Discrete realization of group symmetric LOCC-detection of maximally entangled state

Masahito Hayashi

Graduate School of Information Sciences, Tohoku University, Aoba-ku, Sendai, 980-8579, Japan

Group symmetric LOCC measurement for detecting maximally entangled state is considered. Usually, this type measurement has continuous-valued outcomes. However, any realizable measurement has finite-valued outcomes. This paper proposes discrete realizations of such a group symmetric LOCC measurement.

PACS numbers: 03.65.Wj, 03.65.Ud, 02.20.-a

I. INTRODUCTION

Testing of maximally entangled state is a useful method for guaranteeing the quality of generated maximally entangled states. However, if we require a group symmetric condition for this method, the optimal test often requires infinite-valued measurement. Since any realizable measurement has a finite number of outcomes, it is needed to discretize the optimal measurement.

Now, we focus on the bipartite system $H_d \otimes H_d$, in which, the party $A$ and $B$ have the computational bases $\{ |i\rangle_A \}_{i=0}^{d-1}$ and $\{ |i\rangle_B \}_{i=0}^{d-1}$, respectively. When our target is testing whether the generated state is sufficiently close to the maximal entangled state

$$|\phi_{AB}^0\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_B$$

under a group symmetric condition, the optimal test can be given by

$$T^{1,A-B}_{inv} := \int d|\varphi \rangle \langle \varphi | \varphi \rangle \nu (d\varphi)$$

$$= |\phi_{AB}^0\rangle \langle \phi_{AB}^0 | + \frac{1}{d+1} (I - |\phi_{AB}^0\rangle \langle \phi_{AB}^0 |),$$

where $\nu$ is the group invariant probability measure on the set of pure states, and $\varphi$ and $\overline{\varphi}$ are given as $\varphi = \sum_{i=0}^{d-1} \varphi |i\rangle_A$ and $\overline{\varphi} = \sum_{i=0}^{d-1} \overline{\varphi} |i\rangle_B$. This measurement can be realized by the following procedure. In the first step, the system $A$ performs the local system covariant measurement $\int d|\varphi \rangle \langle \varphi | \nu (d\varphi)$, and sends the system $B$ the outcome $\varphi$. In the second step, the system $B$ performs the two-valued measurement $\{ |\varphi \rangle \langle \varphi |, I - |\varphi \rangle \langle \varphi | \}$. When Bob obtains the event corresponding to $|\varphi \rangle \langle \varphi |$, we support the maximal entangled state $|\phi_{AB}^0\rangle$. This test can be written as the positive semi-definite matrix $T(M)$:

$$T(M) \overset{\text{def}}{=} \sum_{i} p_i |u_i \rangle \langle u_i | (u_i \otimes u_i).$$

Indeed, when the local dimension $d$ is 2, $\text{D'Ariano et al.}$ [1] and Hayashi et al. [2] obtained the discrete own-way LOCC realization of the test $T^{1,A-B}_{inv}$ as test $T(M)$ with an appropriate choice of the local measurement $M$. However, its general dimensional case was an open problem. In this paper, employing the concepts of symmetric informationally complete POVM (SIC-POVM) and mutually unbiased bases (MUB), we propose discrete own-way LOCC realizations of $T^{1,A-B}_{inv}$. Also, the optimality of the proposed realization scheme is shown.

Next, we consider the case when Alice’s system (Bob’s system) is given as $H_{A_1} \otimes H_{A_2}$, and the dimensions of all components coincide, i.e., $\dim H_{A_1} = \dim H_{A_2} = \dim H_{B_1} = \dim H_{B_2} = d$. In this case, we focus on the covariant POVM $M_{cov,u}$:

$$M_{cov,u}(d_1,d_2)$$

$$\overset{\text{def}}{=} \int d^{2}(g_1 \otimes g_2) |u \rangle \langle u | (g_1 \otimes g_2) \nu (d_1) \nu (d_2),$$

where the vector $u$ is a maximally entangled state and $\nu$ is the group invariant probability measure on SU($d$). The optimal test is given as the test $T^{2,A-B}_{inv} \overset{\text{def}}{=} T(M^2_{cov,u})$, which has the form [3]:

$$T^{2,A-B}_{inv}$$

$$= |\phi_{AB}^0\rangle \langle \phi_{AB}^0 | \otimes |\phi_{AB}^0\rangle \langle \phi_{AB}^0 | + \frac{1}{d^2 - 1} (I - |\phi_{AB}^0\rangle \langle \phi_{AB}^0 |) \otimes (I - |\phi_{AB}^0\rangle \langle \phi_{AB}^0 |).$$

Indeed, the positive semi-definite matrix $T^{2,A-B}_{inv}$ does not depend on the choice of the maximally entangled state $u$. In this paper, employing the concept of Clifford group, we provide a discrete own-way LOCC realization of $T^{2,A-B}_{inv}$ when the local system is given as a composite system of a prime-dimensional system. Also, the optimality of the proposed realization scheme is shown.

