A study of LOCC-detection of a maximally entangled state using hypothesis testing

2006 J. Phys. A: Math. Gen. 39 14427

(http://iopscience.iop.org/0305-4470/39/46/013)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 14427–14446 doi:10.1088/0305-4470/39/46/013

A study of LOCC-detection of a maximally entangled state using hypothesis testing

Masahito Hayashi[1], **Keiji Matsumoto**[1,2] **and Yoshiyuki Tsuda**[3,4]

[1] ERATO Quantum Computation and Information Project, JST, 5-28-3-201 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

[2] National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

[3] COE, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

E-mail: masahito@qci.jst.go.jp, keiji@nii.ac.jp and y-tsuda@ism.ac.jp

Received 7 April 2006, in final form 2 October 2006
Published 1 November 2006
Online at stacks.iop.org/JPhysA/39/14427

Abstract

We study how well we can answer the question 'Is the given quantum state equal to a certain maximally entangled state?' using LOCC, in the context of hypothesis testing. Under several locality and invariance conditions, optimal tests will be derived for several special cases by using basic theory of group representations. Some optimal tests are realized by performing quantum teleportation and checking whether the state is teleported. We will also give a finite process for realizing some optimal tests. The performance of the tests will be numerically compared.

PACS numbers: 03.65.Wj, 03.65.Ud, 02.20.−a
Mathematics Subject Classification: 81P15, 94A15

1. Introduction

Entanglement plays an important role in quantum information [2, 3, 6, 21]. An experimental system makes use of a certain maximally entangled state $|\phi^0_{AB}\rangle$ for the realization of quantum information processing. However, a state generated as a maximally entangled state is not necessarily a true maximally entangled state because the entanglement is easily corrupted by interaction with the environment. Hence, it is important to consider how well we can answer the question 'Is the state equal to $|\phi^0_{AB}\rangle$?' using quantum measurement with two outcomes (T_0, T_1) corresponding to (yes, no).

For practical use, it is natural to restrict our measurements to local operation and classical communications (LOCC) because some LOCC are easily implemented. Since the result of the LOCC measurement is probabilistic and the error of incorrect answers is inevitable, it is

[4] Address for correspondence: Institute of Statistical Mathematics, 4-6-7 Minami-Azabu, Minato-ku, Tokyo 106-8569, Japan.

important to consider an optimization problem of the measurement. As a framework of this argument, hypothesis testing is appropriate [13]. We consider two hypotheses

$$H_0 : \text{the state is } \left|\phi^0_{AB}\right\rangle \text{ versus } H_1 : \text{ the state is not } \left|\phi^0_{AB}\right\rangle.$$

Since H_0 is an accumulation point of H_1, the probability of the correct answer 'H_0 is true' when H_0 is really true is almost equal to the probability of the incorrect answer 'H_0 is true' when the state is close to $\left|\phi^0_{AB}\right\rangle$ but different. In the hypothesis testing, considering the two errors:

(i) to answer 'H_1 is true' though H_0 is really true,
(ii) to answer 'H_0 is true' though H_1 is really true,

we minimize the probability of (ii) with the probability of (i) kept small. See section 2 for details.

There are similar studies based on entanglement witness; a physical observable which gives minus outputs for a set of entangled inputs [18, 24]. The concept of entanglement witness is widely adopted, and there are many extensive arguments, especially, by making use of group symmetry. See, for example, theoretical works [20, 9, 5] and experiments [1]. However, in their arguments, analysis of statistical error is not sufficient. Hence it is worth considering this problem in the style of statistical hypothesis testing [19]. Though there have been studies of quantum hypothesis testing [15, 17, 16, 25, 10, 11, 13], there have not been enough arguments for testing entanglement.

In this paper, we give an approach to the hypothesis testing whether the state is $\left|\phi^0_{AB}\right\rangle$ using LOCC measurement between two parties and independent samples. We will derive optimal LOCC tests under some group invariance. The first case we consider is testing one sample of a pair of d-dimensional systems using LOCC between two parties. As a physical meaning, the optimal test is equivalent to optimal teleportation using a given state partially entangled, and the error probability is the same as the fidelity of the input and the output of the teleportation. It is also found that the test is equivalent to the extreme points of LOCC measurement described by Virmani and Plenio [27] and the entanglement witness given in [5]. Next, the result is generalized for the n-sample case. We derive an optimal test which is invariant by $SU(d^n)$, and its asymptotic behaviour ($n \to \infty$). In the asymptotic sense, the optimal LOCC test has the same performance as the optimal test without LOCC restriction. Next, we present the main result of this paper: for $d = n = 2$, the optimal test using LOCC between parties and independent samples, with $SU(2)$-invariance and some additional conditions or requirements. Since these tests are characterized by invariant measure, it contains continuous operations. However, in order to implement it, they need their construction with finite basis. Then, we show how to construct the optimal measurement with finite basis, for experimental realization. Finally, we consider an optimal test using non-local measurement between samples with $SU(2) \times SU(2)$-invariance. This test is equivalent to the entanglement swapping.

This paper is organized as follows. In section 2, a general formulation of hypothesis testing is introduced. In section 3, we state problems treated in this paper. In section 4, we consider a problem to test entanglement based on a single sample pair, and we derive an optimal test T^u. Moreover, we consider a case where there are n-independent pairs of samples to test entanglement. As a direct consequence of the previous section, we derive an optimal LOCC test T^U. It is also shown that this test has the same performance as the optimal test without LOCC restriction in an asymptotic sense. In section 5, an optimal test T^V is derived under an LOCC condition between AB-parties and between samples. In section 6, an optimal test T^W is also derived under another condition which is less restrictive as for locality. In section 7, we discretize the test derived in section 5 using representation of finite groups. In section 8, we compare the performance of these tests for $n = 2$.

2. Hypothesis testing

The main subject of this paper is to test whether a given state is

$$H_0 : \text{the maximally entangled state } \left|\phi^0_{AB}\right\rangle \text{ or } H_1 : \text{any other state}$$

using LOCC. To setup the hypothesis testing formally, we first consider the hypotheses H_0 and H_1 generally consisting of many elements. The hypothesis testing is an optimization problem with respect to the error probability of a measurement with two outcomes corresponding to the two hypotheses. As described later, there are two error probabilities, and one of them will be minimized with the other kept at a given small level.

Let $\mathcal{H}$ be a finite-dimensional Hilbert space which describes a physical system of interest. We denote the set of linear operators (matrices) on $\mathcal{H}$ (of density matrices on $\mathcal{H}$) by $\mathcal{L}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H})$, respectively. In hypothesis testing, we assume two hypotheses the *null hypothesis* H_0 and the *alternative hypothesis* H_1, and choose two non-empty subsets $\mathcal{S}_0$ and $\mathcal{S}_1$ of $\mathcal{S}(\mathcal{H})$ such that $\mathcal{S}_0 \cap \mathcal{S}_1 = \emptyset$, which correspond to our hypotheses. Suppose that the given state $\rho(\in \mathcal{S}(\mathcal{H}))$ of the system is unknown and that $\rho \in \mathcal{S}_0$ or $\rho \in \mathcal{S}_1$. We test

$$H_0 : \rho \in \mathcal{S}_0 \text{ versus } H_1 : \rho \in \mathcal{S}_1 \tag{1}$$

by a measurement with two outcomes $T = (T_0, T_1)$: if the outcome T_i is obtained, then we support the hypothesis H_i. However, the purpose of hypothesis testing is rejecting the null hypothesis H_0 and accepting H_1 with a given confidence level. Hence, we make decision only when the outcome T_1 is observed, and we reserve our decision when the outcome T_0 is observed. For simplicity, the test, or the measurement, T is often described by T_0. In the hypothesis testing, there are two kinds of errors: type 1 error is an event such that H_1 is accepted though H_0 is true. Type 2 error is an event such that H_0 is accepted though H_1 is true. Hence the type 1 error probability $\alpha(T, \rho)$ and the type 2 error probability $\beta(T, \rho)$ are given by

$$\alpha(T, \rho) = \mathrm{Tr}(\rho T_1)(\rho \in \mathcal{S}_0), \beta(T, \rho) = \mathrm{Tr}(\rho T_0)(\rho \in \mathcal{S}_1).$$

A test T is said to be *level-*α when $\alpha(T, \rho) \leqslant \alpha$ for any $\rho \in \mathcal{S}_0$ because α expresses the confidence level of our decision. A quantity $1 - \beta(T, \rho)$ is called *power*. In our main problem, we will consider level-zero tests only.

