Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing

Masahito Hayashi
Graduate School of Information Sciences, Tohoku University,
Aoba-ku, Sendai, 980-8579, Japan
E-mail: hayashi@math.is.tohoku.ac.jp

New Journal of Physics 11 (2009) 043028 (57pp)
Received 24 December 2008
Published 24 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/043028

Abstract. In an asymptotic setting, an optimal test for hypothesis testing of the maximally entangled state is derived under several locality conditions for measurements. The optimal test is obtained in several cases within the asymptotic framework as well as for the finite sample situation. In addition, an experimental scheme for the optimal test is presented.

Contents
1. Introduction 3
2. Mathematical formulation of quantum hypothesis testing 5
3. Our formulations 6
   3.1. Hypothesis 6
   3.2. Restriction I: group action 7
   3.3. Restriction II: locality 8
4. Testing for binomial distributions 11
   4.1. One-sample setting 11
   4.2. n-sample setting 11
   4.3. Asymptotic setting 12
5. Global tests 14
   5.1. One sample setting 14
   5.2. n-sample setting 14
   5.3. Asymptotic setting 15
6. A–B locality
   6.1. Construction of one-way LOCC test ........................................... 16
   6.2. One sample setting ................................................................. 17
   6.3. Two-sample case ................................................................. 19
   6.4. \( n \)-sample setting ............................................................. 20
   6.5. Asymptotic setting ............................................................... 21
7. A–B locality and sample locality .................................................. 22
   7.1. Two-sample setting ................................................................. 22
   7.2. \( n \)-sample setting ............................................................... 23
   7.3. Asymptotic setting ............................................................... 23
8. Two-sample two-dimensional setting ............................................. 25
9. Two different systems .................................................................... 26
   9.1. Formulation ............................................................................. 26
   9.2. One sample setting ................................................................. 26
   9.3. Asymptotic setting ............................................................... 27
10. Three different systems ................................................................. 28
11. Conclusion .................................................................................. 29
Acknowledgments ............................................................................. 30
Appendix A. Proof of lemmas 1 and 2 .................................................. 30
Appendix B. Basic properties of classical tests ..................................... 32
Appendix C. Proof of proposition 1 .................................................... 33
Appendix D. Proof of proposition 2 .................................................... 33
Appendix E. Proof of (9) .................................................................. 34
Appendix F. Proof of lemma 3 ........................................................... 35
Appendix G. Proof of lemma 4 ........................................................... 36
Appendix H. Proof of (15) ................................................................. 37
Appendix I. Proof of (22) ................................................................. 37
Appendix J. Proof of lemma 5 and (24) .............................................. 38
Appendix K. Proof of (34) ................................................................. 39
Appendix L. Proof of the \( U(1) \)-invariance of \( T_{\text{inv}}^{1\rightarrow 2} \) .......... 39
Appendix M. Proof of (35) ................................................................. 40
Appendix N. Proof of (37) ................................................................. 43
Appendix O. Proof of (41) and (40) .................................................... 44
Appendix P. Proof of (42) ................................................................. 51
Appendix Q. Proof of (44) ................................................................. 51
Appendix R. Proof of (45) ................................................................. 52
Appendix S. Proof of (46) ................................................................. 53
Appendix T. Proof of (47) and (48) .................................................... 53
References .................................................................................. 56
1. Introduction

Recently, various methods for quantum information processing have been proposed. Many of them require the use of maximally entangled states [1]–[3]. Hence, it is often desirable to be able to generate maximally entangled states experimentally. If this is done, statistical techniques are necessary to decide whether the state generated experimentally is really the required maximally entangled state.

Currently, the method ‘entanglement witness’ is often used as the standard method [4]–[8]. However, from a statistical viewpoint, this is not necessarily the optimal method. In mathematical statistics, the decision problem for the truth of a given hypothesis is called statistical hypothesis testing, and it has been systematically studied. Hence, we wish to investigate the problem of deciding whether a given quantum state is the required maximally entangled state in this framework of statistical hypotheses testing. In statistical hypotheses testing, we suppose given two hypotheses (the null and alternative hypotheses) to be tested, we assume that one of these is true. Based on observed data, we decide which hypothesis is true. Most earlier studies utilizing quantum hypothesis testing have used only simple hypothesis testing; that is, they have assumed that both the null and the alternative hypothesis each consist of a single quantum state. For example, the quantum Neyman–Pearson lemma [9, 10], the quantum version of Stein’s lemma [11]–[14], the quantum Chernoff bound [15, 16] and the quantum Hoeffding bound [17]–[19] all deal with simple hypotheses.

However, from a practical standpoint, it is unnatural to specify either hypothesis using a single quantum state. Hence, we cannot directly apply the quantum Neyman–Pearson theorem and the quantum Stein’s lemma; we have to utilize composite hypotheses, i.e. the case where both hypotheses consist of plural quantum states. It is also necessary to restrict our measurements for testing among measurements based on local operations and classical communications (LOCC) because the state to be tested is a maximally entangled state.

Recently, based on quantum statistical inference [10, 20, 21], Hayashi et al [22] discussed this testing problem in the context of statistical hypothesis testing with a locality condition. They treated a testing problem where the null hypothesis consists only of the required maximally entangled state. Their analysis has been extended to a more experimental setting [23], and its effectiveness has been experimentally demonstrated [24]. Modifying this setting, Owari and Hayashi [25] clarified the difference in performance between the one-way LOCC restriction and the two-way LOCC restriction in a specific case. In particular, Hayashi et al [22] studied the optimal test and the existence of a uniformly optimal test (whose definition will be presented later) when one or two samples of the state to be tested are provided. Their analysis mainly concentrated on the two-dimensional case.

In this paper, we treat null hypothesis testing of quantum states whose fidelity for the desired maximally entangled state is not greater than \( \epsilon \), and discuss this testing problem in three settings, for several given samples of the tested state in the range of our measurements. (Note that our previous paper [22] treats the case of \( \epsilon = 0 \).) We remark that, for this problem, there are two kinds of locality restriction: \( L_1 \), one is the locality of the two distinct parties; \( L_2 \), the second concerns the locality of the samples. The three settings are as follows: \( M_1 \), all measurements are allowed; \( M_2 \), there is restriction on the locality \( L_1 \), but not on the locality \( L_2 \); \( M_3 \), there is restriction on the locality \( L_2 \) as well as on \( L_1 \). The restriction \( M_3 \) for measurement was first discussed by Virmani and Plenio [28]. Hayashi et al [22] treated the settings \( M_2 \) and \( M_3 \) more systematically.
This paper mainly deals with the case of sufficiently many samples, i.e. the first-order asymptotic theory. In this context, we find that there is no difference in performance between settings $M_1$ and $M_2$ in an asymptotic framework, i.e. in the case when the fidelity between the true state and the target maximally entangled state is parameterized as $1 - (\delta/n)$, where $n$ is the number of samples of the prepared unknown state (theorem 3), whereas Hayashi et al [22] and Virmani and Plenio [28] did not treat such an asymptotic framework. In particular, the test achieving asymptotically optimal performance can be realized by quantum measurement with quantum correlations between only two samples in respective parties, as is illustrated in figure 1. That is, even if we use higher quantum correlations among samples in respective parties, no further improvement is available within the first-order asymptotic framework. In the two-dimensional case, the required measurement with quantum correlations in respective parties is the four-valued Bell measurement between the two samples in both the parties. In the setting $M_3$, we treat the null hypothesis consisting only of the maximally entangled state. Then, it can be proved that even if we use classical correlation between samples in respective parties, there is no further improvement (theorem 5). That is, the optimal protocol can be realized by repeating the optimal measurement in the one sample case in the setting $M_3$.

Concerning the non-asymptotic setting, we derive the optimal test with an arbitrary finite number of samples under a suitable group symmetry without any locality condition (theorem 1). This result can be trivially extended to hypothesis testing of arbitrary pure states. Moreover, we derive the optimal test with two samples under several conditions, and calculate its optimal performance (theorems 4 and 6).

We also consider the case when each sample system consists of two or three different quantum systems whose state is a tensor product state of different states. In this case, even if we have just one sample, every party consists of multiple systems. In this situation, we obtain the optimal test for the one-sample case in both settings $M_2$ and $M_3$. It is proved that repeating the optimal measurement for one sample yields a test achieving asymptotically optimal performance (theorem 8). Moreover, when each sample system consists of two different

Figure 1. Asymptotic optimal testing scheme when $2n$ identical copies are given.
systems, we show that the optimal measurement for the one-sample case can be realized by a four-valued Bell measurement on the respective parties (theorem 7). Repeating this measurement yields the optimal performance in the first-order asymptotic framework. (In fact, it is difficult to perform the quantum measurement with quantum correlation between two samples because we need to prepare two samples from the same source at the same time. However, in this formulation, it is sufficient to prepare two states from different sources.) When each sample system consists of three different systems, the optimal measurement can be described by the Greenberger–Horne–Zeilinger (GHZ) state \((1/\sqrt{d}) \sum_i |i\rangle|i\rangle\), where \(d\) is the dimension of the system (theorem 9). This fact seems to indicate the importance of the GHZ state for the three systems.

Concerning locality restrictions on our measurements, it is natural to treat two-way LOCC, but we treat one-way LOCC and separable measurements, because the separability condition is easier to treat than two-way LOCC. We generally assume separability in this paper, as it is a useful mathematical condition. In contrast, Virmani and Plenio [28] and Hayashi et al [22] used the positive partial transpose (PPT) condition as well as the separability condition.

This paper is organized as follows. The mathematical formulation of statistical hypothesis testing is presented in section 2 and, the group theoretical symmetry is explained in section 3.2. In section 3.3, we explain the restrictions of our measurement for our testing, for example, one-way LOCC, two-way LOCC, separability, etc. In section 4, we review the fundamentals of statistical hypothesis testing for probability distributions. In section 5 (sections 6 and 7), the settings M1 (M2 and M3) are discussed, respectively. Further results for the two-dimensional case are presented in section 8. Finally, in sections 9 and 10, we discuss the cases of two and three different quantum states, respectively.

2. 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 quantum hypothesis testing, it is assumed that the current state \(\rho\) of the system is unknown, but that the system is known to belong to a subset \(\mathcal{S}_0\) or \(\mathcal{S}_1\) of the set of densities. Hence, our task is testing

\[
H_0 : \rho \in \mathcal{S}_0 \quad \text{versus} \quad H_1 : \rho \in \mathcal{S}_1
\]

(1)
based on an appropriate measurement of \(\mathcal{H}\). That is, we are required to decide which hypothesis is true. We call \(H_0\) the null hypothesis, and we call \(H_1\) the alternative hypothesis.

A test for the hypothesis (1) is given by a positive operator valued measure (POVM) on \(\mathcal{H}\) composed of two elements, \(\{T_0, T_1\}\), 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 made based on this test as follows: we accept \(H_0\) (=we reject \(H_1\)) if we observe \(T_0\), and we accept \(H_1\) (=we reject \(H_0\)) if we observe \(T_1\). In order to treat performance, we focus on the following two kinds of errors: a type 1 error is an event for which we accept \(H_1\) though \(H_0\) is true. A type 2 error is an event for which 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

\[
\alpha(T, \rho) = \text{Tr}(\rho T_1) = 1 - \text{Tr}(\rho T)(\rho \in \mathcal{S}_0),
\]

\[
\beta(T, \rho) = \text{Tr}(\rho T_0) = \text{Tr}(\rho T)(\rho \in \mathcal{S}_1).
\]

The quantity \(1 - \beta(T, \rho)\) is called power. A test \(T\) is said to be at level-\(\alpha\) if \(\alpha(T, \rho) \leq \alpha\) for any \(\rho \in \mathcal{S}_0\).
In hypothesis testing, we restrict our attention to tests whose first error probability is smaller than a given constant $\alpha$ for any element $\rho \in S_0$. That is, since a type 1 error is considered to be more serious than a type 2 error in hypothesis testing, it is necessary to ensure that the type 1 error probability is less than a constant, which is called the level of significance or simply level. Hence, a test $T$ is said to be of 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 the power of the test. Therefore, we often optimize the type 2 error probability as follows:

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

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

for any $\rho \in S_1$. In particular, a test $T \in T_{\alpha,S_0}$ is called a most powerful (MP) test of 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,

$$\beta(T, \rho) = \beta_t(S_0\|\rho).$$

Moreover, a test $T \in T_{\alpha,S_0}$ is called a uniformly most powerful (UMP) test if $T$ is MP for any level-$\alpha$ test $\rho \in S_1$, that is,

$$\beta(T, \rho) = \beta_t(S_0\|\rho), \quad \forall \rho \in S_1.$$

However, in certain instances, it is natural to restrict our tests 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 instead of $\beta(T, \rho)$:

$$\beta^{C_2}_{\alpha,C_1}(S_0\|\rho) \overset{\text{def}}{=} \min_{T \in T_{\alpha,S_0}} \{ \beta(T, \rho) \mid T \text{ satisfies } C_1 \text{ and } C_2 \}.$$

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

$$\beta(T, \rho) = \beta^{C_2}_{\alpha,C_1}(S_0\|\rho), \quad \forall \rho \in S_1,$$

it is called a uniformly most powerful $C_1, C_2$ (UMP $C_1, C_2$) test.

### 3. Our formulations

#### 3.1. Hypothesis

Our aim is to test whether the generated state is sufficiently close to the maximal entangled state

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

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 $\sigma_1, \ldots, \sigma_n$ are all equal to a particular density $\sigma$. In this case, the state $\rho$ is called $n$-independent and identically distributed (n-i.i.d.). In the following, we consider two settings for our hypotheses:

$$H_0 : \quad \sigma \in S_{\leq \epsilon} \overset{\text{def}}{=} \{ \sigma | 1 - \langle \phi_{AB}^0 | \sigma | \phi_{AB}^0 \rangle \leq \epsilon \}$$

versus

$$H_1 : \quad \sigma \in S_{\leq \epsilon}^c$$

and

$$H_0 : \quad \sigma \in S_{\geq \epsilon} \overset{\text{def}}{=} \{ \sigma | 1 - \langle \phi_{AB}^0 | \sigma | \phi_{AB}^0 \rangle \geq \epsilon \}$$

versus

$$H_1 : \quad \sigma \in S_{\geq \epsilon}^c.$$

When the null hypothesis is ‘$\sigma \in S_{\leq \epsilon}$’, the set of level $\alpha$-tests is given in the $n$-fold i.i.d. case by

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

Similarly, when the null hypothesis is ‘$\sigma \in S_{\geq \epsilon}$’, the set of level $\alpha$-tests is given in the $n$-fold i.i.d. case by

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

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

3.2. Restriction I: group action

In this paper, we treat these two cases under invariance conditions for the following group actions, which preserve the two hypotheses $H_0$ and $H_1$. The naturalness of these conditions 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

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

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, since this invariance yields easier treatment, it is often adopted only for technical reasons.

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

\[ U(g) \overset{\text{def}}{=} g \otimes \overline{g} \]

and \( \overline{g} \) is the complex conjugate of \( g \) with respect to 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 \( SU(d) \)-action is so small that it will be adopted only for technical reasons.

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 to take as our restriction.

4. \( U(d^2-1) \)-action: as a stronger form of invariance, we can consider 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 includes the \( U(1) \)-action and the \( SU(d) \)-action. Hence, invariance with respect to the \( U(d^2-1) \)-action is stronger than invariance with respect to the preceding three actions. However, this action does not preserve the entanglement property. Thus, based on this definition, we cannot say that this condition is natural for our setting, whereas it is natural if we do not care about entanglement.

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

3.3. 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 on the locality condition. In section 4, as a first step, in order to discuss hypothesis testing with the null hypothesis \( S_{\leq \epsilon} \), we will treat the following optimization:

\[ \beta_{\epsilon, G}(\leq \epsilon \| \sigma) \overset{\text{def}}{=} \min_{T \in \mathcal{T}_{\epsilon, \leq \epsilon}} \{ \beta(T, \sigma^{\otimes n}) | T \text{ is } G\text{-invariant} \}, \]
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 systems, 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

$S(A, B)$: the test is separable between the two systems $\mathcal{H}_A \otimes \mathcal{H}_B$, 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 $\mathcal{H}_A \otimes \mathcal{H}_B$, respectively.

$L(A \rightleftharpoons B)$: the test can be realized by two-way LOCC between the two systems $\mathcal{H}_A \otimes \mathcal{H}_B$.

$L(A \rightarrow B)$: the test can be realized by one-way LOCC from the system $\mathcal{H}_A$ to the system $\mathcal{H}_B$.

$S(A_1, \ldots, A_n, B_1, \ldots, B_n)$: the test is separable among the $2n$ 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:

$$T = \sum_i a_i T_i^{A_1} \otimes \cdots \otimes T_i^{A_n} \otimes T_i^{B_1} \otimes \cdots \otimes T_i^{B_n},$$

where $a_i \geq 0$ and the matrix $T_i^{A_i} (T_i^{B_i})$ is a positive semi-definite matrix on the system $\mathcal{H}_{A_i} \otimes \mathcal{H}_{B_i}$, respectively.

$L(A_1, \ldots, A_n, B_1, \ldots, B_n)$: the test can be realized by two-way LOCC among the $2n$ systems $\mathcal{H}_{A_1}, \ldots, \mathcal{H}_{A_n}$ and $\mathcal{H}_{B_1}, \ldots, \mathcal{H}_{B_n}$.

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

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

$$\beta^C_{\epsilon, \sigma} \triangleq \min_{T \in \mathcal{T}_{\epsilon, \sigma}} \beta(T, \sigma^\oplus) \quad \text{where} \quad T \text{ is } G\text{-invariant and satisfies } C.$$

As can be easily checked, any LOCC operation is separable. Hence, the condition $L(A \rightleftharpoons B)$ 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 relations among these conditions can be illustrated as follows:

$$L(A_1, \ldots, A_n \rightarrow B_1, \ldots, B_n) \Rightarrow L(A \rightarrow B),$$

$$L(A_1, \ldots, A_n \rightarrow B_1, \ldots, B_n) \Rightarrow L(A \rightleftharpoons B),$$

$$S(A_1, \ldots, A_n, B_1, \ldots, B_n) \Rightarrow S(A, B).$$
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
\[
\beta_{a,n,G_1}^C (\leq \epsilon \| \sigma \|) \geq \beta_{a,n,G_2}^C (\leq \epsilon \| \sigma \|) \tag{2}
\]
holds. Moreover, if a condition $C_1$ is stronger than another condition $C_2$, a similar inequality
\[
\beta_{a,n,G}^C (\leq \epsilon \| \sigma \|) \geq \beta_{a,n,G}^{C_2} (\leq \epsilon \| \sigma \|) \tag{3}
\]
holds.

Similarly, we define $\beta_{a,n,G}^C (\geq \epsilon \| \sigma \|)$ by replacing $\leq \epsilon$ by $\geq \epsilon$ on the RHS. When $\epsilon = 0$, $\beta_{a,n,G}^C (\leq \epsilon \| \sigma \|)$ is abbreviated to $\beta_{a,n,G}^C (0 \| \sigma \|)$.

Indeed, if a condition is invariant under 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 tests satisfying the condition $C$ is invariant under the action of $G$. Then

\[
\beta_{a,n,G}^C (\leq \epsilon \| \sigma \|) = \min_{T \in T_n \leq \epsilon} \max_{g \in G} \beta(T, (f(g)\sigma f(g)^+) \otimes^n)
\]

\[
= \min_{T \in T_n \leq \epsilon} \int_{G} \beta(T, (f(g)\sigma f(g)^+) \otimes^n) \nu_G(dg),
\]

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 $\nu$. For a proof see appendix A. This lemma is a special version of the quantum Hunt–Stein lemma [20]. The condition $\emptyset$ is invariant with respect to the actions $U(1)$, $SU(d)$, $SU(d) \times U(1)$ and $U(d^2 - 1)$. However, other conditions $S(A, B)$, $L(A \Rightarrow B)$, $L(A \rightarrow B)$, $S(A_1, \ldots, A_n, B_1, \ldots B_n)$, $L(A_1, \ldots, A_n, B_1, \ldots B_n)$ and $L(A_1, \ldots, A_n \rightarrow B_1, \ldots B_n)$ are invariant only with respect to $SU(d)$. Hence, lemma 1 cannot be applied to a pair of these conditions and the actions $U(1)$, $SU(d) \times U(1)$ and $U(d^2 - 1)$. The following lemma is useful in such a case.

**Lemma 2.** Assume that the group $G_1$ includes another group $G_2$ as a subgroup and the subgroup $G_2$ satisfies the condition of lemma 1. If

\[
\beta_{a,n,G_1}^C (\leq \epsilon \| \sigma \|) = \beta_{a,n,G_2}^C (\leq \epsilon \| \sigma \|), \quad \forall \sigma
\]

then

\[
\beta_{a,n,G_1}^C (\leq \epsilon \| \sigma \|) = \min_{T \in T_n \leq \epsilon} \max_{g \in G_1} \beta(T, (f(g)\sigma f(g)^+) \otimes^n)
\]

\[
= \min_{T \in T_n \leq \epsilon} \int_{G_1} \beta(T, (f(g)\sigma f(g)^+) \otimes^n) \nu_{G_1}(dg).
\]

The proof is given in appendix A.
4. Testing for binomial distributions

In this paper, we use several facts about testing for binomial distributions, in order to test for a maximally entangled state. Hence, we review them here.

