<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>タイトル</td>
<td>ホイポテシステストに対する最大化結合状態（統計推論の記録及び関連統計）</td>
</tr>
<tr>
<td>著者</td>
<td>Hayashi, Masahito</td>
</tr>
<tr>
<td>引用</td>
<td>数理解析研究所講究録 数理解析研究所講究録</td>
</tr>
<tr>
<td>発行日</td>
<td>2005-07</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/47516">http://hdl.handle.net/2433/47516</a></td>
</tr>
<tr>
<td>種別</td>
<td>部門別論文</td>
</tr>
<tr>
<td>テキストバージョン</td>
<td>出版者</td>
</tr>
</tbody>
</table>

京都大学
Hypotheses testing for maximally entangled state

Masahito Hayashi

1Quantum Computation and Information Project, ERATO, JST
5-88-3, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan
Superrobust Computation Project, Information Science and Technology Strategic Core (21st Century COE by MEXT)
Graduate School of Information Science and Technology, The University of Tokyo
7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

In the asymptotic setting, the optimal test for hypotheses testing of the maximally entangled state is derived under several locality conditions for measurements. The optimal test is obtained in several special cases with finite samples. In addition, the experimental scheme for the optimal test is presented.

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

I. INTRODUCTION

Recently various quantum information processing are proposed, and many of them require maximally entangled states as resources[6, 7, 9]. Hence, it is often desired to generate maximally entangled states experimentally. In particular, it must be based on statistical method to decide whether the state generated experimentally is really the required maximally entangled state.

Now, entanglement witness is often used as its standard method [14, 19]. It is, however, not necessarily the optimal method from a viewpoint of statistics. On the other hand, in mathematical statistics, the decision problem of the truth of the given hypothesis is called statistical hypothesis testing, and is systematically studied. Hence, it is desired to treat, under the frame of statistical hypotheses testing, the problem deciding whether the given quantum state is the required maximally entangled state. In statistical hypotheses testing, we suppose two hypotheses (null hypothesis and alternative hypothesis) to be tested a priori, and assume that one of both is true. Based on observed data, we decide which hypothesis is true. Most preceding studies about quantum hypotheses testing concerned only quantum Neymann Pearson lemma [3, 12] and quantum Stein's lemma[11, 13, 20], except Tsuda et al. [1]. In these settings, they treated the case when both of the null and the alternative hypotheses consist of a single quantum state, i.e., they are simple.

However, in our issue, it is unnatural to specify both hypotheses with one quantum state. Hence, we cannot directly apply quantum Neymann Pearson theorem and quantum Stein's lemma, and we have to treat composite hypotheses, i.e., the case where both hypotheses consist of multiple quantum states. It is also required to restrict our measurements for testing among measurements based on LOCC (local operations and classical communications) because the tested state is maximally entangled state.

Recently, based on quantum statistical inference[3, 4, 12], Tsuda et al.[1] discussed this testing problem under statistical hypotheses testing. They treated testing problem where the null hypothesis consists only of the required maximally entangled state. Especially, they studied the optimal test and the existence of the uniformly optimal test (whose definition will be presented later) when one or two samples of the state to be tested are given. Their analysis mainly concentrated the two-dimensional case.

In this paper, we treat the null hypothesis consisting of quantum states whose fidelity for the desired maximally entangled state is less than \( \epsilon \), and discuss this testing problem with several given samples of the tested state in the following three setting concerning the range of our measurements. M1: All measurements are allowed. M2: Only classical communications are allowed as our operations between two distinct parties, but any operations among samples are available. M3: As well as measuring apparatus with quantum correlation between two distinct parties, those with quantum correlation among local samples are forbidden. The restriction M3 for measurement is discussed by Virmani and Plenio [21], the first time. Tsuda et al.[1] treated the settings M2 and M3, more systematically.

This paper mainly treats the case of sufficiently many samples, i.e., first order asymptotic theory. As a result, we find that there is no difference in performances of both settings M1 and M2. Especially, the test achieving the asymptotical optimal performance can be realized by quantum measurement with quantum correlations between only two local samples. That is, even if we use any higher quantum correlations among local samples, no further improvement is available under the first order asymptotic frame work. In the two-dimensional case, the required measurement with local quantum correlations is the four-valued Bell measurement between the local two samples. In the setting M3, we treat the null hypothesis consisting only of the maximally entangled state. Then, it is proved that even if we use classical correlation between local samples for deciding local measurement, there is no further improvement. That is, it
II. MATHEMATICAL FORMULATION OF QUANTUM HYPOTHESIS TESTING

Let $\mathcal{H}$ be a finite-dimensional Hilbert space corresponding to the physical system of interest. Then, the state is described by a density matrix on $\mathcal{H}$. In the quantum hypothesis testing, we assume that the current state $\rho$ of the system is unknown, but is known to belong to a subset $S_0$ or $S_1$ of the set of densities. Hence, our task is to test

$$H_0 : \rho \in S_0 \text{ versus } H_1 : \rho \in S_1$$

based on an appropriate measurement on $\mathcal{H}$. That is, we are required to decide which hypothesis is true. We call $H_0$ a null hypothesis, and we call $H_1$ an alternative hypothesis.

A test for the hypothesis (1) is given by a Positive Operator Valued Measure (POVM) $\{T_0, T_1\}$ on $\mathcal{H}$ composed of two elements, where $T_0 + T_1 = I$. For simplicity, the test $\{T_0, T_1\}$ is described by the operator $T = T_0$. Our decision should be done based on this test as follows: We accept $H_0$ ($\leftarrow$we reject $H_1$) if we observe $T_0$, and we accept $H_1$ ($\leftarrow$we reject $H_0$) if we observe $T_1$. In order to treat its performance, we focus on the following two kinds of errors: A type 1 error is an event such that we accept $H_1$ though $H_0$ is true. A type 2 error is an event such that we accept $H_0$ though $H_1$ is true. Hence, we treat the following two kinds of error probabilities: The type 1 error probability $\alpha(T, \rho)$ and the type 2 error probabilities $\beta(T, \rho)$ are given by

$$\alpha(T, \rho) = \text{Tr}(\rho T_1) = 1 - \text{Tr}(\rho T_0) \ (\rho \in S_0),$$

$$\beta(T, \rho) = \text{Tr}(\rho T_0) = \text{Tr}(\rho T) \ (\rho \in S_1).$$

A quantity $1 - \beta(T, \rho)$ is called power. A test $T$ is said to be level-$\alpha$ if $\alpha(T, \rho) \leq \alpha$ for any $\rho \in S_0$.

In hypothesis testing, we restrict our test to tests whose first error probability is greater than a given constant $\alpha$ for any element $\rho \in S_0$. That is, since the type 1 error is considered to be more serious than the type 2 error in hypothesis testing, it is required to guarantee that the type 1 error probability is less than a constant which is called level of significance or level. Hence, a test $T$ is said to be level-$\alpha$ if $\alpha(T, \rho) \leq \alpha$ for any $\rho \in S_0$.

Then, under this condition, the performance of the test is given by $1 - \beta(T, \rho)$ for $\rho \in S_1$, which is called power. Therefore, we often optimize the type 2 error probability as follows:

$$\beta_\alpha(S_0 \| \rho) \overset{\text{def}}{=} \min_{T \in T_{\alpha, S_0}} \beta(T, \rho),$$

$$T_{\alpha, S_0} \overset{\text{def}}{=} \{ T | 0 \leq T \leq I, \ \alpha(T, \rho) \leq \alpha \rho \in S_0 \}$$

for any $\rho \in S_1$. Especially, a test $T \in T_{\alpha, S_0}$ is called a Most Powerful (MP) test with level $\alpha$ at $\rho \in S_1$ if $\beta(T, \rho) \leq \beta(T', \rho)$ for any level-$\alpha$ test $T'$ in $T_{\alpha, S_0}$, that is,

$$\beta(T, \rho) = \beta_\alpha(S_0 \| \rho).$$
Moreover, a test $T \in T_{n,S_0}$ is called a Uniformly Most Powerful (UMP) test if $T$ is MP for any level-$\alpha$ test $\rho \in S_1$, that is,

$$\beta(T, \rho) = \beta_{\alpha}(S_0; \rho), \quad \forall \rho \in S_1.$$ 

However, in certain instances, it is natural to restrict our testing to those satisfying one or two conditions ($C_1$ or $C_1$ and $C_2$). In such a case, we focus on the following quantity in stead of $\beta(T, \rho)$:

$$\beta_{C_1,C_2}(S_0; \rho) \overset{\text{def}}{=} \min_{T \in T_{n,S_0}} \{\beta(T, \rho)\mid T \text{ satisfies } C_1 \text{ and } C_2\}.$$ 

If a test $T \in T_{n,S_0}$ satisfies conditions $C_1$, $C_2$, and

$$\beta(T, \rho) = \beta_{C_1,C_2}(S_0; \rho), \quad \forall \rho \in S_1,$$

it is called a Uniformly Most Powerful $C_1, C_2$ (UMP $C_1, C_2$) test.

be $T$.

### III. OUR PROBLEMS

#### A. Hypothesis

Our problem in this article is the hypothesis testing of the maximal entangled state

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

on the tensor product space $\mathcal{H}_{A,B}$ of the two $d$-dimensional systems $\mathcal{H}_{A}$ and $\mathcal{H}_{B}$ spanned by $|0\rangle_A, |1\rangle_A, \ldots, |d-1\rangle_A$ and $|0\rangle_B, |1\rangle_B, \ldots, |d-1\rangle_B$, respectively. Note that we refer to $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ as the standard basis. Suppose that $n$ independent samples are provided, that is, the state is given in the form

$$\rho = \bigotimes_{i=1}^{n} \sigma_i = \sigma_1 \otimes \cdots \otimes \sigma_n$$

for $n$ unknown densities $\sigma_1, \ldots, \sigma_n$. We also assume that these densities $\sigma_1, \ldots, \sigma_n$ equal a density $\sigma$. In this case, the state $\rho$ is called $n$-independent and identical density (n.i.d.). In the following, we consider two settings for our hypotheses:

- **H0:** $\sigma \in S_{\leq} \overset{\text{def}}{=} \{\sigma \mid |\langle \phi_{AB}^0 | \phi_{AB}^0 \rangle| \leq \epsilon\}$ versus
- **H1:** $\sigma \in S_{\geq} \overset{\text{def}}{=} \{\sigma \mid |\langle \phi_{AB}^0 | \phi_{AB}^0 \rangle| \geq \epsilon\}$

and

- **H0:** $\sigma \in S_{\leq} \overset{\text{def}}{=} \{\sigma \mid 1 - |\langle \phi_{AB}^0 | \phi_{AB}^0 \rangle| \leq \epsilon\}$ versus
- **H1:** $\sigma \in S_{\geq} \overset{\text{def}}{=} \{\sigma \mid 1 - |\langle \phi_{AB}^0 | \phi_{AB}^0 \rangle| \geq \epsilon\}$

When the null hypothesis is "$\sigma \in S_{\leq} \overset{\text{def}}{=} \{\sigma \mid |\langle \phi_{AB}^0 | \phi_{AB}^0 \rangle| \leq \epsilon\}$", the set of level $\alpha$-tests is given in the $n$-fold i.i.d. case by

$$T_{n,\leq}^{\alpha} \overset{\text{def}}{=} \{T \mid 0 \leq T \leq I, \quad \forall \sigma \in S_{\leq}, \quad 1 - \text{Tr} \sigma^\otimes n T \leq \alpha\}.$$ 

Similarly, when the null hypothesis is "$\sigma \in S_{\geq} \overset{\text{def}}{=} \{\sigma \mid 1 - |\langle \phi_{AB}^0 | \phi_{AB}^0 \rangle| \geq \epsilon\}$", the set of level $\alpha$-tests is given in the $n$-fold i.i.d. case by

$$T_{n,\geq}^{\alpha} \overset{\text{def}}{=} \{T \mid 0 \leq T \leq I, \quad \forall \sigma \in S_{\geq}, \quad 1 - \text{Tr} \sigma^\otimes n T \leq \alpha\}.$$ 

In this paper, we only treat the null hypothesis $S_{\leq}$. However, a large part of obtained results can be trivially extended to the case of the null hypothesis $S_{\geq}$.