The main problem of hypothesis testing is to maximize the power, or equivalently, to minimize the type 2 error probability, of the test T of level-α. A test T of level-α is said to be the *most powerful (MP) level-*α at $\rho \in \mathcal{S}_1$ if $\beta(T, \rho) \leqslant \beta(T', \rho)$ for any level-α test T'. A test T of level-α is said to be *uniformly most powerful (UMP) level-*α if T is MP level-α for any $\rho \in \mathcal{S}_1$. The UMP test is regarded as the best test. However, except for some examples, there is no UMP test because the uniformness is too strict.

In mathematical statistics, it is too difficult to solve problems when both $\mathcal{S}_0$ and $\mathcal{S}_1$ have plural elements, except for some special cases, for example, the classical bioequivalence problem [4]. Hence, it is natural to consider the case where

$$\mathcal{S}_0 := \left\{\left\langle\phi^0_{AB}\right|\rho\left|\phi^0_{AB}\right\rangle \leqslant c\right\}, \qquad \mathcal{S}_1 := \left\{\left\langle\phi^0_{AB}\right|\rho\left|\phi^0_{AB}\right\rangle > c\right\},$$

or

$$\mathcal{S}_0 := \left\{\rho \neq \left|\phi^0_{AB}\right\rangle\!\left\langle\phi^0_{AB}\right|\right\}, \qquad \mathcal{S}_1 := \left\{\rho = \left|\phi^0_{AB}\right\rangle\!\left\langle\phi^0_{AB}\right|\right\}.$$

However, it is also too difficult to treat the above case. Hence, we consider the case $\mathcal{S}_0 := \left\{\left|\phi^0_{AB}\right\rangle\!\left\langle\phi^0_{AB}\right|\right\}$ in this paper.

If any $\rho \in \mathcal{S}_0 \cup \mathcal{S}_1$ is invariant by an action of a group, e.g., transposition of the order of independent samples, we can without loss of generality restrict attention to tests exhibiting the same invariance, because the error probabilities are invariant. We may also require that T_0 should be invariant by a group action leaving $\mathcal{S}_0$ invariant to simplify the problem mathematically. In experiments of entanglement, only LOCC can be used, so it is required that the test is realized by LOCC.

There is a trade-off between requirement and power of a test; if there are two requirements C_1 and C_2 for a test and if C_1 is weaker than C_2, then the optimal test for C_1 is more powerful than that for C_2. If C_1 and C_2 are unitary-invariance conditions, arguments for C_2 tend to be mathematically easier. If they are locality conditions, arguments for C_2 tend to be more difficult. In the next section, we will introduce some different conditions.

3. Problems treated in this paper

Suppose that n-independent samples are provided, that is, the state is given in the form

$$\rho = \sigma^{\otimes n} = \underbrace{\sigma \otimes \cdots \otimes \sigma}_{n} \tag{2}$$

for an unknown density σ of a single sample. We test the following hypothesis with level zero:

$$H_0 : \sigma = \left|\phi^0_{AB}\right\rangle\!\left\langle\phi^0_{AB}\right| \text{ versus } H_1 : \sigma \neq \left|\phi^0_{AB}\right\rangle\!\left\langle\phi^0_{AB}\right|. \tag{3}$$

Here,

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

is a vector of a maximally entangled pair on two d-dimensional parties A and 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. We refer to $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ as the *standard basis*.

Since the state is invariant by transposing the order of independent samples, we can without loss of generality impose that the tests for each case should be invariant by the same transposition. We additionally impose three types of basic conditions on tests, that is, level zero, locality and unitary invariance. Among various level-α conditions, we adopt $\alpha = 0$ because it is the most fundamental and the optimal tests that have analytically simple forms. We use only *AB-local* tests, i.e., LOCC between A and B. In some cases, we also require that tests should be *samplewise local*, i.e., LOCC between independent samples. Unitary invariance of the measurement is imposed for the symmetry of $\sigma^{\otimes n}$ or $\left(\left|\phi^0_{AB}\right\rangle\!\left\langle\phi^0_{AB}\right|\right)^{\otimes n}$.

First, we will make an LOCC test for a product system of two d-dimensional systems. Then, this will be generalized to the case of n-independent pairs of the $d \times d$ systems. For the n-sample case, a samplewise locality condition can be considered. Without the samplewise locality, we will derive optimal tests for any d and n. With the samplewise locality, however, the problem is so difficult that we will derive optimal tests only for $d = n = 2$.

We list three sets of conditions under which we will find best tests in sections 4–6. Unless otherwise mentioned, AB-locality is always imposed.

Remark 1. One may think that it is impossible to prepare the plural samples of the given unknown state σ when the state is easily corrupted by interaction. However, the density σ represents the ensemble of states generated by a specific state generator. Hence, as long as each sample is generated by this generator, it can be regarded as the state σ.

3.1. U-invariance for n-samples

As an action of $SU(d^n)$, *U-action* U_{AB} is defined as

$$U_{AB}(g) = U_A(g) \otimes \overline{U}_B(g) \quad \text{for} \quad g \in SU(d^n), \tag{4}$$

where U_A and U_B are the natural representations of $SU(d^n)$ on the d^n-dimensional subsystems A and B, respectively, and $\overline{X}$ is the contragredient of X with respect to the standard basis, i.e., $(\overline{X})_{i,j} = X_{j,i}$[5]. The state $|\phi^0_{AB}\rangle\langle\phi^0_{AB}|$ is U-invariant in the sense $U_{AB}(g)|\phi^0_{AB}\rangle\langle\phi^0_{AB}|U^\dagger_{AB}(g) = |\phi^0_{AB}\rangle\langle\phi^0_{AB}|$. A test $T = (T_0, T_1)$ is said to be U-invariant if $T_0 = U^\dagger_{AB}(g)T_0U_{AB}(g)$. Under the AB-locality condition, a UMP U-invariant test T^U will be derived. Moreover, it will be shown that, asymptotically, T^U has the same performance as a test which is UMP without the AB-locality or the U-invariance (section 4).

3.2. Samplewise locality and V-invariance for two samples

Let $d = n = 2$. We require samplewise locality, that is, in this case, a test T is realized by LOCC between the first and the second samples. The *V-action* of $SU(2)$ is defined as

$$V_{A_1B_1A_2B_2} := U_{A_1} \otimes \overline{U_{B_1}} \otimes U_{A_2} \otimes \overline{U_{B_2}}. \tag{5}$$

In the same sense as the U -invariance, $\left(|\phi^0_{AB}\rangle\langle\phi^0_{AB}|\right)^{\otimes 2}$ is V-invariant. Moreover, V leaves the set $\mathcal{S}_1$ invariant while U and W (defined below) do not. A test is said to be V-invariant if $V^\dagger_{A_1B_1A_2B_2}T_0V_{A_1B_1A_2B_2}$ is invariant. The V-invariance is not so strict as the V-invariance that its mathematical analysis is difficult. Hence we also consider *AB-invariance*. This invariance by *AB-transpositions* is generated by

$$|i\rangle_{A_1}|j\rangle_{B_1}|k\rangle_{A_2}|l\rangle_{B_2} \mapsto (-1)^{i+j+k+l}|1-j\rangle_{A_1}|1-i\rangle_{B_1}|1-l\rangle_{A_2}|1-k\rangle_{B_2}. \tag{6}$$

A UMP V-invariant test T^V will be derived under the samplewise locality, the AB-invariance and *termwise AB-covariance* defined in definition 1. Moreover, it will be shown that in a subset of density operators, T^V is UMP without the termwise AB-covariance (section 5).

3.3. W-invariance for two samples

Let $d = n = 2$ again. The *W-action* of the direct product $SU(2) \times SU(2)$ is defined as

$$W_{A_1B_1A_2B_2}(g,h) := U_{A_1}(g) \otimes \overline{U_{B_1}}(g) \otimes U_{A_2}(h) \otimes \overline{U_{B_2}}(h) \tag{7}$$

for $g, h \in SU(d)$. $|\phi^0_{AB}\rangle\langle\phi^0_{AB}|$ is again W-invariant, and a test $T = (T_0, T_1)$ is said to be W-invariant if $W^\dagger_{A_1B_1A_2B_2}T_0W_{A_1B_1A_2B_2}$ is invariant. The W-invariance is weaker than the U-invariance but is stronger than the V-invariance. In a subset of density operators, a UMP W-invariant test T^W is obtained (section 6).