4.1. 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 probability $p$ and the event 0 happens with probability $1 - p$, and focus on the null hypothesis $p \in [0, \epsilon]$. In this case, our test can be described by a map $\tilde{T}$ from $\{0, 1\}$ to $[0, 1]$, which means that when the data $k$ is observed, we accept the null hypothesis with probability $\tilde{T}(k)$. Then, the minimum second error probability among level-$\alpha$ tests is given by

$$
\beta^1_{\alpha}(\leq \epsilon \| q) = \min_{\tilde{T}} \left\{ q(\tilde{T}) \mid \forall p \in [0, \epsilon], p(\tilde{T}) \geq 1 - \alpha \right\},
$$

$$p(\tilde{T}) \overset{\text{def}}{=} (1 - p)\tilde{T}(0) + p\tilde{T}(1).$$

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

$$
\tilde{T}^1_{\epsilon, \alpha}(0) = \begin{cases} 
1 - \alpha, & \text{if } \epsilon \leq \alpha, \\
1, & \text{if } \epsilon > \alpha,
\end{cases}
\tilde{T}^1_{\epsilon, \alpha}(1) = \begin{cases} 
0, & \text{if } \epsilon \leq \alpha, \\
\frac{\epsilon - \alpha}{\epsilon}, & \text{if } \epsilon > \alpha,
\end{cases}
$$

the test $\tilde{T}^1_{\epsilon, \alpha}$ satisfies

$$(1 - \epsilon)\tilde{T}^1_{\epsilon, \alpha}(0) + \epsilon\tilde{T}^1_{\epsilon, \alpha}(1) = 1 - \alpha. \tag{4}$$

Moreover, if $p \leq \epsilon$, then

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

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

$$
\beta^1_{\alpha}(\leq \epsilon \| q) = q(\tilde{T}^1_{\epsilon, \alpha}) = \begin{cases} 
\frac{(1 - \alpha)(1 - q)}{1 - \epsilon}, & \text{if } \epsilon \leq \alpha, \\
\frac{\alpha q}{\epsilon}, & \text{if } \epsilon > \alpha.
\end{cases}
\tag{5}
$$

4.2. $n$-sample setting

In the $n$-trial case, the data $k = 0, 1, \ldots, n$ obey the distribution $P_p^n(k) \overset{\text{def}}{=} \binom{n}{k} (1 - p)^{n-k} p^k$ with unknown parameter $p$. Hence, we discuss testing of the null hypothesis $P_{\leq \epsilon}^n \overset{\text{def}}{=} \{ P_p^n(k) \mid p \leq \epsilon \}$ and the alternative hypothesis $(P_{\leq \epsilon}^n)^c$. In this case, our test $\tilde{T}$ can be described by a function

New Journal of Physics 11 (2009) 043028 (http://www.njp.org/)
from the data set \{0, 1, \ldots, n\} to the interval [0, 1]. In this case, when the data element \(k\) is observed, we accept the null hypothesis \(P^n_{\leq \epsilon}\) with probability \(T(k)\). Then, the minimum second error probability among level-\(\alpha\) tests is given by

\[
\beta^n_\alpha (\leq \epsilon \| q) \overset{\text{def}}{=} \min_T \left\{ P^n_{q}(\tilde{T}) \left| \forall p \in [0, \epsilon], 1 - P^n_p(\tilde{T}) \leq \alpha \right. \right\},
\]

\[
P^n_p(\tilde{T}) \overset{\text{def}}{=} \sum_{k=0}^{n} P^n_p(k) \tilde{T}(k).
\]

We define the test \(\tilde{T}^n_{\epsilon, \alpha}\) as follows:

\[
\tilde{T}^n_{\epsilon, \alpha}(k) = \begin{cases} 
1, & k < l^n_{\epsilon, \alpha}, \\
g^n_{\epsilon, \alpha}, & k = l^n_{\epsilon, \alpha}, \\
0, & k > l^n_{\epsilon, \alpha},
\end{cases}
\]

where the integer \(l^n_{\epsilon, \alpha}\) and the real number \(g^n_{\epsilon, \alpha} > 0\) are defined by

\[
l^n_{\epsilon, \alpha} - 1 \sum_{k=0}^{l^n_{\epsilon, \alpha} - 1} P^n_{\epsilon}(k) < 1 - \alpha \leq l^n_{\epsilon, \alpha} \sum_{k=0}^{l^n_{\epsilon, \alpha}} P^n_{\epsilon}(k),
\]

\[
g^n_{\epsilon, \alpha} P^n_{\epsilon}(l^n_{\epsilon, \alpha}) = 1 - \alpha - \sum_{k=0}^{l^n_{\epsilon, \alpha} - 1} P^n_{\epsilon}(k).
\]

**Proposition 1.** The test \(\tilde{T}^n_{\epsilon, \alpha}\) is a level-\(\alpha\) UMP test with null hypothesis \(P^n_{\leq \epsilon}\). Hence,

\[
\beta^n_\alpha (\leq \epsilon \| q) = P^n_{q}(\tilde{T}^n_{\epsilon, \alpha}) = \sum_{k=0}^{l^n_{\epsilon, \alpha} - 1} P^n_{q}(k) + g^n_{\epsilon, \alpha} P^n_{q}(l^n_{\epsilon, \alpha}).
\]

For a proof, see appendix C.

4.3. Asymptotic setting

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

4.3.1. Small deviation theory. It is useful to treat the neighbourhood around \(p = 0\) as the small deviation theory of this problem for a discussion of asymptotic testing for a maximally
entangled state. Hence, we focus on the case that $p = \frac{t}{n}$, since the probability $P_{t/n}(k) = \binom{n}{k}(1 - (t/n))^{n-k}(t/n)^k$ converges to the Poisson distribution $P_t(k) \overset{\text{def}}{=} e^{-t}(t^k/k!)$. Hence, our testing problem with null hypothesis $P_{\delta/n}$ and alternative hypothesis $t'/n$ is asymptotically equivalent to a test of the Poisson distribution $P_t(k)$ with null hypothesis $t \in [0, \delta]$ and alternative hypothesis $t'$. That is, by defining

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

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

the following proposition holds.

**Proposition 2.**

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

The proof is presented in appendix D. Similar to the test $\tilde{T}_{e,\alpha}^n$, we define the test $\tilde{T}_{\delta,\alpha}$ as

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

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

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

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

The following proposition, similar to proposition 1, holds.

**Proposition 3.** The test $\tilde{T}_{\delta,\alpha}$ is a level-$\alpha$ UMP test with null hypothesis $P_{\leq \delta} \overset{\text{def}}{=} \{ P_t \mid t \leq \delta \}$. Hence,

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

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

$$\lim_{n \to \infty} -\frac{1}{n} \log \beta_n^{\alpha}(\leq \epsilon \| p) = d(\epsilon \| p), \quad \text{if } \epsilon < p,$$
$$\lim_{n \to \infty} -\frac{1}{n} \log \beta_n^{\alpha}(\geq \epsilon \| p) = d(\epsilon \| p), \quad \text{if } \epsilon > p,$$

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

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

5. Global tests

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

5.1. One sample setting

When only one sample is prepared, the test $|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|$ is a level-0 test for the null hypothesis $S_0$. If we perform the two-valued measurement $\{ |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|, I - |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}| \}$, the data obey the distribution $\{ 1 - p, p \}$, where

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

Hence, applying the discussion in section 4.1, the test $T_{\alpha}^1(|\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|, \epsilon)$ is a level-$\alpha$ test for the null hypothesis $S_{\leq \epsilon}$, where the operator $T_{\alpha}^1(T, \epsilon)$ is defined by

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

5.2. 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 $\{ |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|, I - |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}| \}$ for respective $n$ systems. Then, if the number of counts $I - |\phi^0_{A,B}\rangle\langle\phi^0_{A,B}|$ is described by $k$, the data $k$ obey the binomial
distribution \( P^\alpha_n(k) \). In this case, our problem can be reduced to hypothesis testing with null hypothesis \( \mathcal{P}_{\leq \alpha}^n \), which has been discussed in section 4.2.

For given \( \alpha \) and \( \epsilon \), the test based on this measurement and the classical test \( \tilde{T}_{\epsilon,a}^n \) is described by the operator \( T_{\epsilon,a}^n \equiv T_{\alpha}^n (|\phi_{A,B}^0 \rangle \langle \phi_{A,B}^0|, \epsilon) \), where \( T_{\alpha}^n (T, \epsilon) \) is defined by

\[
T_{\alpha}^n (T, \epsilon) \equiv \sum_{k=0}^{\mathcal{L}(e)-1} P_k^n (T, I - T) + \gamma_a^n (\epsilon) T_{\gamma_a^n (\epsilon)} (T, I - T),
\]

\[
P_k^n (T, S) \equiv \sum_{k} S \otimes \cdots \otimes S \otimes T \otimes \cdots \otimes T + \cdots + T \otimes \cdots \otimes T \otimes S \otimes \cdots \otimes S.
\]

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

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

\[
\beta_{\alpha,n,U(d^2-1)} (\epsilon) \leq \beta_{\alpha,n} (\epsilon) \leq \beta_{\alpha,n} (\epsilon) = \beta_{\alpha,n} (\epsilon).
\]

On the other hand, as is shown in appendix E,

\[
\beta_{\alpha,n,U(1)} (\epsilon) \geq \beta_{\alpha,n} (\epsilon) \geq \beta_{\alpha,n} (\epsilon).
\]

Since \( U(1) \subset SU(d) \times U(1) \subset U(d^2 - 1) \), the relations (8) and (9) yield the following theorem.

**Theorem 1.** The equation

\[
\beta_{\alpha,n,G} (\epsilon) = \beta_{\alpha,n} (\epsilon) \leq \beta_{\alpha,n} (\epsilon)
\]

holds for \( G = U(1), SU(d) \times U(1) \) and \( U(d^2 - 1) \). The optimal test is \( T_{\epsilon,a}^n \).

Therefore, the test \( T_{\epsilon,a}^n \) is the UMP \( G \)-invariant test, for \( G = U(1), SU(d) \times U(1) \) or \( U(d^2 - 1) \). Moreover, we can derive the same results for the hypothesis \( S_{\geq \epsilon} \).

**5.3. Asymptotic setting**

Next, we proceed to the asymptotic setting. In the small deviation theory, we treat hypothesis testing with the null hypothesis \( S_{\leq \delta/n} \). In this setting, proposition 2 and theorem 1 guarantee that the limit of the optimal second error probability of the alternative hypothesis \( \sigma_n \) is given by \( \beta_{\alpha} (\delta \| t') \) if \( \langle \phi_{A,B}^0 | \sigma_n | \phi_{A,B}^0 \rangle = 1 - (t'/n) \). That is,

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

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

In the large deviation setting, we can obtain the same results as in section 4.3, i.e.

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

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

**New Journal of Physics 11** (2009) 043028 (http://www.njp.org/)
6. A–B locality

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

6.1. Construction of one-way LOCC test

First, we introduce two important one-way LOCC tests, which will be used later. Consider a POVM with the following form on $H_A$:

$$M = \{ p_i |u_i\langle u_i| \}, \quad \|u_i\| = 1, \quad 0 \leq p_i \leq 1,$$

where such a POVM is called rank-one. Based on a rank-one POVM $M$, a suitable test

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

(13)

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

$$0 \leq T(M) \leq 1.$$

(14)

**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 $\{|u_i\rangle \langle u_i|, I - |u_i\rangle \langle u_i|\}$, where $\overline{u_i}$ is the complex conjugate of $u_i$ with respect to the standard basis $|0\rangle_B, |1\rangle_B, \ldots, |d-1\rangle_B$.
3. If Bob observes the event corresponding to $|u_i\rangle \langle u_i|$, the hypothesis $|\phi_0^{A,B}\rangle \langle \phi_0^{A,B}|$ is accepted, otherwise, it is rejected.

Next, we focus on the covariant POVM $M_{\text{cov}}^1$:

$$M_{\text{cov}}^1(\varphi) \overset{\text{def}}{=} d|\varphi\rangle \langle \varphi| \nu(\varphi),$$

where $\nu(\varphi)$ is an invariant measure in the set of pure states with full measure 1. Then, the test

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

has the following form:

$$T_{\text{inv}}^{1,A\rightarrow B} = \int d|\varphi\rangle \langle \varphi| \nu(\varphi) = |\phi_0^{A,B}\rangle \langle \phi_0^{A,B}| + \frac{1}{d+1}(I - |\phi_0^{A,B}\rangle \langle \phi_0^{A,B}|),$$

(15)

where the last equation will be derived in appendix H. Note that the POVM $M_{\text{cov}}^1$ can be realized as follows:

**Realization of $M_{\text{cov}}^1$:**

1. Randomly, we choose $g \in SU(d)$ of invariant measure.
2. Perform POVM $\{ g|i\rangle_{A,A} \langle i|g^\dagger \}$, Then, the realized POVM is $M_{\text{cov}}^1$.
6.2. One sample setting

First, we focus on the simplest case, i.e. the case of $\epsilon = 0$ and $\alpha = 0$. In this case, the test $T(M)$ satisfies

$$\langle \phi^0_{A,B} | T(M) | \phi^0_{A,B} \rangle = 1,$$

(16)

$$\text{Tr} \ T(M) = \sum_i p_i \text{Tr} \ |u_i \otimes \overline{u_i}\rangle \langle u_i \otimes \overline{u_i}|$$

$$= \sum_i p_i \text{Tr} \ |u_i\rangle \langle u_i| = d.$$  

(17)

Hence, it is a level-0 test with the null hypothesis $|\phi^0_{A,B}\rangle \langle \phi^0_{A,B}|$. In particular, in the one-way LOCC setting, our tests can be restricted to tests of this kind, in the following sense.

**Lemma 3.** Let $T$ be a one-way LOCC $(A \to B)$ level-0 test with the null hypothesis $|\phi^0_{A,B}\rangle \langle \phi^0_{A,B}|$. Then, there exists a POVM of the form $M = \{ p_i |u_i\rangle \langle u_i| \}$, such that

$$T \geq T(M),$$

(18)

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 tests of the form (13), even if we do adopt the separable condition.

**Lemma 4.** Assume that a separable test $T$ satisfies

$$\langle \phi^0_{A,B} | T | \phi^0_{A,B} \rangle = 1.$$  

(19)

When the test $T$ has the form

$$T = d \sum_i p_i |u_i \otimes u'_i\rangle \langle u_i \otimes u'_i| + \sum_j q_j |v_j \otimes v'_j\rangle \langle v_j \otimes v'_j|$$

(20)

with the condition $\langle \phi^0_{A,B} | u_i \otimes u'_i \rangle = \frac{1}{\sqrt{d}}$ and $\langle \phi^0_{A,B} | v_i \otimes v'_i \rangle = 0$, we obtain

$$\sum_i p_i u_i \otimes u'_i = \frac{1}{\sqrt{d}} \phi^0_{A,B}.$$
Next, we treat the test $T_{\text{inv}}^{1, A \rightarrow B}$. Since equation (15) guarantees the $U(d^2 - 1)$-invariance of the test $T_{\text{inv}}^{1, A \rightarrow B}$, we obtain

$$\text{Tr} T_{\text{inv}}^{1, A \rightarrow B} \sigma = 1 - p + \frac{p}{d+1} = 1 - \frac{dp}{d+1},$$

which implies

$$\rho_{0,1, U(d^2-1)}^{L(A \rightarrow B)}(0 \| \sigma) \leq 1 - \frac{dp}{d+1}.$$ 

Next, we apply the discussion in section 4.1 to the probability distribution $\{dp/(d+1), 1 - dp/(d + 1)\}$. Then, the test $T_{\epsilon, \alpha}^{1, A \rightarrow B} \equiv T_{\alpha}^{1}(T_{\text{inv}}^{1, A \rightarrow B}, d \epsilon/(d+1))$ is a level-$\alpha$ $U(d^2 - 1)$-invariant test. Since the test $T_{\epsilon, \alpha}^{1, A \rightarrow B}$ can be performed by randomized operation with $T_{\text{inv}}^{1, A \rightarrow B}$ and $I - T_{\text{inv}}^{1, A \rightarrow B}$, we obtain

$$\rho_{\alpha, 1, U(d^2-1)}^{L(A \rightarrow B)}(\leq \epsilon \| \sigma) \leq \text{Tr} T_{\epsilon, \alpha}^{1, A \rightarrow B} \sigma = \begin{cases} \frac{(1-\alpha) \left(1 - \frac{d}{d+1} p\right)}{\left(1 - \frac{d}{d+1} \epsilon\right)}, & \text{if } \frac{d}{d+1} \epsilon \leq \alpha, \\ 1 - \frac{\alpha p}{\epsilon}, & \text{if } \frac{d}{d+1} \epsilon > \alpha. \end{cases}$$ (21)

On the other hand, for $SU(d)$-invariant and separable tests, the equation

$$\rho_{\alpha, 1, SU(d)}^{S(A, B)}(\leq \epsilon \| \sigma) = \text{Tr} T_{\epsilon, \alpha}^{1, A \rightarrow B} \sigma$$ (22)

holds, which is shown in appendix I. The equation in the case of $\alpha = 0$ and $\epsilon = 0$ was obtained by Hayashi et al [22].Virmani and Plenio [28] showed that this POVM is the extremal point under the PPT condition as well as the separable condition, the two-way LOCC condition and the one-way LOCC condition. 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

$$\rho_{\alpha, 1, SU(d)}^{S(A, B)}(\leq \epsilon \| \sigma) \leq \rho_{\alpha, 1, U(d^2-1)}^{S(A, B)}(\leq \epsilon \| \sigma) \leq \rho_{\alpha, 1, U(d^2-1)}^{L(A \rightarrow B)}(\leq \epsilon \| \sigma)$$

hold. Therefore, relations (21) and (22) yield the following theorem.

**Theorem 2.**

$$\rho_{\alpha, 1, G}^{S}(\leq \epsilon \| \sigma) = \begin{cases} \frac{(1-\alpha) \left(1 - \frac{d}{d+1} p\right)}{\left(1 - \frac{d}{d+1} \epsilon\right)}, & \text{if } \frac{d}{d+1} \epsilon \leq \alpha, \\ 1 - \frac{\alpha p}{\epsilon}, & \text{if } \frac{d}{d+1} \epsilon > \alpha, \end{cases}$$ (23)

for $G = SU(d), SU(d) \times U(1), U(d^2 - 1)$ and $C = L(A \rightarrow B), L(A \Rightarrow B), S(A, B)$. The test $T_{\epsilon, \alpha}^{1, A \rightarrow B}$ is the UMP $G$-invariant $C$ test at level $\alpha$ for the null hypothesis $S_{\geq \epsilon}$.

Furthermore, similar results for the null hypothesis $S_{\geq \epsilon}$ can also be obtained.

*New Journal of Physics* 11 (2009) 043028 (http://www.njp.org/)
6.3. Two-sample case

In this section, we construct an \( SU(d) \times U(1) \)-invariant test, which is realized by LOCC between \( A \) and \( B \), and which attains the asymptotically optimal bound (11). For this purpose, we focus on the covariant POVM \( M_{\text{cov}}^2 \):

\[
M_{\text{cov}}^2 (dg_1 dg_2) \overset{\text{def}}{=} d^2 (g_1 \otimes g_2)|u\rangle \langle u| (g_1 \otimes g_2)^* v (dg_1)v (dg_2),
\]

where the vector \( u \) is maximally entangled and \( v \) is the invariant measure on \( SU(d) \). Then, the operator \( T_{\text{inv}}^{2,A \rightarrow B} \overset{\text{def}}{=} T (M_{\text{cov}}^2) \) has the form:

\[
T_{\text{inv}}^{2,A \rightarrow B} = |\phi_{A,B}^0 \rangle \langle \phi_{A,B}^0 | \otimes |\phi_{A,B}^0 \rangle \langle \phi_{A,B}^0 | + \frac{1}{d^2 - 1} (I - |\phi_{A,B}^0 \rangle \langle \phi_{A,B}^0 |) \otimes (I - |\phi_{A,B}^0 \rangle \langle \phi_{A,B}^0 |),
\]

which is shown in appendix J. This equation implies that the testing \( T (M_{\text{cov}}^2) \) does not depend on the choice of the maximally entangled state \( u \). Now, we choose the maximally entangled state \( |\phi_{1,2}^0 \rangle \). Then,

\[
M_{\text{cov}}^2 (dg_1 dg_2) = d^2 (g_1 \otimes I) |u\rangle \langle u| (g_1 \otimes I)^* v (dg_1)v (dg_2).
\]

So, the other local POVM:

\[
\tilde{M}_{\text{cov}}^2 (dg) \overset{\text{def}}{=} d^2 (g \otimes I) |u\rangle \langle u| (g \otimes I)^* v (dg)
\]
satisfies \( T_{\text{inv}}^{2,A \rightarrow B} = T (\tilde{M}_{\text{cov}}^2) \). This test satisfies the equation

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

(25)

because the form (24) guarantees the \( U(d^2 - 1) \)-invariance of the test \( T_{\text{inv}}^{2,A \rightarrow B} \). Since the test \( T_{\text{inv}}^{2,A \rightarrow B} \) is a level-0 test with null hypothesis \( S_0 \), the inequality

\[
\beta_{0,2,U(d^2 - 1)} (0 \| \sigma) \leq 1 - 2p + \frac{d^2 p^2}{d^2 - 1}
\]

holds. Next, we apply the discussion of section 4.1. Then, the test \( T_{\epsilon,2}^{2,A \rightarrow B} \overset{\text{def}}{=} T_{\epsilon}^{1} (T_{\text{inv}}^{2,A \rightarrow B}, 2 \epsilon - \frac{d^2 \epsilon^2}{d^2 + 1}) \) is a level-\( \epsilon \) \( U(d^2 - 1) \)-invariant test. Since the test \( T_{\epsilon,2}^{2,A \rightarrow B} \) can be performed by randomized operation with \( T_{\text{inv}}^{2,A \rightarrow B} \) and \( I - T_{\text{inv}}^{2,A \rightarrow B} \), we obtain

\[
\beta_{\epsilon,2,U(d^2 - 1)} \leq \epsilon \| \sigma \| \leq \text{Tr} T_{\epsilon,2}^{2,A \rightarrow B} \sigma^\otimes 2 = \begin{cases} (1 - \alpha) \left(1 - 2p + \frac{d^2 p^2}{d^2 + 1}\right), & \text{if } 2 \epsilon - \frac{d^2 \epsilon^2}{d^2 + 1} \leq \alpha, \\ 1 - 2\epsilon + \frac{d^2 \epsilon^2}{d^2 + 1}, & \alpha = \left(2p + \frac{d^2 p^2}{d^2 - 1}\right), \\ 2\epsilon - \frac{d^2 \epsilon^2}{d^2 - 1}, & \text{if } 2 \epsilon - \frac{d^2 \epsilon^2}{d^2 + 1} > \alpha. \end{cases}
\]

New Journal of Physics 11 (2009) 043028 (http://www.njp.org/
Furthermore, as a generalization of \((25)\), we obtain the following lemma, which, from an applied viewpoint, is more useful in the asymptotic setting.

**Lemma 5.** Let \(M = \{p_i | u_i \rangle \langle u_i| | \| u_i \| = 1\}\) 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
\[
T(M) = |\phi^0_{A_1,B_1} \otimes \phi^0_{A_2,B_2} \rangle \langle \phi^0_{A_1,B_1} \otimes \phi^0_{A_2,B_2}| + PT(M)P, \tag{26}
\]
and
\[
\langle \phi^0_{AB} | \sigma | \phi^0_{AB} \rangle^2 \leq \text{Tr} \sigma \otimes \text{Tr} T(M) \tag{27}
\]
\[
\leq \langle \phi^0_{AB} | \sigma | \phi^0_{AB} \rangle^2 + (1 - \langle \phi^0_{AB} | \sigma | \phi^0_{AB} \rangle)^2, \tag{28}
\]
where
\[
P \equiv (I - |\phi^0_{A_1,B_1} \rangle \langle \phi^0_{A_2,B_2}|) \otimes (I - |\phi^0_{A_1,B_1} \rangle \langle \phi^0_{A_1,B_1}|) \notag
\]

Indeed, it is difficult to realize the covariant POVM \(M^2_{\text{cov}}\). The Bell measurement \(M^2_{\text{Bell}} = \{ |\phi_{n,m}^0 \rangle \langle \phi_{n,m}^0| \}_{(n,m) = (0,0)}\) can be constructed more easily, where \(\phi_{1,2}^{n,m}\) is defined by
\[
\phi_{1,2}^{0,0} \equiv \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \langle j|, \quad \phi_{1,2}^{n,m} \equiv ((X^Z)^m \otimes I) \phi_{1,2}^{0,0},
\]
\[
X \equiv \sum_{j=1}^{d-1} |j\rangle \langle j| - |0\rangle \langle d-1|, \quad Z \equiv \sum_{j=0}^{d-1} e^{2\pi i j/d} |j\rangle \langle j|. \notag
\]
As will be discussed in section 6.5, the test \(T(M^2_{\text{Bell}})\) can be used as an alternative test of \(T^{2,A \rightarrow B}_{\text{inv}}\) in an asymptotic sense.