#### B. Restriction I: group action

In this paper, we treat these two cases with the invariance conditions for the following group action, which preserve the two hypotheses $H_0$ and $H_1$. The naturality of this condition will be discussed later.

1) $U(1)$-action:

$$\phi \mapsto U_\theta \phi, \quad \phi \in \mathcal{H}_{A,B}, \quad \theta \in \mathbb{R}$$

where $U_\theta$ is defined by

$$U_\theta \overset{\text{def}}{=} e^{i\theta} |\phi_{AB}^0\rangle \langle \phi_{AB}^0 | + (I - |\phi_{AB}^0\rangle \langle \phi_{AB}^0 |).$$

For a vector $|u\rangle$ orthogonal to $\langle \phi_{AB}^0 |$ and a positive number $0 < p < 1$, the entanglement properties of the two states $\sqrt{p} |\phi_{AB}^0\rangle + \sqrt{1-p} |u\rangle$ and $e^{i\theta} \sqrt{p} |\phi_{AB}^0\rangle + \sqrt{1-p} |u\rangle$ are essentially equivalent. Hence, this symmetry is very natural. We can easily check that this action preserves our hypotheses. The $U(1)$-action is so small that it is not suitable to adopt this invariance as our restriction. However, this invariance can be, often, treated so easily that it be adopted only by a technical reason.

2) $SU(d)$-action: We consider the unitary action on the tensor product space $\mathcal{H}_{A,B} = \mathcal{H}_{A} \otimes \mathcal{H}_{B}$.

$$\phi \mapsto U(g) \phi, \quad \phi \in \mathcal{H}_{A,B}, \quad g \in SU(d),$$

where

$$U(g) \overset{\text{def}}{=} g \otimes \bar{g},$$

and $\bar{g}$ is the complex conjugate of $g$ concerning the standard basis $|0\rangle_B, |1\rangle_B, \ldots, |d-1\rangle_B$ on the system $B$. Indeed, this action preserves the maximally entangled state $|\phi_{AB}^0\rangle$. Hence, this action preserves our hypotheses. Furthermore, this action preserves the entanglement property. Similarly to the $U(1)$-invariance, the $SU(1)$-action is so small that it will be adopted only by a technical reason.

3) $SU(d) \times U(1)$-action: Since the $SU(d)$ action and the $U(1)$-action preserve the entanglement property, the following action of the direct sum product group $SU(d) \times U(1)$ of $SU(d)$ and $U(1)$ also preserves this property:

$$\phi \mapsto U(g, \theta) \phi, \quad \phi \in \mathcal{H}_{A,B}, \quad (g, e^{i\theta}) \in SU(d) \times U(1),$$
where
\[ U(g, \theta) \overset{\text{def}}{=} U(g)U_\theta = U_\theta U(g). \]

Thus, this condition is most suitable as our restriction.

4) \( U(d^2 - 1) \)-action: As a stronger invariance, we can consider the invariance of the \( U(d^2 - 1) \)-action, i.e., the following unitary action on the orthogonal space of \( |\phi_{AB}^0\rangle \langle \phi_{AB}^0| \), which is a \( d^2 - 1 \)-dimensional space.

\[ \phi \mapsto V(g)\phi, \quad \phi \in \mathcal{H}_{A,B}, \quad g \in U(d^2 - 1). \]

where
\[ V(g) \overset{\text{def}}{=} g(I - |\phi_{AB}^0\rangle \langle \phi_{AB}^0|) + |\phi_{AB}^0\rangle \langle \phi_{AB}^0|. \]

This group action contains the \( U(1) \)-action and the \( SU(d) \)-action. Hence, the invariance of the \( U(d^2 - 1) \)-action is stronger than the invariances of above three actions. This action does not preserve the entanglement property. Thus, based on this definition, we cannot say that this condition is natural for our setting while it is natural if we are not concerned of entanglement.

Furthermore, in the \( n \)-fold i.i.d. setting, it is suitable to assume the invariance of the \( n \)-tensor product action of the above actions, i.e., \( U_{\otimes n}^A, U(g)^{\otimes n}, U(g, \theta)^{\otimes n}, V(g)^{\otimes n}, \)

etc.

C. Restriction II: locality

When the system consists of two distinct parties \( A \) and \( B \), it is natural to restrict our testing to LOCC measurements between \( A \) and \( B \). Hence, we can consider several restrictions concerning locality condition. Hence, in section IV, as the first step, in order to discuss the hypotheses testing with the null hypothesis \( \mathcal{S}_{\leq \epsilon} \), we will treat the following optimization:

\[ \beta_{\alpha,\cdot,G}^C(\leq \epsilon||\sigma) \overset{\text{def}}{=} \min_{T \in T_{n}^A \cap T_{n}^B} \left\{ \beta(T, \sigma^{\otimes n}) \mid T \text{ is } G\text{-invariant} \right\}, \]

where \( G = U(1), SU(d), SU(d) \times U(1), \) or \( U(d^2 - 1). \) However, since our quantum system consists of two distant system, we cannot necessarily use all measurements. Hence, it is natural to restrict our test to a class of tests. In this paper, we focus on the following seven classes.

\( \emptyset \): No condition

\[ S(A, B) \text{: The test is separable between two systems } \mathcal{H}^A_{\otimes n} \text{ and } \mathcal{H}^B_{\otimes n}, \]

i.e., the test \( T \) has the following form:

\[ T = \sum_i a_i T_i^A \otimes T_i^B, \]

where \( a_i \geq 0 \) and the matrix \( T_i^A \) (\( T_i^B \)) is a positive semi-definite matrix on the system \( \mathcal{H}^A_{\otimes n} \) (\( \mathcal{H}^B_{\otimes n} \)), respectively.

\( L(A \Rightarrow B) \): The test can be realized by two-way LOCC between two systems \( \mathcal{H}^A_{\otimes n} \) and \( \mathcal{H}^B_{\otimes n} \).

\( L(A \rightarrow B) \): The test can be realized by one-way LOCC from the system \( \mathcal{H}^A_{\otimes n} \) to the system \( \mathcal{H}^B_{\otimes n} \).

\( S(A_1, \ldots, A_n, B_1, \ldots, B_n) \): The test is separable among \( 2n \) systems \( \mathcal{H}^A_1, \ldots, \mathcal{H}^A_n, \mathcal{H}^B_1, \ldots, \mathcal{H}^B_n \), i.e., the test \( T \) has the following form:

\[ T = \sum_i a_i T_i^A \otimes \cdots \otimes T_i^{A_n} \otimes T_i^{B_1} \otimes \cdots \otimes T_i^{B_n}, \]

where \( a_i \geq 0 \) and the matrix \( T_i^A \) (\( T_i^B \)) is a positive semi-definite matrix on the system \( \mathcal{H}^A_1 \) (\( \mathcal{H}^B_1 \)), respectively.

\( L(A_1, \ldots, A_n, B_1, \ldots, B_n) \): The test can be realized by two-way LOCC among \( 2n \) systems \( \mathcal{H}^A_1, \ldots, \mathcal{H}^A_n, \mathcal{H}^B_1, \ldots, \mathcal{H}^B_n \). Moreover, the classical communication among two groups \( \mathcal{H}^A_1, \ldots, \mathcal{H}^A_n \) and \( \mathcal{H}^B_1, \ldots, \mathcal{H}^B_n \) is restricted to one-way from the former to the later.

Based on the above conditions, we define the following quantity as the optimal second error probability:

\[ \beta_{\alpha,\cdot,G}^C(\leq \epsilon||\sigma) \overset{\text{def}}{=} \min_{T \in T_{n}^A \cap T_{n}^B} \left\{ \beta(T, \sigma^{\otimes n}) \mid T \text{ is } G\text{-invariant} \right\}. \]

As is easily checked, any LOCC operation is separable. Hence, the condition \( L(A \Rightarrow B) \) is stronger than the condition \( S(A, B) \). Also, the condition \( L(A_1, \ldots, A_n \rightarrow B_1, \ldots, B_n) \) is stronger than the condition \( S(A_1, \ldots, A_n \rightarrow B_1, \ldots, B_n) \). The relation among these conditions can be illustrated as follows.

Next, we focus on the trivial relations of the optimal second error probability. If a group \( G_1 \) is greater than \( G_2 \), the inequality

\[ \beta_{\alpha,\cdot,G_1}^C(\leq \epsilon||\sigma) \geq \beta_{\alpha,\cdot,G_2}^C(\leq \epsilon||\sigma) \]

(2)

holds. Moreover, if a condition \( C_1 \) is stronger than another condition \( C_2 \), the similar inequality

\[ \beta_{\alpha,\cdot,C_1}^C(\leq \epsilon||\sigma) \geq \beta_{\alpha,\cdot,C_2}^C(\leq \epsilon||\sigma) \]

(3)

holds.

Similarly, we define \( \beta_{\alpha,\cdot,G}^C(\geq \epsilon||\sigma) \) by replacing \( \leq \) by \( \geq \) in RHS.

Indeed, if the condition is invariant for the action of \( G \), it is very natural to restrict our test among \( G \)-invariant tests, as is indicated by the following lemma.
Lemma 1 Assume that a set of test satisfying the condition $C$ is invariant for the action of $G$, then

$$\beta_{\alpha,n,G}(\leq \epsilon || \sigma) = \min_{T \in T_{n,\epsilon}, \sigma \in G} \max_{T \in T_{n,\epsilon}, \sigma \in G} \beta(T, (f(g)(f(g)^{-1})^\otimes m),$$

$$= \min_{T \in T_{n,\epsilon}, \sigma \in G} \int_{G} \beta(T, (f(g)(f(g)^{-1})^\otimes m) \nu_{G}(dg),$$

where $\nu_{G}$ is the invariant measure and $f$ denotes the action of $G$.

