pi \mathbb{i} k}{2d}} \tag{2}$$

and the classical bound β_{L} is given explicitly by

$$\beta_{\mathrm{L}} = \frac{1}{2}\left[3\cot\left(\frac{\pi}{4d}\right) - \cot\left(3\frac{\pi}{4d}\right)\right] - 2. \tag{3}$$

Then, the maximal quantum value of $\mathcal{I}_d$ turns out to be $\beta_{\mathrm{Q}}^d = 2(d-1)$. Let us also recall that the sum-of-squares decomposition of the corresponding Bell operator $\hat{\mathcal{I}}_d$ is

$$\beta_{\mathrm{Q}}^d\mathbb{1} - \hat{\mathcal{I}}_d = \frac{1}{2}\sum_{k=1}^{d-1}\left(P_{1,k}^\dagger P_{1,k} + P_{2,k}^\dagger P_{2,k}\right), \tag{4}$$

with

$$P_{i,k} = \mathbb{1} - A_i^k \otimes C_i^{(k)} \tag{5}$$

for $i = 1,2$ and $k = 1,\ldots,d-1$, where

$$C_1^{(k)} = a_k B_1^{-k} + a_k^*\omega^k B_2^{-k}, \qquad C_2^{(k)} = a_k^* B_1^{-k} + a_k B_2^{-k}. \tag{6}$$

Let us notice here that $a_{d-k} = a_k^*$ and therefore $C_i^{(d-k)} = [C_i^{(k)}]^\dagger$ for any $k = 1,\ldots,d-1$ and $i = 1,2$.

Introducing finally the following matrices

$$Z_d = \sum_{i=0}^{d-1}\omega^i|i\rangle\langle i|, \qquad T_d = \sum_{i=0}^{d-1}\omega^{i+\frac{1}{2}}|i\rangle\langle i| - \frac{2}{d}\sum_{i,j=0}^{d-1}(-1)^{\delta_{i,0}+\delta_{j,0}}\omega^{\frac{i+j+1}{2}}|i\rangle\langle j|. \tag{7}$$

we can now state and prove our main theorem.

Theorem. *Assume that the SATWAP Bell inequality (1) is maximally violated by a state $|\psi\rangle \in \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$ and unitary observables A_i, B_i with $i = 1,2$ acting on $\mathcal{H}_{\mathrm{A}}$ and $\mathcal{H}_{\mathrm{B}}$, respectively. Then, the following statements hold true for any d:*

1. *There exist local unitaries $U_{\mathrm{A}} : \mathcal{H}_{\mathrm{A}} \to \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{A}'}$ and $U_{\mathrm{B}} : \mathcal{H}_{\mathrm{B}} \to \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{B}'}$ such that*

$$U_{\mathrm{B}} B_1 U_{\mathrm{B}}^\dagger = Z_d \otimes \mathbb{1}_{\mathrm{B}'}, \qquad U_{\mathrm{B}} B_2 U_{\mathrm{B}}^\dagger = T_d \otimes \mathbb{1}_{\mathrm{B}'}, \tag{8}$$

and

$$U_{\mathrm{A}} A_1 U_{\mathrm{A}}^\dagger = \left[a_1^* Z_d + 2(a_1^*)^3 T_d\right] \otimes \mathbb{1}_{\mathrm{A}'}, \qquad U_{\mathrm{A}} A_2 U_{\mathrm{A}}^\dagger = (a_1 Z_d - a_1^* T_d) \otimes \mathbb{1}_{\mathrm{A}'}, \tag{9}$$

where a_1 is defined in Eq. (2), whereas Z_d and T_d are defined in Eq. (7);

2. *The state is $|\psi\rangle$ equivalent to the maximally entangled state of two qudits $|\phi_d^+\rangle$ in the sense that*

$$U_{\mathrm{A}} \otimes U_{\mathrm{B}}|\psi\rangle = |\phi_d^+\rangle \otimes |\tilde{\psi}\rangle, \tag{10}$$

where $\mathbb{1}_{\mathrm{A}'}$ and $\mathbb{1}_{\mathrm{B}'}$ are identity operators acting on $\mathcal{H}_{\mathrm{A}'}$ and $\mathcal{H}_{\mathrm{B}'}$, respectively, and $|\tilde{\psi}\rangle$ is some state from $\mathcal{H}_{\mathrm{A}'} \otimes \mathcal{H}_{\mathrm{B}'}$.

Proof. The proof consists of three major steps to prove the theorem. First, we establish that the observables measured by Bob act on a Hilbert space of dimension multiple of d and simultaneously obtain their explicit form. Second, exploiting the symmetry of the Bell-operator we recover the desired form of A_i and subsequently characterize the shared entangled state.

Observables. Since the properties of the observables A_i and B_i can only be determined on the supports of the reduced states ρ_{A} and ρ_{B} of $|\psi\rangle$, without any loss of generality we can assume them to be full rank.

We begin our proof by showing that with the aid of the sum-of-squares decomposition (5) one can prove that the following sets of conditions hold true:

$$C_i^{(k)} = \left[C_i^{(1)}\right]^k \tag{11}$$

and

$$C_i^{(d-k)} C_i^{(k)} = \mathbb{1} \tag{12}$$

for $i = 1, 2$ and $k = 1, \ldots, d-1$.

To prove (11) we first notice that for the state $|\psi\rangle$ and observables A_i and B_i the sum-of-squares decomposition (5) implies that

$$A_i^k \otimes C_i^{(k)}|\psi\rangle = |\psi\rangle \tag{13}$$

are satisfied for $i = 1, 2$ and $k = 1, \ldots, d-1$. Exploiting the fact that A_i are unitary we can rewrite the above as

$$\mathbb{1} \otimes C_i^{(k)}|\psi\rangle = (A_i^k)^\dagger \otimes \mathbb{1}|\psi\rangle = (A_i^\dagger)^k \otimes \mathbb{1}|\psi\rangle. \tag{14}$$

We then make use of (13) for $k = 1$ to see that $A_i^\dagger \otimes \mathbb{1}|\psi\rangle = \mathbb{1} \otimes C_i^{(1)}|\psi\rangle$, which allows us to rewrite the above relation as

$$\mathbb{1} \otimes C_i^{(k)}|\psi\rangle = \mathbb{1} \otimes \left[C_i^{(1)}\right]^k |\psi\rangle, \tag{15}$$

which, taking into account that ρ_{B} is full-rank, is equivalent to the relation (11).

To prove (12) we again consider relation (13) and apply $A_i^{d-k} \otimes C_i^{(d-k)}$ to it. This due to the fact that A_i is unitary gives

$$\mathbb{1} \otimes C_i^{(d-k)} C_i^{(k)}|\psi\rangle = |\psi\rangle. \tag{16}$$

In what follows we show that the conditions (11) and (12) are enough to fully characterize Bob's observables. First, in Lemma 1 we show that these conditions imply that

$$\mathrm{Tr}(B_1^n) = \mathrm{Tr}(B_2^n) = 0 \tag{17}$$

for any positive integer n which is a proper divisor of d. Let us then denote by $\lambda_j^{(i)}$ $(j = 0, \ldots, d-1)$ the multiplicities of the eigenvalues ω^j of B_i and use them to define two real polynomials

$$W_i(x) = \sum_{j=0}^{d-1} \lambda_j^{(i)} x^j \qquad (i = 1, 2). \tag{18}$$

After rewriting the identities (17) as

$$\sum_{j=0}^{d-1} \lambda_j^{(i)} \omega^{nj} = 0, \tag{19}$$

one directly finds that ω^n for any n being a proper divisor of d is a root of both $W_i(x)$. By virtue of Lemma 2, this means that the multiplicities $\lambda_j^{(i)}$ of each of Bob's observables B_i are equal, that is, $\lambda_m^{(i)} = \lambda_n^{(i)}$ for $m \neq n$. This fact allows us to draw two conclusions. First, the dimension of Bob's Hilbert space $\mathcal{H}_\mathrm{B}$ is multiple of the number of outcomes d, meaning that

$$\mathcal{H}_\mathrm{B} = \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{B}'}, \tag{20}$$