### 6.4. \(n\)-sample setting

Next, we construct a \(U(d^2 - 1)\)-invariant test when \(2n\) samples of the unknown state \(\sigma\) are prepared. It follows from a discussion similar to section 5.2 that the test \(T^{2n, \epsilon, \alpha}_{\text{inv}} \equiv T^{2n}_{\text{inv}}(T^{2,A \rightarrow B}_{\text{inv}}, 2\epsilon - \frac{d^2 \epsilon^2}{d^2 - 1})\) is of level-\(\alpha\) for given \(\alpha\) and \(\epsilon\). The \(U(d^2 - 1)\)-invariance of the test \(T^{2,A \rightarrow B}_{\text{inv}}\) implies the \(U(d^2 - 1)\)-invariance of the test \(T^{2n, \epsilon, \alpha}_{\text{inv}}\). Since the test \(T^{2n, \epsilon, \alpha}_{\text{inv}}\) can be realized by one-way LOCC \(A \rightarrow B\), the inequality
\[
\beta^{L(A \rightarrow B)}_{\alpha, 2n, U(d^2 - 1)}(\leq \epsilon \| \sigma \|) \leq \text{Tr} T^{2n, \epsilon, \alpha}_{\text{inv}} \sigma^{\otimes 2n} = \beta^{n}_{\alpha} \left( \leq 2\epsilon - \frac{d^2 \epsilon^2}{d^2 - 1} \right) \notag \tag{29}
\]
holds. In addition, we can derive a similar bound for the hypothesis \(S_{\geq \epsilon}\).

For the case \(\epsilon = 0\), we can have another bound as follows. For this purpose, we focus on the test \(T^{1,A \rightarrow B}_{\text{inv}}\) in the case when \(\mathcal{H}_A = \mathcal{H}_{A}^{\otimes n}\) and \(\mathcal{H}_B = \mathcal{H}_{B}^{\otimes n}\). Denoting this test by \(T^{1,A \rightarrow B}_{\text{inv}}\),
we have
\[
T_{\text{inv}}^{1, A^\otimes n \rightarrow B^\otimes n} = |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0|^{\otimes n} + \frac{1}{d^n+1} (I - |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0|)^{\otimes n}
\]

\[
\text{Tr} T_{\text{inv}}^{1, A^\otimes n \rightarrow B^\otimes n} \sigma^{\otimes n} = \frac{d^n(1-p)^n + 1}{d^n+1}
\]

because \(\text{Tr} |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0|^{\otimes n} \sigma^{\otimes n} = (1-p)^n\). Since this test is \(U(d^2-1)-\text{invariant}, we obtain
\[
\beta_{\sigma, n, U^2(1)}^L (|\sigma|) = \frac{d^n(1-p)^n + 1}{d^n+1}.
\]

(30)

6.5. Asymptotic setting

We proceed to the asymptotic setting. First, we show that even if our test satisfies the \(A-B\) LOCC condition, the bound (10) can be attained in the asymptotic small deviation setting. Indeed, since \(P_n^{2(t/2n)-(d^2/(d+1))(t/2n)}(k) \rightarrow P_s(k)\), the equation
\[
\lim_{n \rightarrow \infty} \beta_{\alpha, n}^{L(A \rightarrow B)} \left( \leq \frac{\delta}{2n} - \frac{d^2}{d^2-1} \left( \frac{\delta}{2n} \right)^2 \right) = \beta_{\alpha, n} \left( \leq \frac{\delta}{t'} \right)
\]
can be proven similarly to theorem 2. Hence, equations (2) and (3) yield the following theorem.

**Theorem 3.** When \(\langle \phi_{A,B}^0 | \sigma_n | \phi_{A,B}^0 \rangle = 1 - \frac{t'}{2n}\) and \(t' > \delta\), the equation
\[
\lim_{n \rightarrow \infty} \beta_{\alpha, n}^{G(A \rightarrow B)} \left( \leq \frac{\delta}{n} \right) = \beta_{\alpha, n} \left( \leq \frac{\delta}{t'} \right)
\]

holds for \(G = U(1), SU(d) \times U(1), U(d^2-1)\) and \(C = \emptyset, L(A \rightarrow B), L(A \leftarrow B), S(A, B)\). The optimal test is \(T_{\epsilon,\alpha, n}^{2n}\).

However, it is difficult to realize the covariant POVM \(M_n^{\text{cov}}\) on \(H_A^{\otimes 2}\). Even if the test \(T_{\epsilon,\alpha, n}^{2n}\) is replaced by \(T_{\epsilon,\alpha, Bell}^{2n} \overset{\text{def}}{=} T_{\alpha}^n (TM_{\text{Bell}}^2), 2\epsilon - \frac{d^2\epsilon^2}{d^2-1}\), the bound \(\beta_{\alpha, n} \left( \leq \frac{\delta}{t'} \right)\) can be attained in the following asymptotic sense. The test \(T_{\epsilon,\alpha, Bell}^{2n}\) may not be at level-\(\alpha\) with the null hypothesis \(S_{\delta/2n}\), but it is asymptotically at level-\(\alpha\), i.e.
\[
\text{Tr} T_{\epsilon,\alpha, Bell}^{2n} \sigma_{\delta/2n}^{\otimes 2n} \rightarrow 1 - \delta
\]

(31)

if \(\langle \phi_{A,B}^0 | \sigma_n | \phi_{A,B}^0 \rangle = 1 - \frac{\delta}{n}\). Moreover, if \(\langle \phi_{A,B}^0 | \sigma_n | \phi_{A,B}^0 \rangle = 1 - \frac{t'}{n}\) and \(t' > \delta\), the relation
\[
\text{Tr} T_{\epsilon,\alpha, Bell}^{2n} \sigma_n^{\otimes 2n} \rightarrow \beta_{\alpha, n} \left( \leq \frac{\delta}{t'} \right)
\]

(32)

holds. These relations (31) and (32) follow from lemma 5. Hence, there is no advantage in using entanglement between \(H_A\) and \(H_B\) for this test in the asymptotic small deviation setting. Similar results for the null hypothesis \(S_{\delta/\sqrt{n}}\) can be obtained. The asymptotic optimal testing scheme is illustrated in figure 1.

New Journal of Physics 11 (2009) 043028 (http://www.njp.org/)
Next, we proceed to the large deviation setting. The inequality (30) yields
\[
\lim_{n \to \infty} -\frac{1}{n} \log \beta^{L(A \to B)}_{u,n,U(d^2-1)}(0\|\sigma) \geq \begin{cases} -\log(1-p), & \text{if } 1-p \geq \frac{1}{d}, \\ \log d, & \text{if } 1-p < \frac{1}{d}. \end{cases}
\]
(33)

Hence, the relations (3) and (12) guarantee that if \(1-p \geq 1/d\),
\[
\lim_{n \to \infty} -\frac{1}{n} \log \beta^{L(A \to B)}_{u,n,U(d^2-1)}(0\|\sigma) = -\log(1-p),
\]
for \(G = U(1), SU(d) \times U(1), U(d^2-1)\) and \(C = \emptyset, L(A \to B), L(A \equiv B), S(A, B)\). Hence, we can conclude that if \(1-p \geq 1/d\), there is no advantage in using entanglement between \(\mathcal{H}_A\) and \(\mathcal{H}_B\) for this test, even in this kind of asymptotic large deviation setting.

7. A–B locality and sample locality

In this section, we discuss 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 in section 6, we begin with the case \(n = 2\).

7.1. Two-sample setting

We construct a level-0 \(SU(d)\)-invariant test for the null hypothesis \(S_0 = \{|\phi_{A,B}^0\rangle\langle\phi_{A,B}^0|\}\) as follows. For this purpose, we define a POVM \(M^{1^{-2}}\) on Alice’s space \(\mathcal{H}_A^{\otimes 2}\), which can be realized by one-way LOCC \(A_1 \to A_2\) from the first system \(\mathcal{H}_A\) to the second system \(\mathcal{H}_{A_2}\).

Construction of \(M^{1^{-2}}\):

1. Alice performs the covariant POVM \(M^{1}_c\) on the first system \(\mathcal{H}_A\), and obtains data corresponding to the state \(|\varphi\rangle\langle\varphi|\).
2. We choose the projection-valued measure \(\{|u^{i}(\varphi)\rangle\langle u^{i}(\varphi)|\}\), satisfying
\[
\langle u^{i}(\varphi)|u^{j}(\varphi) \rangle = 0, \quad \langle u^{i}(\varphi)|\varphi \rangle = \frac{1}{\sqrt{d}}.
\]
(34)
The existence of \(\{|u^{i}(\varphi)\rangle\}\), is shown in appendix K.
3. Alice randomly chooses \(g \in U(d-1)\), which acts on the space orthogonal to \(\varphi\) and performs the projection-valued measure \(\{|gu^{i}(\varphi)\rangle\langle gu^{i}(\varphi)|\}\), on the second system \(\mathcal{H}_{A_2}\).

Since Bob’s measurement of the test \(T(M^{1^{-2}})\) can also be realized by one-way LOCC on Bob’s space, this test is an \(L(A_1, A_2 \to B_1, B_2)\) test. Its POVM is given by
\[
M^{1^{-2}}(dg) = d^2(g \otimes g)|u_1 \otimes u_2\rangle\langle u_1 \otimes u_2|\otimes (g \otimes g)^{\dagger}v(dg),
\]
where we choose \(u_1\) and \(u_2\) satisfying \(|u_1|u_2\rangle|u_1|u_2\rangle = 1/d\). Thus, the \(SU(d)\)-covariance of \(M^{1^{-2}}\) guarantees \(SU(d)\)-invariance of the test \(T^{1^{-2}}_{inv}A_1 \to A_2 \to B^{\otimes 2} \overset{\text{def}}{=} T(M^{1^{-2}})\). Moreover, as is shown in appendix L, the test \(T^{1^{-2}}_{inv}A_1 \to A_2 \to B^{\otimes 2}\) is \(U(1)\)-invariant. Hence, the inequality
\[
\rho^{L(A_1, A_2 \to B_1, B_2)}_{0, 2, SU(d) \times U(1)}(0\|\sigma) \leq \text{Tr} T^{A_1 \to A_2 \to B^{\otimes 2}}_{inv} A_1 \to A_2 \to B^{\otimes 2} \sigma \otimes 2
\]
The relation \( p_{0,2,SU(d)}^{L(A_1, A_2 \to B_1, B_2)}(0 \| \sigma) = \text{Tr} \ T_{\text{inv}}^{A_1 \to A_2 \to B_0^2} \sigma \otimes 2 \) holds for \( G = SU(d) \times U(1) \). Then, the test \( T_{\text{inv}}^{A_1 \to A_2 \to B_0^2} \) is a UMP \( L(A_1, A_2 \to B_1, B_2) \) \( G \)-invariant test at level-0 for the null hypothesis \( S_0 \), where \( G = SU(d) \times U(1) \).

### 7.2. \( n \)-sample setting

Next, we proceed to the \( n \)-sample setting. Since the test \( T^{\text{inv}}_{\epsilon, \alpha} \) is a level-\( \alpha \) \( U(d^2 - 1) \)-invariant test for the hypothesis \( S_{\leq \epsilon} \), and satisfies the condition of \( L(A_1, \ldots, A_n \to B_1, \ldots, B_n) \), the inequality

\[
\frac{1}{n} \log \beta_{a,n, SU(d)}^{S(A_1, \ldots, A_n \to B_1, \ldots, B_n)}(0 \| \sigma) \geq \min_{u, u' : \{ u \| u' \} = 1, \| u \| = 1} \int_{SU(d)} \log d(gu \otimes gu' | \sigma | gu \otimes gu') v(dg),
\]

which will be shown in appendix N.

### 7.3. Asymptotic setting

Taking the limit in (36), we obtain

\[
\lim_{n \to \infty} \beta_{a,n, U(d^2 - 1)}^{L(A_1, \ldots, A_n \to B_1, \ldots, B_n)} \left( \leq \frac{\delta}{n} \right) \leq \beta_{\alpha} \left( \leq \frac{d \delta}{d+1} \right) \left( \leq \frac{d' \delta}{d+1} \right)
\]

if \( \langle \phi_{A,B}^0 | \sigma_n | \phi_{A,B}^0 \rangle = 1 - (t' / n) \). Conversely, by using the inequality (37), compactness of the sets \( \{ u, u' : \{ u \| u' \} = 1, \| u \| = 1 \} \) and \( SU(d) \) yield

\[
\lim_{n \to \infty} \log \beta_{a,n, SU(d)}^{S(A_1, \ldots, A_n \to B_1, \ldots, B_n)}(0 \| \sigma_n) \geq \min_{u, u' : \{ u \| u' \} = 1, \| u \| = 1} \int_{SU(d)} \lim_{n \to \infty} n \log d(gu \otimes gu' | \sigma_n | gu \otimes gu') v(dg)
\]

\[
= - \min_{u, u' : \{ u \| u' \} = 1, \| u \| = 1} \int_{SU(d)} \lim_{n \to \infty} n (1 - d(gu \otimes gu' | \sigma_n | gu \otimes gu') ) v(dg)
\]

\[
= - \min_{u, u' : \{ u \| u' \} = 1, \| u \| = 1} \lim_{n \to \infty} n \text{Tr}(I - T_{n, u'}) \sigma_n,
\]
where

\[
T_{u,u'} \overset{\text{def}}{=} \int_{SU(d)} d|gu \otimes \bar{gu}'\rangle\langle gu \otimes \bar{gu}'|v(dg).
\]

Since \(T_{u,u'}\) is \(SU(d)\)-invariant, the test \(T_{u,u'}\) has the form \(t_0 \phi^0_{A,B} \langle \phi^0_{A,B} | + t_1 (I - \phi^0_{A,B} \langle \phi^0_{A,B} |)\).

The condition \(|\langle u|\bar{u}'\rangle| = 1\) guarantees that \(t_0 = 1\). The definition of \(T_{u,u'}\) guarantees that \(\text{Tr} T_{u,u'} \geq d\), which implies \(t_1 \geq 1/(d+1)\). Hence,

\[
\text{Tr}(I - T_{u,u'})\sigma_n \leq \frac{d}{d+1} \text{Tr}(I - \phi^0_{A,B} \langle \phi^0_{A,B} |)\sigma_n
\]

\[
= \frac{d}{d+1} (1 - \langle \phi^0_{A,B} | \sigma | \phi^0_{A,B} \rangle) = \frac{d}{d+1} \frac{t'}{n}. \tag{39}
\]

Thus, we have

\[
\lim_{n \to \infty} \log \frac{\beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}}{0\|\sigma_n} \geq - \frac{dt'}{d+1},
\]

which implies

\[
\lim_{n \to \infty} \beta^{S(A_1,\ldots,A_n,B_1,\ldots,B_n)}_{\alpha,n,SU(d)}(0\|\sigma_n) \geq (1 - \alpha)e^{-dt'/(d+1)}.
\]

Combining (38) in the case of \(\delta = 0\), we obtain the following theorem.

**Theorem 5.** When \(\langle \phi^0_{A,B} | \sigma | \phi^0_{A,B} \rangle = 1 - (t'/n)\),

\[
\lim_{n \to \infty} \beta^{C_1}_{\alpha,n,G}(0\|\sigma_n) = (1 - \alpha)e^{-dt'/(d+1)}
\]

for \(G = SU(d), SU(d) \times U(1), U(d^2 - 1)\) and \(C_1 = S(A_1,\ldots,A_n,B_1,\ldots,B_n), L(A_1,\ldots,A_n,B_1,\ldots,B_n), L(A_1,\ldots,A_n \to B_1,\ldots,B_n)\). The optimal test is \(T'_{0,\alpha}\) given in section 7.2.

Remember that

\[
\lim_{n \to \infty} \beta^{C_2}_{\alpha,n,G}(0\|\sigma_n) = (1 - \alpha)e^{-t'} > (1 - \alpha)e^{-dt'/(d+1)}
\]

for \(C_2 = \emptyset, S(A,B), L(A,B), L(A \to B)\). So, in summary, there is an advantage in using quantum correlation among samples.
8. Two-sample two-dimensional setting

Next, we proceed to the special case $n = 2$ and $d = 2$. For analysis of this case, we define the $3 \times 3$ real symmetric matrix $V = (v_{i,j})_{1 \leq i, j \leq 3}$ and a covariant POVM $M_{op}$ by

$$v_{i,j} \overset{\text{def}}{=} \langle \phi_{A,B}^i | \sigma | \phi_{A,B}^j \rangle$$

$$\phi_{A,B}^1 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|10\rangle + |10\rangle), \quad \phi_{A,B}^2 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (-i|10\rangle + i|10\rangle),$$

$$\phi_{A,B}^3 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle),$$

$$M_{op}(dg) \overset{\text{def}}{=} 4 \int_{SU(2)} g^{-2} |u_{op}\rangle \langle u_{op}| (g^{-2})^T v(dg),$$

where the vector $u_{op}$ is defined as

$$u_{op} \overset{\text{def}}{=} \frac{1}{2} (|01\rangle_{A_1,A_2} - |10\rangle_{A_1,A_2}) + \frac{\sqrt{3}}{2} (|00\rangle_{A_1,A_2} + |11\rangle_{A_1,A_2}).$$

Then, the following theorem holds.

**Theorem 6.** Assume that $\sigma$ satisfies the condition $p \overset{\text{def}}{=} \langle \phi_{A,B}^0 | \sigma | \phi_{A,B}^0 \rangle \leq \frac{1}{2}$. Then,

$$p^{L,SU(2) \times U(1)}_{0,2}(0\|\sigma) = \text{Tr} T(M_{op})\sigma^{-2}$$

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

holds, where $C = L(A \to B)$, $L(A \leftarrow B)$, $S(A, B)$. That is, the test $T(M_{op})$ is the UMP $SU(2) \times U(1)$-invariant $C$ test.

This theorem is shown in appendix O. Since the quantity $\text{Tr} \frac{I}{3} V^2 - (\text{Tr} \frac{I}{3} V)^2$ is greater than 0, the term $\frac{1}{3} (\text{Tr} \frac{I}{3} V^2 - (\text{Tr} \frac{I}{3} V)^2)$ indicates the advantage of this optimal test compared with the test $T_{inv}^{2,A \to B}$ introduced in section 6.3 (see (25)). Note that this advantage disappears if and only if the real symmetric matrix $V$ is constant.

On the other hand, as is shown in appendix P, the RHS of (35) can be evaluated as

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

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

That is, the quantity $\frac{1}{3} (\text{Tr} \frac{I}{3} V^2 - (\text{Tr} \frac{I}{3} V)^2)$ indicates the effect of using classical communication between $A_1$ and $A_2$. This is because the second type error probability is $(p^{L(A_1,A_2 \to B_1,B_2)}_{0,1,SU(2)}(0\|\sigma))^2 = (1 - \frac{2}{3} p)^2$ if we use the optimal test for one-sample case twice.
9. Two different systems

In section 6, we showed that if we can prepare the two identical states simultaneously and 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 from the same source simultaneously. However, as is discussed in this section, if we can prepare two quantum states independently from different sources, this Bell measurement is asymptotically optimal.

9.1. Formulation

Since the state on $\mathcal{H}_{A,B}^{\otimes 2}$ can be described as $\sigma_1 \otimes \sigma_2$, our hypotheses are given as

$$
H_0 : S^2_{\leq \epsilon} \overset{\text{def}}{=} \left\{ \sigma_1 \otimes \sigma_2 \left| (1 - \langle \phi^0_{A,B} | \sigma_1 | \phi^0_{A,B} \rangle) + (1 - \langle \phi^0_{A,B} | \sigma_2 | \phi^0_{A,B} \rangle) \leq \epsilon \right. \right\}
$$

versus

$$
H_1 : S^2_{< \epsilon} \overset{\text{def}}{=} \left\{ \sigma_1 \otimes \sigma_2 \left| (1 - \langle \phi^0_{A,B} | \sigma_1 | \phi^0_{A,B} \rangle) + (1 - \langle \phi^0_{A,B} | \sigma_2 | \phi^0_{A,B} \rangle) > \epsilon \right. \right\}.
$$

For any group action $G$ introduced in section 3.2, these hypotheses are invariant with respect to the $G \times G$-action defined by

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

When only two particles $\mathcal{H}_{A_1,B_1} \otimes \mathcal{H}_{A_2,B_2}$ are prepared, similarly to section 3.3, we can define the quantities $\beta^C_{\alpha,2,G \times G} (\leq \epsilon \| \sigma_1 \otimes \sigma_2)$ for the condition $C = \emptyset, S(A, B), L(A \rightleftarrows B), L(A \rightarrow B), S(A_1, A_2, B_1, B_2), L(A_1, A_2, B_1, B_2, B_3, B_4), L(A_1, A_2, B_1, B_2), L(A_1, A_2 \rightarrow B_1, B_2)$, in which, ‘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 $\beta^C_{\alpha,n,G \times G} (\leq \epsilon \| \sigma_1 \otimes \sigma_2)$ for the condition $C = \emptyset, S(A, B), L(A \rightleftarrows B), L(A \rightarrow B), S(A, B), L(A_1, A_2, B_1, B_2), L(A_1, A_2, B_1, B_2, B_3, B_4), L(A_1, A_2 \rightarrow B_1, B_2, B_3, B_4)$.

9.2. One sample setting

In this section, we treat the one sample and the $\epsilon = 0$ case. In the first step, we focus on the case of $C = \emptyset$. For this case, the relations

$$
\beta^0_{0,2,G \times G} (0 \| \sigma_1 \otimes \sigma_2) = \langle \phi^0_{A,B} \otimes \phi^0_{A,B} | \sigma_1 \otimes \sigma_2 | \phi^0_{A,B} \otimes \phi^0_{A,B} \rangle
$$

$$
= (1 - p_1) (1 - p_2)
$$

hold for $C = \emptyset, U(1), SU(d) \times U(1), U(d^2 - 1)$, where $p_1 = 1 - \langle \phi^0_{A,B} | \sigma_1 | \phi^0_{A,B} \rangle$.

Next, we focus on the case of $C = L(A \rightarrow B), L(A \rightleftarrows B), S(A, B)$. When we use the test $T_{inv}^{2,A \rightarrow B}$, the second error is

$$
\beta (T_{inv}^{2,A \rightarrow B}, \sigma_1 \otimes \sigma_2) = (1 - p_1) (1 - p_2) + \frac{p_1 p_2}{d^2 - 1}.
$$
Moreover, the optimal second error can also be calculated as
\[
\beta_{C, d \times G}^2(0, \sigma_1 \otimes \sigma_2) = (1 - p_1)(1 - p_2) + \frac{p_1 p_2}{d^2 - 1}
\] (43)
for \(C = L(A \rightarrow B), L(A \rightleftharpoons B), S(A, B)\) when \(p_1 p_2/(d^2 - 1) \leq (1 - p_1) p_2, p_1(1 - p_2)\). The proof is given in appendix Q. Hence, we obtain the following theorem.