*Electronic address: hayashi@math.is.tohoku.ac.jp
II. DISCRETE OWN-WAY LOCC REALIZATION OF $T_{\text{inv}}^1 A \rightarrow B$

A. Realizing scheme by SIC-POVM

In order to design the test $T_{\text{inv}}^1 A \rightarrow B$, we focus on the concept "symmetric informationally complete POVM (SIC-POVM)". A rank-one POVM $\{p_i | u_i \rangle \langle u_i | \}$ on $\mathcal{H}_A = \mathbb{C}^d$ is called a symmetric informationally complete POVM (SIC-POVM), if it satisfies the following conditions:

$$\# \{i\} = d^2,$$
$$p_i = \frac{1}{d},$$
$$|\langle u_i | u_j \rangle|^2 = \frac{1}{d+1} \quad \text{for} \ i \neq j$$

(4)

Currently, an SIC-POVM analytically is constructed when the dimension $d$ is 2, 3, 4, 6, 7, 8, 9, 11, or 19. Also, its existence is numerically verified up to $d = 45$. As is shown in Appendix A, any SIC-POVM $M_{\text{sic}} = \{p_i | u_i \rangle \langle u_i | \}$ satisfies

$$T(M_{\text{sic}}) = T_{\text{inv}}^1 A \rightarrow B,$$

(5)

that is, the test $T_{\text{inv}}^1 A \rightarrow B$ can be realized by an SIC-POVM. Moreover, if a POVM $M = \{M_i \}$ on $\mathcal{H}_A$ satisfies

$$T(M) = T_{\text{inv}}^1 A \rightarrow B,$$

the inequality

$$\# \{i\} \geq d^2$$

holds. This is because the rank of the operator $T_{\text{inv}}^1 A \rightarrow B$ (which equal $d^2$) is less than the number of the elements of POVM $M_i$. Hence, we obtain

$$\min \{\# \{i\} | T(M_i) \} = T_{\text{inv}}^1 A \rightarrow B \} = d^2$$

(6)

if there exists an SIC-POVM on $\mathbb{C}^d$. That is, the proposed realizing scheme by SIC-POVM is optimal in the sense of (6).

B. Realizing scheme by MUB

However, any SIC-POVM is not a randomized combination of projection valued measures as well as a projection valued measure. Since a projection valued measure (PVM) are more realizable than other POVM, it is more desired to design Alice’s POVM as a randomized combination of PVMs. For this purpose, we focus on mutually unbiased bases. $d + 1$ orthonormal bases $\{B_1, \ldots, B_{d+1} \}$ are called mutually unbiased bases (MUB) if

$$|\langle u | v \rangle|^2 = \frac{1}{d}, \forall u \in B_i, \forall v \in B_j, i \neq j.$$

The existence of MUB is shown when $d$ is a prime or a prime power. Bandyopadhyay et al. gave a more explicit form in these cases. Any mutually unbiased bases $\{B_1, \ldots, B_{d+1} \}$ make the POVM $M_{B_1, \ldots, B_{d+1}}$, i.e.,

$$M_{B_1, \ldots, B_{d+1}} = \left\{ \frac{1}{d} | u_{i,j} \rangle \langle u_{i,j} | \right\}_{i,j},$$

where $B_j = \{u_{1,j}, \ldots, u_{d,j} \}$. This POVM always produces the desired test $T_{\text{inv}}^1 A \rightarrow B$ as

$$T(M_{B_1, \ldots, B_{d+1}}) = T_{\text{inv}}^1 A \rightarrow B,$$

(7)

which is shown in Appendix B. This construction of the test $T_{\text{inv}}^1 A \rightarrow B$ is optimal in the following sense. Let $\{M^j \}$ be the set of projection-valued measures. A randomized combination of $\{M^j \}$, i.e., $M = \sum_j p_j M_j$ satisfies

$$T(M) = T_{\text{inv}}^1 A \rightarrow B, $$

(8)