where $\mathcal{H}_{\mathrm{B}'}$ is some auxiliary Hilbert space of unknown but finite dimension. Second, there exists a unitary matrix $V_\mathrm{B} : \mathcal{H}_\mathrm{B} \to \mathcal{H}_\mathrm{B}$ such that

$$\widetilde{B}_1 := V_\mathrm{B} B_1 V_\mathrm{B}^\dagger = Z_d \otimes \mathbb{1}_{\mathrm{B}'}, \tag{21}$$

where Z_d is defined in Eq. (7) and $\mathbb{1}_{\mathrm{B}'}$ is the identity acting on $\mathcal{H}_{\mathrm{B}'}$. Thirdly and finally, Lemma 3 implies that there exists another unitary operation $\overline{V}_\mathrm{B}$ that preserves $\widetilde{B}_1 = Z_d \otimes \mathbb{1}_{\mathrm{B}'}$ and

$$\overline{V}_\mathrm{B} (V_\mathrm{B} B_2 V_\mathrm{B}^\dagger) \overline{V}_\mathrm{B}^\dagger = T_d \otimes \mathbb{1}_{\mathrm{B}'} \tag{22}$$

with T_d defined in Eq. (7). Thus, there exist a unitary operation $U_\mathrm{B} : \mathcal{H}_\mathrm{B} \to \mathcal{H}_\mathrm{B}$ given by $U_\mathrm{B} = \overline{V}_\mathrm{B} V_\mathrm{B}$ such that (8) hold true. This completes the first part of the proof.

Alice's observables. Let us now concentrate on Alice's observables. To determine them we will exploit the symmetries of the SATWAP Bell inequality. Precisely, let with the aid of the facts that $a_{d-k} = a_k^*$ and that $A_i^d = B_i^d = \mathbb{1}$, the SATWAP Bell expression $\mathcal{I}_d$ can also be written as

$$\mathcal{I}_d = \sum_{k=1}^{d-1} \left(\overline{C}_1^{(k)} \otimes B_1^k + \overline{C}_2^{(k)} \otimes B_2^k \right), \tag{23}$$

where

$$\overline{C}_1^{(k)} = a_k^* A_1^{-k} + a_k A_2^{-k}, \qquad \overline{C}_2^{(k)} = \omega^{-k} a_k A_1^{-k} + a_k^* A_2^{-k}. \tag{24}$$

Moreover, one can construct another sum-of-squares decomposition for the SATWAP Bell inequality in terms of these combinations of Alice's observables. Precisely, one has

$$\beta_\mathrm{Q}^d \mathbb{1} - \mathcal{B}_d = \frac{1}{2} \sum_{k=1}^{d-1} \left(\overline{P}_{1,k}^\dagger \overline{P}_{1,k} + \overline{P}_{2,k}^\dagger \overline{P}_{2,k} \right), \tag{25}$$

where

$$\overline{P}_{i,k} = \mathbb{1} - \overline{C}_i^{(k)} \otimes B_i^k. \tag{26}$$

Thus, using the same reasoning as in the case of Bob's observables one can show that the $\overline{C}_i^{(k)}$ operators must satisfy the same relations as the $C_i^{(k)}$ operators, that is,

$$\overline{C}_i^{(k)} = \left[\overline{C}_i^{(1)} \right]^k \tag{27}$$

as well as

$$\overline{C}_i^{(d-k)} \overline{C}_i^{(k)} = \mathbb{1} \tag{28}$$

with $i = 1, 2$ and $k = 1, \ldots, d-1$. The crucial step now is to realize that $\overline{C}_1^{(k)}$ and $\overline{C}_2^{(k)}$ have the same form as, respectively, $C_2^{(k)}$ and $C_1^{(k)}$ and hence from the whole analysis performed for Bob's observables we know that

$$\mathcal{H}_\mathrm{A} = \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{A}'} \tag{29}$$

with $\mathcal{H}_{\mathrm{A}'}$ being some auxiliary Hilbert space corresponding to the party A of unknown but finite dimension. Moreover, there exists a unitary operation $V_\mathrm{A} : \mathcal{H}_\mathrm{A} \to \mathcal{H}_\mathrm{A}$ such that

$$\widetilde{A}_1 := V_\mathrm{A} A_1 V_\mathrm{A}^\dagger = Z_d \otimes \mathbb{1}_{\mathrm{A}'}, \qquad \widetilde{A}_2 := V_\mathrm{A} A_2 V_\mathrm{A}^\dagger = T_d \otimes \mathbb{1}_{\mathrm{A}'}. \tag{30}$$

Thus, similarly to Bob's observables we can fully characterize Alice's measurements. In principle we could end our characterization of observables already here, however, for further benefits we will apply another local unitary operation $W_{\mathrm{A}} : \mathbb{C}^d \to \mathbb{C}^d$ to the qudit part of $\widetilde{A}_i$ observables so that

$$W_{\mathrm{A}} Z_d W_{\mathrm{A}}^{\dagger} = a_1^* Z_d + 2(a_1^*)^3 T_d \tag{31}$$

and

$$W_{\mathrm{A}} T_d W_{\mathrm{A}}^{\dagger} = a_1 Z_d - a_1^* T_d. \tag{32}$$

The existence of W_{A} is shown under Fact 2-3 in Appendix . Thus, we have proven the existence of a unitary operation $U_{\mathrm{A}} = (W_{\mathrm{A}} \otimes \mathbb{1}_{\mathrm{A}'})V_{\mathrm{A}}$ such that Eq. (9) hold true. Importantly, by combining Eqs. (31), (32) and (27), application of the unitary U_{A} to $\overline{C}_i^{(k)}$ operators allows us to bring them to

$$U_{\mathrm{A}} \overline{C}_1^{(k)} U_{\mathrm{A}}^{\dagger} = (Z_d^{\dagger})^k \otimes \mathbb{1}_{\mathrm{A}'}, \qquad U_{\mathrm{A}} \overline{C}_2^{(k)} U_{\mathrm{A}}^{\dagger} = (T_d^{\dagger})^k \otimes \mathbb{1}_{\mathrm{A}'}. \tag{33}$$

In particular, if Alice's observables are transformed by applying the unitary U_{A}, then $\overline{C}_1^{(1)} = Z_d^*$ and $\overline{C}_2^{(1)} = T_d^*$. As we will see next this choice of the A_i observables as well as the $\overline{C}_i^{(1)}$ operators guarantees that the self-tested state (up to some additional degrees of freedom) is the maximally entangled state of two qudits written in the standard basis

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle. \tag{34}$$

State. Let us finally prove Eq. (10). From the fact that $|\psi\rangle$ violates maximally the SATWAP Bell inequality we know, by virtue of the SOS decomposition (25) that

$$\overline{C}_1^{(k)} \otimes B_1^k |\psi\rangle = |\psi\rangle, \tag{35}$$

with $i = 1, 2$ and $k = 1, \ldots, d-1$, which after application of $U_{\mathrm{A}} \otimes U_{\mathrm{B}}$ can be rewritten as

$$[(Z_d^*)^{(k)} \otimes Z_d^k \otimes \mathbb{1}_{\mathrm{A}'\mathrm{B}'}]|\psi\rangle = |\psi\rangle \tag{36}$$

and

$$[(T_d^*)^{(k)} \otimes T_d^k \otimes \mathbb{1}_{\mathrm{A}'\mathrm{B}'}]|\psi\rangle = |\psi\rangle, \tag{37}$$

where by $\mathbb{1}_{\mathrm{A}'\mathrm{B}'}$ we denote the identity acting on $\mathcal{H}_{\mathrm{A}'} \otimes \mathcal{H}_{\mathrm{B}'}$.