The U-invariance is the most strict condition and the V-invariance is the weakest as the $SU(2)$ action for $d = n = 2$. As for the locality conditions, the samplewise locality in addition to the AB-locality treated in the V-invariance case is the most strict. As is shown in section 7 with a graph, the power of T^W is the highest, that of T_U is the second and that of T^V is the lowest in a neighbourhood of H_0. Hence it is recommended to use T^W rather than T^U when one can use non-local measurement between the two independent samples. However, asymptotically, T^U is optimal. See section 4.3.

[5] In fact, when we consider the inner product $\rangle x \otimes y|\phi^0_{AB}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1} x_i y_i$, the element y of the system B behaves as the elements of dual space of the system A. Hence, we call $\overline{U}_B$ the contragredient.

4. *U*-invariance

In this section, as the first step, we consider the case of $n = 1$. As the next step, we generalize the result to an arbitrary n.

4.1. One-sample case

Let $n = 1$. Virmani and Plenio [27] have derived extreme points of AB-local measurements using positive partial transpose (PPT). We will derive the same measurement $T^u = \{T_0^u, T_1^u\}$ as a UMP U-invariant test using property of separable measurement.

Theorem 1. *For $n = 1$, a UMP AB-local and U-invariant test T_0^u of level zero is given as follows:*

$$T_0^u = |\phi_{AB}^0\rangle\langle\phi_{AB}^0| + \frac{1}{d+1}(I - |\phi_{AB}^0\rangle\langle\phi_{AB}^0|). \tag{8}$$

The type 2 error probability is

$$\beta(T_0^u, \rho) = \beta(T^u, \sigma) = \frac{\mathrm{d}\theta + 1}{d+1}, \tag{9}$$

where $\theta = \langle\phi_{AB}^0|\sigma|\phi_{AB}^0\rangle$.

The formula (9) shows that the power of the test goes to zero as the state goes to $|\phi_{AB}^0\rangle$. Hence, it is difficult to reject H_0 even if H_1 is true. The case when σ is in a neighbourhood of H_0 will be highlighted in (14) and (15) in the next subsection. Other optimal tests derived in the later sections have the same property.

Remark 2. The protocol for the test T^u is implemented using the teleportation. Suppose that Alice has a state $|\psi\rangle$ in another system A'. She measures her total system $A \otimes A'$ by the Bell basis and then she lets Bob know the result. The teleportation is completed when Bob rotates the system according to Alice's information. The imperfectness causes some error in the teleportation, and the fidelity $|\langle\psi|\psi'\rangle|^2$ of the teleported state $|\psi'\rangle$ is evaluated by the measurement $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$. This process is equivalent to the test T^u with A' ignored, and the fidelity is the same as $\beta(T_0^u, \rho)$.

Remark 3. Virmani and Plenio [27] have proved that T^u is an extreme point of AB-local measurements under invariance conditions. Their work is related to our problem since an optimal test is always an extreme point though the converse is not always true. In the case $n = 1$, they found that there are two extreme points. As a test, however, it is obvious that the measurement other than T^u is not optimum as a test for the hypothesis. Hence we can also conclude that T^u is optimum based on their approach.

D'Ariano *et al* [5] have also considered the same measurement as T^u, as an entanglement witness. However, it is different from the hypothesis testing because the optimization of the error probability was not considered.

Proof of theorem 1. First, we show that T_0^u can be written as a classical mixture of AB-local projective measurements, i.e.,

$$T_0^u = \int_{g\in SU(d)} (U_A(g) \otimes \overline{U}_B(g))^\dagger \left(\sum_{i=1}^d |i\rangle_A|i\rangle_B\langle i|_A\langle i|_B\right)(U_A(g) \otimes \overline{U}_B(g))\mu(\mathrm{d}g), \tag{10}$$

where $\mu(\cdot)$ is the Haar measure on $SU(d)$. (Its full measure is 1.) From the invariance, we can easily see that the LHS has the form $a|\phi^0_{AB}\rangle\langle\phi^0_{AB}| + b(I - |\phi^0_{AB}\rangle\langle\phi^0_{AB}|)$. Since

$$\mathrm{Tr}(\text{LHS of (10)}) = d \text{ and } \langle\phi^0_{AB}|(\text{LHS of (10)})|\phi^0_{AB}\rangle = 1, \tag{11}$$

we obtain (10).

Then, the test

$$\begin{aligned}(U_A(g) \otimes \overline{U}_B(g))^\dagger &\left(\sum_{i=1}^d |i\rangle_A|i\rangle_B\langle i|_A\langle i|_B\right)(U_A(g)\otimes\overline{U}_B(g)) \\ &= \sum_{i=1}^d U_A(g)^\dagger|i\rangle_A\overline{U}_B(g)^\dagger|i\rangle_B\langle i|_A U_A(g)\langle i|_B\overline{U}_B(g)\end{aligned}$$

can be realized by the local measurements based on the bases $\{U_A(g)^\dagger|i\rangle_A\}_{i=1}^d$ and $\{\overline{U}_B(g)^\dagger|i\rangle_B\}_{i=1}^d$. Hence, the test T^u is realized by measuring $T = \{T_0, T_1\}$ by randomly choosing g subject to the Haar measure.

Next, we prove its optimality. A U-invariant test T_0 is written in the following form:

$$T_0 = a|\phi^0_{AB}\rangle\langle\phi^0_{AB}| + b(I - |\phi^0_{AB}\rangle\langle\phi^0_{AB}|),$$

where $0 \leqslant a \leqslant 1$ and $0 \leqslant b \leqslant 1$. Since $\langle\phi^0_{AB}|T_0|\phi^0_{AB}\rangle = a$, T_0 is level zero if and only if $a = 1$. Hence, it is sufficient to show that any LOCC level-zero U-invariant test T satisfies $b \geqslant (d+1)^{-1}$. Further, since $a = 1$, the condition $b \geqslant (d+1)^{-1}$ is equivalent with the condition

$$\mathrm{Tr}\, T_0 \geqslant d. \tag{12}$$

Now, we will show (12). Since an LOCC measurement is separable, T_0 should be separable between A and B, that is,

$$T_0 = \sum_i c_i M_{A,i} \otimes M_{B,i},$$

where $0 \leqslant c_i \leqslant 1$ and where $M_{A,i}$ and $M_{B,i}$ are rank-1 projections on A and B, respectively. Since $\mathrm{Tr}(T_0) = a + b(d^2-1) = 1 + b(d^2-1) = \sum_i c_i$, our problem is to minimize $\sum_i c_i$. Let $F_i = \mathrm{Tr}(M_{A,i}M^T_{B,i})$, where X^T is the transpose of X with respect to the standard basis. Then,

$$1 = \langle\phi^0_{AB}|T_0|\phi^0_{AB}\rangle = \sum_i c_i\langle\phi^0_{AB}|M_{A,i}\otimes M_{B,i}|\phi^0_{AB}\rangle = \frac{\sum_i c_i\,\mathrm{Tr}(M_{A,i}M^T_{B,i})}{d} = \frac{\sum_i c_i F_i}{d}.$$

Since $0 \leqslant F_i \leqslant 1$, we have

$$\mathrm{Tr}(T_0) = \sum_i c_i \geqslant \sum_i c_i F_i = d. \tag{13}$$

□

The unconditionally UMP level-zero test T^g_0 is $T^g_0 = |\phi^0_{AB}\rangle\langle\phi^0_{AB}|$, and its type 2 error is $\beta(T^g_0, \sigma) = \theta$. The AB-locality is reflected in the difference $(1-\theta)/(d+1)$ of type 2 errors of T^u_0 and T^g_0.

Remark 4. In order to prove the optimality, we focused on the trace of T_0. This trace method is very powerful for treating the separable POVM element detecting a given entangled state with probability one. This method was invented in this research for the first time, and was applied to other papers [26, 14].

4.2. *n-sample case*

Theorem 1 is generalized to the case of an arbitrary n as follows.