In the following, we sometimes abbreviate the invariant measure $\nu_{G}$ by $\nu$. This lemma is a special version of quantum Hunt-Steen lemma [2, 3]. The condition $\theta$ is invariant for the actions $U(1), SU(d), SU(d) \times U(1), U(d^2) - 1$. But, other conditions $S(A,B), L(A \Rightarrow B), L(A \rightarrow B), S(A_1, \ldots, A_n, B_1, \ldots B_n), L(A_1, \ldots, A_n, B_1, \ldots B_n), L(A_1, \ldots, B_n)$ are invariant only for $SU(d)$. Hence, Lemma 1 cannot be applied to the pair of these conditions and the actions $U(1), SU(d), SU(d) \times U(1), U(d^2) - 1$. The following lemma is useful in such a case.

Lemma 2 Assume that the group $G_1$ includes another group $G_2$ which satisfies the condition of Lemma 1. If

$$\beta_{\alpha,n,G}(\leq \epsilon || \sigma) = \beta_{\alpha,n,G_1}(\leq \epsilon || \sigma), \forall \sigma$$

then

$$\beta_{\alpha,n,G}(\leq \epsilon || \sigma) = \min_{T \in T_{n,\epsilon}, \sigma \in G_1} \max_{T \in T_{n,\epsilon}, \sigma \in G_1} \beta(T, (f(g)(f(g)^{-1})^\otimes m),$$

$$= \min_{T \in T_{n,\epsilon}, \sigma \in G_1} \int_{G_1} \beta(T, (f(g)(f(g)^{-1})^\otimes m) \nu_{G_1}(dg).$$

IV. TESTING FOR BINOMIAL DISTRIBUTIONS

In this paper, we use several knowledge about testing for binomial distributions for testing for a maximally entangled state. Hence, we review them here.

A. One-sample setting:

As a preliminary, we treat testing for the coin flipping probability $p$ with a single trial. That is, we assume that the event 1 happens with the probability $p$ and the event 0 happens with the probability $1 - p$, and focus on the null hypothesis $p \in [0, \epsilon]$. In this case, our test can be described by a map $T$ from $[0, 1]$ to $[0, 1]$, which means that when the data $k$ is observed, we accept the null hypothesis with the probability $T(k)$. Then, the minimum second error probability among level-$\alpha$ tests is given by

$$\beta_{\alpha}(\leq \epsilon || q) \overset{\text{def}}{=} \min_{T} \left\{ \text{for } k \in [0, \epsilon], p(T) \geq 1 - \alpha \right\} P_{\alpha}^{n}(T(0)) + \overline{T}(1)$$

When we define the test $\overline{T}_{e,\alpha}^{1}$ by

$$\overline{T}_{e,\alpha}^{1}(0) = \left\{ \begin{array}{ll} \frac{n}{\epsilon} & \text{if } \epsilon \leq \alpha \\ 1 & \text{if } \epsilon > \alpha \end{array} \right., \overline{T}_{e,\alpha}^{1}(1) = \left\{ \begin{array}{ll} \infty & \text{if } \epsilon \leq \alpha \\ 1 & \text{if } \epsilon > \alpha \end{array} \right.$$,

the test $\overline{T}_{e,\alpha}^{1}$ satisfies

$$(1 - \epsilon)\overline{T}_{e,\alpha}^{1}(0) + \overline{T}_{e,\alpha}^{1}(1) = 1 - \alpha. \quad (4)$$

Moreover, if $\epsilon \leq \alpha$,

$$(1 - \epsilon)\overline{T}_{e,\alpha}^{1}(0) + \overline{T}_{e,\alpha}^{1}(1) \geq 1 - \alpha.$$

Hence the test $\overline{T}_{e,\alpha}^{1}$ is level-$\alpha$. Furthermore, we can easily check that the minimum of $q(T)$ with the condition (4) for $\overline{T}$ can be attained by $\overline{T} = \overline{T}_{e,\alpha}^{1}$ if $q > \epsilon$. Hence,

$$\beta_{\alpha}^{C}(\leq \epsilon || q) = \min_{T} \left\{ \text{for } k \in [0, \epsilon], p(T) \geq 1 - \alpha \right\} \frac{1}{\infty}.$$

B. $n$-sample setting:

In the $n$-trial case, the data $k = 0, 1, \ldots, n$ obeys the distribution $P_{\alpha}^{n}(k) \overset{\text{def}}{=} (\epsilon)(1 - \epsilon)^{n-k} \epsilon^{k}$ with the unknown parameter $p$. Hence, we discuss the hypothesis testing with the null hypothesis $P_{\alpha}^{n}(k) \overset{\text{def}}{=} \min_{\epsilon \in [0, 1]} \{ P_{\alpha}^{n}(k) \leq \epsilon \}$ and the alternative hypothesis $(P_{\alpha}^{n}(k) \leq \epsilon)$. In this case, our test $T$ can be described by a function from the data set $\{0, 1, \ldots, n\}$ to interval $[0, 1]$. In this case, when the data $k$ is observed, we accept the null hypothesis $P_{\alpha}^{n}(k)$ with the probability of $T(k)$. Then, the minimum second error probability among level-$\alpha$ tests is given by

$$\beta_{\alpha}^{n}(\leq \epsilon || q) \overset{\text{def}}{=} \min_{T} \left\{ \text{for } k \in [0, \epsilon], 1 - P_{\alpha}^{n}(T) \leq \alpha \right\}$$

When we define the test $\overline{T}_{e,\alpha}^{n}$ as follows.

$$\overline{T}_{e,\alpha}^{n}(k) = \left\{ \begin{array}{ll} 1 & \text{if } k < \epsilon \gamma_{e,\alpha}^{n} \\ \gamma_{e,\alpha}^{n} & \text{if } k = \epsilon \gamma_{e,\alpha}^{n} \\ 0 & \text{if } k > \epsilon \gamma_{e,\alpha}^{n} \end{array} \right.$$,

where the integer $\epsilon \gamma_{e,\alpha}^{n}$ and the real number $\epsilon \gamma_{e,\alpha}^{n} > 0$, are defined by

$$\epsilon \gamma_{e,\alpha}^{n} - 1 \leq P_{\alpha}^{n}(k) < 1 - \alpha \leq \sum_{k=0}^{\epsilon \gamma_{e,\alpha}^{n}} P_{\alpha}^{n}(k)$$

$$\gamma_{e,\alpha}^{n} P_{\alpha}^{n}(\epsilon \gamma_{e,\alpha}^{n}) \leq 1 - \alpha - \sum_{k=0}^{\epsilon \gamma_{e,\alpha}^{n} - 1} P_{\alpha}^{n}(k).$$

Theorem 1 The test $\overline{T}_{e,\alpha}^{n}$ is level-$\alpha$ UMP test with the null hypothesis $P_{\alpha}^{n}$. Hence,

$$\beta_{\alpha}^{n}(\leq \epsilon || q) = P_{\alpha}^{n}(\overline{T}_{e,\alpha}^{n}) \overset{\text{def}}{=} \sum_{k=0}^{\epsilon \gamma_{e,\alpha}^{n} - 1} P_{\alpha}^{n}(k) + \gamma_{e,\alpha}^{n} P_{\alpha}^{n}(\epsilon \gamma_{e,\alpha}^{n}).$$
C. Asymptotic setting

In asymptotic theory, there are two settings at least. One is the large deviation setting, in which the parameter is fixed, hence we focus on the exponential component of the error probability. The other is the small deviation setting, in which the parameter is close to a given fixed point in proportion to the number of samples such that the error probability converges to a fixed number. That is, the parameter is fixed in the former, while the error probability is fixed in the later.

1. Small deviation theory

It is useful to treat the neighborhood around $p = 0$ as the small deviation theory of this problem for the asymptotic discussion of testing for an maximally entangled state. Hence, we focus on the case that $p = \frac{\lambda}{n}$: Since the probability $P_{\frac{\lambda}{n}}(k) = \left(\frac{n}{\lambda}\right)(1 - \frac{\lambda}{n})^{n-k} \left(\frac{\lambda}{n}\right)^{k}$ converges to the Poisson distribution $P_{t}(k) \overset{\text{def}}{=} e^{-t}t^{k}$, hence, our testing problem with the null hypothesis $P_{t}$ and the alternative hypothesis $\frac{\lambda}{n}$ is asymptotically equivalent to the testing of Poisson distribution $P_{t}(k)$ with the null hypothesis $t \in [0, \delta]$ and the alternative hypothesis $t'$. That is, by defining

$$\beta_{\alpha}(\leq \delta \| t') \overset{\text{def}}{=} \min \left\{ P_{t}(\tilde{T}) \mid \forall t \in [0, \delta], 1 - P_{t}(\tilde{T}) \leq \alpha \right\}$$

$$P_{t}(\tilde{T}) \overset{\text{def}}{=} \sum_{k=0}^{\infty} P_{t}(k) \tilde{T}(k),$$

the following theorem holds.

Theorem 2

$$\lim \beta_{\alpha}^{n} \left( \leq \frac{\delta}{n} \| \frac{t'}{n} \right) = \beta_{\alpha}(\leq \delta \| t').$$

Similarly to the test $T_{n,\alpha}^{n}$, we define the test $T_{\delta,\alpha}$ as

$$T_{\delta,\alpha}(k) = \begin{cases} 1 & k < l_{\delta,\alpha} \\ \gamma_{\delta,\alpha} & k = l_{\delta,\alpha} \\ 0 & k > l_{\delta,\alpha} \end{cases}$$

where the integer $l_{\delta,\alpha}$ and the real number $\gamma_{\delta,\alpha} > 0$, are defined by

$$l_{\delta,\alpha} = \sum_{k=0}^{l_{\delta,\alpha}-1} P_{t}(k) < 1 - \alpha \leq \sum_{k=0}^{l_{\delta,\alpha}} P_{t}(k)$$

$$\gamma_{\delta,\alpha} = 1 - \alpha - \sum_{k=0}^{l_{\delta,\alpha}-1} P_{t}(k).$$

Similarly to Theorem 1, the following theorem holds.