**Theorem 7.** Assume that the quantities \(p_i = 1 - (\phi_{A,B}^0 | \sigma_i | \phi_{A,B}^0)\) \((i = 1, 2)\) satisfy the condition \(p_1 p_2/(d^2 - 1) \leq (1 - p_1) p_2, p_1(1 - p_2)\). Then,
\[
\beta_{C, d \times G}^2(0, \sigma_1 \otimes \sigma_2) = (1 - p_1)(1 - p_2) + \frac{p_1 p_2}{d^2 - 1}.
\] (44)

The test \(T_{inv}^{2, A \rightarrow B}\) is the C-UMP G-invariant test.

Using the PPT condition, Hayashi et al. [22] 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 \(T_{inv}^{1, A_1 \rightarrow B_1} \otimes T_{inv}^{1, A_2 \rightarrow B_2}\), the second error is
\[
\beta(T_{inv}^{1, A_1 \rightarrow B_1} \otimes T_{inv}^{1, A_2 \rightarrow B_2}, \sigma_1 \otimes \sigma_2) = \left(1 - \frac{d p_1}{d + 1}\right) \left(1 - \frac{d p_2}{d + 1}\right).
\]
In this case, as is proven in appendix R, the optimal second error is calculated as
\[
\beta_{C, d \times G}^2(0, \sigma_1 \otimes \sigma_2) = \left(1 - \frac{d p_1}{d + 1}\right) \left(1 - \frac{d p_2}{d + 1}\right),
\] (45)
for \(G = SU(d), SU(d) \times U(1), U(d^2 - 1)\). Thus, the test \(T_{inv}^{1, A_1 \rightarrow B_1} \otimes T_{inv}^{1, A_2 \rightarrow B_2}\) is the C-UMP G-invariant test. Hayashi et al. [22] derived this optimal test for the case of \(\sigma_1 = \sigma_2\) and \(d = 2\).

9.3. Asymptotic setting

In the small deviation asymptotic setting with \(n\) samples, we focus on the case \(\epsilon = \delta/n\) and \(t'/n = 1 - (\phi_{A,B}^0 | \sigma_i' | \phi_{A,B}^0)\). In this setting, as is shown in appendix S,
\[
\lim_{n \rightarrow \infty} \beta_{\epsilon, 2n, d \times G}^0(\epsilon \sigma_{1,n} \otimes \sigma_{2,n}) = \beta_\epsilon(\leq \delta ||t'_1 + t'_2||)
\] (46)
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 \(T_{inv}^{2, A \rightarrow B}\) for all systems \(H_{A_1} \otimes H_{B_1}, \ldots, H_{A_n} \otimes H_{B_n}\), whose state is \(\sigma_{1,n} \otimes \sigma_{2,n}\), the number \(k\) for detecting \(T_{inv}^{2, A \rightarrow B}\) almost obeys the Poisson distribution \(e^{-||t'_1 + t'_2||}[(t'_1 + t'_2)^k/k!]\). This is because
\[
n \left(1 - \left(1 - \frac{t'_1}{n}\right) \left(1 - \frac{t'_2}{n}\right) + \frac{t'_1 t'_2}{n^2}\right) \rightarrow t'_1 + t'_2.
\]
Considering hypothesis testing for this Poisson distribution, we can show that the \(L(A \rightarrow B)U(d^2 - 1) \times U(d^2 - 1)\)-invariant test \(T_{\epsilon, A}^n \overset{\text{def}}{=} T_{inv}^n(T_{inv}^{2, A \rightarrow B}, \max p_1 + p_2 = \epsilon p_1 + p_2 - [d^2 p_1 p_2/(d^2 - 1)])\) satisfies
\[
\lim_{n \rightarrow \infty} \beta(T_{\epsilon, A}^n, \sigma_{1,n} \otimes \sigma_{2,n}) = \beta_\epsilon(\leq \delta ||t'_1 + t'_2||).
\]
Hence, combining with (46), we obtain the following theorem.
Theorem 8. When \( \frac{t'_i}{n} = 1 - \langle \phi^0_{A,B} | \sigma^i_{t,n} | \phi^0_{A,B} \rangle \) for \( i = 1, 2 \),

\[
\lim_{n \to \infty} \beta^C_{t'_i, 2n; G \times G} \leq \frac{\delta}{n} \| \sigma^i_{t,n} \otimes \sigma^i_{t', 2n} \| = \beta_a(\leq \delta \| t'_1 + t'_2 \|),
\]

for \( C = \emptyset, L(A \rightarrow B), L(A \equiv B), S(A, B) \) and \( G = SU(d) \times U(1), U(d^2 - 1) \). Thus, the test \( T_{C, A,B}^{n, 2} \) is the C-UMP G-invariant test in the asymptotic small deviation setting.

The asymptotic optimal testing scheme is illustrated in figure 1.

Moreover, if we use a test based on the Bell measurement instead of the test \( T_{inv}^{A \rightarrow B} \), the bound \( \beta_a(\leq \delta \| t'_1 + t'_2 \|) \) can be attained for a reason similar to that which applies in lemma 5.

10. Three different systems

Finally, we treat the case of three quantum states that are prepared independently. Similarly to section 9.1, we consider two hypotheses

\[
H_0 : \mathcal{S}_{\leq \epsilon}^3 \equiv \left\{ \prod_{i=1}^3 | \sigma_i | \sum_{i=1}^3 (1 - \langle \phi^0_{A,B} | \sigma_i | \phi^0_{A,B} \rangle) \leq \epsilon \right\}
\]

versus

\[
H_1 : \mathcal{S}_{> \epsilon}^3 \equiv \left\{ \prod_{i=1}^3 | \sigma_i | \sum_{i=1}^3 (1 - \langle \phi^0_{A,B} | \sigma_i | \phi^0_{A,B} \rangle) > \epsilon \right\},
\]

where the given state is assumed to be \( \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \). Similarly we define the quantities \( \beta_{A,3, G \times G}^{C}(\leq \epsilon \| \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \|) \) for the condition \( C = \emptyset, S(A, B), L(A \equiv B), L(A \rightarrow B), L((A_1, A_2, A_3) \rightarrow (B_1, B_2, B_3)) \), \( L(A_1, A_2, A_3, B_1, B_2, B_3) \), \( S(A_1, A_2, A_3, B_1, B_2, B_3) \) under the similar \( G \times G \times G \)-invariance.

Similarly to section 9.2, we focus on the case of \( C = L(A \rightarrow B), L(A \equiv B), S(A, B) \) with one sample. For this case, as has been 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 forms a POVM:

\[
M_{cov}^3 (dg_1, dg_2, dg_3) \equiv d^3 g_1 \otimes g_2 \otimes g_3 |GHZ\rangle \langle GHZ| (g_1 \otimes g_2 \otimes g_3)^\dagger \psi(dg_1) \psi(dg_2) \psi(dg_3).
\]

As is proved in appendix \( T \), the test \( T_{inv}^{3, A \rightarrow B} \equiv T(M_{cov}^3) \) has the form

\[
T_{inv}^{3, A \rightarrow B} = P_1 \otimes P_2 \otimes P_3 + \frac{(d + 2) P_1^c \otimes P_2^c \otimes P_3^c}{(d + 1)^3(d - 1)}
\]

\[
+ \frac{P_1 \otimes P_2^c \otimes P_3^c + P_1^c \otimes P_2 \otimes P_3^c + P_1^c \otimes P_2^c \otimes P_3}{(d + 1)^2(d - 1)},
\]

(47)
Assume that $P_i = |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0|$, $P_i^c = I - P_i$. Thus, this test is $U(d^2 - 1) \times U(d^2 - 1) \times U(d^2 - 1)$-invariant. Hence, when we use the test $T^3_{\text{inv}}$, the second error is

$$\beta(T^3_{\text{inv}}, \sigma_1 \otimes \sigma_2 \otimes \sigma_3) \leq \left(1 - p_1\right)(1 - p_2)(1 - p_3) + \frac{(d + 2)p_1p_2p_3}{(d + 1)^2(d - 1)} + \frac{p_1p_2(1 - p_3) + p_1(1 - p_2)p_3 + (1 - p_1)p_2p_3}{(d + 1)^2(d - 1)}.$$ 

Moreover, the optimal second error can also be calculated as

$$\beta^C_{0,3,G \times G \times G}(0\|\sigma_1 \otimes \sigma_2 \otimes \sigma_3) \geq \left(1 - p_1\right)(1 - p_2)(1 - p_3) + \frac{(d + 2)p_1p_2p_3}{(d + 1)^2(d - 1)} + \frac{p_1p_2(1 - p_3) + p_1(1 - p_2)p_3 + (1 - p_1)p_2p_3}{(d + 1)^2(d - 1)}$$

(48)

for $C = L(A \rightarrow B)$, $L(A \Rightarrow B)$, $S(A, B)$ when $p_i := 1 - |\langle \phi_{A,B}^0 | \sigma_i | \phi_{A,B}^0 \rangle| \leq (d - 1)/d$ for $i = 1, 2, 3$. The proof is given in appendix T. Hence, we obtain the following theorem.

**Theorem 9.** Assume that $p_i := 1 - |\langle \phi_{A,B}^0 | \sigma_i | \phi_{A,B}^0 \rangle| \leq \frac{d - 1}{d}$ for $i = 1, 2, 3$. Then,

$$\beta^C_{0,3,G \times G \times G}(0\|\sigma_1 \otimes \sigma_2 \otimes \sigma_3) \leq \left(1 - p_1\right)(1 - p_2)(1 - p_3) + \frac{(d + 2)p_1p_2p_3}{(d + 1)^2(d - 1)} + \frac{p_1p_2(1 - p_3) + p_1(1 - p_2)p_3 + (1 - p_1)p_2p_3}{(d + 1)^2(d - 1)}.$$ 

The test $T^3_{\text{inv}}$ is the C-UMP $G$-invariant test.

On the other hand, in the case of $C = L(A_1, A_2, A_3 \rightarrow B_1, B_2, B_3)$, $L(A_1, A_2, A_3, B_1, B_2, B_3)$, $S(A_1, A_2, A_3, B_1, B_2, B_3)$, we can show the optimality of the test $T^1_{\text{inv}} \otimes T^1_{\text{inv}} \otimes T^1_{\text{inv}}$, similarly to (45). Moreover, we can derive the same result in the small deviation asymptotic setting with $n$ samples.

### 11. Conclusion

In this paper, we have considered the hypothesis testing problem when the null hypothesis consists only of the required entangled state or is its neighbourhood. In order to treat the entanglement structure, we considered three settings concerning the range of accessible measurements as follows: **M1:** all measurements are allowed. **M2:** a measurement is forbidden if it requires quantum correlation between two distinct parties. **M3:** a measurement is forbidden if it requires quantum correlation between two distinct parties, or such among local samples. As a result, we found that there is no difference between the accuracies of **M1** and **M2** to 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 prepare the two states from the same source. In order to avoid this difficulty, we proved that even if the two states are prepared from different sources, 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 for several examples. Thus, as has been demonstrated by Hayashi et al [24], it is a future target to demonstrate the proposed testing experimentally.

In this paper, the optimal test is constructed based on a continuous valued POVM. However, any realizable POVM is finite valued. Hence, it is desirable to construct the optimal test based on a finite-valued POVM. This problem has been partially discussed by Hayashi et al, and is more deeply discussed in another paper [30].

The obtained protocol is essentially equivalent to the following procedure based on quantum teleportation. First, we perform quantum teleportation from the system $A$ to the system $B$, which succeeds when the true state is the required maximally entangled state. Next, we check whether the state of the system $B$ is the initial state of the system $A$. Hence, an interesting relation between the obtained results and quantum teleportation is expected. Such a relation was partially treated by Virmani and Plenio [28], and will be treated in a forthcoming paper [31] more deeply.

As another problem, Acín et al [26] discussed the problem of testing whether a given $n$-i.i.d. state of an unknown pure state is the $n$-fold tensor product of a pure maximally entangled state (not the specific maximally entangled state) in the two-dimensional system. This problem is closely related to universal entanglement concentration [29]. Its $d$-dimensional case is a future problem.

Acknowledgments

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. We thank the referees and the editor for helpful comments concerning this manuscript.

Appendix A. Proof of lemmas 1 and 2

Assume that a set of tests satisfying the condition $C$ is invariant for the action of $G_2$. Let $T \in T_{a, \leq \epsilon}$ be a test satisfying the condition $C$; then the test $\overline{T} \overset{\text{def}}{=} (f(g)^\dagger)^\otimes n T f(g)^{\otimes n}$ also satisfies the condition $C$ and belongs to the set $T_{a, \leq \epsilon}$. Since

$$\beta(T, (f(g)\sigma f(g)^\dagger)^{\otimes n}) = \beta(f(g)^\dagger T f(g), \sigma^{\otimes n}),$$

we obtain

$$\max_{g \in G} \beta(T, (f(g)\sigma f(g)^\dagger)^{\otimes n}) \geq \int_{G_2} \beta(T, (f(g)\sigma f(g)^\dagger)^{\otimes n}) \nu_G(dg)$$

$$= \beta(\overline{T}, (f(g)\sigma f(g)^\dagger)^{\otimes n}) \geq \beta^C_{a, \leq \epsilon}(\leq \epsilon \| \sigma).$$

Hence,

$$\min_{T \in T_{a, \leq \epsilon}} \max_{g \in G} \beta(T, (f(g)\sigma f(g)^\dagger)^{\otimes n}) \geq \min_{T \in T_{a, \leq \epsilon}} \int_{G} \beta(T, (f(g)\sigma f(g)^\dagger)^{\otimes n}) \nu_G(dg)$$

$$\geq \beta^C_{a, \leq \epsilon}(\leq \epsilon \| \sigma). \quad (A.1)$$
On the other hand, if the $G_2$-invariant test $T \in \mathcal{T}^n_{a,\leq \epsilon}$ satisfies the condition $C$ and
\[ \beta(T, \sigma^\otimes n) = \beta^C_{a,n,G_2}(\leq \epsilon \| \sigma), \]
then
\[ \beta(T, (f(g)\sigma f(g)^\dagger)^\otimes n) = \beta(T, \sigma^\otimes n) = \beta^C_{a,n,G_2}(\leq \epsilon \| \sigma), \quad \forall g \in G_2, \]
which implies
\[ \max_{g \in G} \beta(T, (f(g)\sigma f(g)^\dagger)^\otimes n) = \beta^C_{a,n,G_2}(\leq \epsilon \| \sigma). \]

Thus, we obtain the inequality opposite to (A.1). Therefore, the proof of lemma 1 is completed.

Next, we proceed to prove lemma 2. Since the equation
\[ \int_{G_1} \beta(T, (f(g)\sigma f(g)^\dagger)^\otimes n) v_{G_1}(dg) = \int_{G_1} \beta((f(g')\dagger)^\otimes n T f(g')^\otimes n, (f(g)\sigma f(g)^\dagger)^\otimes n) v_{G_1}(dg) \]
holds for $\forall g' \in G_2$, we obtain
\[
\min_{T \in \mathcal{T}^n_{a,\leq \epsilon}} \max_{g \in G_1} \beta(T, (f(g)\sigma f(g)^\dagger)^\otimes n) \geq \min_{T \in \mathcal{T}^n_{a,\leq \epsilon}} \int_{G_1} \beta(T, (f(g)\sigma f(g)^\dagger)^\otimes n) v_{G_1}(dg)
\]
\[ = \min_{T \in \mathcal{T}^n_{a,\leq \epsilon}} \int_{G_1} \int_{G_1} \beta((f(g')\dagger)^\otimes n T f(g')^\otimes n, (f(g)\sigma f(g)^\dagger)^\otimes n)
\]
\[ \times v_{G_1}(dg) v_{G_2}(dg') \]
\[ = \min_{T \in \mathcal{T}^n_{a,\leq \epsilon}} \int_{G_1} \beta((\overline{T}, (f(g)\sigma f(g)^\dagger)^\otimes n) v_{G_1}(dg)
\]
\[ \geq \int_{G_1} \beta^C_{a,n,G_2}(\leq \epsilon \| f(g)\sigma f(g)^\dagger) v_{G_1}(dg)
\]
\[ = \int_{G_1} \beta^C_{a,n,G_1}(\leq \epsilon \| f(g)\sigma f(g)^\dagger) v_{G_1}(dg). \quad (A.2) \]

Since $\beta(T', \sigma) = \beta(T', f(g)\sigma f(g)^\dagger)$ for any $G_1$-invariant test $T'$, we have
\[ \beta^C_{a,n,G_1}(\leq \epsilon \| \sigma) = \beta^C_{a,n,G_1}(\leq \epsilon \| f(g)\sigma f(g)^\dagger), \]
which implies
\[ \int_{G_1} \beta^C_{a,n,G_1}(\leq \epsilon \| f(g)\sigma f(g)^\dagger) v_{G_1}(dg) = \beta^C_{a,n,G_1}(\leq \epsilon \| \sigma). \]

We choose a $G_1$-invariant test $T \in \mathcal{T}^n_{a,\leq \epsilon}$ satisfying the condition $C$ and
\[ \beta^C_{a,n,G_1}(\leq \epsilon \| \sigma) = \beta(T, \sigma). \]

Then,
\[ \max_{g \in G_1} \beta(T, (f(g)\sigma f(g)^\dagger)^\otimes n) = \beta(T, \sigma) = \beta^C_{a,n,G_1}(\leq \epsilon \| \sigma). \]

Thus, we obtain the inequality opposite to (A.2), which yields lemma 2.

*New Journal of Physics* **11** (2009) 043028 (http://www.njp.org/)
Appendix B. Basic properties of classical tests

In classical hypothesis testing, the Neyman–Pearson lemma plays a central role.

**Lemma 6.** Assume that the null hypothesis involves one probability distribution \( P_0 \) and the alternative one involves another probability distribution \( P_1 \). For any \( 1 > \alpha > 0 \), we choose \( r \) and \( \gamma \) such that

\[
\begin{align*}
P_0 \left\{ x \left| \frac{P_0(x)}{P_1(x)} > r \right. \right\} & \leq 1 - \alpha, \\
P_0 \left\{ x \left| \frac{P_0(x)}{P_1(x)} < r \right. \right\} & \leq \alpha, \\
\gamma P_0 \left\{ x \left| \frac{P_0(x)}{P_1(x)} = r \right. \right\} & = 1 - \alpha - P_0 \left\{ x \left| \frac{P_0(x)}{P_1(x)} > r \right. \right\},
\end{align*}
\]

and define the test \( \tilde{T}_{P_0, P_1, \alpha} \) as

\[
\tilde{T}_{P_0, P_1, \alpha}(x) = \begin{cases} 
1, & \text{if } \frac{P_0(x)}{P_1(x)} > r, \\
\gamma, & \text{if } \frac{P_0(x)}{P_1(x)} = r, \\
0, & \text{if } \frac{P_0(x)}{P_1(x)} < r.
\end{cases}
\] (B.1)

Then, the test \( T_{P_0, P_1, \alpha} \) is the MP level-\( \alpha \) test.

In classical statistics, the function \( \frac{P_0(x)}{P_1(x)} \) is called the *likelihood ratio*, which plays an important role.

**Proof.** Assume that \( \tilde{T}^* \) is a level-\( \alpha \) test. We focus on the weighted sum of two kinds of error probabilities

\[
\sum_x P_0(x)(1 - \tilde{T}^*(x)) + r \sum_x P_1(x) \tilde{T}^*(x) \leq \sum_x (P_0(x) - r P_1(x)) \tilde{T}^*(x) \leq \sum_x (P_0(x) - r P_1(x)) \tilde{T}_x(x),
\]

we can see

\[
\sum_x P_0(x)(1 - \tilde{T}^*(x)) + r \sum_x P_1(x) \tilde{T}^*(x) = 1 - \sum_x (P_0(x) - r P_1(x)) \tilde{T}^*(x) \geq 1 - \sum_x (P_0(x) - r P_1(x)) \tilde{T}_{P_0, P_1, \alpha}(x) = \sum_x P_0(x)(1 - \tilde{T}_{P_0, P_1, \alpha}(x)) + r \sum_x P_1(x) \tilde{T}_{P_0, P_1, \alpha}(x).
\]

Hence, the relation

\[
\sum_x P_0(x)(1 - \tilde{T}^*(x)) = \sum_x P_0(x)(1 - \tilde{T}_{P_0, P_1, \alpha}(x)) = \alpha
\]

yields

\[
\sum_x P_1(x) \tilde{T}^*(x) \geq \sum_x P_1(x) \tilde{T}_{P_0, P_1, \alpha}(x).
\]
Corollary 2. If the test $\tilde{T}$ has the form (B.1), i.e. has the form of a likelihood ratio test, then the inequality

$$\sum_x P_0(x)(1 - \tilde{T}(x)) \leq \sum_x P_1(x)(1 - \tilde{T}(x))$$

holds.

Proof. We focus on the test $\tilde{T}'(x) \overset{\text{def}}{=} 1 - \alpha$. Since the test $\tilde{T}'$ is trivially at level-$\alpha$, lemma 6 guarantees that $\sum_x P_1(x)\tilde{T}'(x) \leq \sum_x P_1(x)\tilde{T}'(x) = 1 - \alpha$, which implies that $\sum_x P_0(x)(1 - \tilde{T}(x)) = \alpha \leq \sum_x P_1(x)(1 - \tilde{T}(x))$. □

Appendix C. Proof of proposition 1

Since the likelihood ratio $P_n^\epsilon(k)/P_n^p(k)$ is a monotonic decreasing function of $k$, the test $\tilde{T}_{\epsilon,\alpha}$ equals the test $\tilde{T}_{p_n,\epsilon,\alpha}$. Lemma 6 in appendix B guarantees that the test $\tilde{T}_{\epsilon,\alpha}$ is the MP level-$\alpha$ test for the null hypothesis $P_n^\epsilon$. Since a level-$\alpha$ test for the null hypothesis $P_n^{\epsilon,\beta}$ is a level-$\alpha$ test for the null hypothesis $P_n^\epsilon$, $\beta^\alpha_{\epsilon} (\leq \epsilon \| q) \geq P_n^{\epsilon,\beta}(\tilde{T}_{\epsilon,\alpha})$.

(C.1)

Since the likelihood ratio $P_n^\epsilon(k)/P_n^p(k)$ is a monotonic decreasing function of $k$ for $p_0 < p_1$, the test $\tilde{T}_{\epsilon,\alpha}$ is a likelihood ratio test of $P_n^\epsilon$ and $P_n^p$. Hence, corollary 2 guarantees that $P_n^\epsilon(\tilde{T}_{\epsilon,\alpha}) \geq P_n^p(\tilde{T}_{\epsilon,\alpha})$. That is, the probability $P_n^\epsilon(\tilde{T}_{\epsilon,\alpha})$ is a monotonic decreasing function of $p$. Since the definition of the test $\tilde{T}_{\epsilon,\alpha}$ implies that $P_n^\epsilon(\tilde{T}_{\epsilon,\alpha}) = 1 - \alpha$, $P_n^p(\tilde{T}_{\epsilon,\alpha}) \leq 1 - \alpha$ if $p \leq \epsilon$. In other words, the test $\tilde{T}_{\epsilon,\alpha}$ is level-$\alpha$ for the null hypothesis $P_n^{\epsilon,\beta}$. Hence, it follows from the inequality (C.1) that the test $\tilde{T}_{\epsilon,\alpha}$ is level-$\alpha$ UMP test for the null hypothesis $P_n^{\epsilon,\beta}$.