Theorem 2. *For any $n \geqslant 1$, a UMP AB-local and U-invariant test of level zero is*

$$T_0^U = \left(\left|\phi_{AB}^0\right\rangle\left\langle\phi_{AB}^0\right|\right)^{\otimes n} + \frac{1}{d^n+1}\left(I - \left(\left|\phi_{AB}^0\right\rangle\left\langle\phi_{AB}^0\right|\right)^{\otimes n}\right).$$

The type 2 error probability is

$$\beta\left(T_0^U, \sigma^{\otimes n}\right) = \frac{d^n\theta^n + 1}{d^n+1},$$

where $\theta = \left\langle\phi_{AB}^0\middle|\sigma\middle|\phi_{AB}^0\right\rangle$.

Proof. The proof of theorem 1 is directly applied by replacing the space A in theorem 1 with $A_1 \otimes \cdots \otimes A_n$, B with $B_1 \otimes \cdots \otimes B_n$, the dimension d with d^n and the group $SU(d)$ with $SU(d^n)$. □

4.3. *Asymptotic property*

For comparison, let us consider other tests:

$$T_0^{u,n} = \left(T_0^u\right)^{\otimes n} \quad \text{and} \quad T_0^G = \left(T_0^g\right)^{\otimes n} = \left(\left|\phi_{AB}^0\right\rangle\left\langle\phi_{AB}^0\right|\right)^{\otimes n}.$$

Note that they are both level zero since T_0^u and T_0^g are level zero. We also note that T_0^G is UMP level zero without any condition. The type 2 error probabilities are

$$\beta\left(T_0^{u,n}, \sigma^{\otimes n}\right) = \left(\frac{d\theta+1}{d+1}\right)^n, \qquad \beta\left(T_0^G, \sigma^{\otimes n}\right) = \theta^n.$$

Hence we have

$$\beta\left(T_0^G, \sigma^{\otimes n}\right) < \beta\left(T_0^U, \sigma^{\otimes n}\right) < \beta\left(T_0^{u,n}, \sigma^{\otimes n}\right) \qquad (n \geqslant 2).$$

On the other hand, the asymptotic behaviour of $\beta\left(T_0^U, \sigma^{\otimes n}\right)$ is

$$\lim_{n\to\infty} \frac{\beta\left(T_0^U, \sigma^{\otimes n}\right)}{\theta^n} = 1 \quad \text{if} \quad \theta \geqslant 1/d, \tag{14}$$

$$\lim_{n\to\infty} \frac{\beta\left(T_0^U, \sigma^{\otimes n}\right)}{1/d^n} = 1 \quad \text{if} \quad \theta < 1/d. \tag{15}$$

It means that if $\theta = \left\langle\phi_{AB}^0\middle|\sigma\middle|\phi_{AB}^0\right\rangle \geqslant 1/d$, then T_0^U and T_0^G have the same asymptotic performance not only for the exponent but also for the coefficient of the type 2 error probabilities. In this sense, the restriction of AB-locality and U-invariance does not reduce the performance of the UMP level-zero test T_0^G.

5. Samplewise locality, V-invariance for $n = d = 2$

We consider the case $n = d = 2$. First, we derive a UMP test T^V under the conditions of samplewise locality, V-invariance, AB-invariance and the *termwise AB-covariance* (defined in definition 1). We then prove that this test is also UMP without the termwise AB-covariance for a subset $\mathcal{S}'$ of density operators.

Before defining termwise covariance, we note that if T_0 is AB-local and samplewise-local then T_0 is AB-separable and samplewise separable, that is,

$$T_0 = \sum_i p_i M_{A_1,i} \otimes M_{B_1,i} \otimes M_{A_2,i} \otimes M_{B_2,i},$$

where M_X is a rank-1 projection on the system X.

Definition 1. *The test T_0 is said to be termwise AB-covariant if*

$$\mathrm{Tr}\big(M_{A_1,i}\overline{M^T_{B_1,i}}\big) = 1 \quad \textit{and} \quad \mathrm{Tr}\big(M_{A_2,i}\overline{M^T_{B_2,i}}\big) = 1$$

holds.

The meaning of the termwise AB-covariance will be clarified by Hayashi [12]. Define $|\phi^1_{AB}\rangle$, $|\phi^2_{AB}\rangle$ and $|\phi^3_{AB}\rangle$ as follows:

$$\begin{aligned}|\phi^1_{AB}\rangle &:= \tfrac{\sqrt{-1}}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B),\\ |\phi^2_{AB}\rangle &:= \tfrac{1}{\sqrt{2}}(-|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B),\\ |\phi^3_{AB}\rangle &:= \tfrac{\sqrt{-1}}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B).\end{aligned}$$

In this section, we frequently use the matrix expression $x_{ij} = \langle\phi^i_{AB}|\sigma|\phi^j_{AB}\rangle$ for the sake of notational convenience.

Remark 5. There is a two-to-one group homomorphism of $SU(2)$ onto $SO(3)$ as the three-dimensional subrepresentation of $U_A \otimes \overline{U_B}$. It irreducibly acts on $\mathrm{span}\{|\phi^1_{AB}\rangle, |\phi^2_{AB}\rangle, |\phi^3_{AB}\rangle\}$. Now, we regard the tensor product space $(\mathrm{span}\{|\phi^0_{AB}\rangle, |\phi^1_{AB}\rangle, |\phi^2_{AB}\rangle, |\phi^3_{AB}\rangle\})^{\otimes 2}$ as the space$M$ of 4×4 matrices spanned by the basis $e^{ij} := |\phi^i_{AB}\rangle_1|\phi^j_{AB}\rangle_2$. $SU(2)$ acts on M by $V_{A_1B_1A_2B_2}$ as follows:

$$\left[\begin{array}{c|c}1 & 0\\ \hline 0 & S\end{array}\right]\left[\begin{array}{c|ccc}e^{00} & e^{01} & e^{02} & e^{03}\\ \hline e^{10} & e^{11} & e^{12} & e^{13}\\ e^{20} & e^{21} & e^{22} & e^{23}\\ e^{30} & e^{31} & e^{32} & e^{33}\end{array}\right]\left[\begin{array}{c|c}1 & 0\\ \hline 0 & S^T\end{array}\right] \tag{16}$$

for $S \in SO(3)$. Let $K^\pm_i$, $L^\pm_i$ be i-dimensional subspaces of M defined as follows:

K^+_6: The space of all 3×3 symmetric matrices spanned by $e^{ij}(1 \leqslant i, j \leqslant 3)$,
K^+_1: the one-dimensional subspace of K^+_6 spanned by the 3×3 identity matrix,
K^+_3: the three-dimensional subspace of K^+_6 spanned by $e^{ij} + e^{ji} (i \neq j)$,
K^+_2: the two-dimensional space spanned by

$$e^{11} + \omega e^{22} + \omega^2 e^{33} \text{ and } e^{11} + \omega^2 e^{22} + \omega e^{33},$$

where ω is a solution to $\omega^2 + \omega + 1 = 0$,
$K^+_5 := K^+_6 - K^+_1 = K^+_3 + K^+_2$,
K^-_3: the space of all 3×3 alternating matrices spanned by e^{ij} $(1 \leqslant i, j \leqslant 3)$,
M^+_{10}: the ten-dimensional space of all 4×4 symmetric matrices,
M^-_6: the six-dimensional space of all 4×4 alternating matrices,
L^+_1: the one-dimensional space spanned by $e^{00} = |\phi^0_{AB}\rangle^{\otimes 2}$,
$L^+_3 := M^+_{10} - K^+_6 - L^+_1$,
$L^-_3 := M^-_6 - K^-_3$.

The V-action $V = U_{A_1} \otimes \overline{U_{B_1}} \otimes U_{A_2} \otimes \overline{U_{B_2}}$ is equivalent to $U_{A_1} \otimes U_{B_1} \otimes U_{A_2} \otimes U_{B_2}$ as group representation. By the V-action (or, equivalently, by the SO(3) action of the form (16)), M is decomposed into subspaces of irreducible representations as

$$M = K^+_5 \underbrace{\oplus K^-_3 \oplus L^+_3 \oplus L^-_3}_{\text{equivalent}} \underbrace{\oplus K^+_1 \oplus L^+_1}_{\text{equivalent}}. \tag{17}$$

See [7, 8] for details. The decompositions into the three spaces K^-_3 and $L^\pm_3$ and into the two spaces K^+_1 and L^+_1 in (17) are not unique because they have the equivalent representations of three dimension and one dimension, respectively.