Theorem 3

The test $T_{\delta,\alpha}$ is level-$\alpha$ UMP test with the null hypothesis $P_{\leq \delta} \overset{\text{def}}{=} \{ P_{t} \mid t \leq \delta \}$. Hence,

$$\beta_{\alpha}^{n}(\leq \delta \| t') = \sum_{k=0}^{l_{\delta,\alpha}-1} P_{t}(k) + \gamma_{\delta,\alpha} P_{t}(l_{\delta,\alpha}).$$

2. Large deviation theory

Next, we proceed to the large deviation theory. Using the knowledge of mathematical statistics, we can calculate the exponents of the 2nd error probabilities $\beta_{\alpha}^{n}(\epsilon \| p)$ and $\beta_{\alpha}^{n}(\epsilon \| p)'$ for any $\alpha > 0$ as

$$\lim \frac{-1}{n} \log \beta_{\alpha}^{n}(\leq \epsilon \| p) = d(\epsilon \| p), \quad \text{if } \epsilon < p$$

$$\lim \frac{-1}{n} \log \beta_{\alpha}^{n}(\geq \epsilon \| p) = d(\epsilon \| p), \quad \text{if } \epsilon > p,$$

where the binary relative entropy $d(\epsilon \| p)$ is defined as

$$d(\epsilon \| p) \overset{\text{def}}{=} \epsilon \log \frac{\epsilon}{p} + (1 - \epsilon) \log \frac{1 - \epsilon}{1 - p}.$$

In the case of $\alpha = 0$, we have

$$\frac{-1}{n} \log \beta_{\alpha}^{n}(\epsilon \| p) = \begin{cases} -\log(1 - p) & \text{if } \epsilon = 0 \\ 0 & \text{if } \epsilon \neq 0. \end{cases}$$

V. GLOBAL TESTS

First, we treat the hypotheses testing with a given group invariance condition with no locality restriction.

A. One-sample setting:

When only one sample is prepared, the test $|\phi_{A,B}^{0} \langle \phi_{A,B}^{0}|$ is a level-$0$ test for the null hypothesis $S_{0}$. If we perform the two-valued measurement $\{\phi_{A,B}^{0}, (I - |\phi_{A,B}^{0} \langle \phi_{A,B}^{0}|)$, the data obeys the distribution $\{1 - p, p\}$, where

$$p \overset{\text{def}}{=} 1 - \langle \phi_{A,B}^{0} | \sigma | \phi_{A,B}^{0} \rangle.$$

Hence, applying the discussion in subsection IV A, the test $T_{\alpha}^{4}(\langle \phi_{A,B}^{0} | \phi_{A,B}^{0} \rangle, 0)$ is a level-$\alpha$ test for the null hypothesis $S_{\leq \epsilon}$, where the operator $T_{\alpha}^{4}(T, \epsilon)$ is defined by

$$T_{\alpha}^{4}(T, \epsilon) \overset{\text{def}}{=} \begin{cases} \frac{1 - \epsilon}{\epsilon} T \quad \text{if } \epsilon \leq \alpha \\ T + \frac{\epsilon}{\epsilon - \alpha} (I - T) \quad \text{if } \epsilon > \alpha. \end{cases}$$

B. n-sample setting:

In the $n$-sample setting, we construct a test for the null hypothesis $S_{\leq \epsilon}$ as follows. First, we perform the two-valued measurement $\{\phi_{A,B}^{0}, (I - |\phi_{A,B}^{0} \langle \phi_{A,B}^{0}|$ for...
respectively \(n\) systems. Then, if the number of counting \(I - |\phi_{A,B}^0\rangle\langle \phi_{A,B}^0|\) is described by \(k\), the data \(k\) obeys the binomial distribution \(P_n^k\). In this case, our problem can be reduced to the hypothesis testing with the null hypothesis \(P_n^k\), which has been discussed in subsection IV.B.

For given \(\alpha\) and \(\epsilon\), the test based on this measurement and the classical test \(T_{\alpha}\) is described by the operator \(T_{\alpha} = \sum_{k=0}^{n-1} P_n^k\), where \(T_{\alpha}\) is defined by

\[
T_{\alpha}(T, \epsilon) \equiv \sum_{k=0}^{n-1} P_n^k(T, I - T) + \gamma_{\alpha}(\epsilon)P_n^0(T, I - T)
\]

\[
P_{n,k}(T, S) \equiv S \otimes \cdots \otimes S \otimes T \otimes \cdots \otimes T
\]

\[
+ \cdots + T \otimes \cdots \otimes T \otimes S \otimes \cdots \otimes S
\]

Note that the above sum contains all tensor products of \(k\) times of \(S\) and \(n-k\) times of \(T\).

Since the operators \(|\phi_{A,B}^0\rangle\langle \phi_{A,B}^0|\) are \(U(d^2 - 1)\)-invariant, the test \(T_{\alpha}\) is level-\(\alpha\) \(U(d^2 - 1)\)-invariant test with the hypothesis \(S_{\alpha}\). Hence,

\[
\beta_{\alpha,\gamma}^0(\leq \epsilon\|\sigma) \leq \beta_{n,\alpha}^0(\leq \epsilon\|p).
\]

(6)

\[
\beta_{\alpha,\gamma}^0(\leq \epsilon\|\sigma) = \beta_{\alpha,n}(\leq \epsilon\|p).
\]

(7)

Since \(U(1) \subset SU(d) \times U(1) \subset U(d^2 - 1)\), the relations (6) and (7) yield the following theorem.

**Theorem 4** The equation

\[
\beta_{\alpha,\gamma}^0(\leq \epsilon\|\sigma) = \beta_{\alpha,n}(\leq \epsilon\|p)
\]

holds for \(G = U(1), SU(d) \times U(1), U(d^2 - 1)\).

Therefore, the test \(T_{\alpha}\) is the UMP-\(G\)-invariant test, for

\[
G = U(1), SU(d) \times U(1) \times U(d^2 - 1).
\]

Moreover, we can derive the same results for the hypothesis \(S_{\alpha}\).

**C. Asymptotic setting**

Next, we proceed to the asymptotic setting. In the small deviation theory, we treat the hypothesis testing with the null hypothesis \(S_{\Delta/\epsilon}\). In this setting, Theorem 2 and Theorem 4 guarantee that the limit of the optimal second error probability of the alternative hypothesis \(\sigma_n\) is given by \(\beta_\alpha(\delta)\) if \(\langle \phi_{A,B}^0|\sigma_n|\phi_{A,B}^0\rangle = 1 - \frac{\epsilon'}{n}\). That is,

\[
\lim_{n \to \infty} \beta_{\alpha,\gamma}^0\left(\leq \epsilon\|\sigma_n\right) = \beta_\alpha(\leq \delta\|p')
\]

for \(G = U(1), SU(d) \times U(1), U(d^2 - 1)\).

In the large deviation setting, we can obtain the same results as subsection IV.C, i.e.,

\[
\lim_{n \to \infty} \frac{1}{n} \log \beta_{\alpha,\gamma}^0(\leq \epsilon\|\sigma) = \begin{cases} 
\frac{d\epsilon}{p} & \text{if } \alpha > 0 \\
- \log(1 - p) & \text{if } \alpha = 0, \epsilon = 0 \\
0 & \text{if } \alpha = 0, \epsilon > 0 
\end{cases}
\]

(10)

If \(\epsilon < p = 1 - \langle \phi_{A,B}^0|\sigma|\phi_{A,B}^0\rangle\). Moreover, we can derive similar results with the null hypothesis \(S_{\alpha}\).

**VI. A-B LOCALITY**

In this section, we treat optimization problems with several conditions regarding the locality between A and B.

**A. One-sample setting**

First, we focus on the simplest case, i.e., the case of \(\epsilon = 0\) and \(\alpha = 0\). For this purpose, we focus on a POVM with the following form on \(H_A\)

\[
M = \{p_i|u_i\rangle\langle u_i|\}, \quad |u_i| = 1, \quad 0 \leq p_i \leq 1,
\]

where such a POVM is called rank-one. Based on a rank-one POVM \(M\), a suitable test \(T(M)\)

\[
T(M) \equiv \sum p_i|u_i\rangle\langle u_i|\otimes |\overline{u_i}\rangle\langle \overline{u_i}|
\]

(11)

can be realized by the following one-way LOCC protocol. From the definition, of course, we can easily check that \(T(M)\) satisfies the condition of test, i.e.,

\[
0 \leq T(M) \leq 1.
\]

(12)

**One-way LOCC protocol of \(T(M)\):**

1) Alice performs the measurement \(\{p_i|u_i\rangle\langle u_i|\}\), and sends her data \(i\) to Bob.

2) Bob performs the two-valued measurement \(\{|\overline{u_i}\rangle\langle \overline{u_i}|\}\), where \(\overline{u_i}\) is the complex conjugate of \(u_i\) concerning the standard basis \(|0\rangle_B, |1\rangle_B, \ldots, |d-1\rangle_B\).

3) If Bob observes the event corresponding to \(|\overline{u_i}\rangle\langle \overline{u_i}|\), the hypothesis \(|\phi_{A,B}^0\rangle\langle \phi_{A,B}^0|\) is accepted. Otherwise, it is rejected.

This test satisfies

\[
\langle \phi_{A,B}^0|T(M)|\phi_{A,B}^0\rangle = 1,
\]

(13)

\[
\text{Tr} T(M) = \sum p_i \text{Tr} |u_i\rangle\langle u_i|\otimes |\overline{u_i}\rangle\langle \overline{u_i}|
\]

(14)

Hence, it is a level-0 test with the null hypothesis \(|\phi_{A,B}^0\rangle\langle \phi_{A,B}^0|\). In particular, in the one-way LOCC setting, our test can be restricted to this kind of tests as the following sense.
Lemma 3 Let $T$ be a one-way LOCC ($A \rightarrow B$) level-0 test with the null hypothesis $|\phi_{A,B}^{0}\rangle=|\phi_{A,B}^{0}\rangle$. Then, there exists a POVM with the form $M = \{p_{i}|u_{i}\rangle\langle u_{i}|\}_{i}$ such that
\[ T \geq T(M), \tag{15} \]
i.e., the test $T(M)$ is better than the test $T$.

Moreover, concerning the separable condition, the following lemma holds. Hence, Corollary 1 indicates that it seems natural to restrict our test to the test with the form (11) even if we adopt the separable condition.

Lemma 4 Assume that a separable test $T$: satisfies
\[ \langle\phi_{A,B}^{0}|T|\phi_{A,B}^{0}\rangle = 1. \tag{16} \]
When we describe the test $T$ as
\[ T = d \sum_{i} p_{i}|u_{i} \otimes u_{i}'\rangle\langle u_{i} \otimes u_{i}'| + \sum_{j} q_{j}|v_{j} \otimes v_{j}'\rangle\langle v_{j} \otimes v_{j}'|, \tag{17} \]
such that $\langle\phi_{A,B}^{0}|u_{i} \otimes u_{i}'\rangle = \frac{1}{\sqrt{d}}$ and $\langle\phi_{A,B}^{0}|v_{j} \otimes v_{j}'\rangle = 0$, we obtain
\[ \sum_{i} p_{i}|u_{i} \otimes u_{i}'\rangle = \frac{1}{\sqrt{d}}|\phi_{A,B}^{0}\rangle. \tag{18} \]

Note that we can easily obtain the same statement if we replace the summation $\sum_{i}$ by the integral $\int$ at (17). Since any separable test $T$ has the form (17), the following corollary holds concerning the completely mixed state $\frac{1}{d}I$.