Appendix D. Proof of proposition 2

$\tilde{T}_{\delta/n,\epsilon,\alpha}$ is a level-$\alpha$ test for the null hypothesis $P_{\delta/n}$, $\forall t \in [0, \delta] \limsup_{n \to \infty} 1 - \sum_k P_1(k)\tilde{T}_{\delta/n,\epsilon,\alpha}(k) = \limsup_{n \to \infty} 1 - \sum_k P_{t/n}(k)\tilde{T}_{\delta/n,\epsilon,\alpha}(k) \leq \alpha$. Hence, for $\forall \epsilon > 0$ there exists $N$ such that $\forall n \geq N, \forall t \in [0, \delta] 1 - P_t(\tilde{T}_{\delta/n,\epsilon,\alpha}) \leq \alpha + \epsilon$. Hence,

$$P_t(\tilde{T}_{\delta/n,\epsilon,\alpha}) \geq \beta_{\alpha + \epsilon}(\leq \delta \| t').$$

Since $\liminf_{n \to \infty} P_t(\tilde{T}_{\delta/n,\epsilon,\alpha}) = \liminf_{n \to \infty} P_{t/n}(\tilde{T}_{\delta/n,\epsilon,\alpha}) = \liminf_{n \to \infty} \beta_{\alpha}(\leq \delta \| t')$, \n
$$\liminf_{n \to \infty} \beta_{\alpha}(\leq \delta \| t') \geq \beta_{\alpha}(\leq \delta \| t').$$

Since the continuity of $\alpha \mapsto \beta_{\alpha}(\leq \delta \| t')$ follows from proposition 3,

$$\liminf_{n \to \infty} \beta_{\alpha}(\leq \delta \| t') \geq \beta_{\alpha}(\leq \delta \| t').$$
Since $\tilde{T}_{\delta,\alpha-\epsilon}$ is a level-$\alpha$ test for the null hypothesis $t \in [0, \delta]$ for $\forall \epsilon > 0$, we have $\forall t \in [0, \delta]$ \[ \lim_{n \to \infty} \sup P_{t/n}(\tilde{T}_{\delta,\alpha-\epsilon}) = \lim_{n \to \infty} 1 - \sum_k P_1(k) \tilde{T}_{\delta,\alpha-\epsilon}(k) \leq \alpha - \epsilon. \]

Hence, there exists $N$ such that $\forall n \geq N$, $\forall t \in [0, \delta]$ \[ \limsup_{n \to \infty} \frac{1}{2^n} \sum_{k} P_1(k) \tilde{T}_n(t') \leq \alpha - \epsilon. \]

Thus, $\beta_n(\leq \delta \| t' \|) \leq \beta_{\alpha-\epsilon}(\leq \delta \| t' \|)$, which implies \[ \limsup_{n \to \infty} \beta_n(\leq \delta \| t' \|) \leq \beta_{\alpha-\epsilon}(\leq \delta \| t' \|). \]

The continuity of $\alpha \mapsto \beta_{\alpha}(\leq \delta \| t' \|)$ guarantees that \[ \limsup_{n \to \infty} \beta_n(\leq \delta \| t' \|) \leq \beta_{\alpha}(\leq \delta \| t' \|). \]

Appendix E. Proof of (9)

For a fixed density matrix $\sigma$ on $\mathcal{H}_{A,B}$, we define a density matrix $\sigma_q$ by $\sigma_q \triangleq \sigma_{q}$. Let $T$ be a $U(1)$-invariant test at level-$\alpha$. $U(1)$-invariance yields \[ \text{Tr} U_{\alpha}^{\otimes n} T U_{\alpha}^{\otimes n} = \text{Tr} \sigma_{q}^{\otimes n} T \sigma_{q}^{\otimes n}. \]

Hence, \[ \text{Tr} \sigma_{q}^{\otimes n} = \frac{1}{2\pi} \int_0^{2\pi} \text{Tr} U_{\alpha}^{\otimes n} T \sigma_{q}^{\otimes n} U_{\alpha}^{\otimes n} d\theta = \text{Tr} \sigma_{q}^{\otimes n}. \]

where we define $\sigma_{q}$ as $\sigma_{q} \triangleq \frac{1}{2\pi} \int_0^{2\pi} \langle \phi_{\alpha}^0 | \sigma_{q} \sigma_{q}^{\dagger} | \phi_{\alpha}^0 \rangle d\theta$. 

New Journal of Physics 11 (2009) 043028 (http://www.njp.org/)
By using the notation $P^n_{k,|\phi_{A,B}^0\rangle}$ defined in (7), the unitary $U^\otimes_n$ is diagonalized as $U^\otimes_n = \sum_{k=0}^n e^{i\theta_k} P^n_{k,|\phi_{A,B}^0\rangle}$. Since

$$A^\otimes_q = \sum_{k=0}^n \sqrt{\frac{q}{p}} \sqrt{\frac{1-q}{1-p}} P^n_{k,|\phi_{A,B}^0\rangle}$$

is commutative with the projection $P^n_{k,|\phi_{A,B}^0\rangle}$, we obtain

$$\sigma^n_q = \sum_{k=0}^n P^n_{k,|\phi_{A,B}^0\rangle} \sigma^\otimes_q P^n_{k,|\phi_{A,B}^0\rangle}$$

$$= \sum_{k=0}^n P^n_{k,|\phi_{A,B}^0\rangle} A^\otimes_q \sigma^\otimes_p A^\otimes_q P^n_{k,|\phi_{A,B}^0\rangle}$$

$$= \sum_{k=0}^n \left( \frac{q}{p} \right)^k \left( \frac{1-q}{1-p} \right)^{n-k} P^n_{k,|\phi_{A,B}^0\rangle} \sigma^\otimes_p P^n_{k,|\phi_{A,B}^0\rangle}.$$

In the following, we focus on hypothesis testing of the null hypothesis $\sigma^n_{\epsilon}$ and the alternative hypothesis $\sigma^n_{p}$ because the test $T$ is a level-$\alpha$ test with the null hypothesis $\sigma^n_{\epsilon}$ at least. Since $P^n_{k,|\phi_{A,B}^0\rangle} \sigma^\otimes_p P^n_{k,|\phi_{A,B}^0\rangle}$ does not depend on $q$, two states $\sigma^n_{\epsilon}$ and $\sigma^n_{p}$ commute. So, there exists a common basis $\{|e_{k,l}\rangle\}$ diagonalizing them. As they are written as $\sigma_{\epsilon} = \sum_k \sum_l P^n_{0,|e_{k,l}\rangle}$ and $\sigma_p = \sum_k \sum_l P^n_{1,|e_{k,l}\rangle}$, our problem is essentially equivalent to classical hypothesis testing of the null hypothesis $P_0 \overset{\text{def}}{=} (P^n_{0,|e_{k,l}\rangle})$ and the alternative hypothesis $P_1 \overset{\text{def}}{=} (P^n_{1,|e_{k,l}\rangle})$. Since the likelihood ratio is given by the ratio $(e^k(1-\epsilon)^{n-k}/p^k(1-p)^{n-k})$, we have

$$T^n_{\epsilon,\alpha} = \sum_k \sum_l \tilde{T}^n_{\epsilon,\alpha}(k)|e_{k,l}\rangle|e_{k,l}\rangle,$$

where $\tilde{T}^n_{\epsilon,\alpha}(k)$ is given in (6). Hence, lemma 6 in appendix B guarantees that

$$\text{Tr } T^n_{\epsilon,\alpha} \sigma^n_p \geq \text{Tr } T^n_{\epsilon,\alpha} \sigma^n_{\epsilon}$$

because the test $T$ is a level-$\alpha$ test of the null hypothesis $\sigma^n_{\epsilon}$. Since $T^n_{\epsilon,\alpha}$ is $U(1)$-invariant, equation (E.1) guarantees that

$$\text{Tr } T^n_{\epsilon,\alpha} \sigma^n_{\epsilon} \geq \text{Tr } T^n_{\epsilon,\alpha} \sigma^n_{p}.$$

The equation $\text{Tr } T^n_{\epsilon,\alpha} \sigma^n_{\epsilon} = \beta^n_{\epsilon} (\leq \epsilon \parallel p)$ yields (9).

**Appendix F. Proof of lemma 3**

Let $T$ be a one-way LOCC ($A \rightarrow B$) level-0 test for the null hypothesis $|\phi_{A,B}^0\rangle|\phi_{A,B}^0\rangle$. We denote Alice’s first measurement by $M = \{M_l\}$. In this case, Bob’s measurement can be described by
the two-valued measurement \( \{ T'_0, I - T'_0 \} \), where \( T'_0 \) corresponds to the decision accepting the state \( |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0| \). Hence the test \( T \) can be described as

\[
T = \sum_i M_i \otimes T'_0.
\]

When Alice observes the data \( i \), Bob’s state is \( \frac{1}{\text{Tr} M_i} M_i \). Since this test is at level-0, \( T'_0 \geq P_i \), where \( P_i \) is the projection to the range of the matrix \( M_i \).

Here, we diagonalize \( M_i \) as \( M_i = \sum_j p_{i,j} |u_{i,j}\rangle \langle u_{i,j}| \). Since \( P_i \geq |u_{i,j}\rangle \langle u_{i,j}| \), the POVM \( M' = \{ p_{i,j} |u_{i,j}\rangle \langle u_{i,j}| \}_{i,j} \), satisfies

\[
T(M') = \sum_{i,j} p_{i,j} |u_{i,j}\rangle \langle u_{i,j}| \otimes P_i = \sum_i M_i \otimes P_i \leq \sum_i M_i \otimes T'_0 = T.
\]

**Appendix G. Proof of lemma 4**

It follows from condition (19) that \( \sum_i p_i = 1 \). We choose the vector \( \phi \equiv \sqrt{d} \sum_i p_i u_i \otimes u'_i \). Since the function \( x \rightarrow |x|^2 \) is convex, we obtain

\[
\langle \phi | T | \phi \rangle \geq \sum_i p_i \langle \phi | u_i \otimes u'_i \rangle \langle u_i \otimes u'_i | \phi \rangle
\]

\[
= d \sum_i p_i |\langle \phi | u_i \otimes u'_i \rangle|^2 \geq d |\sum_i p_i \langle \phi | u_i \otimes u'_i \rangle|^2
\]

\[
= d \left| \frac{1}{\sqrt{d}} \langle \phi | \phi \rangle \right|^2 = \| \phi \|^4.
\]

Hence,

\[
1 \geq \text{Tr} T \frac{|\langle \phi | \phi \rangle|}{\| \phi \|^2} = \| \phi \|^2.
\]

On the other hand,

\[
\langle \phi_{A,B}^0 | \phi \rangle = \sqrt{d} \sum_i p_i \langle \phi_{A,B}^0 | u_i \otimes u'_i \rangle = 1.
\]
Since $\|\phi_{A,B}^0\| = 1$, we obtain

$$\varphi = \phi_{A,B}^0.$$  

Appendix H. Proof of (15)

The representation space $H_A \otimes H_B$ of an $SU(d)$-action can be irreducibly decomposed into two subspaces: one is the one-dimensional space $\langle \phi_{A,B}^0 \rangle$ spanned by $\phi_{A,B}^0$. The other is its orthogonal complement $\langle \phi_{A,B}^0 \rangle^\perp$. Since $T_{\text{inv}}^{1,A\to B}$ is $SU(d)$-invariant, it has the form

$$T_{\text{inv}}^{1,A\to B} = t_0|\phi_{A,B}^0\rangle\langle \phi_{A,B}^0| + t_1(I - |\phi_{A,B}^0\rangle\langle \phi_{A,B}^0|).$$

The equation $\langle \phi_{A,B}^0 | T_{\text{inv}}^{1,A\to B} | \phi_{A,B}^0 \rangle = 1$ implies that $t_0 = 1$. Its trace can be calculated as

$$\text{Tr} T_{\text{inv}}^{1,A\to B} = \int \text{d} \text{Tr} |\varphi \otimes \overline{\varphi}\rangle\langle \varphi \otimes \overline{\varphi}|\nu(d\varphi) = d.$$ 

Hence, $t_1 = (d - 1)/(d^2 - 1) = 1/(d + 1)$.

Appendix I. Proof of (22)

Lemma 7. If the test $T$ is separable on the space $H_A \otimes H_B$, then

$$\text{Tr} T \geq d \langle \phi_{A,B}^0 | T | \phi_{A,B}^0 \rangle,$$  

where $d$ is the dimension of $H_A$.

Proof. Since $T$ is separable, $T$ has the form $T = \sum_i |u_i \otimes u_i'|\langle u_i \otimes u_i'|$. For any two vectors $u, u'$, the Schwarz inequality yields

$$\langle u \otimes u' | u \otimes u' \rangle = \langle u | u \rangle \langle u' | u' \rangle = \langle u | u \rangle \langle u' | u' \rangle \geq |\langle u | u' \rangle|^2 = d |\langle \phi_{A,B}^0 | u \otimes u' \rangle|^2.$$ 

Hence, we have

$$\text{Tr} |u_i \otimes u_i'|\langle u_i \otimes u_i'| \geq d \langle \phi_{A,B}^0 | u_i \otimes u_i' \rangle \langle u_i \otimes u_i' | \phi_{A,B}^0 \rangle.$$ 

Taking the sum, we obtain (I.1). \qed

Assume that $T$ is an $SU(d)$-invariant separable test. From the discussion in appendix H, the test $T$ has the form

$$T = t_0|\phi_{A,B}^0\rangle\langle \phi_{A,B}^0| + t_1(I - |\phi_{A,B}^0\rangle\langle \phi_{A,B}^0|).$$
Lemma 7 implies that \( t_1 (d^2 - 1) + t_0 \geq d t_0 \), i.e. \( t_1 \geq (1/(d + 1)) t_0 \). Hence, the test \( T \) has another form

\[
T = t_0' \left( |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0| + \frac{1}{d+1} (I - |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0|) \right) + t_1' \frac{d}{d+1} (I - |\phi_{A,B}^0\rangle \langle \phi_{A,B}^0|)
\]

\[
= t_0' T_{\text{inv}}^{1,A\rightarrow B} + t_1' (I - T_{\text{inv}}^{1,A\rightarrow B}).
\]

Since

\[
\text{Tr} \sigma T_{\text{inv}}^{1,A\rightarrow B} = 1 - \frac{dp}{d+1}, \quad \text{Tr} \sigma (I - T_{\text{inv}}^{1,A\rightarrow B}) = \frac{dp}{d+1},
\]

our problem is equivalent to hypothesis testing with the probability \( (1 - (dp/(d+1)), dp/(d+1)) \). Thus, we obtain (22).

**Appendix J. Proof of lemma 5 and (24)**

**Lemma 8.** A state \( u \in \mathcal{H}_A \otimes \mathcal{H}_B \) is maximally entangled if and only if

\[
|\phi_{A_1,B_1}^0\rangle \langle \phi_{A_1,B_1}^0| \otimes (I - |\phi_{A_2,B_2}^0\rangle \langle \phi_{A_2,B_2}^0|) u \otimes \bar{u} = 0,
\]

\[
(I - |\phi_{A_1,B_1}^0\rangle \langle \phi_{A_1,B_1}^0|) \otimes |\phi_{A_2,B_2}^0\rangle \langle \phi_{A_2,B_2}^0| u \otimes \bar{u} = 0.
\]

**Proof.** The condition (J.1) is equivalent to the condition that \( \langle \phi_{A_1,B_1}^0| u \otimes \bar{u} \rangle \) equals constant times \( |\phi_{A_2,B_2}^0\rangle \). When we choose the matrix \( U \) as \( u = \sum_{i,j} \frac{U_{ij}}{\sqrt{d}} |i\rangle_{A_1} |j\rangle_{A_2} \), this condition equals the condition that \( U U^\dagger \) is a constant matrix. Thus, if and only if \( u \) is maximally entangled, \( U \) is unitary, which is equivalent to the condition (J.1). Similarly, we can show that if and only if \( u \) is maximal entangled, the condition (J.2) holds. Hence, the desired argument is proved. \( \square \)

The relations (14) and (16) guarantee that \( \phi_{A_1,B_1}^0 \otimes \phi_{A_2,B_2}^0 \) is an eigenvector of \( T(M) \) for the eigenvalue 1. Hence, lemma 8 implies (26). On the other hand,

\[
\text{Tr} P \sigma \otimes^2 P = (\text{Tr} \sigma (I - |\phi_{A_1,B_1}^0\rangle \langle \phi_{A_1,B_1}^0|))^2 = (1 - \langle \phi_{A_1,B_1}^0| \sigma |\phi_{A_1,B_1}^0\rangle)^2.
\]

Since \( 0 \leq PT(M)P \leq I \), we obtain (28).

Next, we consider the case of \( M = M^2_{\text{cov}} \). The test \( T(M^2_{\text{cov}}) \) is invariant with respect to the following action, i.e.

\[
U(g_1) \otimes U(g_2) T(M^2_{\text{cov}}) (U(g_1) \otimes U(g_2))^\dagger = T(M^2_{\text{cov}})
\]

Since the subspace \( \langle \phi_{A_1,B_1}^0\rangle \otimes \langle \phi_{A_2,B_2}^0\rangle \) is an irreducible subspace, the equation (26) implies that

\[
T(M^2_{\text{cov}}) = |\phi_{A_1,B_1}^0 \otimes \phi_{A_2,B_2}^0\rangle \langle \phi_{A_1,B_1}^0 \otimes \phi_{A_2,B_2}^0| + tP,
\]

where \( t \) is a constant. Since the equation (17) implies that \( \text{Tr} T(M^2_{\text{cov}}) = d^2 \), we obtain

\[
t = (d^2 - 1)/(d^2 - 1)^2 = 1/(d^2 - 1).
\]

*New Journal of Physics* **11** (2009) 043028 (http://www.njp.org/)
Appendix K. Proof of (34)

We focus on the vertex of the simplex of the \(d - 1\)-dimensional subspace orthogonal to \(\varphi\). That is, there exist \(d\) vectors \(u_1(\varphi), \ldots, u_d(\varphi)\) such that

\[
\langle u_i(\varphi) | u_j(\varphi) \rangle = \begin{cases} 
\frac{-1}{d}, & i \neq j, \\
\frac{d - 1}{d}, & i = j.
\end{cases}
\]

Hence, the vectors \(u_i(\varphi) \overset{\text{def}}{=} u_i(\varphi) + \frac{1}{\sqrt{d}} \varphi (i = 1, \ldots, d)\) satisfy condition (34).

Appendix L. Proof of the \(U(1)\)-invariance of \(T_{\text{inv}}^{1-2}\)

As is proved later, the test \(T_{\text{inv}}^{1-2}\) has the form

\[
T_{\text{inv}}^{A_1 \rightarrow A_2 \rightarrow B^{\otimes 2}} = d^2 \int_G (g \otimes g) \otimes (g \otimes g) | u_1 \otimes \overline{u}_1 \otimes u_2 \otimes \overline{u}_2 \rangle \langle u_1 \otimes \overline{u}_1 \otimes u_2 \otimes \overline{u}_2 | (g \otimes g)^\dagger \otimes (g \otimes g)^\dagger \nu(v(dg))
\]

\[
= d^2 \int_G (g \otimes g) \otimes (g \otimes g) \left( \frac{1}{d^2} \phi_{A_1, B_1}^0 \otimes \phi_{A_2, B_2}^0 \right) \left( \frac{1}{d^2} \phi_{A_1, B_1}^0 \otimes \phi_{A_2, B_2}^0 \right) + \frac{1}{d} \phi_{A_1, B_1}^0 \otimes \left( u_2 \otimes \overline{u}_2 - \frac{1}{d} \phi_{A_1, B_2}^0 \right) \left( \frac{1}{d} \phi_{A_1, B_1}^0 \otimes \left( u_2 \otimes \overline{u}_2 - \frac{1}{d} \phi_{A_1, B_2}^0 \right) \right) \right.
\]

\[
\left. \times \left( \left( u_1 \otimes \overline{u}_1 - \frac{1}{d} \phi_{A_1, B_1}^0 \right) \otimes \left( u_2 \otimes \overline{u}_2 - \frac{1}{d} \phi_{A_1, B_2}^0 \right) \right) \right) (g \otimes g)^\dagger \otimes (g \otimes g)^\dagger \nu(v(dg)). \quad (L.1)
\]

Since we can easily check that the matrix \(T_{\text{inv}}^{1-2}\) is commutative with the matrix

\[
U_{\theta}^{\otimes 2} = e^{2 \theta | \phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 | \otimes | \phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |} + e^{\theta | \phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 | \otimes (I_{A_2, B_2} - | \phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |)}
\]

\[
+ e^{\theta (I_{A_1, B_1} - | \phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 | \otimes | \phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |)} + (I_{A_1, B_1} - | \phi_{A_1, B_1}^0 \rangle \langle \phi_{A_1, B_1}^0 | \otimes (I_{A_2, B_2} - | \phi_{A_2, B_2}^0 \rangle \langle \phi_{A_2, B_2}^0 |),
\]

we obtain \(U(1)\)-invariance.

Next, we prove (L.1). Since

\[
u(u_1 \otimes \overline{u}_1 \otimes u_2 \otimes \overline{u}_2 = \frac{1}{d^2} \phi_{A_1, B_1}^0 \otimes \phi_{A_2, B_2}^0 + \frac{1}{d} \phi_{A_1, B_1}^0 \otimes \left( u_2 \otimes \overline{u}_2 - \frac{1}{d} \phi_{A_1, B_2}^0 \right) \right.
\]

\[
\left. \times \left( \left( u_1 \otimes \overline{u}_1 - \frac{1}{d} \phi_{A_1, B_1}^0 \right) \otimes \left( u_2 \otimes \overline{u}_2 - \frac{1}{d} \phi_{A_1, B_2}^0 \right) \right) \right) (g \otimes g)^\dagger \otimes (g \otimes g)^\dagger \nu(v(dg)).
\]
it is sufficient to prove that the integrals of the cross terms are equal to 0. We denote the invariant subgroup of \( u \) by \( G_u \) and its invariant measure by \( \nu_u \). Then, we can calculate

\[
\int_{G_u} (g' \otimes \overline{g'}) \left( u_2 \otimes \overline{u_2} - \frac{1}{d} \phi_{A_2, B_2}^0 \right) \nu_u (dg') = \frac{1}{d} \phi_{A_2, B_2}^0 - \frac{1}{d} \phi_{A_2, B_2}^0 = 0.
\]

Hence, the integral of one cross term can be calculated as

\[
d^2 \int_G (g \otimes \overline{g}) \otimes (g \otimes \overline{g}) \left( u_1 \otimes \overline{u_1} - \frac{1}{d} \phi_{A_1, B_1}^0 \right) \left( u_1 \otimes \overline{u_1} - \frac{1}{d} \phi_{A_1, B_1}^0 \right) \otimes \frac{1}{d} \phi_{A_2, B_2}^0 \left( u_2 \otimes \overline{u_2} - \frac{1}{d} \phi_{A_2, B_2}^0 \right) \left( g \otimes \overline{g} \right) \left( g' \otimes \overline{g'} \right) \nu_u (dg) \nu (dg) = 0.
\]

Similarly, we can check that the integrals of the other cross terms are 0.