The AB-transposition simultaneously maps $|\phi^0_{AB}\rangle_i$ to $-|\phi^0_{AB}\rangle_i$ for $i = 1, 2$, while it leaves other $|\phi^i_{AB}\rangle_i$ invariant. Hence it acts on M as

$$M \ni X \mapsto \begin{pmatrix} -1 & 0 \\ 0 & I_3 \end{pmatrix} X \begin{pmatrix} -1 & 0 \\ 0 & I_3 \end{pmatrix} \tag{18}$$

where I_3 is the three-dimensional identity matrix. Hence it makes -1-multiplication on $L_3^{\pm}$ while K_3^- is left invariant. Transposition of the order of the independent samples corresponds to the matrix transposition of M. Hence it makes -1-multiplication on K_3^- and L_3^- while L_3^+ is left invariant. Therefore, by the V-action with the two types of transposition, M is decomposed as

$$M = K_5^+ \oplus \underbrace{K_3^- \oplus L_3^+ \oplus L_3^- \oplus}_{\text{not equivalent}} \underbrace{K_1^+ \oplus L_1^+}_{\text{equivalent}}.$$

By the W-action, M is decomposed as

$$M = L_1^+ \oplus L_3' \oplus L_3'' \oplus K_9,$$

where L_3' and L_3'' are the three-dimensional spaces spanned by $x_{i,0}$ and $x_{0,j}$, respectively, and K_9 is the nine-dimensional space spanned by $x_{i,j}$ $(1 \leqslant i, j \leqslant 3)$. Though L_3' and L_3'' have the same dimension, this decomposition is unique because the first and the second element of $SU(2) \times SU(2)$ independently act on L_3' and L_3''. The transposition of the order of independent samples corresponds to transposing L_3' and L_3''. Hence the W-invariant test for $\sigma^{\otimes 2}$ has the same weight on L_3' and L_3''.

5.1. Termwise AB-covariance

We use the symbols $K_i^{\pm}$ and $L_i^{\pm}$ not only as the spaces but also as the projection operators. Any operator X invariant by the V-action, the AB-transposition and the transposition of the order of independent samples is of the form

$$X = w_1 K_5^+ + w_2 K_3^- + w_3 L_3^+ + w_4 L_3^- + J,$$

where $0 \leqslant w_i \leqslant 1$ and J is an operator on the two-dimensional space $J_2 := K_1^+ \oplus L_1^+$. Each weight w_i and the form of N of the optimal test for $|\phi^0_{AB}\rangle$ is obtained as follows.

Theorem 3. *A UMP AB-local, samplewise local, V-invariant, AB-invariant and termwise AB-covariant test of level zero is given as*

$$T_0^V = \tfrac{1}{10} K_5^+ + \tfrac{1}{3} L_3^+ + \left(|\phi^0_{AB}\rangle\langle\phi^0_{AB}|\right)^{\otimes 2} + \tfrac{1}{6} K_3^- + \tfrac{1}{3} L_3^-. \tag{19}$$

The type 2 error of T_0^V is

$$\beta\left(T_0^V, \sigma^{\otimes 2}\right) = v^T Z v - \tfrac{2}{15}(\mathrm{Re}(x_{12})^2 + \mathrm{Re}(x_{23})^2 + \mathrm{Re}(x_{31})^2) \tag{20}$$

where

$$v = \begin{pmatrix} x_{11} & -1/2 \\ x_{22} & -1/2 \\ x_{33} & -1/2 \end{pmatrix}, \qquad Z = \frac{1}{15}\begin{pmatrix} 6 & 7 & 7 \\ 7 & 6 & 7 \\ 7 & 7 & 6 \end{pmatrix}.$$

Proof of theorem 3. First, all the conditions of locality and invariance are checked by calculating the weight for each projection of

$$T_0^V = \int_{g \in SU(2)} \left(V_{A_1B_1A_2B_2}(g)\right)^{\dagger} (\Pi_{00} + \Pi_{01} + \Pi_{10} + \Pi_{11}) \left(V_{A_1B_1A_2B_2}(g)\right) \mu(\mathrm{d}g), \tag{21}$$

where $\mu(\cdot)$ is the Haar measure on $SU(2)$ and where Π_{ij} $(i, j = 0, 1)$ is the projection on the one-dimensional subspace spanned by

$$|i\rangle_{A_1} \otimes |i\rangle_{B_1} \otimes \frac{|0\rangle_{A_2} + (-1)^j |1\rangle_{A_2}}{\sqrt{2}} \otimes \frac{|0\rangle_{B_2} + (-1)^j |1\rangle_{B_2}}{\sqrt{2}} \tag{22}$$

(see also section 7.2 bellow).

Next, we show that the type 2 error of T_0^V is minimized. Any test satisfying all those conditions is given in the form

$$T_0 = \sum_i q_i \int_{g\in SU(2)} U_{A_1}(g)^\dagger |0\rangle_{A_1}\langle 0|_{A_1} U_{A_1}(g) \otimes U_{B_1}(g)^T |0\rangle_{B_1}\langle 0|_{B_1} \overline{U}_{B_1}(g)$$
$$\otimes U_{A_2}(g)^T \left|\psi_{F_i}\right\rangle_{A_2}\left\langle\psi_{F_i}\right|_{A_2} \overline{U}_{A_2}(g) \otimes U_{B_2}(g)^T \left|\psi_{F_i}\right\rangle_{B_2}\left\langle\psi_{F_i}\right|_{B_2} \overline{U}_{B_2}(g)\mu(\mathrm{d}g)$$

where $q_i \geqslant 0$ and

$$|\psi_F\rangle_X = \frac{\sqrt{F}|0\rangle_X + \sqrt{1-F}|1\rangle_X}{\sqrt{2}} \qquad (0 \leqslant F \leqslant 1).$$

For the invariance conditions, T_0 can be written as

$$T_0 = w_1 K_5^+ + w_2 L_3^+ + J + w_3 K_3^- + w_4 L_3^- \qquad (0 \leqslant w_i \leqslant 1).$$

To satisfy the level-zero condition, the weight of J for L_1^+ should be one. To minimize the type 2 error, the weight of J for K_1^+ should be zero. Hence T_0 should be

$$T_0 = w_1 K_5^+ + w_2 L_3^+ + L_1^+ + w_3 K_3^- + w_4 L_3^-.$$

Define

$$m(X) = \langle 0|_{A_1}\langle 0|_{B_1}\langle\psi_F|_{A_2}\langle\psi_F|_{B_2} X |0\rangle_{A_1}|0\rangle_{B_1}|\psi_F\rangle_{A_2}|\psi_F\rangle_{B_2}.$$

By direct calculation, $m(X)$ is given as follows:

$$m(K_5^+) = \frac{F^2 - F + 1}{6}, \qquad m(L_3^+) = \frac{F}{2}, \qquad m(K_1^+) = \frac{(2F-1)^2}{12}, \qquad m(L_1^+) = \frac{1}{4},$$
$$m(K_3^-) = \frac{F(1-F)}{2}, \qquad m(L_3^-) = \frac{1-F}{2}.$$

Moreover,

$$\mathrm{Tr}(\sigma^{\otimes 2} K_5^+) = \frac{1}{3}(x_{11} + x_{22} + x_{33})^2 + \frac{1}{6}\sum_{1\leqslant i<j\leqslant 3}(x_{ii} + x_{jj})^2$$
$$- \frac{4}{3}\sum_{1\leqslant i<j\leqslant 3}(\mathrm{Im}\, x_{ij})^2 + \frac{1}{3}\sum_{1\leqslant i<j\leqslant 3}|x_{ij}|^2, \tag{23}$$

$$\mathrm{Tr}(\sigma^{\otimes 2} L_3^+) = \sum_{i=1}^{3}(x_{00}x_{ii} + |x_{0i}|^2), \tag{24}$$

$$\mathrm{Tr}(\sigma^{\otimes 2} K_1^+) = \frac{1}{3}\sum_{1\leqslant i,j\leqslant 3} x_{ij}^2, \tag{25}$$

$$\mathrm{Tr}(\sigma^{\otimes 2} L_1^+) = x_{00}^2, \tag{26}$$

$$\mathrm{Tr}(\sigma^{\otimes 2} K_3^-) = \sum_{1\leqslant i<j\leqslant 3} x_{ii}x_{jj} - \sum_{1\leqslant i<j\leqslant 3}|x_{ij}|^2, \tag{27}$$

$$\mathrm{Tr}(\sigma^{\otimes 2} L_3^-) = \sum_{i=1}^{3}(x_{00}x_{ii} - |x_{0i}|^2). \tag{28}$$