Since the state $|\psi\rangle$ belongs to $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathcal{H}_{\mathrm{A}'} \otimes \mathcal{H}_{\mathrm{B}'}$ we can decompose it as

$$|\psi\rangle = \sum_{i,j=0}^{d-1} |ij\rangle |\psi_{ij}\rangle, \tag{38}$$

where $|\psi_{ij}\rangle \in \mathcal{H}_{\mathrm{A}'} \otimes \mathcal{H}_{\mathrm{B}'}$ are some in general nonorthogonal and not normalized states. With this decomposition the condition (36) with $k = 1$ implies that

$$\sum_{i,j=0}^{d-1} \omega^{j-i} |ij\rangle |\psi_{ij}\rangle = \sum_{i,j=0}^{d-1} |ij\rangle |\psi_{ij}\rangle. \tag{39}$$

This condition directly implies that

$$|\psi_{ij}\rangle = 0 \tag{40}$$

for any pair $i, j = 0, \ldots, d-1$ such that $i \neq j$.

Let us now exploit the other condition (37) with $k = 1$, which after projecting onto the ket $\langle ii|$ gives

$$|\psi_{ii}\rangle = \sum_{k=0}^{d-1} \langle i|T_d^*|k\rangle \langle i|T_d|k\rangle |\psi_{kk}\rangle = \sum_{k=0}^{d-1} |\langle i|T_d|k\rangle|^2 |\psi_{kk}\rangle \tag{41}$$

where we have used the fact $\langle i|T_d^*|k\rangle = \langle k|T_d^*|i\rangle$ as T_d is symmetric. Using the explicit form of T_d given in (7) we can rewrite the above as

$$|\psi_{ii}\rangle = \frac{4}{d^2}\sum_{k=0}^{d-1}|\psi_{kk}\rangle + \left[\left(1-\frac{2}{d}\right)^2 - \frac{4}{d^2}\right]|\psi_{ii}\rangle = \frac{4}{d^2}\sum_{k=0}^{d-1}|\psi_{kk}\rangle + \left[1-\frac{4}{d}\right]|\psi_{ii}\rangle. \tag{42}$$

We now move the $|\psi_{ii}\rangle$ ket to the left-hand side of the equality (for $d = 4$ there is nothing to move) and obtain the following relation,

$$\forall i, \quad \frac{4}{d}|\psi_{ii}\rangle = \frac{4}{d^2}\sum_{k=0}^{d-1}|\psi_{kk}\rangle, \tag{43}$$

from which it follows that all $|\psi_{ii}\rangle$ are equal. This together with (40) allows us to conclude that

$$U_{\mathrm{A}} \otimes U_{\mathrm{B}}|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle \otimes |\widetilde{\psi}\rangle \tag{44}$$

with $|\widetilde{\psi}\rangle = \sqrt{d}|\psi_{ii}\rangle$. We thus recover (10), completing the proof. □

Below we append three lemmas used in the proof of the above theorem. Remark that, series of Observations are employed inside the proof of Lemma 1 and Lemma 3.

Lemma 1. *Consider two unitary observables B_i ($i \in \{1,2\}$) acting on a finite-dimensional Hilbert space whose eigenvalues are ω^l ($l \in \{0,\ldots,d-1\}$). If they satisfy the conditions (11) and (12), then for any proper divisor n of d, that is, a positive integer such that $n < d$ and $d/n \in \mathbb{N}$,*

$$\mathrm{Tr}(B_1^n) = \mathrm{Tr}(B_2^n) = 0. \tag{45}$$

Proof. Plugging the explicit form of $C_2^{(k)}$ given in Eq. (6) into Eq. (12) and using the fact that $B_i^{d-k} = B_i^{-k}$, we arrive at

$$(a_{d-k}^* B_1^k + a_{d-k}B_2^k)(a_k^* B_1^{-k} + a_k B_2^{-k}) = \mathbb{1}. \tag{46}$$

Using then the fact that $a_k^* = a_{d-k}$ and $a_k^*/a_k = \mathbb{i}\omega^{\frac{k}{2}}$, a simple calculation leads us to the following condition

$$B_1^k B_2^{-k} = \omega^{-k} B_2^k B_1^{-k} \tag{47}$$

with $k = 1,\ldots,d-1$. Due to the fact that $B_i^d = \mathbb{1}$, the above relation (47) extends to any integer $k \in \mathbb{Z}$. We now establish some relations under observations 1.1 and 1.2 which will be used later in the proof.

Observation 1.1. *First, we show that the following identities hold true for any non-negative integers $s,x,y \in \mathbb{N}\cup\{0\}$*

$$\mathrm{Tr}(B_1^x) = \omega^{sx}\,\mathrm{Tr}\left(B_1^{(2s+1)x}B_2^{-2sx}\right). \tag{48}$$

and

$$\mathrm{Tr}(B_2^y) = \omega^{sy}\,\mathrm{Tr}\left(B_1^{2sy}B_2^{(-2s+1)y}\right). \tag{49}$$

We present only the proof of the first identity as that of the second one is analogous. It is pretty straightforward and consists of multiple application of the identity (47). Let us thus focus on the right-hand side of Eq. (48) and consider (47) for $k = 2sx$, multiply it by B_1^x and trace both sides of the resulting equation. This gives

$$\mathrm{Tr}\left(B_1^{(2s+1)x}B_2^{-2sx}\right) = \omega^{-2sx}\mathrm{Tr}\left(B_2^{2sx}B_1^{(-2s+1)x}\right). \tag{50}$$

We consider again (47) for $k = (2s-1)x$, multiply it by B_2^x and then trace both sides, which results in

$$\mathrm{Tr}\left(B_2^{2sx}B_1^{-(2s-1)x}\right) = \omega^{(2s-1)x}\left(B_1^{(2s-1)x}B_2^{-(2s-2)x}\right). \tag{51}$$

After plugging Eq. (51) into Eq. (50) we obtain

$$\mathrm{Tr}\left(B_1^{(2s+1)x}B_2^{-2sx}\right) = \omega^{-x}\left(B_1^{(2s-1)x}B_2^{-(2s-2)x}\right). \tag{52}$$

We have thus lowered the power of B_1 from $(2s+1)x$ in Eq. (50) to $(2s-1)x$ in Eq. (52). We repeat this double substitution until the power of B_1 is x, each time acquiring the phase ω^{-x} (notice that in this case the power of B_2 goes from $-2sx$ in Eq. (50) to zero). As a result we arrive at

$$\mathrm{Tr}\left(B_1^{(2s+1)x}B_2^{-2sx}\right) = \omega^{-sx}\mathrm{Tr}(B_1^x), \tag{53}$$

which is what we wanted to show.

Observation 1.2. *Next, the following simple relation between traces of powers of B_i operators holds true*

$$\mathrm{Tr}(B_1^x) = \omega^{-\frac{x}{2}}\mathrm{Tr}(B_2^x), \qquad x = 1,\ldots,\left\lfloor\frac{d}{2}\right\rfloor. \tag{54}$$

In order to prove this observation let us consider (11) for $k = 2x$, which we can equivalently state as

$$\left[C_2^{(2x)}\right]^\dagger = \left\{\left[C_2^{(x)}\right]^2\right\}^\dagger. \tag{55}$$

This after taking into account (6) implies

$$\omega^{\frac{x}{2}}B_1^{2x} + \omega^{-\frac{x}{2}}B_2^{2x} = \{B_1^x, B_2^x\}. \tag{56}$$

We then multiply the above by B_1^{-x} and by taking trace on both sides we find

$$\omega^{\frac{x}{2}}\mathrm{Tr}(B_1^x) + \omega^{-\frac{x}{2}}\mathrm{Tr}(B_1^{-x}B_2^{2x}) = 2\mathrm{Tr}(B_2^x). \tag{57}$$

We then use (47) with $k = x$, i.e., $B_2^xB_1^{-x} = \omega^x B_1^x B_2^{-x}$. By multiplying it by B_2^x and tracing both sides we obtain

$$\mathrm{Tr}(B_1^{-x}B_2^{2x}) = \omega\mathrm{Tr}(B_1^x). \tag{58}$$

Further, substituting the expression of $\mathrm{Tr}(B_1^{-x}B_2^{2x})$ from Eq. (58) into Eq. (57) leads us to (54).

Let us now make use of the above observations for finally prove the validity of (45). We consider the cases of even and odd d separately.