Corollary 1 If a separable test $T$ satisfies the conditions
\[ \langle\phi_{A,B}^{0}|T|\phi_{A,B}^{0}\rangle = 1 \]
\[ \text{Tr} T' \frac{d}{d^2} = d = \min_{T' \in S(A,B)} \left\{ \text{Tr} T' \frac{d}{d^2} \left| \langle\phi_{A,B}^{0}|T'|\phi_{A,B}^{0}\rangle = 1 \right. \right\} \]
then the test $T$ has a form (11).

Next, we focus on the covariant POVM $M_{\text{cov}}^{1}$:
\[ M_{\text{cov}}^{1}(dp) \overset{\text{def}}{=} d(\varphi)\varphi|\nu(d\varphi), \]
where $\nu(d\varphi)$ is the invariant measure in the set of pure states with the full measure is 1. Then, the test $T_{\text{inv}}^{1,A-B} \overset{\text{def}}{=} T(M_{\text{cov}}^{1})$ has the following form
\[ T_{\text{inv}}^{1,A-B} = \int d(\varphi \otimes \varphi')\varphi \otimes \varphi'\nu(d\varphi) = \delta_{\phi_{A,B}^{0}}(\phi_{A,B}^{0}) + \frac{1}{d+1}(|I - \delta_{\phi_{A,B}^{0}}(\phi_{A,B}^{0})|). \tag{18} \]

Note that the POVM $M_{\text{cov}}^{1}$ can be realized as follows:

Realization of $M_{\text{cov}}^{1}$:
1) Randomly, we choose $g \in SU(\mathit{d})$ with the invariant measure.
2) Perform POVM $\{g|i\}_A \{i|g\}_B$. Then, the realized POVM is $M_{\text{cov}}^{1}$.

Since the equation (18) guarantees the $U(d^2 - 1)$-invariance of the test $T_{\text{inv}}^{1,A-B}$, we obtain
\[ \frac{(1-d)}{d+1} \leq \frac{d}{d+1} \leq 1 \]
which implies
\[ \beta_{0,1,U(d^2-1)}(0||\sigma) \leq \frac{1}{1 - \frac{d}{d+1}}. \tag{19} \]

Next, we apply the discussion in subsection IV-A to the probability distribution $(\frac{dp}{d+1}, 1 - \frac{dp}{d+1})$. Then, the test $T_{\text{inv}}^{1,A-B} \overset{\text{def}}{=} T_{\text{inv}}^{1}(T_{\text{cov}}^{1,A-B}, \frac{dp}{d+1})$ is a level-\(\alpha\) $U(d^2 - 1)$-invariant test. Since the test $T_{\text{inv}}^{1,A-B}$ can be performed by randomized operation with $T_{\text{inv}}^{1,A-B}$ and $I - T_{\text{inv}}^{1,A-B}$, we obtain
\[ \beta_{0,1,U(d^2-1)}(0||\sigma) \leq \frac{1}{1 - \frac{d}{d+1}}. \tag{19} \]

On the other hand, concerning $SU(d)$-invariance and separable tests, the equation
\[ \beta_{0,1,SU(d)}^{S(A,B)}(0||\sigma) \leq \text{Tr} T_{\text{inv}}^{1,A-B} \sigma \tag{20} \]
holds. The equation in the case of $\alpha = 0, \epsilon = 0$ is obtained by Tsuda et al. [1]. A similar result with the PPT condition is appeared in Virmani and Plenio [21].

Since $U(d^2 - 1)$ is a larger group action than $SU(d)$ and the condition $L(A \rightarrow B)$ is stricter than the condition $S(A,B)$, the trivial inequalities
\[ \beta_{0,1,SU(d)}^{S(A,B)}(0||\sigma) \leq \beta_{0,1,U(d^2-1)}^{S(A,B)}(0||\sigma) \leq \beta_{0,1,U(d^2-1)}^{SU(d)}(0||\sigma) \]
hold. Therefore, relations (19) and (20) yield
\[ \beta_{0,1,U(G)}^{S(A,B)}(0||\sigma) \geq \begin{cases} \frac{(1-\alpha)(1-d)}{d+1} & \text{if } \frac{dp}{d+1} \leq \alpha, \\ \frac{1}{1 - \frac{d}{d+1}} & \text{if } \frac{dp}{d+1} > \alpha, \end{cases} \tag{21} \]
for $G = SU(d)$, $SU(d) \times U(1)$, $U(d^2 - 1)$, and $C = L(A \rightarrow B), L(A \rightarrow B), S(A,B)$. That is, the test $T_{\text{inv}}^{1,A-B}$ is the UMP $G$-invariant $C$ test with level $\alpha$ for the null hypothesis $S_{\geq \alpha}$. Furthermore, similar results for the null hypothesis $S_{\geq \alpha}$ can be also obtained.

B. Two-sample case

In this section, we construct a $SU(d) \times U(1)$-invariant test which is realized by LOCC between $A$ and $B$, and
which attains the asymptotically optimal bound (9). For this purpose, we focus on the covariant POVM $M_{cov}$:

$$M_{cov}^{2}(dg_{1}, dg_{2})$$

$$\equiv \mathbb{E}(g_{1} \otimes g_{2})[n](g_{1} \otimes g_{2})^{*}n_{2}(g_{1})n_{2}(g_{2}),$$

where the vector $u$ is maximally entangled and $n$ is the invariant measure on $SU(2)$. Then, the operator $T_{inv}^{2, A \rightarrow B}$ has the form:

$$\mathcal{T}_{inv}^{2, A \rightarrow B} \equiv T(M_{cov}^{2})$$

This equation implies that the testing $T(M_{cov}^{2})$ does not depend on the choice of the maximally entangled state $u$. It also guarantees the $U(d^{2} - 1)$-invariance of the test $T_{inv}^{2, A \rightarrow B}$. We also obtain the equation

$$\text{Tr} T_{inv}^{2, A \rightarrow B} \sigma^{\otimes 2} = (1 - p)^{2} + \frac{p^{2}}{d^{2} - 1} = 1 - 2p + \frac{d^{2}p^{2}}{d^{2} - 1}. \quad (23)$$

Since the test $T_{inv}^{2, A \rightarrow B}$ is a level-0 test with the null hypothesis $S_{0}$, the inequality

$$\beta_{0,2,U(d^{2}-1)}(0\parallel\sigma) \leq 1 - 2p + \frac{d^{2}p^{2}}{d^{2} - 1}$$

holds. Next, we apply the discussion of subsection IV.A. Then, the test $T_{inv}^{2, A \rightarrow B}$ is a level-$U(d^{2} - 1)$-invariant test. Since the test $T_{inv}^{2, A \rightarrow B}$ can be performed by randomized operation with $T_{inv}^{2, A \rightarrow B}$ and $I - T_{inv}^{2, A \rightarrow B}$, we obtain

$$\beta_{0,2,U(d^{2}-1)}(\leq \alpha) \leq \text{Tr} T_{inv}^{2, A \rightarrow B} \sigma^{\otimes 2}$$

$$= \begin{cases} (1 - \alpha)(1 - 2p + \frac{d^{2}p^{2}}{d^{2} - 1}) & \text{if } 2p - \frac{d^{2}p^{2}}{d^{2} - 1} \leq \alpha \\ \frac{2 - \alpha}{2p - \frac{d^{2}p^{2}}{d^{2} - 1}} & \text{if } 2p - \frac{d^{2}p^{2}}{d^{2} - 1} > \alpha. \end{cases}$$

Furthermoe, as a generalization of (23), we obtain the following lemma, which is more useful in the asymptotic setting from an applied viewpoint.

**Lemma 5** Let $\mathcal{M} = \{p_{i}u_{i}\langle u_{i} \parallel u_{i} \rangle = 1\}$ be a POVM on $A$'s two-sample space $\mathcal{H}_{A}^{\otimes 2}$. If every state $|u_{i}\rangle$ is a maximally entangled state on $\mathcal{H}_{A}^{\otimes 2}$, the test $T(M)$ satisfies

$$\langle \phi_{AB}^{0} | \sigma | \phi_{AB}^{0} \rangle^{2} \leq \text{Tr} \sigma^{\otimes 2} T(M)$$

$$\leq \langle \phi_{AB}^{0} | \sigma | \phi_{AB}^{0} \rangle^{2} + (1 - \langle \phi_{AB}^{0} | \sigma | \phi_{AB}^{0} \rangle)^{2}.$$
D. Asymptotic setting

We proceed to test asymptotic setting. First, we show that even if our test satisfies the A-B LOCC condition, the bound (8) can be attained in the asymptotic small deviation setting. Indeed, since \( \frac{d^{2}}{2n} - \frac{d^{2}}{d^{2} - 1} (\frac{n}{\epsilon^{2}}) \) \( (k) \to P(k) \), the equation

\[
\lim \beta_{\alpha}^m \left( 2, \delta \right) \leq \frac{d^{2}}{2n} - \frac{d^{2}}{d^{2} - 1} \left( \begin{array}{c}
\delta \\
2n
\end{array} \right) \frac{t'}{2} \leq \frac{d^{2}}{2n} - \frac{d^{2}}{d^{2} - 1} \left( \begin{array}{c}
t' \\
2n
\end{array} \right)
\]

\[
= \beta_{\alpha} \left( \leq \delta \right)
\]

is true, and can be proven similarly to Theorem 2. Hence, from (2) and (3), we have

\[
\lim \beta_{\alpha,2n,O} \left( \leq \frac{\delta}{n} \right) = \beta_{\alpha} \left( \leq \delta \right)
\]

for \( G = U(1), SU(d) \times U(1), U(d^2 - 1), C = \emptyset, L(A \to B), L(A \equiv B), S(A, B) \). However, it is difficult to realize the covariant POVM \( M_{s_{o_{v}}}^{A} \) on \( H_{0,1}^{A,cov} \). Even if the test \( T^{2n}_{s_{o_{v}}} \) is replaced by \( T^{2n}_{s_{o_{v}}, Bell} \) \( (M_{s_{o_{v}}}^{B, bell}) \), the bound \( \beta_{\alpha} \left( \leq \delta \right) \) can be attained in the following asymptotic sense. The test \( T^{2n}_{s_{o_{v}}, Bell} \) may be non-level- \( \alpha \) with the null hypothesis \( S_{\leq \delta/2\eta} \), but is asymptotically level- \( \alpha \), i.e.,

\[
\Tr T_{s_{o_{v}}, Bell}^{2n} \rightarrow \beta_{\alpha} \left( \leq \delta \right) \].