**Appendix M. Proof of (35)**

Let \( T \) be an \( SU(d) \)-invariant \( L(A_1, A_2 \to B_1, B_2) \) test at level-0. Using the discussion in the appendix F, we can find a POVM \( M' = \{ d^2 |u_1^\xi \otimes u_2^\xi \rangle \langle u_1^\xi \otimes u_2^\xi | \mu (dx) \} \) satisfying condition (18), where \( \mu \) is a probability measure. We define the covariant POVM \( M \) as

\[
M(dg \, dx) = d^2 |g^{\otimes 2} u_1^\xi \otimes u_2^\xi \rangle \langle g^{\otimes 2} u_1^\xi \otimes u_2^\xi | \nu (dg) \mu (dx).
\]

The \( SU(d) \)-invariance of \( T \) guarantees that

\[
T \geq \int_{SU(d)} U(g)^{\otimes 2} T(M') (U(g)^{\otimes 2})^\dagger \nu (dg) = T(M).
\]

Note the test \( T(M) \) can be expressed as

\[
T(M) = \int_{SU(d)} d^2 |U(g)u_1^\xi \otimes u_1^\xi \rangle \langle U(g)u_1^\xi \otimes \overline{u_1^\xi} | \otimes |U(g)u_2^\xi \otimes u_2^\xi \rangle \langle U(g)u_2^\xi \otimes \overline{u_2^\xi} | \nu (dg) \mu (dx).
\]

Thus, we can restrict our attention to tests \( T(M) \) of the form (M.1). First, we calculate the following value:

\[
\text{Tr} \int_{SU(d)} |U(g)u_1^\xi \otimes u_1^\xi \rangle \langle U(g)u_1^\xi \otimes u_1^\xi | \otimes |U(g)u_2^\xi \otimes u_2^\xi \rangle \langle U(g)u_2^\xi \otimes \overline{u_2^\xi} | \nu (dg) \sigma^{\otimes 2}.
\]

*New Journal of Physics* **11** (2009) 043028 (http://www.njp.org/)
Indeed, from the $SU(d)$-invariance, this value depends only on the inner product $r \overset{\text{def}}{=} |\langle u_1^x, u_2^x \rangle|^2$. Hence, we can denote it by $f(r)$. Without loss of generality, we can assume that $u_1^x = |0\rangle$ and $u_2^x = \sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle$. The group $SU(d)$ has the subgroup:

$$G' \overset{\text{def}}{=} \left\{ g_0 \overset{\text{def}}{=} e^{i\theta/2}|0\rangle \langle 0| + e^{-i\theta/2}|1\rangle \langle 1| + \sum_{i=2}^{d-1} |i\rangle \langle i| \mid \theta \in [0, 2\pi] \right\}.$$

Hence,

$$\begin{align*}
\int_0^{2\pi} & |U(g_0)u_1^x \otimes u_1^x \rangle \langle U(g_0)u_1^x \otimes u_1^x |U(g_0)u_2^x \otimes u_2^x \rangle \langle U(g_0)u_2^x \otimes u_2^x |d\theta \\
& = |00\rangle \langle 00| \otimes \left( p(1-p)|01\rangle \langle 01| + p(1-p)|10\rangle \langle 10| \\
& \quad + (p|00\rangle + (1-p)|11\rangle \langle 00|) (p|00\rangle + (1-p)|11\rangle \langle 00|) \right) \\
& = |00\rangle \langle 00| \otimes \left( p(1-p)|10\rangle \langle 10| + p(1-p)|01\rangle \langle 01| \\
& \quad + p^2|00\rangle \langle 00| + p(1-p)(|00\rangle \langle 00| + |11\rangle \langle 11|) + (1-p)^2|11\rangle \langle 11| \right) \\
& = |00\rangle \langle 00| \otimes \left( |11\rangle \langle 11| + p^2(-|01\rangle \langle 01| - |10\rangle \langle 10| + |00\rangle \langle 00| + |11\rangle \langle 11| - |00\rangle \langle 11| - |11\rangle \langle 00|) \\
& \quad + p(|01\rangle \langle 01| + |10\rangle \langle 10| - 2|11\rangle \langle 11| + |00\rangle \langle 11| + |11\rangle \langle 00|) \right).
\end{align*}$$

We put

$$C_1(\sigma) \overset{\text{def}}{=} \int_{SU(d)} \langle 00|U(g)\sigma U(g)^\dagger|00\rangle$$

$$\times \left( -\langle 01|U(g)\sigma U(g)^\dagger|01\rangle - \langle 10|U(g)\sigma U(g)^\dagger|10\rangle + \langle 00|U(g)\sigma U(g)^\dagger|00\rangle \right) v(dg),$$

$$C_2(\sigma) \overset{\text{def}}{=} \int_{SU(d)} \langle 00|U(g)\sigma U(g)^\dagger|00\rangle \left( \langle 01|U(g)\sigma U(g)^\dagger|01\rangle + \langle 10|U(g)\sigma U(g)^\dagger|10\rangle \\
- 2\langle 11|U(g)\sigma U(g)^\dagger|11\rangle + \langle 11|U(g)\sigma U(g)^\dagger|11\rangle + \langle 00|U(g)\sigma U(g)^\dagger|00\rangle \right) v(dg),$$

$$C_3(\sigma) \overset{\text{def}}{=} \int_{SU(d)} \langle 00|U(g)\sigma U(g)^\dagger|00\rangle \langle 11|U(g)\sigma U(g)^\dagger|11\rangle v(dg).$$

Hence, putting $p(x) \overset{\text{def}}{=} |\langle u_1^x | u_2^x \rangle|^2$, we have

$$\text{Tr} \, T(M) \sigma^\otimes 2 = \int d^2 \left( C_1(\sigma) p(x)^2 + C_2(\sigma) p(x) + C_3(\sigma) \right) \mu(dx).$$
Denoting the projection to the symmetric subspace of $\mathcal{H}_A^{\otimes 2}$ by $P_S$, we obtain

$$\frac{d(d+1)}{2} = \text{Tr} P_S I P_S = \int \int_{SU(d)} d^2 \text{Tr} P_S |gu_x^1 \otimes gu_x^2)(gu_x^1 \otimes gu_x^2|P_S v(dg)\mu(dx)$$

$$= \int \int_{SU(d)} d^2 \frac{1+|\langle gu_x^1|gu_x^2\rangle|^2}{2} v(dg)\mu(dx) = \int d^2 \frac{1+|\langle u_x^1|u_x^2\rangle|^2}{2} \mu(dx),$$

which implies

$$\int p(x)\mu(dx) = \frac{1}{d}$$

because $|\langle u_x^1|u_x^2\rangle|^2 = p(x)$. As is shown later, $C_1(\sigma)$ is positive. Since $\int p(x)^2\mu(dx) \geq 1/d^2$,

$$\text{Tr} T(M)\sigma^{\otimes 2} \geq d^2 \left( \frac{C_1(\sigma)}{d^2} + \frac{C_2(\sigma)}{d} + C_3(\sigma) \right).$$

The equality holds if $p(x) = 1/d$ for all $x$. That is, if $T = T_{\text{inv}}^{1-2}$, the equality holds. Therefore, we obtain (35).

Letting

$$g' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g,$$

we obtain

$$\int_{SU(d)} \langle 00|U(g)\sigma U(g)^\dagger|00\rangle \left( -\langle 01|U(g)\sigma U(g)^\dagger|01\rangle - \langle 10|U(g)\sigma U(g)^\dagger|10\rangle \\
+\langle 00|U(g)\sigma U(g)^\dagger|00\rangle + \langle 11|U(g)\sigma U(g)^\dagger|11\rangle - \langle 11|U(g)\sigma U(g)^\dagger|00\rangle \\
-\langle 00|U(g)\sigma U(g)^\dagger|11\rangle - \langle 11|U(g)\sigma U(g)^\dagger|10\rangle \\
+\langle 00|U(g')\sigma U(g')^\dagger|00\rangle + \langle 11|U(g')\sigma U(g')^\dagger|11\rangle - \langle 11|U(g')\sigma U(g')^\dagger|00\rangle \\
-\langle 00|U(g')\sigma U(g')^\dagger|11\rangle \right) v(dg)$$

$$= \int_{SU(d)} \langle 11|U(g')\sigma U(g')^\dagger|11\rangle \left( -\langle 01|U(g')\sigma U(g')^\dagger|01\rangle - \langle 10|U(g')\sigma U(g')^\dagger|10\rangle \\
+\langle 00|U(g')\sigma U(g')^\dagger|00\rangle + \langle 11|U(g')\sigma U(g')^\dagger|11\rangle - \langle 11|U(g')\sigma U(g')^\dagger|00\rangle \\
-\langle 00|U(g')\sigma U(g')^\dagger|11\rangle \right) v(dg').$$

Hence,

$$C_1(\sigma) = \int_{SU(d)} \frac{1}{2} \left( \langle 00|U(g)\sigma U(g)^\dagger|00\rangle + \langle 11|U(g)\sigma U(g)^\dagger|11\rangle \right)$$

$$\times \left( -\langle 01|U(g)\sigma U(g)^\dagger|01\rangle - \langle 10|U(g)\sigma U(g)^\dagger|10\rangle + \langle 00|U(g)\sigma U(g)^\dagger|00\rangle \\
+ \langle 11|U(g)\sigma U(g)^\dagger|11\rangle - \langle 11|U(g)\sigma U(g)^\dagger|11\rangle \right) v(dg).$$

\hspace{1cm} (M.2)
By using the notations

\[ \varphi^0_{A,B} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle), \quad \varphi^1_{A,B} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|10\rangle + |10\rangle), \]

\[ \varphi^2_{A,B} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (-i|10\rangle + i|10\rangle), \quad \varphi^3_{A,B} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle), \]

\( C_1(\sigma) \) can be calculated as

\[ C_1(\sigma) = \int_{SU(d)} \frac{1}{2} \left( \langle \phi^0_{A,B} | U(g) \sigma U(g)^\dagger | \phi^0_{A,B} \rangle + \langle \phi^3_{A,B} | U(g) \sigma U(g)^\dagger | \phi^3_{A,B} \rangle \right) \]

\[ \times \left( 2 \langle \phi^3_{A,B} | U(g) \sigma U(g)^\dagger | \phi^3_{A,B} \rangle - \langle \phi^3_{A,B} | U(g) \sigma U(g)^\dagger | \phi^3_{A,B} \rangle \right) v(dg). \]

Similarly to (M.2), by focusing on the elements \( g_{1,2}, g_{2,3}, g_{3,1} \) of \( SU(d) \) such that

\[ g_{1,2} : (\phi^1_{A,B}, \phi^2_{A,B}, \phi^3_{A,B}) \rightarrow (\phi^2_{A,B}, -\phi^1_{A,B}, \phi^3_{A,B}) \]

\[ g_{2,3} : (\phi^1_{A,B}, \phi^2_{A,B}, \phi^3_{A,B}) \rightarrow (\phi^1_{A,B}, \phi^3_{A,B}, -\phi^2_{A,B}) \]

\[ g_{3,1} : (\phi^1_{A,B}, \phi^2_{A,B}, \phi^3_{A,B}) \rightarrow (-\phi^3_{A,B}, \phi^2_{A,B}, \phi^1_{A,B}) \]

we can prove

\[ C_1(\sigma) = \int_{SU(d)} \frac{1}{3} \left( \sum_{i=1}^{3} \langle \phi^i_{A,B} | U(g) \sigma U(g)^\dagger | \phi^i_{A,B} \rangle \right)^2 \]

\[ - \sum_{i>j} \langle \phi^i_{A,B} | U(g) \sigma U(g)^\dagger | \phi^i_{A,B} \rangle \langle \phi^j_{A,B} | U(g) \sigma U(g)^\dagger | \phi^j_{A,B} \rangle \right) v(dg) \]

\[ = \int_{SU(d)} \frac{1}{6} \sum_{i>j} \left( \langle \phi^i_{A,B} | U(g) \sigma U(g)^\dagger | \phi^i_{A,B} \rangle - \langle \phi^j_{A,B} | U(g) \sigma U(g)^\dagger | \phi^j_{A,B} \rangle \right)^2 v(dg) \geq 0. \]

Appendix N. Proof of (37)

Let \( T \) be an \( SU(d) \)-invariant separable level-\( \alpha \) test among \( A_1, \ldots, A_n \) and \( B_1, \ldots, B_n \) for the null hypothesis \( S_0 \). Then, \( T \) has the following form:

\[ T = \sum_k \alpha_k |u^k_1 \otimes u^k_1\rangle \langle u^k_1 \otimes u^k_1| \otimes \cdots \otimes |u^k_n \otimes u^k_n\rangle \langle u^k_n \otimes u^k_n|, \]
where \(\|u_k^i\| = 1\), \(\langle u_k^i | u_k^i \rangle = 1\). Since \(T\) is level-\(\alpha\) and \(\langle \phi_{A,B}^0 | u_1^k \otimes u_1^k \rangle \langle u_1^k \otimes u_1^k | \phi_{A,B}^0 \rangle = 1/d\), we have

\[
1 - \alpha = \langle \phi_{A,B}^0 \otimes^n | T | \phi_{A,B}^0 \otimes^n \rangle = \sum_k a_k \frac{1}{d^n}.
\]

It follows from the \(SU(d)\)-invariance of \(T\) that

\[
T = \int_{SU(d)} \sum_k a_k |gu_1^k \otimes \bar{g}u_1^k \rangle \langle gu_1^k \otimes \bar{g}u_1^k | \otimes \cdots \otimes |gu_n^k \otimes \bar{g}u_n^k \rangle \langle gu_n^k \otimes \bar{g}u_n^k |\rangle v(dg).
\]

The concavity of the function \(x \mapsto \log x\) implies that

\[
\log \text{Tr} \left( \int_{SU(d)} |gu_1^k \otimes \bar{g}u_1^k \rangle \langle gu_1^k \otimes \bar{g}u_1^k | \otimes \cdots \otimes |gu_n^k \otimes \bar{g}u_n^k \rangle \langle gu_n^k \otimes \bar{g}u_n^k |\rangle v(dg) \right)^{\otimes n}
= \log \int_{SU(d)} \text{Tr} (gu_1^k \otimes \bar{g}u_1^k | \otimes \cdots \otimes \text{Tr} (gu_n^k \otimes \bar{g}u_n^k | v(dg)
\geq \int_{SU(d)} \sum_{i=1}^n \log \text{Tr} (gu_i^k \otimes \bar{g}u_i^k | v(dg)
\geq n \min_{u, u' : |u| = 1, |u'| = 1} \int_{SU(d)} \log \text{Tr} (gu \otimes \bar{g}u' | v(dg).
\]

Denoting the RHS by \(C\), we obtain

\[
\text{Tr} T \sigma^{\otimes n} \geq \sum_k a_k e^C = e^C \sum_k a_k = e^C d^n (1 - \alpha).
\]

Hence,

\[
\log \frac{\text{Tr} T \sigma^{\otimes n}}{1 - \alpha} \geq n \log d + C,
\]

which implies (37).

**Appendix O. Proof of (41) and (40)**

Let \(T\) be an \(SU(2) \times U(1)\)-invariant \(A-B\) separable test. Then, \(SU(2)\)-invariance guarantees that \(T = U(g)^{\otimes 2} T (U(g)^{\otimes 2})^\dagger\) for \(\forall g \in SU(2)\). Hence, \(T = \int_{SU(2)} U(g)^{\otimes 2} T (U(g)^{\otimes 2})^\dagger v(dg)\). Thus, the test \(T\) has the form

\[
T = \int 4 \int_{SU(2)} U(g, \theta)^{\otimes 2} |u_x \otimes u'_x \rangle \langle u_x \otimes u'_x | U(g, \theta)^{\otimes 2})^\dagger v(dg) \mu(dx),
\]

where \(u_x \in \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_1}\), \(u'_x \in \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_1}\), \(\langle \phi_{A_1,B_1}^0 \otimes \phi_{A_2,B_2}^0 | u_x \otimes u'_x \rangle = \frac{1}{2}\) and \(\mu\) is an arbitrary probability measure. Since our purpose is calculating the minimum value of the second error...
probability $\text{Tr} \, T \, \sigma^{\otimes 2}$, we can assume that the second term of (20) is 0 without loss of generality. Therefore, lemma 4 implies that

$$
\int 4 \int_{SU(2)} (g^{\otimes 2} u_x) \otimes (g^{\otimes 2} u_x^*) v(\text{d}g) \mu(\text{d}x) = 2\phi^0_{A_1, B_1} \otimes \phi^0_{A_2, B_2}
$$

Moreover, $SU(2) \times U(1)$-invariance guarantees that $T = U(g, \theta)^{\otimes 2} T (U(g, \theta)^{\otimes 2})^\dagger$ for $\forall g \in SU(2)$ and $\forall \theta \in \mathbb{R}$. Hence,

$$
\text{Tr} \, T \sigma^{\otimes 2} = \text{Tr} \, (U(g, \theta)^{\otimes 2})^\dagger \sigma^{\otimes 2} U(g, \theta)^{\otimes 2}.
$$

Taking the integral, we obtain

$$
\text{Tr} \, T \sigma^{\otimes 2} = \text{Tr} \, T \frac{1}{2\pi} \int_0^{2\pi} \int_{SU(2)} (U(g, \theta)^{\otimes 2})^\dagger \sigma^{\otimes 2} U(g, \theta)^{\otimes 2} v(\text{d}g) d\theta.
$$

Therefore, the RHS can be written using projections of irreducible spaces with respect to the action of the group $SU(2) \times U(1)$. Indeed, the tensor product space $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ can be decomposed to the direct sum product of the following irreducible spaces with respect to the action of the group $SU(2) \times U(1)$:

$$
\Sigma^0_3 \overset{\text{def}}{=} \left\{ \frac{1}{\sqrt{2}} (|1, 2\rangle_{1,2} + |2, 1\rangle_{1,2}), \frac{1}{\sqrt{2}} (|2, 3\rangle_{1,2} + |3, 2\rangle_{1,2}), \frac{1}{\sqrt{2}} (|3, 1\rangle_{1,2} + |1, 3\rangle_{1,2}), \frac{1}{\sqrt{3}} (|1, 1\rangle_{1,2} + \omega |2, 2\rangle_{1,2} + \omega^2 |3, 3\rangle_{1,2}), \frac{1}{\sqrt{3}} (|1, 1\rangle_{1,2} + \omega^2 |2, 2\rangle_{1,2} + \omega |3, 3\rangle_{1,2}) \right\},
$$

$$
\Sigma^1_3 \overset{\text{def}}{=} \left\{ \frac{1}{\sqrt{2}} (|0, 1\rangle_{1,2} + |1, 0\rangle_{1,2}), \frac{1}{\sqrt{2}} (|0, 2\rangle_{1,2} + |2, 0\rangle_{1,2}), \frac{1}{\sqrt{2}} (|0, 3\rangle_{1,2} + |3, 0\rangle_{1,2}) \right\},
$$

$$
\Sigma^2_3 \overset{\text{def}}{=} \left\{ |0, 0\rangle_{1,2} \right\},
$$

$$
\Sigma^0_1 \overset{\text{def}}{=} \left\{ \frac{1}{\sqrt{3}} (|1, 1\rangle_{1,2} + |2, 2\rangle_{1,2} + |3, 3\rangle_{1,2}) \right\},
$$

$$
\Lambda^0_3 \overset{\text{def}}{=} \left\{ \frac{1}{\sqrt{2}} (|1, 2\rangle_{1,2} - |2, 1\rangle_{1,2}), \frac{1}{\sqrt{2}} (|2, 3\rangle_{1,2} - |3, 2\rangle_{1,2}), \frac{1}{\sqrt{2}} (|3, 1\rangle_{1,2} - |1, 3\rangle_{1,2}) \right\},
$$

$$
\Lambda^0_1 \overset{\text{def}}{=} \left\{ \frac{1}{\sqrt{2}} (|0, 1\rangle_{1,2} - |1, 0\rangle_{1,2}), \frac{1}{\sqrt{2}} (|0, 2\rangle_{1,2} - |2, 0\rangle_{1,2}), \frac{1}{\sqrt{2}} (|0, 3\rangle_{1,2} - |3, 0\rangle_{1,2}) \right\},
$$

where $|i, j\rangle_{1,2}$ denotes the vector $\phi^i_{A_1, B_1} \otimes \phi^j_{A_2, B_2}$ and $\omega = (-1 + \sqrt{3} i)/2$. The meaning of this notation is as follows. The superscript $k = 0, 1, 2$ denotes the $U(1)$-action, i.e. the element $e^{i\theta}$ acts on this space as $e^{ik\theta}$. The subscript $l = 1, 3, 5$ denotes the dimension of the space. In the spaces labelled as $\Sigma$, the action $|i, j\rangle_{1,2} \to |j, i\rangle_{1,2}$ is described as the action of the constant 1. But, in the spaces labelled as $\Lambda$, it is described as the action of the constant $-1$. In the following, for simplicity, we abbreviate the projections to the subspaces $\Sigma^k_l$ and $\Lambda^k_l$ as $\Sigma^k_l$.
and $\Lambda_i^k$, respectively. Hence, we obtain

\[
\frac{1}{2\pi} \int_0^{2\pi} \left( U(g, \theta) \right)^{\otimes 2} \left( U(g, \theta) \right)^{\otimes 2} \nu(d\theta) = \text{Tr} \sigma^{\otimes 2} \sum_3^{\otimes 2} + \text{Tr} \sigma^{\otimes 2} \sum_1^{\otimes 2} \sum_1^{\otimes 1} + (\text{Tr} \sigma^{\otimes 2} \sum_2^{\otimes 2}) \sum_2^{\otimes 2} + (\text{Tr} \sigma^{\otimes 2} \sum_0^{\otimes 2}) \sum_0^{\otimes 2} + \frac{\Lambda_3^{\otimes 2} \Lambda_3^{\otimes 2}}{3} + \frac{\Lambda_1^{\otimes 2} \Lambda_1^{\otimes 2}}{3}.
\]