Even *d.* Let n be a divisor of d, i.e., $d/n \in \mathbb{N}$. There are two possibilities, d/n is even or odd, i.e., there exists integer s such that $n = d/(2s)$ or $n = d/(2s+1)$, respectively. Whenever d/n is even, we consider Eq. (48) for $x = n = d/(2s)$, which reads

$$\mathrm{Tr}(B_1^n) = \omega^{d/2}\,\mathrm{Tr}\left(B_1^{d+n}B_2^{-d}\right). \tag{59}$$

Using then the facts that $B_i^d = \mathbb{1}$ and $\omega^{d/2} = -1$, the above relation simplifies to,

$$\mathrm{Tr}(B_1^n) = (-1)\mathrm{Tr}\left(B_1^n\right). \tag{60}$$

Thus, for any n such that d/n is even, $\mathrm{Tr}(B_1^n) = 0$. Similarly, by taking $y = d/(2s)$ in Eq. (49) one can conclude the same for B_2, i.e., $\mathrm{Tr}(B_2^n) = 0$.

Now, for any divisor n of d for which d/n is odd, we choose $x = n = d/(2s+1)$ in Eq. (48), which leads us to

$$\mathrm{Tr}(B_1^n) = (-1)\omega^{-n/2}\,\mathrm{Tr}\left(B_2^n\right). \tag{61}$$

The above relation together with Eq. (54) imply $\mathrm{Tr}(B_i^n) = 0$ for any n such that d/n is odd and $n \leq d/2$. Thus, we have shown that for any n which is a divisor of d and $n \neq d$, $\mathrm{Tr}(B_i^n) = 0$ for $i = 1,2$.

Odd *d.* Since d is odd, there exists an integer s such that $2s+1 = d$. Plugging $s = (d-1)/2$ in Eq. (48) we get

$$\mathrm{Tr}(B_1^x) = \omega^{(d-1)x/2}\,\mathrm{Tr}\left(B_1^{dx}B_2^{-(d-1)x}\right), \tag{62}$$

which due to the facts that $B_2^d = \mathbb{1}$ and $\omega^{d/2} = -1$ simplifies to

$$\mathrm{Tr}(B_1^x) = (-1)^x\omega^{-x/2}\,\mathrm{Tr}\left(B_2^x\right). \tag{63}$$

Now, for any odd x such that $x \leq \lfloor d/2 \rfloor$ we obtain from Eqs. (54) and (63) that $\mathrm{Tr}(B_1^x) = \mathrm{Tr}(B_2^x) = 0$. Since all the divisors of an odd d (except d) are odd and less than $\lfloor d/2 \rfloor$, we conclude (45). $\square$

Lemma 2. *Consider a real polynomial*

$$W(x) = \sum_{i=0}^{d-1} \lambda_i x^i \tag{64}$$

with rational coefficients $\lambda_i \in \mathbb{Q}$. Assume that ω^n with $\omega = \mathrm{e}^{2\pi \mathbb{i}/d}$ 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, $\lambda_0 = \lambda_1 = \ldots = \lambda_{d-1}$.

To be able to prove this lemma we need to introduce the following two relevant concepts.

Euclidean division algorithm. Let $F(x), G(x) \in \mathbb{F}[x]$ be two nonzero polynomials over the field $\mathbb{F}$ such that $\deg G(x) \leq \deg F(x)$. Then there exist two polynomials $Q(x), R(x) \in \mathbb{F}[x]$ such that $F(x) = Q(x)G(x) + R(x)$ and $\deg R(x) < \deg G(x)$.

Cyclotomic polynomials. Let n be any positive integer. The nth cyclotomic polynomial $\phi_n(x)$ is defined as the unique irreducible polynomial over the field of rational numbers whose root is the primitive root of unity $\exp(2\pi\mathbb{i}/n)$, and is given explicitly by the following formula

$$\phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - e^{\frac{2\pi \mathbb{i} k}{n}} \right). \tag{65}$$

Let us then consider a positive integer d and denote by $n_1 < n_2 < \ldots < n_k$ its proper divisors with $n_1 = 1$ and $n_k < d$. Then, it is known that the product of the cyclotomic polynomials ϕ_{d/n_i} over all these proper divisors can be represented by the following simple formula

$$\prod_{i=1}^{k} \phi_{d/n_i}(x) = \frac{x^d - 1}{x - 1} \equiv \sum_{i=0}^{d-1} x^i. \tag{66}$$

Let us finally notice for further purposes that ω^{n_i} for some divisor n_i is a root of $\phi_{d/n_i}(x)$ but not of $\phi_{d/n_j}(x)$ for any other divisor $n_j \neq n_i$ of d.

Proof. Let $n_1 < n_2 < n_3 < \ldots < n_k < d$ with $n_1 = 1$ and $n_k < d$ be the proper divisors of d. From the assumption we know that ω^{n_i} is a root of $W(x)$, that is

$$W(\omega^{n_i}) = 0, \qquad i = 1, \ldots, k. \tag{67}$$

We now use this last condition along with the Euclidean division algorithm to prove that the polynomial $W(x)$ must be a product of cyclotomic polynomials $\phi_{d/n_i}(x)$. We do it in a recursive way

Let us begin with $n_1 = 1$. The Euclidean division algorithm implies that

$$W(x) = Q_1(x)\phi_d(x) + R_1(x) \tag{68}$$

with $Q_1(x), R_1(x) \in \mathbb{Q}[x]$ such that $\deg R_1(x) < \deg \phi_d(x)$. From Eq. (67) we know that $W(\omega) = 0$, implying that $R_1(\omega) = 0$. As $\phi_d(x)$ is the unique polynomial of minimal degree over the rational field whose root is ω, the latter implies that $R_1(x) \equiv 0$. Thus,

$$W(x) = Q_1(x)\phi_d(x). \tag{69}$$

Let us then move on to the next divisor of d, $n_2 > n_1$. Due to the fact that ω^{n_2} is not a root of $\phi_d(x)$, the condition (67) implies that $Q_1(\omega^{n_2}) = 0$. We therefore apply the Euclidean division algorithm to $Q_1(x)$, that is,

$$Q_1(x) = Q_2(x)\phi_{d/n_2}(x) + R_2(x) \tag{70}$$

with $Q_2(x), R_2(x) \in \mathbb{Q}[x]$ such that $\deg R_2 < \deg \phi_{d/n_2}(x)$. Due to the fact that ω^{n_2} is a root of Q_1 we see that $R_2(\omega^{n_2}) = 0$. Again, due to the fact that $\phi_{d/n_2}(x)$ is the unique polynomial of minimal degree over the rational field whose root is ω^{n_2}, the latter implies $R_2(x) \equiv 0$. Consequently,

$$Q_1(x) = Q_2(x)\phi_{d/n_2}(x). \tag{71}$$

Applying the above procedure iteratively for every divisor n_i of d it is now not difficult to see that our initial polynomial $W(x)$ is of the following form

$$W(x) = \widetilde{Q}(x) \prod_{i=1}^{k} \phi_{d/n_i}(x), \tag{72}$$

with $\widetilde{Q}(x)$ is a rational polynomial. Owing to the fundamental relation satisfied by the cyclotomic polynomials given in Eq. (66) one sees that the degree of the above product of cyclotomic polynomials is $d-1$ and equals the degree of $W(x)$, which directly implies that $\widetilde{Q}(x)$ is simply a constant factor, denoted $\widetilde{Q}$. Moreover, by comparing Eqs. (64) and (72) and taking into account Eq. (66), we immediately see that $\lambda_i = \widetilde{Q}$ for $i = 0, \ldots, d-1$, meaning that $\lambda_0 = \lambda_1 = \ldots = \lambda_{d-1}$, which completes the proof. □

Lemma 3. *Consider two unitary operators B_1 and B_2 acting on $\mathbb{C}^d \otimes \mathcal{H}_{\mathrm{B}'}$ such that $B_i^d = \mathbb{1}$ with $i = 1, 2$. Assume moreover that $B_1 = Z_d \otimes \mathbb{1}_{\mathrm{B}'}$ and that they both satisfy the conditions (11). Then, then there exists a unitary U such that $UB_1U^\dagger = B_1$ and $UB_2U^\dagger = T_d \otimes \mathbb{1}_{\mathrm{B}'}$ with T_d defined in (7).*