Then, as is proven in Appendix C

$$\# \{j\} \geq d + 1,$$

(9)

which implies the optimality of the POVM consisting of MUB. Hence,

$$\min_{M_j \in \text{VM}} \{\# \{j\} | T \left( \sum_j p_j M_j \right) = T_{\text{inv}}^1 A \rightarrow B \} = d + 1$$

(10)

if $d$ is a prime or a prime power. That is, the proposed realizing scheme by MUB is optimal in the sense of (10).

III. DISCRETE OWN-WAY LOCC REALIZATION OF $T_{\text{inv}}^2 A \rightarrow B$

Next, we proceed to the case when both local systems consist of two subsystems. Given a finite group $G$ and its projective representation $f$ on $\mathcal{H}_{A_1} = \mathbb{C}^d$, by regarding $\mathcal{H}_{A_2}$ as the dual space of $\mathcal{H}_{A_1}$, the matrix $f(g)$ can be regarded as an element $|f(g)|$ of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$.

Theorem 1 We assume the two conditions: (1) The representation $f$ is irreducible. (2) The action $f \otimes \check{f}$ of $G$ to $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ has only two irreducible components, i.e., the irreducible subspaces of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ for the action

$$v_1 \otimes v_2 \rightarrow f(g)v_1 \otimes \overline{f(g)}v_2$$

are only the one-dimensional space $\langle \phi_{A_1, A_2} \rangle$ and its orthogonal space $\langle \phi_{A_1, A_2} \rangle^\perp$. Then, the resolution $M_f = \left\{ \frac{d^2}{|G|} \left| \frac{1}{\sqrt{d}} f(g) \right\rangle \left\langle \frac{1}{\sqrt{d}} f(g) \right| \right\}_{g \in G}$ satisfies the condition for a POVM, and

$$T(M_f) = T_{\text{inv}}^2 A \rightarrow B.$$

(11)
Its proof is given in Appendix E. This theorem yields a discrete own-way LOCC realization of $T^2_{inv} A \rightarrow B$ from the representation $f$ satisfying the above two conditions.

For example, Clifford group satisfies this assumption. For readers’ convenience, we give its definition and prove that Clifford group satisfies this assumption. Clifford group $C(d)$ for $d$-dimensional system is given by

$$C(d) := \{U \in U(d) | U G P(d) U^\dagger = G P(d) \}$$

where $G P(d) := \{e^{i \sqrt{d} \xi} W(i, j) | \xi \in \mathbb{R}, i, j \in \mathbb{Z} \}$ and $I(d) := \{e^{i \sqrt{d} \xi} | \xi \in \mathbb{R} \}$, where $\omega$ is the $d$-th root of 1. As is shown in Appendix E the natural representation of the group $C(d)$ satisfies the conditions (1) and (2). Then, the natural projective representation of the group $C(d)/I(d)$ satisfies the conditions (1) (2). As is shown in Lemma 5 in Appleby [8], when $d$ is prime, the cardinality $|C(d)/I(d)|$ is $d^d(d^2-1)$. In the general case, $|C(d)/I(d)| = d^2 \left( \sum_{n=0}^{d-1} \nu(n, d) \nu(n+1, d) \right)$, where $\nu(n, d)$ is the number of distinct ordered pairs $(x, y) \in \mathbb{Z}_d^2$ such that $xy = n \pmod{d}$.

### IV. DISCUSSION

This paper has treated discretization of own-way LOCC protocols. Using the concepts of symmetric informationally complete POVM (SIC-POVM), mutually unbiased bases (MUB), and Clifford group, we have proposed discrete own-way LOCC realizations of $T^1_{inv} A \rightarrow B$ and $T^2_{inv} A \rightarrow B$. This result indicates the importance of these concept in discrete mathematics. Since the existence of SIC-POVM and MUB is proven in limited cases, we cannot construct a discrete own-way LOCC realization of $T^1_{inv} A \rightarrow B$ in the general case. Thus, further investigation for these concepts are required.

While the optimal test is given as $T^1_{inv} A \rightarrow B$ when the local system consists of three subsystems by Hayashi [8], its discretization has not been obtained. Since the optimal test $T^1_{inv} A \rightarrow B$ is closely related to GHZ state [8], its discretization may be related to GHZ state. Its construction remains as a future research.