Hence, the type 2 error probability is given by

$$\beta(T_0, \sigma^{\otimes 2}) = \sum_i q_i \left(a F_i^2 + b F_i + c\right), \tag{29}$$

where

$$a = \frac{(x_{11} - x_{22})^2 + (x_{22} - x_{33})^2 + (x_{33} - x_{11})^2}{15} + \frac{2}{5}((\mathrm{Re}\, x_{12})^2 + (\mathrm{Re}\, x_{23})^2 + (\mathrm{Re}\, x_{31})^2),$$

$$b = -a + \frac{(\mathrm{Im}\, x_{01})^2 + (\mathrm{Im}\, x_{02})^2 + (\mathrm{Im}\, x_{03})^2}{6},$$

$$c = -\frac{(\mathrm{Im}\, x_{01})^2 + (\mathrm{Im}\, x_{02})^2 + (\mathrm{Im}\, x_{03})^2}{3} + \frac{(\mathrm{Re}\, x_{12})^2 + (\mathrm{Re}\, x_{23})^2 + (\mathrm{Re}\, x_{31})^2}{15} + v_0^T Z_0 v_0,$$

and where

$$v_0 = \begin{pmatrix} x_{11} & -1/2 \\ x_{22} & -1/2 \\ x_{33} & -1/2 \end{pmatrix}, \qquad Z_0 = \frac{1}{30}\begin{pmatrix} 4 & 3 & 3 \\ 3 & 4 & 3 \\ 3 & 3 & 4 \end{pmatrix}.$$

We minimize (29) under necessary conditions on $\sum_i q_i$ and $\sum_i q_i F_i$ as follows. Since T_0 is level zero, we have

$$\frac{1}{4}\sum_i q_i = \langle \phi_{AB}^0 |^{\otimes 2} T_0 | \phi_{AB}^0 \rangle^{\otimes 2} = 1. \tag{30}$$

We have

$$\sum_i q_i F_i = 2. \tag{31}$$

Hence, the type 2 error probability (29) is minimized if $\sum_i q_i F_i^2$ is minimized under (30) and (31). From Jensen's inequality,

$$\sum_i q_i F_i^2 = 4 \sum_i \frac{q_i}{4} F_i^2 \geqslant 4 \left(\sum_i \frac{q_i}{4} F_i \right)^2 = 1.$$

The equality holds if $q_1 = \cdots = q_4 = 1$ and $F_1 = \cdots = F_4 = 1/2$ so that the type 2 error probability is uniformly minimized if $T_0 = T_0^V$. Hence we obtain (19) and (20). □

5.2. *Optimality without termwise AB-covariance*

In this subsection, we discuss the optimality of T^V under another conditions, removing the termwise AB-locality. In this argument, we use PPT instead of separability of measurement. PPT is a class of tests which strictly includes the set of separable/LOCC tests. Hence, a test is best among LOCC if it is LOCC and is best among PPT. The set of PPT tests satisfies some linear inequalities for weights on projections $K_i^{\pm}$ and $L_i^{\pm}$. So T^V is optimal in PPT if it uniformly minimizes error probability under the condition of the linear inequalities.

We consider parameterized subsets of states as follows.

Definition 2. *Let $S(\vartheta)$ be a set of density operators σ satisfying the following two conditions for $x_{ij} = \langle \phi_{AB}^i | \sigma | \phi_{AB}^j \rangle$:*

$$\theta = x_{00} = \langle \phi_{AB}^0 | \sigma | \phi_{AB}^0 \rangle \geqslant \vartheta,$$

and

$$\frac{1}{2} \sum_{1\leqslant i<j\leqslant 3} (x_{ii} - x_{jj})^2 + 3 \sum_{1\leqslant i<j\leqslant 3} |x_{ij}|^2 \geqslant 4 \sum_{1\leqslant i<j\leqslant 3} (\mathrm{Im}\, x_{ij})^2, \tag{32}$$

or equivalently,

$$3\,\mathrm{Tr}\big(\sigma^{\otimes 2}K_1^+\big) \geqslant \mathrm{Tr}(\sigma^{\otimes 2}K_3^-). \tag{33}$$

This condition (32) is satisfied if

$$\sigma = (1-p-q-r)|\phi_{AB}^0\rangle\langle\phi_{AB}^0| + p|\phi_{AB}^1\rangle\langle\phi_{AB}^1| + q|\phi_{AB}^2\rangle\langle\phi_{AB}^2| + r|\phi_{AB}^3\rangle\langle\phi_{AB}^3|.$$

Indeed, it holds that

$$3\,\mathrm{Tr}\big(\sigma^{\otimes 2}K_1^+\big) - \mathrm{Tr}(\sigma^{\otimes 2}K_3^-) = \frac{(p-q)^2 + (q-r)^2(r-p)^2}{2} \geqslant 0.$$

Theorem 4. *There is $\theta_0 < 1$ such that T_0^V is UMP AB-local, samplewise local, V-invariant, weakly AB-invariant with level zero in $\mathcal{S}(\theta_0)$.*

Proof. In this proof, we deal with the alternative side $T_1 = I - T_0$ of the measurement because it makes the calculation simple; T_1 has the zero weight on L_1^+. If T_1 satisfies all the locality and invariance conditions and if it is level zero, then T_1 is given by

$$T_1 = w_1K_5^+ + w_2L_3^+ + w_3K_1^+ + w_4K_3^+ + w_5L_3^-.$$

The power of the test is given as

$$\mathrm{Tr}\big(\sigma^{\otimes 2}T_1\big) = w_1\,\mathrm{Tr}\big(\sigma^{\otimes 2}K_5^+\big) + w_2\,\mathrm{Tr}\big(\sigma^{\otimes 2}L_3^+\big) + w_3\,\mathrm{Tr}\big(\sigma^{\otimes 2}K_1^+\big) \\ + w_4\,\mathrm{Tr}(\sigma^{\otimes 2}K_3^-) + w_5\,\mathrm{Tr}(\sigma^{\otimes 2}L_3^-).$$

Lemma 1 shows that, if $1-\theta$ is small, the power is maximized if

$$5w_1 + 3w_2, \quad w_2, \quad w_3, \quad 5w_1 + 3w_2 + w_3 + 3w_4 + 3w_5, \quad \text{and} \quad w_5 \tag{34}$$

are simultaneously maximized. From lemmas 2–4 in the appendix, $w_1, \ldots, w_5$ should satisfy

$$\frac{10w_1 + 6w_2 - w_3}{12} \leqslant 1, \tag{35}$$

$$\frac{w_3 + 2(w_4 + w_5)}{4} \leqslant 1, \tag{36}$$

$$w_2 = w_5, \tag{37}$$

$$\frac{3}{4}(w_2 + w_5) \leqslant 1. \tag{38}$$

Therefore,

$$\max\{5w_1 + 3w_2 \mid (35), 0 \leqslant w_i \leqslant 1\} = \tfrac{13}{2},$$
$$\max\{w_2 \mid (37), (38), 0 \leqslant w_i \leqslant 1\} = \tfrac{2}{3},$$
$$\max\{w_3 \mid (35), (36), 0 \leqslant w_i \leqslant 1\} = 1,$$
$$\max\{5w_1 + 3w_2 + w_3 + 3w_4 + 3w_5 \mid 0 \leqslant w_i \leqslant 1\} = 12,$$
$$\max\{w_5 \mid (37), (38), 0 \leqslant w_i \leqslant 1\} = \tfrac{2}{3},$$

and we have (19) as a solution to the linear maximization problem. □

6. W-invariance for $n = d = 2$

Let $d = n = 2$. In this section, we test the following hypothesis with level zero:

$$H_0 : \sigma = |\phi^0_{AB}\rangle\langle\phi^0_{AB}| \text{ versus } H_1 : 1/4 \leqslant \langle\phi^0_{AB}|\sigma|\phi^0_{AB}\rangle < 1. \tag{39}$$

In other words, we consider the case where the set of possible states is $\mathcal{S}' = \{\sigma \mid \langle\phi^0_{AB}|\sigma|\phi^0_{AB}\rangle \geqslant 1/4\}$.