Proof. We begin by proving the following relation for B_1 and B_2 matrices:

$$B_2^k = -(k-1)\omega^{\frac{k}{2}} B_1^k + \omega^{\frac{k-1}{2}} \sum_{m=0}^{k-1} B_1^m B_2 B_1^{k-1-m}, \qquad k = 1, \ldots, d. \tag{73}$$

We prove this relation by induction. For $k = 1$ it is not difficult to see that both its sides equal B_2. Assuming then that (73) holds true we will prove it for $k+1$. To this end, let us rewrite (11) as

$$\left[C_2^{(k+1)}\right]^\dagger = \left[C_2^{(1)} C_2^{(k)}\right]^\dagger \tag{74}$$

for $k = 1, \ldots, d-1$, which in terms of B_i [cf. Eq. (6)] can be rewritten as

$$B_2^{k+1} = -\omega^{\frac{k+1}{2}} B_1^{k+1} + \omega^{\frac{k}{2}} B_1^k B_2 + \omega^{\frac{1}{2}} B_2^k B_1. \tag{75}$$

Now, substituting B_2^k from (73), we have

$$\begin{aligned} B_2^{k+1} &= -\omega^{\frac{k+1}{2}} B_1^{k+1} + \omega^{\frac{k}{2}} B_1^k B_2 + \omega^{\frac{1}{2}} \left[-(k-1)\omega^{\frac{k}{2}} B_1^k + \omega^{\frac{k-1}{2}} \sum_{m=0}^{k-1} B_1^m B_2 B_1^{k-1-m} \right] B_1 \\ &= -k\omega^{\frac{k+1}{2}} B_1^{k+1} + \omega^{\frac{k}{2}} \sum_{m=0}^{k} B_1^m B_2 B_1^{k-m}. \end{aligned} \tag{76}$$

Having established (73), let us now write B_2 as

$$B_2 = \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes F_{ij}, \tag{77}$$

where F_{ij} are some matrices acting on $\mathcal{H}_{\mathrm{B}'}$. Our aim now is to determine F_{ij} using the conditions (73). We first focus on F_{ii} and then move on to F_{ij} with $i \neq j$.

Finding F_{ii}. Taking the relation (73) for $k = d-1$, we obtain

$$B_2^\dagger = -(d-2)\omega^{\frac{d-1}{2}} B_1^{d-1} + \omega^{\frac{d-2}{2}} \sum_{m=0}^{d-2} B_1^m B_2 B_1^{d-2-m}, \tag{78}$$

which after taking into account that $B_1 = Z_d \otimes \mathbb{1}_{\mathrm{B}'}$ and that B_2 is given by Eq. (77), can be rewritten as

$$\sum_{i,j=0}^{d-1} |j\rangle\langle i| \otimes F_{ij}^\dagger = -(d-2)\omega^{\frac{d-1}{2}} \sum_{i=0}^{d-1} \omega^{(d-1)i} |i\rangle\langle i| \otimes \mathbb{1}_{\mathrm{B}'} + \omega^{\frac{d-2}{2}} \sum_{i,j=0}^{d-1} \sum_{m=0}^{d-2} \omega^{(d-2)j + m(i-j)} |i\rangle\langle j| \otimes F_{ij}. \tag{79}$$

By projecting the first subsystem onto $|i\rangle\langle i|$, we arrive at the following condition for F_{ii} matrices

$$F_{ii}^\dagger = -(d-2)\omega^{\frac{d-1}{2}} \omega^{-i} \mathbb{1}_{\mathrm{B}'} + (d-1)\omega^{\frac{d-2}{2}} \omega^{-2i} F_{ii}. \tag{80}$$

Conjugating the above equation on both sides we obtain

$$F_{ii} = -(d-2)\omega^{-\frac{d-1}{2}}\omega^{i}\,\mathbb{1}_{\mathrm{B}'} + (d-1)\omega^{-\frac{d-2}{2}}\omega^{2i}F_{ii}^{\dagger}. \tag{81}$$

After plugging into the above relation $F_{ii}^{\dagger}$ from Eq. (80) we obtain an equation for F_{ii} whose solution is

$$F_{ii} = \frac{d-2}{d}\omega^{i+\frac{1}{2}}\mathbb{1}_{\mathrm{B}'}. \tag{82}$$

Finding F_{ij}. Let us now move on to determining the F_{ij} matrices for $i \neq j$. We formulate our derivation as a sequence of observations.

First, by comparing the matrices appearing on $|i\rangle\langle j|$ position of both sides of (79) with $i \neq j$, we obtain the following equation

$$F_{ji}^{\dagger} = \omega^{\frac{d-2}{2}}\omega^{-2j}\sum_{m=0}^{d-2}\omega^{m(i-j)}F_{ij}, \tag{83}$$

which after taking into account the fact that for $i \neq j$,

$$\sum_{m=0}^{d-2}\omega^{m(i-j)} = -\omega^{-(i-j)}, \tag{84}$$

reduces to

$$F_{ij} = \omega^{i+j+1}F_{ji}^{\dagger}. \tag{85}$$

Thus, (78) only provides a relation between the symmetric elements of B_2 in the form (85). To find the explicit form of F_{ij}, we have to look for equations involving higher order terms in F_{ij}. To this aim, let us prove the following observation.

Observation 3.1. *The following conditions hold true*

$$\begin{aligned}
&-(k-1)\omega^{\frac{k}{2}}\sum_{i,j=0}^{d-1}\omega^{ki}|i\rangle\langle j|\otimes F_{ij} + \omega^{\frac{k-1}{2}}\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\left[\sum_{\substack{l=0\\ l\neq i}}^{d-1}\left(\frac{\omega^{ki}-\omega^{kl}}{\omega^{i}-\omega^{l}}\right)F_{il}F_{lj} + k\omega^{(k-1)i}F_{ii}F_{ij}\right]\\
&= -k\omega^{\frac{k+1}{2}}\sum_{i=0}^{d-1}\omega^{(k+1)i}|i\rangle\langle i|\otimes\mathbb{1}_{\mathrm{B}'} + \omega^{\frac{k}{2}}\sum_{i,j=0}^{d-1}\left(\sum_{m=0}^{k}\omega^{kj+m(i-j)}|i\rangle\langle j|\otimes F_{ij}\right), \qquad k=1,\ldots,d-1.
\end{aligned} \tag{86}$$

From (73) we know that

$$B_2^{k+1} = -k\omega^{\frac{k+1}{2}}B_1^{k+1} + \omega^{\frac{k}{2}}\sum_{m=0}^{k}B_1^{m}B_2B_1^{k-m}. \tag{87}$$

Again using (73) for B_2^k, the left-hand side of the above equation can be written as

$$B_2^{k+1} = B_2^kB_2 = -(k-1)\omega^{\frac{k}{2}}B_1^kB_2 + \omega^{\frac{k-1}{2}}\sum_{m=0}^{k-1}B_1^mB_2B_1^{k-1-m}B_2. \tag{88}$$

Let us now focus on the sum appearing in Eq. (88). After substituting the explicit forms of B_1 and B_2 into it, we can rewrite it as

$$\sum_{m=0}^{k-1}B_1^mB_2B_1^{k-1-m}B_2 = \sum_{i,j,l=0}^{d-1}\omega^{(k-1)l}\sum_{m=0}^{k-1}\omega^{m(i-l)}|i\rangle\langle j|\otimes F_{il}F_{lj}. \tag{89}$$

After splitting the above summations into the cases of $i = l$ and $i \neq l$, we obtain

$$\begin{aligned}\sum_{m=0}^{k-1} B_1^m B_2 B_1^{k-1-m} B_2 &= \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes \left[k\omega^{(k-1)i} F_{ii} F_{ij} + \sum_{\substack{l=0\\ l\neq i}}^{d-1} \left(\omega^{(k-1)l} \sum_{m=0}^{k-1} \omega^{m(i-l)} F_{il} F_{lj} \right) \right] \\ &= \sum_{i,j=0}^{d-1} |i\rangle\langle j| \otimes \left[\sum_{\substack{l=0\\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{lj} + k\omega^{(k-1)i} F_{ii} F_{ij} \right]. \end{aligned} \tag{90}$$

Let us then consider the sum appearing in Eq. (87). After plugging the explicit forms of B_1 and B_2 into it we arrive at

$$\sum_{m=0}^{k} B_1^m B_2 B_1^{k-m} = \sum_{i,j=0}^{d-1} \omega^{kj} \sum_{m=0}^{k} \omega^{m(i-j)} |i\rangle\langle j| \otimes F_{ij}. \tag{91}$$

We finally substitute B_2^{k+1} from Eq. (87) into Eq. (88), and then plug the explicit forms of B_1 and B_2 as well as the expressions (90) and (91) into the resulting equations, which leads us to (86). This completes the proof of observation 3.1.