Further, the optimal protocol is often given as a protocol with infinite elements in quantum information. In such a case, it is required to discretize this protocol. This kind of discretization is an interesting interdisciplinary topic between quantum information and discrete mathematics.

### Acknowledgment

This research was partially supported by a Grant-in-Aid for Scientific Research on Priority Area ‘Deepening and Expansion of Statistical Mechanical Informatics (DEX-SMI)’, No. 18079014 and a MEXT Grant-in-Aid for Young Scientists (A) No. 20686026.

### APPENDIX A: PROOF OF (5)

First, we show that $u_1 \otimes \bar{u}_1, \ldots, u_{d^2} \otimes \bar{u}_{d^2}$ are linearly independent. We choose complex numbers $a_1; \ldots, a_{d^2}$ such that

$$\sum_i a_i u_i \otimes \bar{u}_i = 0.$$ 

Taking trace, we have

$$a_1 + \sum_{i \neq 1} a_i = 0.$$ 

On the other hand, 

$$0 = \langle u_1 \otimes \bar{u}_1 | \sum_i a_i u_i \otimes \bar{u}_i \rangle = a_1 + \frac{1}{d+1} \sum_{i \neq 1} a_i.$$ 

Hence, we obtain $a_1 = 0$. Similarly, we can show $a_i = 0$, which implies the linear independence.

Since the dimension of $\mathcal{H}_A \otimes \mathcal{H}_B$ is $d^2$, any element of $\mathcal{H}_A \otimes \mathcal{H}_B$ can be expressed as

$$\sum_j a_j u_j \otimes \bar{u}_j.$$
we obtain
\[
\left\langle \sum_i a_i u_i \otimes u_i \right| T_{inv}^{A \rightarrow B} \left| \sum_j a_j u_j \otimes u_j \right\rangle = \left\langle \sum_i a_i u_i \otimes u_i \right| T(M_{sin}) \left| \sum_j a_j u_j \otimes u_j \right\rangle.
\]
\[
= \frac{d}{d+1} \left( \frac{1}{d+1} \left| \sum_k a_k \right|^2 + \frac{1}{d+1} \sum |a_k|^2 \right) + \frac{1}{d+1} \left( \frac{1}{d+1} \left| \sum_k a_k \right|^2 + \frac{1}{d+1} \sum |a_k|^2 \right) = \left\langle \sum_i a_i u_i \otimes u_i \right| T(M_{sin}) \left| \sum_j a_j u_j \otimes u_j \right\rangle.
\]
Therefore, we obtain (5).

**APPENDIX B: PROOF OF (7)**

We focus on the subspace \(< \phi_{A,B}^0 >^\perp \) orthogonal to \(\phi_{A,B}^0\). The subspace \(B_j^d = \{ u_{i,j} \otimes u_{i,j} - \frac{1}{d} \phi_{A,B}^0, \ldots, u_{d-1,j} \otimes u_{d-1,j} - \frac{1}{d} \phi_{A,B}^0 \}\) belongs to the subspace \(< \phi_{A,B}^0 >^\perp \), and its dimension is \(d - 1\). Since
\[
\langle u_{i,j} \otimes u_{i,j} - \frac{1}{d} \phi_{A,B}^0 | u_{i',j'} \otimes u_{i',j'} - \frac{1}{d} \phi_{A,B}^0 \rangle = 0, \quad j \neq j',
\]
(B1)

The spaces \(B_1^d, \ldots, B_{d+1}^d\) are orthogonal to each other. Since the dimension of the subspace \(< \phi_{A,B}^0 >^\perp \) is \(d^2 - 1\), the subspace \(< \phi_{A,B}^0 >^\perp \) is spanned by the spaces \(B_1^d, \ldots, B_{d+1}^d\). Therefore, any element of the space \(H_A \otimes H_B\) can be expressed as \(\sum_{j=1}^{d+1} \sum_{i=1}^{d} a_{i,j} u_{i,j} \otimes u_{i,j}\). In the following, we abbreviate the sum \(\sum_{j=1}^{d+1} \sum_{i=1}^{d} \) as \(\sum_{j,i}\).