Theorem 5. *A UMP AB-local, and W-invariant for (39) of level zero is given as follows:*

$$T^W_0 = |\phi^0_{AB}\rangle\langle\phi^0_{AB}|^{\otimes 2} + \tfrac{1}{3}\left(I - |\phi^0_{AB}\rangle\langle\phi^0_{AB}|\right)^{\otimes 2}. \tag{40}$$

The type 2 error probability of T^W_0 is

$$\beta\left(T^W_0, \sigma^{\otimes 2}\right) = \theta^2 + \frac{(1-\theta)^2}{3}. \tag{41}$$

Remark 6. The test T^W is implemented, by using the entanglement swapping from $A_1 \otimes B_1$ and $A_2 \otimes B_2$ to $B_1 \otimes B_2$; measuring $A_1 \otimes A_2$ in the Bell basis can create entanglement in $B_1 \otimes B_2$. The success rate, or the fidelity to the maximally entangled state, of the swapping is equivalent to the type 2 error probability $\beta\left(T^W_0, \sigma^{\otimes 2}\right)$.

Proof of theorem 5. T_0 is W-invariant (see remark 5). It is also AB-local because

$$\begin{aligned} T^W_0 = \int_{g,h\in SU(2)} &(W_{A_1B_1A_2B_2}(g,h))^\dagger \left(|\phi^0_{12}\rangle_A|\phi^0_{12}\rangle_B\langle\phi^0_{12}|_A\langle\phi^0_{12}|_B\right.\\ &+ |\Psi^+_{12}\rangle_A|\Psi^+_{12}\rangle_B\langle\Psi^+_{12}|_A\langle\Psi^+_{12}|_B + |\Psi^-_{12}\rangle_A|\Psi^-_{12}\rangle_B\langle\Psi^-_{12}|_A\langle\Psi^-_{12}|_B\\ &\left.+ |\Phi^-_{12}\rangle_A|\Phi^-_{12}\rangle_B\langle\Phi^-_{12}|_A\langle\Phi^-_{12}|_B\right)(W_{A_1B_1A_2B_2}(g,h))\,d\mu(g,h), \end{aligned}$$

where $\mu(\cdot,\cdot)$ is the Haar measure on $SU(2) \times SU(2)$ and where

$$|\Phi^\pm_{12}\rangle_X = \frac{|0\rangle_{X_1}|0\rangle_{X_2} \pm |1\rangle_{X_1}|1\rangle_{X_2}}{\sqrt{2}}, \qquad |\Psi^\pm_{12}\rangle_X = \frac{|0\rangle_{X_1}|1\rangle_{X_2} \pm |1\rangle_{X_1}|0\rangle_{X_2}}{\sqrt{2}} \quad (X = A, B).$$

By remark 5, a W-invariant test T_0 is of the form

$$T_0 = w_1\left(K^+_5 + K^-_3 + K^+_1\right) + w_2\left(L^+_3 + L^-_3\right) + w_3|\phi^0_{AB}\rangle\langle\phi^0_{AB}|^{\otimes 2}.$$

By the level-zero condition, $w_3 = 1$. If $\sigma \in \mathcal{S}'$ then

$$9^{-1}\operatorname{Tr}\left(\sigma^{\otimes 2}\left(K^+_5 + K^+_1 + K^-_3\right)\right) \leqslant 6^{-1}\operatorname{Tr}\left(\sigma^{\otimes 2}(L^+_3 + L^-_3)\right) \tag{42}$$

because

$$\begin{aligned} &6^{-1}\operatorname{Tr}\left(\sigma^{\otimes 2}\left(L^+_3 + L^-_3\right)\right) - 9^{-1}\operatorname{Tr}\left(\sigma^{\otimes 2}\left(K^+_5 + K^+_1 + K^-_3\right)\right)\\ &\quad = 3^{-1}\left(x_{00} - \frac{x_{11} + x_{22} + x_{33}}{3}\right)(x_{11} + x_{22} + x_{33}). \end{aligned}$$

As theorem 4, the type 2 error probability is uniformly minimized if $3w_1 + 2w_2$ and w_2 are simultaneously minimized (see lemma 5). From (13), we have

$$\min\{9w_1 + 6w_2 \mid AB\text{-locality}\} = 3.$$

Therefore $w_1 = 1/3$ and $w_2 = w_4 = 0$ are the solutions to the minimization problem, and the theorem is derived. □

7. Discretization of measurements

We have expressed T^u and T^V as probabilistic mixtures of continuously many separable operators labelled by $SU(2)$-elements. Such continuous expressions are simple and convenient in a theoretical argument. A basic method to realize a SU-invariant measurement is to operate the system as for an unitary element randomly chosen with respect to the Haar measure. However, in this method, we need to prepare continuously many operations. Therefore, it is worth noting that T^u and T^V are also expressed as mixtures of a few operators locally realized.

7.1. Discretization of T^u

We rewrite T as

$$\begin{aligned}T_0^u &= \tfrac{2}{3}(|0_A0_B\rangle\langle 0_A0_B| + |1_A1_B\rangle\langle 1_A1_B|)\\ &\quad + \tfrac{1}{3}(|0_A1_B\rangle\langle 0_A1_B| + |1_A0_B\rangle\langle 1_A0_B| + |0_A1_B\rangle\langle 1_A0_B| + |1_A0_B\rangle\langle 0_A1_B|)\\ &= 3^{-1}\big(|0_A0_B\rangle\langle 0_A0_B| + |1_A1_B\rangle\langle 1_A1_B| + |D_AD_B\rangle\langle D_AD_B|\\ &\quad + |X_AX_B\rangle\langle X_AX_B| + |R_AL_B\rangle\langle R_AL_B| + |L_AR_B\rangle\langle L_AR_B|\big),\end{aligned}$$

where

$$|D\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |X\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$
$$|R\rangle = \frac{|0\rangle + \sqrt{-1}|1\rangle}{\sqrt{2}}, \qquad |L\rangle = \frac{|0\rangle - \sqrt{-1}|1\rangle}{\sqrt{2}}.$$

This means that one can realize T^u by the two-values POVM $T = \{T_0, T_1\}$ given in the form

$$T_0 = |x_Ax_B\rangle\langle x_Ax_B| + |y_Ay_B\rangle\langle y_Ay_B|,$$

where the orthonormal pair (x, y) is chosen from $\{(0, 1), (D, X), (R, L)\}$ completely at random.

We also note that a finite subgroup $\mathbb{O}$ of $SU(2)$ generated by

$$\begin{pmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix} \text{ and } \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$$

transitively acts on $\{|x_Ax_B\rangle \mid x = 0, 1, D, X, R, L\}$ by $U_{AB}(\cdot)$. $\mathbb{O}$ is the octahedral group, which is the (special) symmetry group of the octahedron and the cube. Therefore, one can also realize T^u by

$$T_0 = |0_A0_B\rangle\langle 0_A0_B| + |1_A1_B\rangle\langle 1_A1_B|$$

after a transformation $U_{AB}(g)$ for randomly selected $g \in \mathbb{O}$.

Remark 7. D'Ariano *et al* [5] have proposed a discretization of an entanglement witness: the same measurement as T^u. Their discretized measurement is also equivalent to ours. However, their analysis is not enough in the sense of hypothesis testing.