Next, we proceed to the large deviation setting. The inequality (25) yields

\[
\lim -\frac{1}{n} \log \beta_{\alpha, n, U(d^2 - 1)} \left( 0 \right) \sigma \geq \left\{ \begin{array}{l}
-\log (1 - p) \text{ if } 1 - p \geq \frac{1}{d} \\
\log d \text{ if } 1 - p < \frac{1}{d}
\end{array} \right.
\]

Hence, the relations (3) and (10) guarantee that if \( 1 - p \geq \frac{1}{d} \),

\[
\lim -\frac{1}{n} \log \beta_{\alpha, n, U(d^2 - 1)} \left( 0 \right) \sigma = -\log (1 - p),
\]

for \( G = U(1), SU(d) \times U(1), U(d^2 - 1), C = \emptyset, L(A \to B), L(A \equiv B), S(A, B) \). Hence, we can conclude that if \( 1 - p \geq \frac{1}{d} \), there is no advantage of use of entanglement between \( H_{A} \) and \( H_{B} \) for this testing even in this kind of the asymptotic large deviation setting.

VII. A-B LOCALITY AND SAMPLE LOCALITY

In this section, we discuss the locality among \( A_{1}, B_{1}, \ldots, A_{n}, B_{n} \). Since the case \( n = 1 \) of this setting is the same as that of the setting section VI. Hence, we treat the case \( n = 2 \), at first.

A. Two-sample setting

We construct a level-0 SU(\( d \))-invariant test for the null hypothesis \( S_{0} = \{ \phi_{A,B}^{0} \} \). As for this purpose, we define a POVM \( M_{s_{o_{v}}}^{A} \) on Alice’s space \( H_{A}^{2} \), which can be realized by one-way LOCC \( A_{1} \to A_{2} \) from the first system \( H_{A} \) to the second system \( H_{A_{2}} \).

Construction of \( M_{s_{o_{v}}}^{A} \):

1. Alice performs the covariant POVM \( M_{s_{o_{v}}}^{A} \) on the first system \( H_{A_{1}} \), and obtain the data corresponding to the state \( |\varphi \rangle \langle \varphi | \).

2. We choose the Projection-valued measure \( \{ u^{t}(\varphi) | u^{t}(\varphi) \} \), satisfying

\[
\langle u^{t}(\varphi) | u^{t}(\varphi) \rangle = 0, \quad (u^{t}(\varphi) | \varphi) = \frac{1}{\sqrt{d}}.
\]

3. Alice randomly chooses \( g \in U(d - 1) \) which acts on the space of the orthogonal to \( \varphi \), and performs the Projection-valued measure \( \{ |u^{t}(\varphi) \rangle \langle u^{t}(\varphi) | \} \) on the second system \( H_{A_{2}} \).

Since Bob’s measurement of the test \( T(M_{s_{o_{v}}}^{A}) \) can be also realized by one-way LOCC on Bob’s space, this test is a \( L(A_{1}, A_{2} \rightarrow B_{1}, B_{2}) \) test. Its POVM is given by

\[
M_{s_{o_{v}}}^{A} = d^{2}(g \otimes g) |u_{1} \otimes u_{2}, v_{1} \otimes v_{2}, 0 \rangle \langle 0 | u_{1} \otimes u_{2}, v_{1} \otimes v_{2}, 0 | v_{1} \otimes v_{2}, 0 \rangle
\]

where we choose \( U_{1} \) and \( U_{2} \) satisfying \( \{ |u_{1} \rangle |u_{2} \rangle \} = \frac{1}{d} \).

Thus, the SU(\( d \))-covariance of \( M_{s_{o_{v}}}^{A} \) guarantees the SU(\( d \))-invariance of the test \( T_{s_{o_{v}}}^{A_{1} \rightarrow A_{2} \rightarrow B_{1} \otimes B_{2}} = T(M_{s_{o_{v}}}^{A}) \), the test \( T_{s_{o_{v}}}^{A_{1} \rightarrow A_{2} \rightarrow B_{1} \otimes B_{2}} \) is \( U(1) \)-invariant. Hence, the inequality

\[
\beta_{0,2, SU(d) \times U(1)} \left( 0 \right) \sigma \leq \Tr T_{s_{o_{v}}}^{A_{1} \rightarrow A_{2} \rightarrow B_{1} \otimes B_{2}} \sigma
\]

holds. On the other hand, the equation

\[
\beta_{0,2, SU(d)} \left( 0 \right) \sigma = \Tr T_{s_{o_{v}}}^{A_{1} \rightarrow A_{2} \rightarrow B_{1} \otimes B_{2}} \sigma
\]

holds. Tsuda et al.[1] have obtained a similar result in the two-dimensional case. Thus,

\[
\beta_{0,2, SU(d)} \left( 0 \right) \sigma = \beta_{0,2, SU(d) \times U(1)} \left( 0 \right) \sigma
\]

Therefore, the test \( T_{s_{o_{v}}}^{A_{1} \rightarrow A_{2} \rightarrow B_{1} \otimes B_{2}} \) is a UMP \( L(A_{1}, A_{2} \rightarrow B_{1}, B_{2}) \) G-invariant test with level-0 for the null hypothesis \( S_{0} \), where \( G = SU(d), SU(d) \otimes U(1) \).
B. $n$-sample setting

Next, we proceed to $n$-sample setting. Since the test $T_{\alpha}^{n,\epsilon,c_{n}} \overset{\text{def}}{=} T_{\epsilon,n}^{n,\epsilon,\alpha,A \rightarrow B,d_{n}}$ is level-$\alpha$ $U(d^{2}-1)$-invariant test with the hypothesis $S_{c_{n}}$ and satisfies the condition of $L(A_{1},\ldots,A_{n} \rightarrow B_{1},\ldots,B_{n})$, the inequality

$$
\beta_{\alpha,n,\epsilon,d_{n}}^{L(A_{1},\ldots,A_{n} \rightarrow B_{1},\ldots,B_{n})}(\leq \|\sigma\|) \\
\leq \text{Tr} T_{\epsilon}^{n,\alpha}\sigma^{\otimes n} = \beta_{n}^{(n)} \left( \leq \frac{d \epsilon}{d + 1} \frac{d p}{d + 1} \right)
$$

(31)

holds. Conversely, as a lower bound of $\beta_{n,n,\epsilon,SU(d)}^{n}(\leq \epsilon\|\sigma\|)$, we obtain

$$
\frac{1}{n} \log \min_{u,u' \mid \|u\| = 1, \|u'\| = 1} \int_{SU(d)} \text{log} d(gu \otimes \overline{u'} | \sigma | gu \otimes \overline{u'}) \nu(dg).
$$

(32)

C. Asymptotic setting

Taking the limit in (31), we obtain

$$
\lim_{\epsilon \rightarrow 0} \beta_{\alpha,n,\epsilon,d_{n}}^{L(A_{1},\ldots,A_{n} \rightarrow B_{1},\ldots,B_{n})}(\leq \|\sigma\|) \\
\leq \beta_{n} \left( \leq \frac{d \epsilon}{d + 1} \frac{d p}{d + 1} \right)
$$

(33)

if $(\phi_{A}^{j}B | \sigma | \phi_{A}^{j}B) = 1 - \frac{\epsilon_{n}}{n}$. Conversely, by using the inequality (32), the compactness of the sets $\{u,u' \mid \|u\| = 1, \|u'\| = 1\}$ and $SU(d)$ yields

$$
\lim_{\epsilon \rightarrow 0} \frac{1}{n} \log \min_{u,u' \mid \|u\| = 1, \|u'\| = 1} \int_{SU(d)} \text{log} d(gu \otimes \overline{u'} | \sigma | gu \otimes \overline{u'}) \nu(dg)
$$

where

$$
T_{u,u'} \overset{\text{def}}{=} \int_{SU(d)} d(gu \otimes \overline{u'})(gu \otimes \overline{u'}) \nu(dg).
$$

Since $T_{u,u'}$ is $SU(d)$-invariant. The test $T_{u,u'}$ has the form $t_{0} |\phi_{A,B}^{0}\rangle \langle \phi_{A,B}^{0}| + t_{1} (I - |\phi_{A,B}^{0}\rangle \langle \phi_{A,B}^{0}|)$. The condition $(\|u\|) = 1$ guarantees that $t_{0} = 1$. The definition of $T_{u,u'}$ guarantees that $\text{Tr} T_{u,u'} \geq d$, which implies $t_{1} \geq \frac{d}{d + 1}$. Hence,

$$
\text{Tr} (I - T_{u,u'}) \sigma \leq \frac{d}{d + 1} \text{Tr} (I - |\phi_{A,B}^{0}\rangle \langle \phi_{A,B}^{0}|) \sigma
$$

(34)

Thus, we have

$$
\lim_{n \rightarrow \infty} \frac{d}{d + 1} \frac{1}{\alpha} \text{log} \beta_{\alpha,n,\epsilon,G}^{S(A_{1},\ldots,A_{n},B_{1},\ldots,B_{n})}(0\|\sigma_{n}) \leq \frac{dt'}{d + 1},
$$

which implies

$$
\lim_{n \rightarrow \infty} \beta_{\alpha,n,\epsilon,G}^{S(A_{1},\ldots,A_{n},B_{1},\ldots,B_{n})}(0\|\sigma_{n}) \geq (1 - \alpha) e^{-\frac{dt'}{d + 1}}.
$$

Combining (33) in the case of $n$, we obtain

$$
\lim_{n \rightarrow \infty} \beta_{\alpha,n,\epsilon,G}^{S(A_{1},\ldots,A_{n},B_{1},\ldots,B_{n})}(0\|\sigma_{n}) = (1 - \alpha) e^{-\frac{dt'}{d + 1}}
$$

for $G = SU(d), SU(d) \times U(1), U(d^{2} - 1), C = S(A_{1},\ldots,A_{n},B_{1},\ldots,B_{n}), L(A_{1},\ldots,A_{n},B_{1},\ldots,B_{n}), L(A_{1},B_{1},\ldots,B_{n})$. Since $(1 - \alpha) e^{-\frac{dt'}{d + 1}} < (1 - \alpha) e^{-\frac{dt'}{d + 1}}$, there is an advantage to use of quantum correlation among samples.