We calculate
\[
\left\langle \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right| T(M_{B_1 \ldots B_{d+1}}) \left| \sum_{j',i'} a_{i',j'} u_{i',j'} \otimes u_{i',j'} \right\rangle
\]
\[
= \left\langle \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right| \left( \sum_{l,k} \frac{1}{d+1} |u_{k,l} \otimes u_{k,l}| |u_{k,l} \otimes u_{k,l}| \right) \left| \sum_{j',i'} a_{i',j'} u_{i',j'} \otimes u_{i',j'} \right\rangle
\]
\[
= \frac{1}{d+1} \sum_{j,i} \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i,j} u_{i,j} \otimes u_{i,j}| \right) \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i',j'} u_{i',j'} \otimes u_{i',j'}| \right)^2
\]
\[
\left. = \frac{1}{d+1} \sum_{j,i} \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i,j} u_{i,j} \otimes u_{i,j}| \right)^2 = \frac{1}{d+1} \sum_{j,i} \left| a_{i,j} \right|^2 \right. = \frac{1}{d+1} \sum_{j,i} \left| a_{i,j} \right|^2
\]
\[
= \frac{1}{d+1} \sum_{j,i} \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i,j} u_{i,j} \otimes u_{i,j}| \right) \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i',j'} u_{i',j'} \otimes u_{i',j'}| \right)^2
\]
\[
= \frac{1}{d+1} \sum_{j,i} \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i,j} u_{i,j} \otimes u_{i,j}| \right)^2 = \frac{1}{d+1} \sum_{j,i} \left| a_{i,j} \right|^2 \right.
\]
\[
\left. = \frac{1}{d+1} \sum_{j,i} \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i,j} u_{i,j} \otimes u_{i,j}| \right) \left( \frac{1}{d+1} \sum_{j',i'} \sum_{l,k} |a_{i',j'} u_{i',j'} \otimes u_{i',j'}| \right)^2
\]

On the other hand, its norm is calculated as
\[
\left\| \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right\| = \frac{1}{d+1} \sum_{j,i} \left| a_{i,j} \right|^2 = \frac{1}{d+1} \sum_{j,i} \left| a_{i,j} \right|^2
\]

Since
\[
\left\langle \phi_{A,B}^0 \left| \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right\rangle \right|^2 = \frac{1}{d^2} \left| a_{i,j} u_{i,j} \right|^2,
\]
we obtain
\[
\left\langle \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right| T_{inv}^{A \rightarrow B} \left| \sum_{j',i'} a_{i',j'} u_{i',j'} \otimes u_{i',j'} \right\rangle
\]
\[
= \left\langle \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right| \left( \frac{1}{d+1} \left| \phi_{A,B}^0 \right| \left| \phi_{A,B}^0 \right| + \frac{1}{d+1} I \right) \left| \sum_{j',i'} a_{i',j'} u_{i',j'} \otimes u_{i',j'} \right\rangle
\]
\[
= \left\langle \sum_{j,i} a_{i,j} u_{i,j} \otimes u_{i,j} \right| T(M_{B_1 \ldots B_{d+1}}) \left| \sum_{j',i'} a_{i',j'} u_{i',j'} \otimes u_{i',j'} \right\rangle.
\]

Therefore, we obtain (7).
APPENDIX C: PROOF OF (9)

Let $M^2 = \{ |u_{i,j}\rangle \langle u_{i,j}| \}$. We focus on the projection $P$ to the subspace $\langle \phi_{A,B}^{\emptyset} \rangle^\perp$ orthogonal to $\phi_{A,B}^0$ and the subspace $B_j^\emptyset = \langle u_{1,j} \otimes u_{1,j} \rangle \cdots \langle u_{d,j} \otimes u_{d,j} \rangle$. The image $PB_j^\emptyset$ is $\langle u_{1,j} \otimes u_{1,j} \rangle \cdots \langle u_{d,j} \otimes u_{d-j} - \phi_{A,B}^0 \rangle$. The condition (8) implies that the sum of the rank of the space $PB_j^\emptyset$ is greater than $d^2 - 1$, i.e., the dimension of the space $\langle \phi_{A,B}^0 \rangle^\perp$. Thus, #\{j\}$(d-1) \geq d^2 - 1$, which implies the inequality (9).