Now, having the formula (86), we proceed as before. That is, we first look at the diagonal elements of it and solve the resulting equations. Then, we consider the off-diagonal elements of Eq. (86) to have full characterization of F_{ij}. As for the diagonal part of Eq. (86) we establish the following observation.

Observation 3.2. *The following conditions hold true*

$$\sum_{\substack{j=0\\ j\neq i}}^{d-1} \left(\frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}} \right) F_{ij} F_{ij}^{\dagger} = \frac{4k}{d^2} \mathbb{1}_{\mathrm{B}'}, \qquad k = 0, \ldots, d-1, \qquad i = 0, \ldots, d-1. \tag{92}$$

To prove the above relation let us consider the $|i\rangle\langle i|$ elements of (86) which, after some algebra, gives us the following relation

$$\sum_{\substack{l=0\\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{li} = k\omega^{ki} \left[2\omega^{\frac{1}{2}} F_{ii} - \omega^{-i} F_{ii}^2 - \omega^{i+1} \mathbb{1}_{\mathrm{B}'} \right], \tag{93}$$

which after substituting F_{ii} from Eq. (82) into it simplifies to

$$\sum_{\substack{l=0\\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il} F_{li} = -\frac{4k}{d^2} \omega^{i(k+1)+1} \mathbb{1}_{\mathrm{B}'}. \tag{94}$$

This after some manipulations can further be rewritten as

$$\sum_{\substack{l=0\\ l\neq i}}^{d-1} \left(\frac{1-\omega^{k(l-i)}}{1-\omega^{i-l}} \right) F_{il} F_{li} \omega^{-(i+l+1)} = \frac{4k}{d^2} \mathbb{1}_{\mathrm{B}'}, \tag{95}$$

and after taking into account (85) and changing the index l to j, we obtain the desired relation (92).

The subsequent observation provides the solution of equations (92).

Observation 3.3. *The solution of* (92) *is given by*

$$F_{ij} F_{ij}^{\dagger} = \frac{4}{d^2} \mathbb{1}_{\mathrm{B}'}, \qquad i \neq j. \tag{96}$$

We multiply Eq. (92) by ω^{kn} with $k=0,\ldots,d-1$ and $n=1,\ldots,d-1$ and then sum the resulting identity over all k's, which leads us to

$$-\sum_{\substack{j=0\\j\neq i}}^{d-1}\frac{1}{1-\omega^{i-j}}F_{ij}F_{ij}^{\dagger}\sum_{k=0}^{d-1}\omega^{k(j-i+n)}=\frac{4}{d^2}\mathbb{1}_{\mathrm{B}'}\sum_{k=0}^{d-1}k\omega^{kn}, \tag{97}$$

where we have exploited the fact that for any $n=1,\ldots,d-1$,

$$\sum_{k=0}^{d-1}\omega^{kn}=0. \tag{98}$$

Applying then Eq. (116) to the right-hand side of Eq. (97) and the fact that

$$\sum_{k=0}^{d-1}\omega^{k(j-i+n)}=\delta_{j,i-n \mod d} \tag{99}$$

to its left-hand side we can bring it to

$$F_{i(i-n \mod d)}F_{i(i-n \mod d)}^{\dagger}=\frac{4}{d^2}\mathbb{1}_{\mathrm{B}'}. \tag{100}$$

To complete the proof it suffices to realize that for any $i=0,\ldots,d-1$ there exist $n=1,\ldots,d-1$ such that $i-n$ mod d is any number from $\{0,\ldots,d-1\}$ different than i.

The relation (96) is unfortunately not sufficient to fully characterize F_{ij}. However, we can find a unitary operation U that preserves B_1 and allows us to obtain an explicit form of a few matrices F_{ij} from Eq. (96).

To be more precise, let us consider a unitary matrix U acting on $\mathbb{C}^d\otimes\mathcal{H}_{\mathrm{B}'}$ of the form

$$U=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes U_i, \tag{101}$$

where

$$U_0=\mathbb{1}_{\mathrm{B}'},\qquad U_i=\frac{d}{2}\omega^{-\frac{i+1}{2}}F_{0i},\qquad i=1,\ldots,d-1. \tag{102}$$

We can readily check that $UB_1U^{\dagger}=B_1$. Let us then denote

$$UB_2U^{\dagger}=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes U_iF_{ij}U_j^{\dagger}:=\sum_{i,j=0}^{d-1}|i\rangle\langle j|\otimes\tilde{F}_{ij}. \tag{103}$$

Note that, all the algebraic relations for F_{ij} obtained so far hold also for $\tilde{F}_{ij}$, and $\tilde{F}_{ii}=F_{ii}$.

Now, we see that

$$\tilde{F}_{0j}=U_0F_{0j}U_j^{\dagger}=\frac{d}{2}\omega^{\frac{j+1}{2}}F_{0j}F_{0j}^{\dagger}=\frac{2}{d}\omega^{\frac{j+1}{2}}\mathbb{1}_{\mathrm{B}'}, \tag{104}$$

where to obtain the last equality we employed Eq. (96). Using Eq. (85) we then obtain $\tilde{F}_{j0}$.

Thus, the remaining part of the proof of Lemma 3 is to obtain the elements F_{ij} such that $i,j\neq 0$ and $i\neq j$. To do so, we use the off-diagonal elements of (92) to obtain a set of relations as follows.

Observation 3.4. *The following conditions hold true*

$$\sum_{\substack{i=1\\i\neq j}}^{d-1}\frac{1-\omega^{ki}}{1-\omega^{i}}\omega^{i/2}F_{ij}=\frac{2}{d}\omega^{\frac{j+1}{2}}\left(k+\frac{1-\omega^{kj}}{1-\omega^{j}}\omega^{j}\right),\qquad k=1,\ldots,d-1,\qquad j=1,\ldots,d-1. \tag{105}$$

Taking the inner product with $\langle i| \,.\, |j\rangle$ (where $i \neq j$) on the both side of (86) we obtain

$$-(k-1)\omega^{ki}F_{ij} + \omega^{-\frac{1}{2}} \sum_{\substack{l=0\\ l\neq i}}^{d-1} \left(\frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} \right) F_{il}F_{lj} + k\omega^{(k-1)i}\omega^{-\frac{1}{2}} F_{ii}F_{ij} = \frac{\omega^{(k+1)i} - \omega^{(k+1)j}}{\omega^i - \omega^j} F_{ij}. \tag{106}$$

After rearranging some terms and using the formula for F_{ii} given above, we express the above equation as

$$\sum_{\substack{l=0\\ l\neq i}}^{d-1} \frac{\omega^{ki} - \omega^{kl}}{\omega^i - \omega^l} F_{il}F_{lj} = \omega^{\frac{1}{2}} \left[\frac{\omega^{(k+1)i} - \omega^{(k+1)j}}{\omega^i - \omega^j} + \left(\frac{2k}{d} - 1 \right) \omega^{ki} \right] F_{ij}. \tag{107}$$

Next, we set $i = 0$ and obtain

$$\sum_{l=1}^{d-1} \frac{1 - \omega^{kl}}{1 - \omega^l} F_{0l}F_{lj} = \omega^{\frac{1}{2}} \left(\frac{1 - \omega^{(k+1)j}}{1 - \omega^j} + \frac{2k}{d} - 1 \right) F_{0j} \tag{108}$$

and then substitute $\tilde{F}_{0j}$ from (104) which gives

$$\sum_{l=1}^{d-1} \frac{1 - \omega^{kl}}{1 - \omega^l} \omega^{\frac{l+1}{2}} F_{lj} = \omega^{\frac{j}{2}+1} \left(\frac{1 - \omega^{(k+1)j}}{1 - \omega^j} + \frac{2k}{d} - 1 \right) \mathbb{1}_{B'}. \tag{109}$$

Let us then take the term corresponding to $l = j$ out of the sum and use Eq. (82) to express F_{jj}. This after some simplifications allows us to rewrite Eq. (109) as

$$\sum_{\substack{l=1\\ l\neq j}}^{d-1} \left(\frac{1 - \omega^{kl}}{1 - \omega^l} \right) \omega^{\frac{l}{2}} F_{lj} = \frac{2}{d} \omega^{\frac{j+1}{2}} \left(k + \frac{1 - \omega^{kj}}{1 - \omega^j} \omega^j \right) \mathbb{1}_{B'}. \tag{110}$$

Finally, changing the index l to i leads us to (105). Note that the equations derived for F_{ij} are also valid for $\tilde{F}_{ij}$, and $\tilde{F}_{ii} = F_{ii}$.