VIII. TWO-SAMPLE TWO-DIMENSIONAL SETTING

Next, we proceed to the special case $n = 2 = d = 2$. For the analysis of this case, we define the $3 \times 3$ real symmetric matrix $V = \{v_{i,j}\} \leq i,j \leq 3$ as

$$
\begin{align*}
\begin{array}{c}
\nu_{i,j} \overset{\text{def}}{=} \Re (\phi_{A,B}^{i} | \sigma | \phi_{A,B}^{j}) \\
\phi_{A,B}^{1} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|10\rangle + |10\rangle), \\
\phi_{A,B}^{2} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (-i|10\rangle + i|10\rangle), \\
\phi_{A,B}^{3} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle).
\end{array}
\end{align*}
$$

When $\sigma$ satisfies the following condition $p \leq \frac{1}{2}$, the equation

$$
\beta_{0,2,SU(3) \times U(1)}^{(0)\|\sigma)}
$$

(35)

holds, where $C = L(A \rightarrow B), L(A \equiv B), S(A \rightarrow B)$. Since the quantity $\text{Tr} \frac{1}{3} V^{2} - (\text{Tr} \frac{I}{3} V)^{2}$ is greater than 0, its $\frac{3}{5}$ times give the advantage of this optimal test against the test introduced in subsection VI.B. Hence, this merit vanish if and only if the real symmetric matrix $V$ is constant. In addition, the optimal test $T$ is given as follows. First, we define a covariant POVM

$$
M_{op}(dg) \overset{\text{def}}{=} 4 \int_{SU(2)} g^{\otimes 2} |u_{op}\rangle \langle u_{op}| (g^{\otimes 2})^{2} \nu(dg),
$$
where the vector $u_{op}$ is defined as

$$u_{op} = \frac{1}{2} \left[(01)_{A_1, A_2} - (10)_{A_1, A_2}\right] + \sqrt{\frac{3}{2}} \left[(00)_{A_1, A_2} + (11)_{A_1, A_2}\right].$$

The relation

$$\beta_{0,2,SU(2)\times U(1)}^C(0||\sigma_{1}\otimes\sigma_{2}) = \text{Tr} T(M_{op})^{0\otimes 2}$$

holds. That is, the test $T(M_{op})$ is the UMP SU(2) $\times$ U(1)-invariant C test with the condition $p \leq \frac{1}{2}$, where $C = L(A \rightarrow B), L(A \leftarrow B), S(A, B)$. On the other hand, the RHS of (30) is calculated as

$$\beta_{0,2,SU(2)}^{L(A_1, A_2 \rightarrow B_1, B_2)}(0||\sigma) = \beta_{0,2,SU(2)\times U(1)}^{L(A_1, A_2 \rightarrow B_1, B_2)}(0||\sigma)$$

$= (1 - \frac{2}{3})^2 - \frac{1}{5} \left(\text{Tr}\frac{I}{3}V^2 - \left(\text{Tr}\frac{I}{3}V\right)^2\right).$ (37)

That is, the quantity $\frac{1}{5} \left(\text{Tr}\frac{I}{3}V^2 - \left(\text{Tr}\frac{I}{3}V\right)^2\right)$ presents the effect of use of classical communication between $A_1$ and $A_2$.

IX. TWO DIFFERENT STATES

In section VI, we showed that if we can prepare the two identical states simultaneously and we can perform Bell measurement on this joint system, the asymptotically optimal test can be realized. However, it is a bit difficult to prepare two identical states simultaneously. However, as is discussed in this section, if we can prepare two quantum states independently, even if they are not identical, this Bell measurement is asymptotically optimal.

A. Formulation

Since the state on $H_{A_1,B}$ can be described as $\sigma_1 \otimes \sigma_2$, our hypotheses are given as

$$H_0: S_{\leq \epsilon}^{2,2} = \left\{\sigma_1 \otimes \sigma_2 \left| \begin{array}{c}
(1 - \langle \phi_{A,B}^0|\sigma_1|\phi_{A,B}^0\rangle) \\
(1 - \langle \phi_{A,B}^0|\sigma_2|\phi_{A,B}^0\rangle) \leq \epsilon
\end{array} \right. \right\}$$

versus

$$H_1: S_{> \epsilon}^{2,2} = \left\{\sigma_1 \otimes \sigma_2 \left| \begin{array}{c}
(1 - \langle \phi_{A,B}^0|\sigma_1|\phi_{A,B}^0\rangle) \\
(1 - \langle \phi_{A,B}^0|\sigma_2|\phi_{A,B}^0\rangle) > \epsilon
\end{array} \right. \right\}. $$

For any group action $G$ introduced in subsection III B, these hypotheses are invariant for $G \times G$-action defined as

$$\phi \mapsto (g_1 \otimes g_2)\phi \quad \forall(g_1, g_2) \in G \times G.$$ 

When only two particles $H_{A_1,B_1} \otimes H_{A_2,B_2}$ are prepared, similarly to subsection IIIC, we can define the quantities $\beta_{0,2,G \times G}^C(\leq \epsilon ||\sigma_1 \otimes \sigma_2)$ for the condition $C = \emptyset, S(A, B), L(A \leftarrow B), L(A \rightarrow B), S(A_1, A_2, B_1, B_2), L(A_1, A_2 \rightarrow B_1, B_2)$, in which, $\sigma_1 \otimes \sigma_2$ means two particles, i.e., there is only one sample of $\sigma_1 \otimes \sigma_2$. When $n$ samples $(\sigma_1 \otimes \sigma_2)^{\otimes n}$ are prepared, we also define the quantities $\beta_{0,2,G \times G}^C(\leq \epsilon ||\sigma_1 \otimes \sigma_2)$ for the condition $C = \emptyset, S(A, B), L(A \leftarrow B), L(A \rightarrow B), S(A_1, A_2, B_1, B_2), L(A_1, A_2, B_1, B_2), L(A_1, A_2 \rightarrow B_1, B_2)$. In this section, we treat the case of one sample and $\epsilon = 0$ case. In the first step, we focus on the case of $C = \emptyset$. In this case, the relations

$$\beta_{0,2,G \times G}^C(0||\sigma_1 \otimes \sigma_2) = (1 - p_1)(1 - p_2) + \frac{p_1p_2}{d^2 - 1}$$

hold for $G = \emptyset, U(1), SU(d) \times U(1), U(d^2 - 1)$, where $p_1 = 1 - \langle \phi_{A,B}^0|\sigma_1|\phi_{A,B}^0\rangle$. Next, we focus on the case of $C = L(A \rightarrow B), L(A \leftarrow B), S(A, B)$. When we use the test $T_{inv}^{A \rightarrow B}$, the second error is

$$\beta(T_{inv}^{A \rightarrow B}, \sigma_1 \otimes \sigma_2) = (1 - p_1)(1 - p_2) + \frac{p_1p_2}{d^2 - 1}.$$ 

Moreover, the optimal second error can also be calculated as

$$\beta_{0,2,G \times G}^C(0||\sigma_1 \otimes \sigma_2) = (1 - p_1)(1 - p_2) + \frac{p_1p_2}{d^2 - 1}$$

for $C = L(A \rightarrow B), L(A \leftarrow B), S(A, B)$ when $\frac{p_1p_2}{d^2 - 1} \leq (1 - p_1)p_2, p_1(1 - p_2)$. Hence, the test $T_{inv}^{A \rightarrow B}$ is the C-UMP G-invariant test. Using the PPT condition, Tsuda et al.[1] derived this optimal test in the case of $\sigma_1 = \sigma_2, d = 2$.

Finally, we proceed to the case of $C = L(A_1, A_2 \rightarrow B_1, B_2), L(A_1, A_2, B_1, B_2), S(A_1, A_2, B_1, B_2)$. When we use the test $T_{inv}^{A \rightarrow B_1} \otimes T_{inv}^{A \rightarrow B_2}$, the second error is

$$\beta(T_{inv}^{A \rightarrow B_1} \otimes T_{inv}^{A \rightarrow B_2}, \sigma_1 \otimes \sigma_2)$$

$$= \left(1 - \frac{dp_1}{d+1}\right) \left(1 - \frac{dp_2}{d+1}\right),$$

the optimal second error is calculated as

$$\beta_{0,2,G \times G}^C(0||\sigma_1 \otimes \sigma_2) = \left(1 - \frac{dp_1}{d+1}\right) \left(1 - \frac{dp_2}{d+1}\right),$$

for $G = SU(d), SU(d) \times U(1), U(d^2 - 1)$. Thus, the test $T_{inv}^{A \rightarrow B_1} \otimes T_{inv}^{A \rightarrow B_2}$ is the C-UMP G-invariant test. Tsuda et al.[1] derived this optimal test in the case of $\sigma_1 = \sigma_2, d = 2$. 
C. Asymptotic setting

In the small deviation asymptotic setting with $n$ samples, we focus on the case $\epsilon = \frac{\delta}{n}$ and $\frac{1}{n} = 1 - \langle \phi_{A,B} | \sigma_{1,n} | \phi_{A,B} \rangle$.

$$\lim \beta(\mathcal{G}, \mathcal{H}_{\Lambda_{1}} \otimes \mathcal{H}_{B_{1}}, k) = \beta(1 - \delta | \epsilon'_{1} + \epsilon'_{2}).$$

for $G = U(1), SU(d) \times U(1), U(d^2 - 1)$.

Next, we consider the case of $C = L(A \rightarrow B)$. When we perform the test $T_{\text{inv}}^{A \rightarrow B}$ for all systems $\mathcal{H}_{A_{1}} \otimes \mathcal{H}_{B_{1}}, \ldots, \mathcal{H}_{A_{n}} \otimes \mathcal{H}_{B_{n}}$, whose state is $\sigma_{1,n} \otimes \sigma_{2,n}$, the number $k$ of detecting $T_{\text{inv}}^{A \rightarrow B}$ almost obeys the Poisson distribution $e^{-\left( (1 - \frac{\delta}{n}) \epsilon_{1} + \frac{1}{n} \epsilon_{2} \right)}$. This is because

$$n \left( 1 - (1 - \frac{\delta}{n}) \epsilon_{1} + \frac{1}{n} \epsilon_{2} \right) \rightarrow \epsilon_{1} + \epsilon_{2}.$$  

Treating the hypothesis testing of this Poisson distribution, we can show that the $L(A \rightarrow B) U(d^2 - 1) \times U(d^2 - 1)$-invariant test $T_{\text{inv},2}^{A \rightarrow B}$ satisfies

$$\lim \beta(T_{\text{inv},2}^{A \rightarrow B}, \sigma_{1,n} \otimes \sigma_{2,n}) = \beta(1 - \delta | \epsilon'_{1} + \epsilon'_{2}).$$

Hence, combining (40), we obtain

$$\lim \beta_{C}(\mathcal{G}, \mathcal{H}_{\Lambda_{1}} \otimes \mathcal{H}_{B_{1}}, \mathcal{H}_{C_{1}} \otimes \mathcal{H}_{C_{2}}) = \beta(1 - \delta | \epsilon_{1} + \epsilon_{2}).$$

for $C = G, L(A \rightarrow B), L(A \leftrightarrow B), S(A, B), G = SU(d) \times U(1), U(d^2 - 1)$. Therefore, the test $T_{\text{inv},2}^{A \rightarrow B}$ is C-UMP invariant test in the asymptotic small deviation setting.

Moreover, if we use the test based on the Bell measurement in stead of the test $T_{\text{inv},2}^{A \rightarrow B}$, the bound $\beta(1 - \delta | \epsilon_{1} + \epsilon_{2})$ can be attained because a lemma similar to Lemma 5 holds.