In order to calculate the quantities $\text{Tr} \sigma^{\otimes 2} \sum_i^k$ and $\text{Tr} \sigma^{\otimes 2} \Lambda_i^k$, we describe the matrix elements of $\sigma$ on the basis of $\langle \phi_{A,B}^0, \ldots, \phi_{A,B}^1 \rangle$ by $x_{i,j} \equiv \langle \phi_{A,B}^i | \sigma | \phi_{A,B}^j \rangle$. For convenience, we treat this matrix by use of the notation

\[
(x_{i,j}) = \begin{pmatrix} a & b^t \\ b & C \end{pmatrix},
\]

where $a$ is a real number, $b$ is a three-dimensional complex-valued vector, $C$ is a $3 \times 3$ Hermitian matrix. Thus, the quantities $\text{Tr} \sigma^{\otimes 2} \sum_i^k$ and $\text{Tr} \sigma^{\otimes 2} \Lambda_i^k$ are evaluated as

\[
\text{Tr} \sigma^{\otimes 2} \sum_{i=1}^{3} x_{i,i} + \sum_{1 \leq i < j \leq 3} x_{i,j} x_{j,i} + |x_{i,j}|^2 - \frac{1}{3} (x_{i,j}^2 + x_{j,i}^2) = \frac{1}{2} \left( (\text{Tr} C)^2 + (\text{Tr} C)^2 \right) - \frac{1}{3} \text{Tr} C C^t
\]

\[
\text{Tr} \sigma^{\otimes 2} \sum_{i=1}^{3} x_{0,i}^2 = a \text{Tr} C + |b|^2,
\]

\[
\text{Tr} \sigma^{\otimes 2} \sum_{i=1}^{3} x_{i,j}^2 = \frac{1}{3} \text{Tr} C C^t,
\]

\[
\text{Tr} \sigma^{\otimes 2} \Lambda_{3}^0 = \sum_{i < j} x_{i,j} x_{j,i} - |x_{i,j}|^2 = \frac{1}{2} \left( (\text{Tr} C)^2 - (\text{Tr} C)^2 \right),
\]

\[
\text{Tr} \sigma^{\otimes 2} \Lambda_{3}^1 = \sum_{i=1}^{3} (x_{0,i} x_{i,i} - |x_{i,i}|^2) = a \text{Tr} C - |b|^2,
\]

where $C^t$ is the complex conjugate of $C$. As is proved later, the inequalities

\[
\text{Tr} \sigma^{\otimes 2} \Lambda_{3}^1 - \text{Tr} \sigma^{\otimes 2} \Lambda_{3}^0 \geq 0 \quad \text{(O.3)}
\]

\[
5 \text{Tr} \sigma^{\otimes 2} \sum_{i=1}^{3} - 3 \text{Tr} \sigma^{\otimes 2} \sum_{j=0}^{3} \geq 0 \quad \text{(O.4)}
\]

\[
10 \text{Tr} \sigma^{\otimes 2} \sum_{i=1}^{3} + \text{Tr} \sigma^{\otimes 2} \sum_{j=0}^{3} - 5 \text{Tr} \sigma^{\otimes 2} \Lambda_{3}^0 \geq 0 \quad \text{(O.5)}
\]

hold, when $p = \text{Tr} C \leq \frac{1}{2}$. 

\[\text{New Journal of Physics} 11 (2009) 043028 (http://www.njp.org/)\]
On the other hand, we focus on the following basis of the space $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$:

$$\varphi_{A_1,A_2}^0 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|01\rangle_{A_1,A_2} - |10\rangle_{A_1,A_2}), \quad \varphi_{A_1,A_2}^1 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|00\rangle_{A_1,A_2} + |11\rangle_{A_1,A_2}),$$

$$\varphi_{A_1,A_2}^2 \overset{\text{def}}{=} \frac{i}{\sqrt{2}} (|00\rangle_{A_1,A_2} - |11\rangle_{A_1,A_2}), \quad \varphi_{A_1,A_2}^3 \overset{\text{def}}{=} \frac{i}{\sqrt{2}} (|01\rangle_{A_1,A_2} + |10\rangle_{A_1,A_2}).$$

The other space $\mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ is spanned by the complex conjugate basis:

$$\varphi_{B_1,B_2}^0 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|01\rangle_{B_1,B_2} - |10\rangle_{B_1,B_2}), \quad \varphi_{B_1,B_2}^1 \overset{\text{def}}{=} \frac{1}{\sqrt{2}} (|00\rangle_{B_1,B_2} + |11\rangle_{B_1,B_2}),$$

$$\varphi_{B_1,B_2}^2 \overset{\text{def}}{=} \frac{-i}{\sqrt{2}} (|00\rangle_{B_1,B_2} - |11\rangle_{B_1,B_2}), \quad \varphi_{B_1,B_2}^3 \overset{\text{def}}{=} \frac{-i}{\sqrt{2}} (|01\rangle_{B_1,B_2} + |10\rangle_{B_1,B_2}).$$

Using this basis, the irreducible subspaces of $\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ can be written as

$$\Sigma^2_1 = \left\{ \frac{1}{2} (|00\rangle_{A,B} + |11\rangle_{A,B} + |22\rangle_{A,B} + |33\rangle_{A,B}) \right\},$$

$$\Sigma^0_2 = \left\{ \frac{1}{\sqrt{2}} (|11\rangle_{A,B} + |22\rangle_{A,B}), \quad \frac{1}{\sqrt{2}} (|22\rangle_{A,B} + |33\rangle_{A,B}), \quad \frac{1}{\sqrt{2}} (|33\rangle_{A,B} + |11\rangle_{A,B}) \right\},$$

$$\Sigma^1_3 = \left\{ \frac{1}{\sqrt{3}} (|11\rangle_{A,B} + \omega|22\rangle_{A,B} + \omega^2|33\rangle_{A,B}), \quad \frac{1}{\sqrt{3}} (|11\rangle_{A,B} + \omega^2|22\rangle_{A,B} + \omega|33\rangle_{A,B}) \right\},$$

$$\Sigma^0_4 = \left\{ \frac{3}{\sqrt{12}} (|00\rangle_{A,B} + |11\rangle_{A,B} + |22\rangle_{A,B} + |33\rangle_{A,B}) \right\},$$

$$\Lambda^0_3 = \left\{ \frac{1}{\sqrt{2}} (|00\rangle_{A,B} + |11\rangle_{A,B}), \quad \frac{1}{\sqrt{2}} (|00\rangle_{A,B} + |22\rangle_{A,B}), \quad \frac{1}{\sqrt{2}} (|00\rangle_{A,B} + |33\rangle_{A,B}) \right\},$$

$$\Lambda^1_3 = \left\{ \frac{1}{\sqrt{2}} (|00\rangle_{A,B} + |11\rangle_{A,B}), \quad \frac{1}{\sqrt{2}} (|00\rangle_{A,B} + |22\rangle_{A,B}), \quad \frac{1}{\sqrt{2}} (|00\rangle_{A,B} + |33\rangle_{A,B}) \right\},$$

where $|i, j\rangle_{A,B}$ denotes the vector $\varphi_{A_1,A_2}^i \otimes \varphi_{B_1,B_2}^j$.

In the following, we denote the vectors $u_x \in \mathcal{H}_{A_1,A_2}$ and $u'_x \in \mathcal{H}_{B_1,B_2}$ using scalars $a_x, a_x'$ and three-dimensional vectors $w_x, w'_x$ as

$$u_x = (a_x, w_x) \overset{\text{def}}{=} a_x \varphi_{A_1,A_2}^0 + \sum_{i=1}^{3} w_{x,i} \varphi_{A_1,A_2}^i, \quad u'_x = (a'_x, w'_x) \overset{\text{def}}{=} a'_x \varphi_{B_1,B_2}^0 + \sum_{i=1}^{3} w'_{x,i} \varphi_{B_1,B_2}^i.$$

The condition (O.1) implies that

$$\int a_x a'_x \mu(dx) = \frac{1}{4}, \quad \int (w_x | w'_x) \mu(dx) = \frac{3}{4}.$$
where the inner product \((w_x|w'_x)\) is defined by \((w_x|w'_x) \equiv \sum_{i=1}^{3} w_{x,i} w'_{x,i}\). The condition
\[
\langle \phi_{A_1,B_1}^{0} \otimes \phi_{A_2,B_2}^{0} | u_x \otimes u'_x \rangle \overset{\text{def}}{=} \frac{1}{2}
\]
yields
\[
a_x a'_x + (w_x|w'_x) = 1,
\]
because of (O.2). Using this notation, we obtain
\[
\langle u_x \otimes u'_x | \Sigma^0_3 | u_x \otimes u'_x \rangle = \left\| \frac{1}{2} \left( w_x \otimes w'_x + w'_x \otimes w_x \right) - \frac{(w_x|w'_x)}{3} I_{3 \times 3} \right\|^2,
\]
\[
\langle u_x \otimes u'_x | \Sigma^1_3 | u_x \otimes u'_x \rangle = \left\| \frac{1}{2} \left( w_x \otimes w'_x - w'_x \otimes w_x \right) \right\|^2,
\]
\[
\langle u_x \otimes u'_x | \Sigma^2_3 | u_x \otimes u'_x \rangle = \left\| \frac{1}{2} \left( a_x a'_x + (w_x|w'_x) \right) \right\|^2 = \frac{1}{4},
\]
\[
\langle u_x \otimes u'_x | \Lambda^0_3 | u_x \otimes u'_x \rangle = \left\| \frac{1}{2} \left( a_x w'_x + a'_x w_x \right) \right\|^2,
\]
\[
\langle u_x \otimes u'_x | \Lambda^1_3 | u_x \otimes u'_x \rangle = \left\| \frac{1}{2} \left( a_x w'_x - a'_x w_x \right) \right\|^2,
\]
where \(\Re x\) denotes the real part of \(x\). Since we can evaluate
\[
\left\| \frac{1}{2} \left( a_x w'_x + a'_x w_x \right) \right\|^2 + \left\| \frac{1}{2} \left( a_x w'_x - a'_x w_x \right) \right\|^2 = \|a_x w'_x\|^2 + \|a'_x w_x\|^2 \geq 2 |a_x a'_x \Re (w_x|w'_x)|,
\]
\[
\left\| \frac{1}{2} \left( w_x \otimes w'_x + w'_x \otimes w_x \right) - \frac{(w_x|w'_x)}{3} I_{3 \times 3} \right\|^2 + \left\| \frac{1}{2} \left( w_x \otimes w'_x - w'_x \otimes w_x \right) \right\|^2
\]
\[
= \left\| w_x \otimes w'_x - \frac{(w_x|w'_x)}{3} I_{3 \times 3} \right\|^2 \geq \frac{2}{3} |(w_x|w'_x)|^2 \geq \frac{2}{3} (\Re (w_x|w'_x))^2,
\]
the inequalities (O.3) and (O.4) yield
\[
\frac{\Tr \sigma^0 \Lambda^0_3}{3} \langle u_x \otimes u'_x | \Lambda^0_3 | u_x \otimes u'_x \rangle + \frac{\Tr \sigma^0 \Lambda^1_3}{3} \langle u_x \otimes u'_x | \Lambda^1_3 | u_x \otimes u'_x \rangle
\]
\[
\geq \Tr \sigma^0 \Lambda^0_3 \cdot 2 |a_x a'_x \Re (w_x|w'_x)|,
\]
\[
\frac{\Tr \sigma^0 \Sigma^0_3}{5} \langle u_x \otimes u'_x | \Sigma^0_3 | u_x \otimes u'_x \rangle + \frac{\Tr \sigma^0 \Sigma^1_3}{3} \langle u_x \otimes u'_x | \Sigma^1_3 | u_x \otimes u'_x \rangle
\]
\[
\geq \Tr \sigma^0 \Sigma^0_3 \cdot \frac{2}{3} (\Re (w_x|w'_x))^2.
\]
Letting $r(x) = \Im a_x a_x'$, we have
\[
\frac{1}{4} Tr T \sigma \otimes \sigma \geq \int \frac{\Tr \sigma \otimes \sigma R^2}{4} + \Tr \sigma \otimes \sigma (-h + (w_x | w_x')^2) + \frac{2}{3} \Tr \sigma \otimes \sigma \Lambda' \Im (w_x | w_x') + \frac{2}{3} \Tr \sigma \otimes \sigma \Lambda' \Im (w_x | w_x')^2 \mu(\mathrm{d}x)
\]
\[
= \frac{\Tr \sigma \otimes \sigma \Sigma^2}{4} + \frac{\Tr \sigma \otimes \sigma \Sigma^0}{12} + \frac{2}{15} \Tr \sigma \otimes \sigma \Sigma^0 + \frac{1}{4} \left( -\frac{2}{3} \Tr \sigma \otimes \sigma \Sigma^0 - \frac{4}{15} \Tr \sigma \otimes \sigma \Sigma^0 + \frac{2}{3} \Tr \sigma \otimes \sigma \Lambda_3 \right) \int r(x)^2 \mu(\mathrm{d}x)
\]
\[
\geq \frac{\Tr \sigma \otimes \sigma \Sigma^2}{4} + \frac{\Tr \sigma \otimes \sigma \Sigma^0}{12} + \frac{2}{15} \Tr \sigma \otimes \sigma \Sigma^0 + \frac{1}{4} \left( -\frac{2}{3} \Tr \sigma \otimes \sigma \Sigma^0 + \frac{4}{15} \Tr \sigma \otimes \sigma \Sigma^0 + \frac{2}{3} \Tr \sigma \otimes \sigma \Lambda_3 \right)
\]
\[
= \frac{1}{4} \left( 1 - \frac{1}{2} \Tr C + \frac{7}{20} (\Tr C)^2 - \frac{1}{20} \Tr (\Im C)^2 \right). \quad (O.6)
\]
Note that the inequality (*) follows from the inequality (O.5) and the inequality $\int r(x)^2 \mu(\mathrm{d}x) \geq \frac{1}{16}$, and the equation (**) follows from the equation $a = 1 - \Tr C$. Since the RHS of (O.6) equals RHS of (41)/4, we obtain the part $\geq$ of (41).

Conversely, the vector $u_{op} \otimes \overline{u_{op}}$ satisfies
\[
\langle u_{op} \otimes \overline{u_{op}} | \Sigma^0 | u_{op} \otimes \overline{u_{op}} \rangle = \langle u_{op} \otimes \overline{u_{op}} | \Lambda_3^0 | u_{op} \otimes \overline{u_{op}} \rangle = \frac{3}{8}, \quad \langle u_{op} \otimes \overline{u_{op}} | \Sigma^2 | u_{op} \otimes \overline{u_{op}} \rangle = \frac{1}{4}
\]
\[
\langle u_{op} \otimes \overline{u_{op}} | \Sigma^1 | u_{op} \otimes \overline{u_{op}} \rangle = \langle u_{op} \otimes \overline{u_{op}} | \Sigma^0 | u_{op} \otimes \overline{u_{op}} \rangle = \langle u_{op} \otimes \overline{u_{op}} | \Lambda_3^0 | u_{op} \otimes \overline{u_{op}} \rangle = 0.
\]
Hence,
\[
\frac{1}{4} Tr T(M_{op}) \sigma \otimes \sigma = \frac{1}{4} \Tr \sigma \otimes \sigma \Sigma^2 + \frac{3}{8} \left( \Tr \sigma \otimes \sigma \Sigma^0 + \frac{3}{8} \Tr \sigma \otimes \sigma \Lambda_3^0 \right)
\]
\[
= \frac{1}{4} \left( 1 - \frac{1}{2} \Tr C + \frac{7}{20} (\Tr C)^2 - \frac{1}{20} \Tr (\Im C)^2 \right).
\]
Therefore, we obtain (40), which implies the part $\leq$ of (41).
Finally, we proceed to prove the inequalities (O.3)-(O.5). The inequality (O.5) is shown as

\[10 \text{Tr}\sigma^\otimes_2\Sigma_1^0 + \text{Tr}\sigma^\otimes_2\Sigma_5^0 - 5 \text{Tr}\sigma^\otimes_2\Lambda_3^0 = 3 \text{Tr}\ C^2 + C\overline{C}) - 2(\text{Tr}\ C)^2 \\
= 2\left(3 \text{Tr}(\Re C)^2 - (\text{Tr}\ C)^2\right) \geq 0.
\]

In order to prove (O.3), we denote the eigenvalues of \(C\) by \(\lambda_1, \lambda_2, \lambda_3\) in decreasing order, i.e. \(\lambda_1 > \lambda_2 > \lambda_3\). First, we prove that \(a\lambda_1 \geq |b|^2\) as follows. Let \(s\) be an arbitrary real number. Then,

\[0 \leq \langle (s, b)|\sigma|(s, b)\rangle = as^2 + 2s||b||^2 + \langle b|C|b\rangle.
\]

Since the discriminant is positive, we have \(||b||^4 \leq a\langle b|C|b\rangle\), i.e. \(||b||^2 \leq a\langle b|C|b\rangle/ ||b||^2 \leq a\lambda_1\). Hence, using the relation \(a = 1 - \text{Tr} C\), we have

\[\text{Tr}\sigma^\otimes_2\Lambda_3^1 - \text{Tr}\sigma^\otimes_2\Lambda_3^0 \geq a(\text{Tr} C - \lambda_1) - \frac{1}{2}(\text{Tr}(C)^2 - \text{Tr}C^2) \\
= (1 - 2\lambda_1 - (\lambda_2 + \lambda_3))(\lambda_2 + \lambda_3) - \lambda_2\lambda_3 \\
\geq (1 - 2\lambda_1 - (\lambda_2 + \lambda_3))(\lambda_2 + \lambda_3) - \left(\frac{\lambda_2 + \lambda_3}{2}\right)^2 \\
= \frac{\lambda_2 + \lambda_3}{2}\left(2 - 4\lambda_1 - 5\frac{\lambda_2 + \lambda_3}{2}\right) \\
\geq \frac{\lambda_2 + \lambda_3}{2}\left(2 - 4\lambda_1 - 8\frac{\lambda_2 + \lambda_3}{2}\right) \\
= 4\frac{\lambda_2 + \lambda_3}{2}\left(\frac{1}{2} - \text{Tr} C\right) \geq 0,
\]

which implies (O.3). Next, we proceed to (O.4). For this proof, we focus on the relations

\[\text{Tr} C^2 \leq (\text{Tr}\ C)^2, \quad \text{Tr}\ (\Re C)^2 \leq (\text{Tr}\ C)^2,
\]

which follow from \(C \geq 0\), where \(\Re x\) denotes the imaginary part of \(x\). Hence,

\[5 \text{Tr}\sigma^\otimes_2\Sigma_4^1 - 3 \text{Tr}\sigma^\otimes_2\Sigma_4^0 = 5(1 - \text{Tr} C)\text{Tr} C + 5||b||^2 - 3\left(\frac{1}{2} \left(\text{Tr} C^2 + (\text{Tr} C)^2\right) - \frac{1}{2}\text{Tr} C\overline{C}\right) \\
\geq 5(1 - \text{Tr} C)\text{Tr} C - 3\left(\frac{1}{2} \left(\text{Tr} C^2 + (\text{Tr} C)^2\right) - \frac{1}{2}\text{Tr} C\overline{C}\right) \\
= 5\text{Tr} C - \frac{13}{2}(\text{Tr} C)^2 - \frac{1}{2}\text{Tr} C^2 - 2\text{Tr}(\Re C)^2 \\
\geq 5\text{Tr} C - 8(\text{Tr} C)^2 = \text{Tr} C(5 - 8 \text{Tr} C) \geq 0,
\]

which implies (O.4).
Appendix P. Proof of (42)

In this section, we use the same notation as in appendix O. By using the vector \( u_1 = |0\rangle_{A_1} \), \( u_2 = \frac{1}{\sqrt{2}}(|0\rangle_{A_2} + |1\rangle_{A_2}) \), the POVM \( M^{1 \rightarrow 2} \) can be written as

\[
M^{1 \rightarrow 2}(dg) = d^2 (g \otimes g)|u_1 \otimes u_2\rangle\langle u_1 \otimes u_2| (g \otimes g)^\dagger v(dg).
\]

Since \( |u_1 \otimes u_2\rangle = \frac{1}{2}(\varphi^0_{A_1, A_2} + \varphi^1_{A_1, A_2} - i\varphi^2_{A_1, A_2} - i\varphi^3_{A_1, A_2}) \), we have

\[
\begin{align*}
(u_1 \otimes u_2 \otimes \bar{u}_1 \otimes \bar{u}_2) & |u_1 \otimes u_2\rangle = \frac{1}{8}, \\
(u_1 \otimes u_2 \otimes \bar{u}_1 \otimes \bar{u}_2) & \Lambda_{\frac{1}{2}} |u_1 \otimes u_2\rangle = \frac{1}{8}, \\
(u_1 \otimes u_2 \otimes \bar{u}_1 \otimes \bar{u}_2) & \Sigma_{\frac{1}{2}} |u_1 \otimes u_2\rangle = 0, \\
(u_1 \otimes u_2 \otimes \bar{u}_1 \otimes \bar{u}_2) & \Sigma_{1} |u_1 \otimes u_2\rangle = \frac{1}{4}, \\
(u_1 \otimes u_2 \otimes \bar{u}_1 \otimes \bar{u}_2) & \Lambda_{\frac{1}{2}} |u_1 \otimes u_2\rangle = \frac{1}{4}.
\end{align*}
\]

Hence,

\[
\text{Tr} T(M^{1 \rightarrow 2})^\sigma_{D2} = (1 - \text{Tr} C)^2 + \frac{2}{3} \text{Tr} C - \frac{8}{15} (\text{Tr} C)^2 - \frac{1}{13} \text{Tr}(\text{tr} C)^2,
\]

which implies (42).