The following observation provides the solution of (105).

Observation 3.5. *The solution of the equation* (105) *is*

$$F_{ij} = -\frac{2}{d} \omega^{\frac{i+j+1}{2}} \mathbb{1}_{B'}, \qquad i,j = 1,\ldots,d-1, \quad i \neq j. \tag{111}$$

We multiply Eq. (105) by ω^{-kn} with $n \in \{1,\ldots,d-1\}$ such that $n \neq j$ and then sum both sides of the resulting formula over $k = 0,\ldots,d-1$, obtaining

$$\sum_{\substack{i=1\\ i\neq j}}^{d-1} \frac{\omega^{i/2}}{1 - \omega^i} F_{ij} \sum_{k=0}^{d-1} \left(\omega^{-kn} - \omega^{k(i-n)} \right) = \frac{2}{d} \omega^{\frac{j+1}{2}} \left[\sum_{k=0}^{d-1} k\omega^{-kn} + \frac{\omega^{j/2}}{1 - \omega^j} \sum_{k=0}^{d-1} \left(\omega^{-kn} - \omega^{k(j-n)} \right) \right] \mathbb{1}_{B'}. \tag{112}$$

We now notice that the first sum on the left-hand side of the above and the last two sums on the right-hand side simply vanish due to Eq. (98) and the fact that $n \neq j$. Exploiting then Eq. (117) as well as the fact that

$$\sum_{k=0}^{d-1} \omega^{k(n-i)} = d\delta_{n,i} \tag{113}$$

holds true for any $x, y \in \{0,\ldots,d-1\}$, we obtain

$$-d \frac{\omega^{n/2}}{1 - \omega^n} F_{nj} = \frac{2}{d} \omega^{\frac{j+1}{2}} \left(\frac{d}{\omega^{-n} - 1} \right) \mathbb{1}_{B'}, \tag{114}$$

which after some manipulations leads us to (111). Finally, taking into account Eqs. (77), (82) and (111) we conclude that

$$UB_2U^\dagger = T_d \otimes \mathbb{1}_{B'} \tag{115}$$

with T_d given by Eq. (7). □

Fact 1. *The following identities hold*

$$\sum_{\substack{j=0\\j\neq i}}^{d-1}\frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}}=k,\qquad k=1,\ldots,d-1,\qquad i=0,\ldots,d-1, \tag{116}$$

and

$$\sum_{k=0}^{d-1}k\omega^{kn}=\frac{d}{\omega^{n}-1},\qquad n=1,\ldots,d-1. \tag{117}$$

Proof. To prove the first relation (116) we first notice that its left-hand side can be rewritten as

$$\sum_{\substack{j=0\\j\neq i}}^{d-1}\frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}}=-\sum_{\substack{j=0\\j\neq i}}^{d-1}\omega^{j-i}\frac{1-\omega^{k(j-i)}}{1-\omega^{j-i}}. \tag{118}$$

Observing then that the expression appearing on the right-hand side under the sum is actually a sum of a geometric series, one can rewrite the above equation as

$$\sum_{\substack{j=0\\j\neq i}}^{d-1}\frac{1-\omega^{k(j-i)}}{1-\omega^{i-j}}=-\sum_{\substack{j=0\\j\neq i}}^{d-1}\left(\omega^{j-i}+\omega^{2(j-i)}+\ldots+\omega^{k(j-i)}\right)=-\sum_{n=1}^{k}\omega^{-ni}\sum_{\substack{j=0\\j\neq i}}^{d-1}\omega^{nj}. \tag{119}$$

Let us finally notice that for any $n=1,\ldots,d-1$ one has the following chain of equalities

$$\sum_{\substack{j=0\\j\neq i}}^{d-1}\omega^{nj}=\sum_{j=0}^{d-1}\omega^{nj}-\omega^{ni}=-\omega^{ni}. \tag{120}$$

After plugging this last formula into Eq. (120) we arrive at Eq. (116).

To show the second identity we use the following relation

$$\sum_{k=0}^{d-1}x^{k}=\frac{1-x^{d}}{1-x}. \tag{121}$$

Taking the derivative and multiplying by x on both sides, we get

$$\sum_{k=0}^{d-1}kx^{k}=x\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{1-x^{d}}{1-x}\right)=\frac{-dx^{d}}{1-x}+\frac{x(1-x^{d})}{(1-x)^{2}}\,. \tag{122}$$

Substituting $x=\omega^{n}$ and using the fact that $\omega^{d}=1$ we obtain (117). □

Unitary equivalence to CGLMP measurements

Let us first define the d-dimensional CGLMP measurements as

$$A'_{k}=\sum_{r=0}^{d-1}\omega^{r}|r\rangle\langle r|_{A_k},\qquad B'_{k}=\sum_{r=0}^{d-1}\omega^{r}|r\rangle\langle r|_{B_k} \tag{123}$$

with $k=1,2$, where the eigenvectors are defined as

$$|r\rangle_{A_k}=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\omega^{(r-\alpha_k)q}|q\rangle,\qquad |r\rangle_{B_k}=\frac{1}{\sqrt{d}}\sum_{q=0}^{d-1}\omega^{-(r-\beta_k)q}|q\rangle, \tag{124}$$

where $\alpha_k=(k-1/2)/2$ and $\beta_k=k/2$ [1].

Fact 2. *There exist unitary operators $W_1, W_2 : \mathbb{C}^d \to \mathbb{C}^d$ that transform Z_d, T_d (7) to the d-dimensional CGLMP measurements in the following way: $A_1' = W_1 Z_d W_1^\dagger, A_2' = W_1 T_d W_1^\dagger$ and $B_1' = W_2 Z_d W_2^\dagger, B_2' = W_2 T_d W_2^\dagger$.*

Proof. We know that the following spectral decomposition holds, $Z_d = \sum_{q=0}^{d-1} \omega^q |q\rangle\langle q|$, and $T_d = \sum_{r=0}^{d-1} \omega^r |r\rangle\langle r|_{T_d}$ where

$$|r\rangle_{T_d} = \frac{2}{d} \sum_{q=0}^{d-1} (-1)^{\delta_{q,0}} \frac{\omega^{-\frac{q}{2}}}{1 - \omega^{\left(r-q-\frac{1}{2}\right)}} |q\rangle. \tag{125}$$

For clarity, we verify the spectral decomposition of T_d,

$$\begin{aligned} T_d |r\rangle_{T_d} &= \left(\sum_{i=0}^{d-1} \omega^{i+\frac{1}{2}} |i\rangle\langle i| - \frac{2}{d} \sum_{i,j=0}^{d-1} (-1)^{\delta_{i,0}+\delta_{j,0}} \omega^{\frac{i+j+1}{2}} |i\rangle\langle j| \right) \left(\frac{2}{d} \sum_{q=0}^{d-1} (-1)^{\delta_{q,0}} \frac{\omega^{\frac{-q}{2}}}{1-\omega^{r-q-\frac{1}{2}}} |q\rangle \right) \\ &= \frac{2}{d} \sum_{q=0}^{d-1} (-1)^{\delta_{q,0}} \omega^{\frac{q+1}{2}} \left(\frac{1}{1-\omega^{r-q-\frac{1}{2}}} - \frac{2}{d} \sum_{k=0}^{d-1} \frac{1}{1-\omega^{r-k-\frac{1}{2}}} \right) |q\rangle. \end{aligned} \tag{126}$$