X. THREE DIFFERENT STATES

Finally, we treat the case of three quantum states that are prepared independently. Similarly to section IX A, we put two hypotheses

$$H_{0} : S_{\leq \epsilon}^{3} \equiv \left\{ \sum_{i=1}^{3} \sigma_{i} \left| \sum_{i=1}^{3} \langle \phi_{A_{i},B_{i}} | \sigma_{i} | \phi_{A_{i},B_{i}} \rangle \leq \epsilon \right. \right\}$$

versus

$$H_{1} : S_{\geq \epsilon}^{3} \equiv \left\{ \sum_{i=1}^{3} \sigma_{i} \left| \sum_{i=1}^{3} \langle \phi_{A_{i},B_{i}} | \sigma_{i} | \phi_{A_{i},B_{i}} \rangle \geq \epsilon \right. \right\},$$

where the given state is assumed to be $\sigma_{1} \otimes \sigma_{2} \otimes \sigma_{3}$. Similarly we define the quantities $\beta_{C}(\mathcal{G}, \mathcal{H}_{\Lambda_{1}} \otimes \mathcal{H}_{B_{1}}, \mathcal{H}_{C_{1}} \otimes \mathcal{H}_{C_{2}}) \leq \epsilon \sigma_{1} \otimes \sigma_{2} \otimes \sigma_{3}$ for the condition $C = G, S(A, B), L(A \rightarrow B), L(A \leftrightarrow B), L(A_{1}, A_{2}, A_{3}, B_{1}, B_{2}, B_{3})$. For $C = L(A \rightarrow B), L(A \leftrightarrow B), S(A, B)$ we require the similar $G \times G$-invariance.

Similarly to subsection IX B, we focus on the case of

$$C = L(A \rightarrow B), L(A \leftrightarrow B), S(A, B) \text{ with one sample.}$$

In this case, as is mentioned, the GHZ state $|GHZ\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{A_{1}} |i\rangle_{A_{2}} |i\rangle_{A_{3}}$ plays an important role. Since the $SU(d) \times SU(d) \times SU(d)$-action on $\mathcal{H}_{A_{1}} \otimes \mathcal{H}_{A_{2}} \otimes \mathcal{H}_{A_{3}}$, is irreducible, the following is a POVM:

$$M_{c}^{3}(d_{1}, d_{2}, d_{3})$$

$$\frac{1}{d^{3}} C_{L(A \rightarrow B), L(A \leftrightarrow B), S(A, B)}.$$
which is difficult to realize. In this section, we seek finite-valued POVMs on Alice’s space realizing the desired test instead of infinite-valued measurements.

A. Design for the test $T^{1,A\rightarrow B}_{\text{inv}}$

In order to design the test $T^{1,A\rightarrow B}_{\text{inv}}$, 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:

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

(43)

Currently, an SIC-POVM analytically is constructed when the dimension $d$ is $2,3[23,25,4\{22,25\}],5[25,6\{24,7\},8\{23\},19\{26\}]$. Also, its existence is numerically verified up to $d = 45[22]$. Any SIC-POVM $M_{\text{sic}} = \{p_i|u_i\rangle\langle u_i|\}$, satisfies

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

(44)

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

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

the inequality

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

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

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

if there exists an SIC-POVM on $\mathbb{C}^d$.

However, any SIC-POVM is not a randomized combination of projection valued measures as well as a projection valued measure. Since projection valued measures are more realizable than other POVM, it is more desired to design Alice’s POVM as a randomized combination of projection valued measures. 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[27] or a prime power[28]. Bandyopadhyay et al. gave a more explicit form in these cases [29]. Any mutually unbiased bases $\{B_1, \ldots, B_{d+1}\}$ make the POVM $M_{B_1, \ldots, B_{d+1}}$, i.e.,

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

where $B_j = \{u_{ij}, \ldots, u_{jd}\}$. This POVM always produces the desired test $T^{1,A\rightarrow B}_{\text{inv}}$ as

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

(45)

This construction of the test $T^{1,A\rightarrow B}_{\text{inv}}$ 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

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

(46)

Then,

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

(47)

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

$$\min_{M_j \text{POVM}} \#\{j\} \left| T^j \left( \sum p_j M_j \right) = T^{1,A\rightarrow B}_{\text{inv}} \right\} = d + 1$$

if $d$ is a prime or a prime power.

B. Design for $T^{2,A\rightarrow B}_{\text{inv}}$

Next, we proceed to the construction of the test $T^{2,A\rightarrow B}_{\text{inv}}$. Let $f$ be an irreducible action of group $G$ acts to $\mathcal{H}_{A_1} = \mathbb{C}^d$. 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 of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Since the irreducibility of the action $f$ guarantees that

$$\left| \sum_{g \in G} \langle k|f(g)|l\rangle\langle l'|f(g)|k'\rangle \right|^2$$

we obtain

$$\left| \sum_{k,l} \sum_{g \in G} a_{k,l} E_{k,l} f(g) \right|^2$$

Next, we proceed to the construction of the test $T^{2,A\rightarrow B}_{\text{inv}}$. Let $f$ be an irreducible action of group $G$ acts to $\mathcal{H}_{A_1} = \mathbb{C}^d$. 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 of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Since the irreducibility of the action $f$ guarantees that

$$\left| \sum_{g \in G} \langle k|f(g)|l\rangle\langle l'|f(g)|k'\rangle \right|^2$$

we obtain

$$\left| \sum_{k,l} \sum_{g \in G} a_{k,l} E_{k,l} f(g) \right|^2$$

Next, we proceed to the construction of the test $T^{2,A\rightarrow B}_{\text{inv}}$. Let $f$ be an irreducible action of group $G$ acts to $\mathcal{H}_{A_1} = \mathbb{C}^d$. 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 of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Since the irreducibility of the action $f$ guarantees that

$$\left| \sum_{g \in G} \langle k|f(g)|l\rangle\langle l'|f(g)|k'\rangle \right|^2$$

we obtain

$$\left| \sum_{k,l} \sum_{g \in G} a_{k,l} E_{k,l} f(g) \right|^2$$

Next, we proceed to the construction of the test $T^{2,A\rightarrow B}_{\text{inv}}$. Let $f$ be an irreducible action of group $G$ acts to $\mathcal{H}_{A_1} = \mathbb{C}^d$. 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 of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$. Since the irreducibility of the action $f$ guarantees that

$$\left| \sum_{g \in G} \langle k|f(g)|l\rangle\langle l'|f(g)|k'\rangle \right|^2$$

we obtain

$$\left| \sum_{k,l} \sum_{g \in G} a_{k,l} E_{k,l} f(g) \right|^2$$
which implies
\[
\frac{d^2}{|G|} \sum_{g \in G} \left| \frac{1}{\sqrt{d}} f(g) \right\rangle \left\langle \frac{1}{\sqrt{d}} f(g) \right| = \mathbb{I}_{A_1, A_2}.
\]
Hence, \( M_f = \left\{ \frac{d^2}{|G|} \left| \frac{1}{\sqrt{d}} f(g) \right\rangle \left\langle \frac{1}{\sqrt{d}} f(g) \right| \right\}_{g \in G} \) is a POVM.

Furthermore, we assume that the action \( f \otimes \overline{f} \) of \( G \) to \( \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \) has only two irreducible components, i.e., the irreducible subspaces of \( \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \) are only the one-dimensional space \( \phi^{0}_{A_1, A_2} \) and its orthogonal space \( \phi^{0}_{A_1, A_2} \perp \). In this case, The test \( T(M_f) \) satisfies
\[
T(M_f) = T^{A \rightarrow B}_{\text{inv}}.
\]
In particular, the action of Clifford group on \( \mathbb{C}^d \) satisfies this condition when \( d \) is prime[26]. Hence, we can construct a finite-valued POVM producing the test \( T^{A \rightarrow B}_{\text{inv}} \).

\[\text{XII. CONCLUSION}\]

In this paper, we treated the hypotheses testing problem when the null hypothesis consists only of the required entangled state or is its neighborhood. In order to treat the structure of entanglement, we consider three settings concerning the range of accessible measurements as follows: M1: All measurement is allowed. M2: A measurement is forbidden if it requires the quantum correlation between two distinct parties. M3: A measurement is forbidden if it requires the quantum correlation between two distinct parties, or that among local samples. As a result, we found that there is difference between the accuracies of M1 and M2 in the first order asymptotics. The protocol achieving the asymptotic bound has been proposed in the setting M2. In this setting, it is required to prepare two identical samples at the same time. However, it is difficult to keep their colinearity. In order to avoid this difficulty, we proved that even if they do not coincide, this proposed protocol works effectively. In particular, this protocol can be realized in the two-dimensional system if the four-valued Bell measurement can be realized. Moreover, concerning the finite samples case, we derived optimal testing in several examples.

In this paper, the optimal test is constructed based on continuous valued POVM. However, any realizable POVM is finite valued.

The obtained protocol is essentially equivalent with the following procedure based on the quantum teleportation.

First, we perform quantum teleportation from the system \( A \) to the system \( B \), which succeed when the true state is the required maximally entangled state. Next, we check whether the state on the system \( B \) is the initial state on the system \( A \). Hence, an interesting relation between the obtained results and the quantum teleportation is expected, and it will be treated in another forthcoming paper [33].

As a related research, the following testing problem has been discussed [30, 31]. Assume that \( N \) qubits state are given, and we can measure only \( M \) qubits. The required problem is testing whether the remaining \( N - M \) qubits are the desired maximally entangled state. Indeed, this problem is important not only for guarantee of the quality of the prepared maximally entangled state, but also for the security for the quantum key distribution. The problem discussed in this paper is different from the preceding problem in testing the given state by measuring the whole system. In order to apply our result to the preceding problem, we have to randomly choose \( M \) qubits among the given \( N \) qubits, and test the \( N \) qubits. When the given \( N \) qubits do not satisfy the independent and identical condition, their method [30, 31] is better than our method. Since their method [30, 31] requires the quantum correlation among whole \( M \) qubits, it is difficult to realize their method for testing the prepared maximally entangled state, but it is possible to apply their method to testing the security of quantum key distribution [30]. This is because the maximally entangled state is only virtually discussed in the latter case. Hence, for testing the prepared maximally entangled state, it is natural from the practical viewpoint to restrict our test among random sampling method. Since our results can be applied this setting, they can be expected to be applied to the check of the quality of maximally entangled state.

As another problem, Acin et al. [5] discussed the problem testing whether the given \( n \)-i.i.d. state of the unknown pure state is the \( n \)-tensor product of a pure maximally entangled state (not the specific maximally entangled state) in the two-dimensional system. Its \( d \)-dimensional case is discussed in Matsumoto and Hayashi [32], and this problem is closely related to universal entanglement concentration.

This problem is different from our setting, but is very important. Hence, it is needed to discuss this setting with the mixed state case.

local positive-operator-valued measures under symmetry," 

[22] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, 
"Symmetric Informationally Complete Quantum Measurements," 