APPENDIX D: PROOF OF THEOREM 4

First, we prove that $M_f$ satisfies the condition for POVM. The irreducibility of the action $f$ guarantees that

$$
\frac{d^2}{|G|} \sum_{g \in G} \left| \langle f(g) | l' \rangle \langle f(g) | k' \rangle \right|^2 = \langle f(g) | \left( \sum_{k,l} a_{k,l} | k \rangle \otimes | l \rangle \right) | f(g) \rangle
$$

we obtain

$$
\frac{d^2}{|G|} \sum_{g \in G} \left| \sum_{k,l} a_{k,l} | k \rangle \otimes | l \rangle \right|^2
= \frac{d^2}{|G|} \sum_{g \in G} \sum_{k,l,k',l'} a_{k,l} \overline{a}_{k',l'} | \langle k | f(g) | l' \rangle \langle f(g) | k' \rangle |
= \sum_{k,l} a_{k,l} \overline{a}_{k,l},
$$
which implies

$$
\frac{d^2}{|G|} \sum_{g \in G} \left| \langle f(g) | l' \rangle \langle f(g) | k' \rangle \right|^2
= \left| \langle f(g) | (\sum_{k,l} a_{k,l} | k \rangle \otimes | l \rangle) | f(g) \rangle \right|^2.
$$

Hence, $M_f = \left\{ \frac{d^2}{|G|} \left| \langle f(g) | l' \rangle \langle f(g) | k' \rangle \right|^2 \right\}_{g \in G}$ is a POVM.

Next, we show (11). We focus on the action of the group $G \times G$ to the total space $H_{A_1} \otimes H_{A_2} \otimes H_{B_1} \otimes H_{B_2}$ as

$$
u_1 \otimes \nu_2 \otimes v_1 \otimes v_2
\rightarrow f(g_1) |u_1 \otimes f(g_2) |u_2 \otimes f(g_1) |v_1 \otimes f(g_2) |v_2
$$
for $u_i \in H_{A_i}$, $v_i \in H_{B_i}$, and any pair $(g_1, g_2) \in G \times G$. Due to the condition (2), the irreducible decomposition of the space $H_{A_1} \otimes H_{A_2} \otimes H_{B_1} \otimes H_{B_2}$ is given as

$$
\langle \phi_{A,B}^\emptyset \rangle \otimes \langle \phi_{A,B}^\emptyset \rangle \otimes \langle \phi_{A,B}^\emptyset \rangle \otimes \langle \phi_{A,B}^\emptyset \rangle \oplus \langle \phi_{A,B}^\emptyset \rangle \otimes \langle \phi_{A,B}^\emptyset \rangle \otimes \langle \phi_{A,B}^\emptyset \rangle \otimes \langle \phi_{A,B}^\emptyset \rangle
$$

As is checked below, the test $T(M_f)$ is invariant for this action:

$$
f(g_1) \otimes f(g_2) \otimes f(g_1) \otimes f(g_2) T(M_f) \left( f(g_1) \otimes f(g_2) \otimes f(g_1) \otimes f(g_2) \right)^\dagger
= \frac{d^2}{|G|} \sum_{g \in G} \left| \frac{1}{d} f(g_1) |f(g)| f(g_2) \right|^2 \otimes \left| \frac{1}{d} f(g_1) |f(g)| f(g_2) \right|^2
$$

where we denote $g_1 g_2^{-1}$ by $g'$. Hence, the test $T(M_f)$ has the form

$$
T(M_f) = a |\phi_{A_1,B_1}^0 \rangle \langle \phi_{A_1,B_1}^0 | \otimes |\phi_{A_2,B_2}^0 \rangle \langle \phi_{A_2,B_2}^0 | + b(I - |\phi_{A_1,B_1}^0 \rangle \langle \phi_{A_1,B_1}^0 |) \otimes |\phi_{A_2,B_2}^0 \rangle \langle \phi_{A_2,B_2}^0 | + c |\phi_{A_1,B_1}^0 \rangle \langle \phi_{A_1,B_1}^0 | \otimes (I - |\phi_{A_2,B_2}^0 \rangle \langle \phi_{A_2,B_2}^0 |)
+ d(I - |\phi_{A_1,B_1}^0 \rangle \langle \phi_{A_1,B_1}^0 |) \otimes (I - |\phi_{A_2,B_2}^0 \rangle \langle \phi_{A_2,B_2}^0 |).
Since $f(g)$ is the unitary matrix, $\frac{1}{\sqrt{d}}f(g)$ is a maximally entangled state on $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Since $\frac{1}{\sqrt{d}}f(g)$ is maximally entangled, Lemma 5 in Hayashi \cite{3} yields that

$$T(M_f) = |\phi_{A_1, B_1}^0 \otimes \phi_{A_2, B_2}^0 \rangle \langle \phi_{A_1, B_1}^0 \otimes \phi_{A_2, B_2}^0 | + PT(M_f)P,$$