Using the relation

$$\sum_{l=0}^{d-1} \omega^{(r-k-\frac{1}{2})l} = \frac{2}{1-\omega^{r-k-\frac{1}{2}}}, \tag{127}$$

we evaluate the sum

$$\sum_{k=0}^{d-1} \frac{1}{1-\omega^{r-k-\frac{1}{2}}} = \frac{1}{2} \sum_{l=0}^{d-1} \left(\sum_{k=0}^{d-1} \omega^{(r-k-\frac{1}{2})l} \right). \tag{128}$$

The above sum is nonzero iff $l = 0$, which gives

$$\sum_{k=0}^{d-1} \frac{1}{1-\omega^{r-k-\frac{1}{2}}} = \frac{d}{2}. \tag{129}$$

Substituting the above relation (129) in Eq. (126) and the replacing the form of $|r\rangle_{T_d}$ from (125), we get

$$\begin{aligned} T_d |r\rangle_{T_d} &= \frac{2}{d} \sum_{q=0}^{d-1} (-1)^{\delta_{q,0}} \omega^{\frac{q+1}{2}} \left(\frac{1}{1-\omega^{r-q-\frac{1}{2}}} - 1 \right) |q\rangle \\ &= \omega^r |r\rangle_{T_d}. \end{aligned} \tag{130}$$

Next we define the unitary operators W_1, W_2 as follows:

$$W_1 = M_1^\dagger F Y^\dagger, \qquad W_2 = S M_2^\dagger F Y^\dagger, \tag{131}$$

where

$$Y = \sum_{j=0}^{d-1} (-1)^{1-\delta_{j,0}} \omega^{\frac{d-j}{2}} |j\rangle\langle j|, \qquad S = \sum_{j=0}^{d-1} |j\rangle\langle d-1-j|, \tag{132}$$

and F, M_x $(x = 1,2)$ are explicitly given by

$$F = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} |i\rangle\langle j|, \qquad M_x = \sum_{j=0}^{d-1} \omega^{\frac{jx}{4}} |j\rangle\langle j|. \tag{133}$$

Here $\delta_{i,j}$ denotes the Kronecker delta, that is, $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ for $i \neq j$. To this fact it is sufficient to show that the proposed unitary transforms the eigenstates of one observable to the eigenstates of another observable up to a complex number. By expanding $W_1 = M_1^\dagger F Y^\dagger$ we obtain,

$$W_1 = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} (-1)^{1-\delta_{j,0}} \omega^{-\frac{i}{4}+ij+\frac{j}{2}} |i\rangle\langle j|, \tag{134}$$

and further

$$W_1^\dagger|r\rangle_{A_1} = \frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{1-\delta_{j,0}}\omega^{(r-j)q}\omega^{-\frac{j}{2}}|j\rangle. \tag{135}$$

The sum on the right-hand-side of the above equation would only exist if $r = j$ as $\sum_{k=0}^{d-1}\omega^{kn} = 0$ whenever n is a non-zero integer, and thus

$$W_1^\dagger|r\rangle_{A_1} = e^{\mathbb{i}\pi(1-\delta_{r,0}-\frac{r}{d})}|r\rangle. \tag{136}$$

Similarly, the expression

$$W_1^\dagger|r\rangle_{A_2} = \frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{1-\delta_{j,0}}\omega^{(r-j-\frac{1}{2})q}\omega^{-\frac{j}{2}}|j\rangle. \tag{137}$$

Carrying the above sum over q and using the fact that $\omega^{\frac{dn}{2}} = -1$ for any non-negative odd integer n, with the aid of (125) we get

$$W_1^\dagger|r\rangle_{A_2} = -|r\rangle_{T_d}. \tag{138}$$

Similarly, for Bob's observables B_k', expansion of $W_2 = SM_2^\dagger FY^\dagger$ leads to

$$W_2 = \frac{1}{\sqrt{d}}\sum_{i,j=0}^{d-1}(-1)^{1-\delta_{j,0}}\omega^{-\frac{i}{2}+ij+\frac{j}{2}}|d-1-i\rangle\langle j|, \tag{139}$$

and further

$$W_2^\dagger|r\rangle_{B_1} = \frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{1-\delta_{j,0}}\omega^{(j-r)q+(d-1)(\frac{1}{2}-j)-\frac{j}{2}}|j\rangle. \tag{140}$$

The sum on the right-hand-side of the above equation would only exist if $r = j$ as $\sum_{k=0}^{d-1}\omega^{kn} = 0$ whenever n is a non-zero integer, and thus

$$W_2^\dagger|r\rangle_{B_1} = e^{\mathbb{i}\pi(2-\frac{r-1}{d}-\delta_{r,0})}|r\rangle. \tag{141}$$

While, the following expression

$$W_2^\dagger|r\rangle_{B_2} = \frac{1}{d}\sum_{j,q=0}^{d-1}(-1)^{1-\delta_{j,0}}\omega^{(j+\frac{1}{2}-r)q+(d-1)(\frac{1}{2}-j)-\frac{j}{2}}|j\rangle, \tag{142}$$

which after carrying the sum over q and using (125) simplifies to

$$W_2^\dagger|r\rangle_{B_2} = -\omega^{r-1}|r\rangle_{T_d}. \tag{143}$$

Altogether, Eqs. (136), (138), (141), and (143) complete the proof. □

Fact 3. *There exists a unitary operator $W_{\mathrm{A}} : \mathbb{C}^d \to \mathbb{C}^d$ such that*

$$W_{\mathrm{A}}Z_dW_{\mathrm{A}}^\dagger = a_1^*Z_d + 2(a_1^*)^3T_d, \quad W_{\mathrm{A}}T_dW_{\mathrm{A}}^\dagger = a_1Z_d - a_1^*T_d. \tag{144}$$

Proof. Due to the fact that the CGLMP measurements together with the maximally entangled state $|\phi_d^+\rangle$ yield the maximum violation of SATWAP Bell inequality [2], the following relations hold true,

$$(B_1')^* = a_1^*(A_1')^\dagger + a_1(A_2')^\dagger, \qquad (B_2')^* = a_1\omega^*(A_1')^\dagger + a_1^*(A_2')^\dagger. \tag{145}$$

Substituting the CGLMP measurements from Fact 2, we get

$$\begin{aligned}(W_2Z_dW_2^\dagger)^* &= a_1^*(W_1Z_dW_1^\dagger)^\dagger + a_1(W_1T_dW_1^\dagger)^\dagger,\\ (W_2T_dW_2^\dagger)^* &= a_1\omega^*(W_1Z_dW_1^\dagger)^\dagger + a_1^*(W_1T_dW_1^\dagger)^\dagger.\end{aligned} \tag{146}$$

Taking the transpose-conjugate on both sides, and then multiplying W_2^{T} and W_2^* from left end and right end, respectively, of the above equations, we further obtain

$$Z_d = a_1 W_{\mathrm{A}} Z_d W_{\mathrm{A}}^\dagger + a_1^* W_{\mathrm{A}} T_d W_{\mathrm{A}}^\dagger, \quad T_d = a_1^* \omega W_{\mathrm{A}} Z_d W_{\mathrm{A}}^\dagger + a_1 W_{\mathrm{A}} T_d W_{\mathrm{A}}^\dagger \tag{147}$$

where $W_{\mathrm{A}} = W_2^{\mathrm{T}} W_1$. Consequently, the above equations lead us to the desired relation (144). $\square$

[1] J. Barrett, A. Kent, and S. Pironio, Maximally Nonlocal and Monogamous Quantum Correlations, Phys. Rev. Lett. **97**, 170409 (2006).

[2] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Bell Inequalities Tailored to Maximally Entangled States, Phys. Rev. Lett. **119**, 040402 (2017).