Appendix Q. Proof of (44)

Let \( T \) be an \( SU(d) \times SU(d) \)-invariant \( A-B \) separable test at level 0. Then, \( SU(d) \times SU(d) \)-invariance implies that the test \( T \) has the following form:

\[
T = a_{0,0} |\phi^0_{A_1, B_1}\rangle \langle \phi^0_{A_1, B_1}| \otimes |\phi^0_{A_2, B_2}\rangle \langle \phi^0_{A_2, B_2}| + a_{1,0} (I - |\phi^0_{A_1, B_1}\rangle \langle \phi^0_{A_1, B_1}|) \otimes |\phi^0_{A_2, B_2}\rangle \langle \phi^0_{A_2, B_2}| \]
\[
+ a_{0,1} |\phi^0_{A_1, B_1}\rangle \langle \phi^0_{A_1, B_1}| \otimes (I - |\phi^0_{A_2, B_2}\rangle \langle \phi^0_{A_2, B_2}|) + a_{1,1}(I - |\phi^0_{A_1, B_1}\rangle \langle \phi^0_{A_1, B_1}|) \otimes (I - |\phi^0_{A_2, B_2}\rangle \langle \phi^0_{A_2, B_2}|).
\]

Since the test \( T \) is at level 0, \( a_{0,0} = 1 \). Lemma 7 yields \( \text{Tr} T = d^2 \). Hence,

\[
d^2 - 1 = (a_{1,0} + a_{0,1})(d^2 - 1) + a_{1,1}(d^2 - 1)^2.
\]

In this case, the second error \( \text{Tr} \sigma_1 \otimes \sigma_2 T \) can be calculated as

\[
\text{Tr} \sigma_1 \otimes \sigma_2 T = (1 - p_1)(1 - p_2) + (1 - p_1)p_2 a_{0,1} + p_1(1 - p_2) a_{1,0} + p_1 p_2 a_{1,1}
\]
\[
= (1 - p_1)(1 - p_2) + \frac{(1 - p_1)p_2}{d^2 - 1} t_{0,1} + \frac{p_1(1 - p_2)}{d^2 - 1} t_{1,0} + \frac{p_1 p_2}{(d^2 - 1)^2} t_{1,1}.
\]
where $t_{0,1} \overset{\text{def}}{=} a_{0,1}(d^2 - 1)$, $t_{1,0} \overset{\text{def}}{=} a_{1,0}(d^2 - 1)$, $t_{1,1} \overset{\text{def}}{=} a_{1,1}(d^2 - 1)^2$. Since $p_1 p_2/(d^2 - 1)^2 \leq ((1 - p_1) p_2)/(d^2 - 1)$, $(p_1(1 - p_2))/(d^2 - 1)$,

$$\text{Tr} \sigma_1 \otimes \sigma_2 T \geq (1 - p_1)(1 - p_2) + \frac{p_1 p_2}{(d^2 - 1)^2} (d^2 - 1).$$

### Appendix R. Proof of (45)

Let $T$ be an $SU(d) \times SU(d)$-invariant $A_1, A_2, B_1, B_2$ separable test at level 0. $SU(d) \times SU(d)$-invariance implies that the test $T$ has the form

$$T = \sum_i p_i \int_{SU(d)} g_1 \otimes g_1 \otimes g_2 \otimes g_2 |u_{i,A_1} \otimes u_{i,A_2} \otimes u_{i,B_1} \otimes u_{i,B_2}\rangle$$

$$\times \langle u_{i,A_1} \otimes u_{i,A_2} \otimes u_{i,B_1}|(g_1 \otimes g_1 \otimes g_2) \otimes (g_2 \otimes g_2)\rangle^\dagger v(dg_1) v(dg_2),$$

where $\langle \phi^0_{A_1,B_1}|u_{i,A_1} \otimes u_{i,B_1}\rangle = \langle \phi^0_{A_2,B_2}|u_{i,A_2} \otimes u_{i,B_2}\rangle = 1/\sqrt{d}$. In this case, $\sum_i p_i = d^2$. Thus,

$$T = \sum_i p_i \int_{SU(d)} g_1 \otimes g_1 |u_{i,A_1} \otimes u_{i,B_1}\rangle \langle u_{i,A_1} \otimes u_{i,B_1}|(g_1 \otimes g_1)\rangle^\dagger v(dg_1)$$

$$\otimes \int_{SU(d)} g_2 \otimes g_2 |u_{i,A_2} \otimes u_{i,B_2}\rangle \langle u_{i,A_2} \otimes u_{i,B_2}|(g_2 \otimes g_2)\rangle^\dagger v(dg_2)$$

$$= \sum_i p_i \left( \frac{1}{d} |\phi^0_{A_1,B_1}\rangle \langle \phi^0_{A_1,B_1}| + a_i (I - |\phi^0_{A_1,B_1}\rangle \langle \phi^0_{A_1,B_1}|) \right)$$

$$\otimes \left( \frac{1}{d} |\phi^0_{A_2,B_2}\rangle \langle \phi^0_{A_2,B_2}| + b_i (I - |\phi^0_{A_2,B_2}\rangle \langle \phi^0_{A_2,B_2}|) \right).$$

Lemma 7 implies that $a_i, b_i \geq 1/d(d + 1)$. Thus,

$$T \leq \sum_i p_i \left( \frac{1}{d} |\phi^0_{A_1,B_1}\rangle \langle \phi^0_{A_1,B_1}| + \frac{1}{d(d + 1)} (I - |\phi^0_{A_1,B_1}\rangle \langle \phi^0_{A_1,B_1}|) \right)$$

$$\otimes \left( \frac{1}{d} |\phi^0_{A_2,B_2}\rangle \langle \phi^0_{A_2,B_2}| + \frac{1}{d(d + 1)} (I - |\phi^0_{A_2,B_2}\rangle \langle \phi^0_{A_2,B_2}|) \right)$$

$$= \left( |\phi^0_{A_1,B_1}\rangle \langle \phi^0_{A_1,B_1}| + \frac{1}{d + 1} (I - |\phi^0_{A_1,B_1}\rangle \langle \phi^0_{A_1,B_1}|) \right)$$

$$\otimes \left( |\phi^0_{A_2,B_2}\rangle \langle \phi^0_{A_2,B_2}| + \frac{1}{d + 1} (I - |\phi^0_{A_2,B_2}\rangle \langle \phi^0_{A_2,B_2}|) \right)$$

$$= T_{\text{inv}}^{1,A_1 \rightarrow B_1} \otimes T_{\text{inv}}^{1,A_2 \rightarrow B_2}.$$}

Hence

$$\text{Tr} T \sigma_1 \otimes \sigma_2 \leq \text{Tr} T_{\text{inv}}^{1,A_1 \rightarrow B_1} \otimes T_{\text{inv}}^{1,A_2 \rightarrow B_2} \sigma_1 \otimes \sigma_2 = \left( 1 - \frac{dp_1}{d + 1} \right) \left( 1 - \frac{dp_2}{d + 1} \right).$$

New Journal of Physics 11 (2009) 043028 (http://www.njp.org/)
Appendix S. Proof of (46)

Similarly to the proof of theorem 1, $U(1) \times U(1)$-invariance implies that this testing problem can be reduced to the testing problem for the probability distribution $P_{n}(k_1, k_2) \overset{\text{def}}{=} P_{p_1, p_2}(k_1) P_{p_2}(k_2)$ with the null hypothesis $p_1 + p_2 \leq \delta / n$. When $n$ is large enough, the probability distribution $P_{n/t_1/n, t_2/n}(k_1, k_2)$ can be approximated by the Poisson distribution

$$P_{t_1, t_2}(k_1, k_2) = e^{-t_1} e^{-t_2} \frac{t_1^{k_1} t_2^{k_2}}{k_1! k_2!} \frac{(t_1 + t_2)^{k_1+k_2}}{(k_1 + k_2)!} \left( \frac{t_1}{k_1 + t_2} \right)^{k_1} \left( \frac{t_2}{t_1 + t_2} \right)^{k_2}. $$

In order to calculate the lower bound of the optimal second error probability of the probability distribution $P_{t_1, t_2}(k_1, k_2)$, we treat hypothesis testing of the null hypothesis $t_1 + t_2 \leq \delta$ only for the one-parameter probability distribution family $\{P_{s, t_1, t_2}(k_1, k_2)\}_{0 \leq s < \infty}$. In this case, the probability distribution $P_{s, t_1, t_2}(k_1, k_2)$ has the form

$$P_{s, t_1, t_2}(k_1, k_2) = e^{-s(t_1' + t_2')} \frac{s(t_1' + t_2')}{(k_1 + k_2)!} \left( \frac{t_1'}{k_1 + t_2'} \right)^{k_1} \left( \frac{t_2'}{t_1' + t_2'} \right)^{k_2}. $$

Hence, the likelihood ratio $P_{s, t_1, t_2}(k_1, k_2) / P_{s', t_1, t_2}(k_1, k_2)$ depends only on the sum $k_1 + k_2$. Since

$$\sum_{k=0}^{k} P_{s, t_1, t_2}(k_1, k - k_1) = e^{-s(t_1' + t_2')} \frac{s(t_1' + t_2')^{k}}{k!};$$

this hypothesis test reduces to a hypothesis test of the Poisson distribution $e^{-t_1' / k!}$ with the null hypothesis $t \leq \delta$. In this case, when the true distribution is $e^{-(t_1' + t_2')} ((t_1' + t_2')^k / k!)$, the second error is greater than $\beta_{\alpha} (\leq \delta \| t_1' + t_2' \|)$. Therefore, we can conclude that

$$\lim_{n \to \infty} \beta_{n, s, t_1, t_2}(\delta, \frac{\| \sigma_{1, n}^r \otimes \sigma_{2, n}^s \|}{n}) \geq \beta_{\alpha} (\leq \delta \| t_1' + t_2' \|).$$

Conversely, focusing only on the random variable $k = k_1 + k_2$, we obtain the probability distribution $e^{-s(t_1' + t_2')} ((t_1' + t_2')^k / k!)$. Using optimal hypothesis testing of the Poisson distribution, we can construct a test achieving the lower bound $\beta_{\alpha} (\leq \delta \| t_1' + t_2' \|)$.

Appendix T. Proof of (47) and (48)

Let $T$ be an $SU(d) \times SU(d) \times SU(d)$-invariant $A - B$ separable test at level 0. $SU(d) \times SU(d) \times SU(d)$-invariance implies that the test $T$ has the form

$$T = \sum_{i} q_i \int_{SU(d)} \int_{SU(d)} \int_{SU(d)} g_1 \otimes g_3 \otimes g_3 \otimes g_1 \otimes g_2 \otimes g_2 |u_{i, A} \otimes u_{i, B}| \langle u_{i, A} \otimes u_{i, B}| u_{i, A} \otimes u_{i, B} \rangle \times (g_1 \otimes g_3 \otimes g_2 \otimes g_1 \otimes g_2 \otimes g_2) \nu(dg_1) \nu(dg_2) \nu(dg_3),$$

New Journal of Physics 11 (2009) 043028 (http://www.njp.org/)
where \( \langle \phi^0_{A_1, B_1} \otimes \phi^0_{A_2, B_2} \otimes \phi^0_{A_3, B_3} | u_{i, A} \otimes u_{i, B} \rangle = 1 / \sqrt{d^3} \). In this case, \( \sum_i q_i = 1 \). First, we focus on

\[
\begin{align*}
T_i & \overset{\text{def}}{=} d^3 \int_{SU(d)} \int_{SU(d)} \int_{SU(d)} \frac{d^3 g}{d^3 g} \frac{d^3 g}{d^3 g} \frac{d^3 g}{d^3 g} | g_1 \otimes g_3 \otimes g_1 \otimes \bar{g}_3 \otimes \bar{g}_3 | u_{i, A} \otimes u_{i, B} \rangle \langle u_{i, A} \otimes u_{i, B} | \\
& \quad \times \left( g_1 \otimes g_3 \otimes g_1 \otimes \bar{g}_3 \otimes \bar{g}_3 \right)^\dagger v(dg_1)v(dg_2)v(dg_3) \\
& = P_1 \otimes P_2 \otimes P_3 + a^i_{0, 0, 1} P_1 \otimes P_2 \otimes P_3 + a^i_{1, 0, 0} P_1 \otimes P_2 \otimes P_3 \\
& \quad + a^i_{0, 1, 1} P_1 \otimes P_2 \otimes P_3 + a^i_{1, 1, 0} P_1 \otimes P_2 \otimes P_3 + a^i_{1, 1, 1} P_1 \otimes P_3 \otimes P_3 \\
& \quad + a^i_{1, 1, 1} P_1 \otimes P_3 \otimes P_3. 
\end{align*}
\]

In order to calculate the coefficients \( a^i_{j,k,l} \), we treat the quantities \( \| \langle \phi^0_{A_1, B_1} | u_{i, A} \otimes u_{i, B} \rangle \|^2 \), \( \| \langle \phi^0_{A_2, B_2} \otimes \phi^0_{A_3, B_3} | u_{i, A} \otimes u_{i, B} \rangle \|^2 \), etc. In the following, we omit the subscript \( i \). Let \( X = (x_{i,j})_{1 \leq i,j \leq d} \) be a \( d \times d \) matrix corresponding to the vector \( u_A (u_B) \) of the entangled state between the two systems \( \mathcal{H}_{A_1} \) and \( \mathcal{H}_{A_2} \otimes \mathcal{H}_{A_3} (\mathcal{H}_{B_1} \) and \( \mathcal{H}_{B_2} \otimes \mathcal{H}_{B_3} \), respectively. Then,

\[
\begin{align*}
\langle \phi^0_{A_1, B_1} | u_A \otimes u_B \rangle & = \frac{1}{\sqrt{d}} \sum_{l_A=1}^d \sum_{l_B=1}^d (Y^t X)_{i_1, l_A} | l_A, l_B \rangle, \\
\langle \phi^0_{A_2, B_2} \otimes \phi^0_{A_3, B_3} | u_A \otimes u_B \rangle & = \frac{1}{\sqrt{d^2}} \sum_{k=1}^d \sum_{k_B=1}^d (X^t Y)_{k, k_B} | k_A, k_B \rangle. 
\end{align*}
\]

Hence,

\[
\begin{align*}
\| \langle \phi^0_{A_1, B_1} | u_A \otimes u_B \rangle \|^2 & = \frac{1}{d} \text{Tr}(Y^t X)(Y^t X)^\dagger, \\
\| \langle \phi^0_{A_2, B_2} \otimes \phi^0_{A_3, B_3} | u_A \otimes u_B \rangle \|^2 & = \frac{1}{d^2} \text{Tr}(X^t Y)(X^t Y)^\dagger = \frac{1}{d^2} \text{Tr}(Y^t X)(Y^t X)^\dagger.
\end{align*}
\]

That is, when we put \( \beta_1 \overset{\text{def}}{=} \| \langle \phi^0_{A_1, B_1} | u_A \otimes u_B \rangle \|^2 \), \( \beta_2 = \| \langle \phi^0_{A_2, B_2} \otimes \phi^0_{A_3, B_3} | u_A \otimes u_B \rangle \|^2 \). Since \( \frac{1}{\sqrt{d^3}} = \langle \phi^0_{A_1, B_1} \otimes \phi^0_{A_2, B_2} \otimes \phi^0_{A_3, B_3} | u_A \otimes u_B \rangle = \frac{1}{\sqrt{d^3}} \text{Tr}(Y^t X), \)

\[
d\beta_1 = \text{Tr}(Y^t X)(Y^t X)^\dagger \geq \frac{1}{d}.
\]

The equality holds if and only if \( (Y^t X) \) is a completely mixed state. Hence, the equality holds when \( u_A = u_B = |GHZ\rangle \). Similarly, we define the quantities \( \beta_2 \) and \( \beta_3 \). We also define \( \gamma \overset{\text{def}}{=} \| u_A \|_2 \| u_B \|_2 \), which satisfies the inequality

\[ \gamma \geq 1. \]

Indeed, when \( u_A = u_B = |GHZ\rangle \), \( \gamma = 1 \). Thus, by calculating the trace of the products of corresponding projections and \( | u_{i, A} \otimes u_{i, B} \rangle \langle u_{i, A} \otimes u_{i, B} | \), the coefficients can be
calculated as

\[
\begin{align*}
\alpha_{0,0,1} &= \frac{d^3}{(d^2 - 1)^2} \left( \beta_3 \rho - \frac{1}{d^3} \right), \\
\alpha_{0,1,1} &= \frac{d^3}{(d^2 - 1)^2} \left( \beta_2 \rho - \frac{1}{d^3} \right), \\
\alpha_{1,0,1} &= \frac{d^3}{(d^2 - 1)^2} \left( \beta_2 \rho - \frac{1}{d^3} \right), \\
\alpha_{1,0,0} &= \frac{d^3}{(d^2 - 1)^2} \left( \beta_1 \rho - \frac{1}{d^3} \right), \\
\alpha_{1,1,0} &= \frac{d^3}{(d^2 - 1)^2} \left( \beta_1 \rho - \frac{1}{d^3} \right), \\
\alpha_{1,1,1} &= \frac{d^3}{(d^2 - 1)^2} \left( \beta_1 \rho - \frac{1}{d^3} \right).
\end{align*}
\]

Therefore, substituting \( \beta = 1/d^2 \), \( \gamma = 1 \), we obtain (47).

Moreover,

\[
\text{Tr} T_i \sigma_1 \otimes \sigma_2 \otimes \sigma_3 = C_0 + C_1 \rho + C_2 \rho + C_3 \rho + \frac{p_1 p_2 p_3 d^3}{(d^2 - 1)^3} \gamma,
\]

where

\[
\begin{align*}
C_0 &\equiv (1 - p_1)(1 - p_2)(1 - p_3) + \frac{3p_1 p_2 p_3 - 2(p_1 p_2 + p_2 p_3 + p_3 p_1)}{d^2 - 1} p_1 + p_2 + p_3 \\
&\quad + \frac{3p_1 p_2 p_3 + (p_1 p_2 + p_2 p_3 + p_3 p_1)}{(d^2 - 1)^2} + \frac{p_1 p_2 p_3}{(d^2 - 1)^3}, \\
C_1 &\equiv \frac{d^2}{(d^2 - 1)^2(d + 1)} \left( d(d + 1) \left( 1 - \frac{d}{d + 1} p_1 \right) p_2 p_3 \\
&\quad + p_1 (d + 1)^2 (d - 1) \left( 1 - \frac{d}{d - 1} p_2 \right) \left( 1 - \frac{d}{d + 1} p_3 \right) \right), \\
C_2 &\equiv \frac{d^2}{(d^2 - 1)^2(d + 1)} \left( d(d + 1) \left( 1 - \frac{d}{d + 1} p_2 \right) p_3 p_1 \\
&\quad + p_2 (d + 1)^2 (d - 1) \left( 1 - \frac{d}{d - 1} p_3 \right) \left( 1 - \frac{d}{d + 1} p_1 \right) \right), \\
C_3 &\equiv \frac{d^2}{(d^2 - 1)^2(d + 1)} \left( d(d + 1) \left( 1 - \frac{d}{d + 1} p_3 \right) p_1 p_2 \\
&\quad + p_3 (d + 1)^2 (d - 1) \left( 1 - \frac{d}{d - 1} p_1 \right) \left( 1 - \frac{d}{d + 1} p_2 \right) \right).
\end{align*}
\]

It follows from the condition \( p_i \leq (d - 1)/d \) that these coefficients \( C_1, C_2 \) and \( C_3 \) are positive. Hence,

\[
\begin{align*}
\text{Tr} T_i \sigma_1 \otimes \sigma_2 \otimes \sigma_3 &\geq C_0 + (C_1 + C_2 + C_3) \frac{1}{d^2} + \frac{p_1 p_2 p_3 d^3}{(d^2 - 1)^3} \\
&= (1 - p_1)(1 - p_2)(1 - p_3) + \frac{(d + 2)p_1 p_2 p_3}{(d + 1)^2(d - 1)} + \frac{p_1 p_2 (1 - p_3) + p_1 (1 - p_2) p_3 + (1 - p_1) p_2 p_3}{(d + 1)^2(d - 1)}.
\end{align*}
\]
Therefore,
\[
\text{Tr} \left( \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \right) = \sum_i q_i \text{Tr} \left( \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \right)
\]
\[
\geq \left( 1 - p_1 \right) \left( 1 - p_2 \right) \left( 1 - p_3 \right) + \frac{(d + 2)p_1p_2p_3}{(d + 1)^2(d - 1)} + \frac{p_1p_2(1 - p_3) + p_1(1 - p_2)p_3 + (1 - p_1)p_2p_3}{(d + 1)^2(d - 1)}.
\]

Thus, we obtain (48) for \( G = SU(d) \). Moreover, since this bound can be attained by a \( U(d^2 - 1) \times U(d^2 - 1) \times U(d^2 - 1) \)-invariant test, the equation (48) holds for \( G = U(d^2 - 1) \).

References

[1] Bennett C, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels Phys. Rev. Lett. 70 1895

[2] Bennett C and Wiesner S J 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states Phys. Rev. Lett. 69 2881

[3] Ekert A 1991 Phys. Rev. Lett. 67 661

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

[5] Gühne O, Hyllus P, Brus D, Ekert A, Lewenstein M, Macchiavello C and Sanpera A 2002 Detection of entanglement with few local measurements Phys. Rev. A 66 062305

[6] Horodecki M, Horodecki P and Horodecki R 1996 Phys. Lett. A 223 1

[7] Lewenstein M, Kraus B, Cirac J I and Horodecki P 2000 Phys. Rev. A 62 052310

[8] Terhal B M 2000 Bell inequalities and the separability criterion Phys. Lett. A 271 319

[9] Holevo A S 1972 An analogue of the theory of statistical decisions in noncommutative theory of probability Trudy Moskov. Mat. Obšč. 26 133–49

Holevo A S 1972 Trans. Moscow Math. Soc. 26 133–49 (Engl. Transl.)

[10] Helstrom C W 1976 Quantum Detection and Estimation Theory (New York: Academic)

[11] Hiai F and Petz D 1991 The proper formula for relative entropy and its asymptotics in quantum probability Commun. Math. Phys. 143 99–114

[12] Ogawa T and Nagaoka H 2000 Strong converse and Stein’s lemma in quantum hypothesis testing Trans. IEEE Inf. Theory 46 2428–33

[13] Nagaoka H 2001 Strong converse theorems in quantum information theory Proc. Symp. ’ERATO Workshop on Quantum Information Science 2001’ p 33

Nagaoka H 2005 Asymptotic Theory of Quantum Statistical Inference ed M Hayashi (Singapore: World Scientific) chapter 3

[14] Hayashi M 2002 Optimal sequence of quantum measurements in the sense of Stein’s lemma in quantum hypothesis testing J. Phys. A: Math. Gen. 35 10759–73

[15] Audenaert K M R, Calsamiglia J, Munoz-Tapia R, Bagan E, Masanes L, Acin A and Verstraete F 2007 Discriminating states: the quantum Chernoff bound Phys. Rev. Lett. 98 160501

[16] Nussbaum M and Szkoła A 2009 A lower bound of Chernoff type for symmetric quantum hypothesis testing Ann. Stat. 37 1040–57

[17] Ogawa T and Hayashi M 2004 On error exponents in quantum hypothesis testing Trans. IEEE Inf. Theory IT-50 1368–72

[18] Hayashi M 2007 Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding Phys. Rev. A 76 062301

[19] Nagaoka H 2006 The converse part of the theorem for quantum hoeffding bound arXiv:quant-ph/0611289

[20] Holevo A S 1982 Probabilistic and Statistical Aspects of Quantum Theory (Amsterdam: North-Holland)
[21] Hayashi M (ed) 2005 Asymptotic Theory of Quantum Statistical Inference: Selected Papers (Singapore: World Scientific)
[22] Hayashi M, Matsumoto K and Tsuda Y 2006 A study of LOCC-detection of a maximally entangled state using hypothesis testing J. Phys. A: Math. Gen. 39 14427–46
[23] Hayashi M, Tomita A and Matsumoto K 2008 Statistical analysis of testing of an entangled state based on the Poisson distribution framework New J. Phys. 10 043029
[24] Hayashi M, Shi B-S, Tomita A, Matsumoto K, Tsuda Y and Jiang Y-K 2006 Hypothesis testing for an entangled state produced by spontaneous parametric down conversion Phys. Rev. A 74 062321
[25] Owari M and Hayashi M 2008 Two-way classical communication remarkably improves local distinguishability New J. Phys. 10 013006
[26] Acin A, Tarrach R and Vidal G 2000 Optimal estimation of two-qubit pure-state entanglement Phys. Rev. A 61 62307
[27] Lehmann E L 1986 Testing Statistical Hypotheses 2nd edn (New York: Wiley)
[28] Virmani S and Plenio M B 2003 Construction of extremal local positive-operator-valued measures under symmetry Phys. Rev. A 67 062308
[29] Matsumoto K and Hayashi M 2007 Universal distortion-free entanglement concentration Phys. Rev. A 75 062338
[30] Hayashi M 2008 Discrete realization of group symmetric LOCC-detection of maximally entangled state arXiv:0810.3381
[31] Hayashi M in preparation