(D1)

where

$$P \overset{\text{def}}{=} (I - |\phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |) \otimes (I - |\phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 |).$$

This relation implies that $b = c = 0$. Thus, the relation $\text{Tr} T(M_f) = d^2$ yields

$$T(M_f) = |\phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 | \otimes |\phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |$$

$$+ \frac{1}{d^2 - 1}(I - |\phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 |) \otimes (I - |\phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |),$$

which implies \ref{11}.

**APPENDIX E: PROOF OF IRREDUCIBILITY**

It is known that the natural representation of the subgroup $\text{GP}(d) \subset C(d)$ satisfies the condition (1). Hence, it is sufficient to show the condition (2). The irreducible spaces of the subgroup $\text{GP}(d) \subset C(d)$ are $d^2$ one-dimensional subspaces generated by $|W(i, j)\rangle$ for $i, j$. The representation of $\text{GP}(d)$ on each irreducible subspaces is different. Thus, the irreducible subspaces of the larger group $C(d)$ should be represented as the direct sum of these subspaces. As is shown in Lemma 1 in Appleby \cite{3}, for any $(i, j)$ and any $F \in \text{SL}(2, \mathbb{Z}/d)$, there exists an element $U \in C(d)$ such that $f(U) \otimes g(U)|W(i, j)\rangle = e^{\frac{i\pi}{2d}}\theta_{i,j,F} |W(F(i, j))\rangle$, where

$$\theta := \begin{cases} \frac{d}{2} & \text{if } d \text{ is odd} \\ 2d & \text{if } d \text{ is even}. \end{cases}$$

For any pair $(i, j) \neq (0, 0)$, there exists an element $F \in \text{SL}(2, \mathbb{Z}/d)$ such that $(i, j) = F(1, 0)$. Since any irreducible subspace should be spanned by the subset of $\{ |W(i, j)\rangle \}_{i,j}$, the space spanned by $\{ |W(i, j)\rangle \}_{(i,j)\neq(0,0)}$ is irreducible. Thus, the condition (2) holds.

\[\text{References}\]

[1] G. M. D’Ariano, C. Macchiavello, and M. G. A. Paris, “Local observables for entanglement witnesses,” *Phys. Rev. A* 67 042310, 2003.

[2] M. Hayashi, K. Matsumoto, and Y. Tsuda, “A study of LOCC-detection of a maximally entangled state using hypothesis testing,” *J. Phys. A: Math. and Gen.*, 39 14427-14446 (2006).

[3] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled state using hypothesis testing, arXiv:0810.3380

[4] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, “Symmetric Informationally Complete Quantum Measurements,” *J. Math. Phys.*, 45, 2171-2180 (2004); quant-ph/0310075

[5] A. Koldobsky and H. König, “Aspects of the Isometric Theory of Banach Spaces,” in *Handbook of Geometry of Banach Spaces*, Vol. 1, edited by W. B. Johnson and J. Lindenstrauss (North-Holland, Dordrecht, 2001), pp.899-939.

[6] Grassl, M., “On SIC-POVMs and MUBs in dimension 6,” *Proceedings of EQIS’04*, pp. 60-61, (2004); quant-ph/0406175

[7] Zauner, G., “Quantum designs—foundations of a non-commutative theory of designs,” (in German), Ph.D. thesis, University of Vienna, (1999).

[8] Appleby, D M, “SIC-POVMs and the Extended Clifford Group,” *J. Math. Phys.*, 46, 052107 (2005).

[9] I. D. Ivanovic, “Geometrical description of quantum state determination,” *J. Phys. A: Math. and Gen.*, 14, No. 12, 3241-3245, (1981).

[10] W. K. Wootters and B. D. Fields, “Optimal state-determination by mutually unbiased measurements,” *Annals of Physics*, 191, No. 2, 363-381, (1989).

[11] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, “A New Proof for the Existence of Mutually Unbiased Bases,” *Algorithmica*, 34 (2002), pp. 512-528; quant-ph/0103162