7.2. Discretization of T^V

The test T^V is also expressed as a mixture of finite measurements as follows:

$$T_0^V = \frac{1}{24}\sum_{g\in\mathbb{O}}(V_{A_1B_1A_2B_2}(h^*g))^\dagger\left(\sum_{0\leqslant i,j\leqslant 1}\frac{\Pi_{ij} + \tau_{12}(\Pi_{ij})}{2}\right)V_{A_1B_1A_2B_2}(h^*g), \tag{43}$$

where $h^* \in SU(2)$ is defined by

$$h^* : \cos\left(\frac{\arccos\sqrt{3/5}}{4}\right)|0\rangle + \sin\left(\frac{\arccos\sqrt{3/5}}{4}\right)|1\rangle \mapsto |0\rangle$$

and where $\tau_{12}(\cdot)$ is the transposition of $A_1 \otimes B_1$ and $A_2 \otimes B_2$. Therefore, one can realize T^V as follows. First, transform by $V_{A_1B_1A_2B_2}(h^*g)$ where $g \in \mathbb{O}$ is chosen completely at random. Next, by probability $1/2$, replace the sample numbering, that is, apply τ_{12}. Next, measure the subsystems by

A_1	B_1	A_2	B_2
$\{\|0\rangle, \|1\rangle\}$	$\{\|0\rangle, \|1\rangle\}$	$\{\|D\rangle, \|X\rangle\}$	$\{\|D\rangle, \|X\rangle\}$

independently. The hypothesis H_0 is accepted if A_1 and B_1 have the same measurement result and A_2 and B_2 have the same one.

One can check (43) as follows. The subspaces $K_3^{\pm}$, K_2^{+}, K_1^{+}, L_1^{+} and $L_3^{\pm}$ are irreducible by the V-restriction $\mathbb{O} \subset SU(2)$, and, in particular, the three-dimensional actions of $\mathbb{O}$ for K_3^{+} and L_3^{+} are mutually inequivalent. and, by calculation,

$$\mathrm{Tr}\big(K_3^{+}V_{A_1B_1A_2B_2}(h_x)^{\dagger}\Pi_{ij}V_{A_1B_1A_2B_2}(h_x)\big) = \frac{\cos^2(4x)}{8}, \tag{44}$$

$$\mathrm{Tr}\big(K_2^{+}V_{A_1B_1A_2B_2}(h_x)^{\dagger}\Pi_{ij}V_{A_1B_1A_2B_2}(h_x)\big) = \frac{\sin^2(4x)}{8}, \tag{45}$$

where

$$SU(2) \ni h_x : \cos x|0\rangle + \sin x|1\rangle \mapsto |0\rangle,$$

and hence (44) = (45) if $x = (\arccos\sqrt{3/5})/4$.

8. Discussion and conclusion

For $d = n = 2$, we have proposed five measurements T^G, $T^{u,2}$, T^U, T^V and T^W as optimal tests (for subsets of states, if necessary,) in the corresponding classes of tests, that is,

$\mathcal{T}^G$: the class of level-zero tests,
$\mathcal{T}^{u,2}$: the class of level-zero tests of the form $T_0^{\otimes 2}$ where T_0 is AB-local U-invariant for each sample,
$\mathcal{T}^U$: the class of AB-local U-invariant level-zero tests,
$\mathcal{T}^V$: the class of AB-local, samplewise local, V-invariant, weakly AB-invariant, termwise AB-covariant and level-zero tests,
$\mathcal{T}^W$: the class of AB-local W-invariant tests.

The inclusion relations of these classes are not totally ordered. For example, from the locality,

$$\mathcal{T}^{u,2}, \qquad \mathcal{T}^V \subset \mathcal{T}^U, \qquad \mathcal{T}^W \subset \mathcal{T}^G$$

while from the unitary invariance,

$$\mathcal{T}^U \subset \mathcal{T}^{u,2}, \qquad \mathcal{T}^W \subset \mathcal{T}^V \subset \mathcal{T}^G.$$

On the other hand, the type 2 error probabilities of the optimal tests are totally ordered:

$$\beta(\sigma^{\otimes 2}, T^G) < \beta(\sigma^{\otimes 2}, T^W) < \beta(\sigma^{\otimes 2}, T^U) < \beta(\sigma^{\otimes 2}, T^V) < \beta(\sigma^{\otimes 2}, T^{u,2})$$

in a set of states close to $|\phi_{AB}^0\rangle$. In figure 1, the type 2 error probabilities β are plotted with respect to $\theta = x_{00} = \langle\phi_{AB}^0|\sigma|\phi_{AB}^0\rangle$ of $T^{u,2}$ (the highest solid line), T^U (the second highest solid

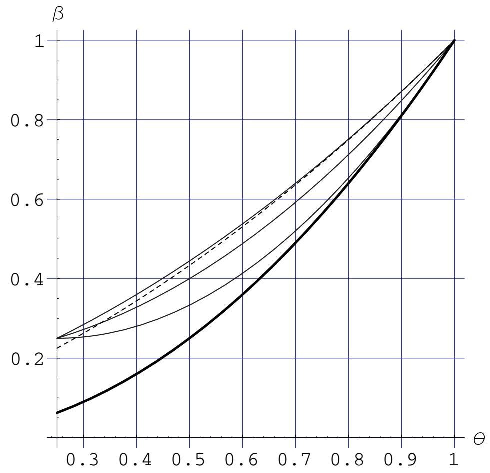

Figure 1. The type 2 error probabilities β with respect to $\theta = x_{00} = \langle\phi^0_{AB}|\sigma|\phi^0_{AB}\rangle$ of $T^{u,2}$ (the highest solid line), T^U (the second highest solid line), T^W (the third highest solid line), T^G (the thick line) and T^V (the dashed line) where x_{ij} are the same for $1 \leqslant i, j \leqslant 3$.

line), T^W (the third highest solid line), T^G (the thick line) and T^V (the dashed line) where x_{ij} are the same for $1 \leqslant i, j \leqslant 3$. If $x_{ij} = 0$ for $i \neq j$, then the line of T^V coincides with that of T^U and there is no change for other tests. In such a way, the framework of hypothesis testing clarifies the hierarchy of requirements for measurements from the viewpoint of performance of optimal tests.

We have considered hypothesis testing for entanglement under locality and invariance conditions. We have derived optimal tests for some settings. In our derivations of UMP tests, the separability of LOCC measurements played an important role. The UMP U-invariant and level-zero test T^U were shown to have the asymptotically same performance as T^G. The PPT approach of Virmani and Plenio [27] was also useful to obtain UMP tests.

We may have some problems remained. One problem is how we can develop our results for general level α $(0 < \alpha < 1)$, sample size n and dimension d. Another is what test is an appropriate test for

$$H_0 : \theta \geqslant c_0 \text{ versus } H_1 : \theta < c_0, \qquad H_0 : \theta \leqslant c_0 \text{ versus } H_1 : \theta > c_0 \tag{46}$$

for a constant c_0 very close to one. Indeed, if H_0 of (46) is rejected by a test with small level, then the statement 'The state is very close to $|\phi^0_{AB}\rangle$' will be strongly supported. Hence, it is significant to treat the hypothesis of the form (46). This problem will be treated in a forthcoming paper [12]. It is also a problem remained to remove technical assumptions such as (32) in section 5.2.

Acknowledgment

The authors thank the referees for useful comments.

Appendix. Lemmas for theorems 4, 5

Lemma 1 (For theorem 4)**.** *If $1 - \theta$ is small enough, then the power of the test in theorem 4 is uniformly maximized if (34) is simultaneously maximized.*

Proof. Since $K_i^{\pm}$ is spanned by x_{ij} and $L_i^{\pm}$ is spanned by $x_{i,0}$ and $x_{0,j}$ for $1 \leqslant i, j \leqslant 3$, it holds that

$$\mathrm{Tr}\big(\sigma^{\otimes 2} K_i^{+}\big) = O((1-\theta)^2) \qquad \text{and} \quad \mathrm{Tr}\big(\sigma^{\otimes 2} L_i^{+}\big) = O(1-\theta) \tag{A.1}$$

as $\theta \to 1-0$, except for L_1^{+}. By (23) and (24),

$$\begin{aligned}\mathrm{Tr}\big(\sigma^{\otimes 2}\big(3K_5^{+} - 5K_3^{-}\big)\big) &= (x_{11}-x_{22})^2 + (x_{22}-x_{33})^2 + (x_{33}-x_{11})^2 \\ &\quad + 4(\mathrm{Im}\, x_{12})^2 + 4(\mathrm{Im}\, x_{23})^2 + 4(\mathrm{Im}\, x_{31})^2 + 6(|x_{12}|^2 + |x_{23}|^2 + |x_{31}|^2) \\ &\geqslant 0.\end{aligned} \tag{A.2}$$

Define column vectors v and w by

$$v = \big(\mathrm{Tr}\big(\sigma^{\otimes 2} K_5^{+}\big) \quad \mathrm{Tr}\big(\sigma^{\otimes 2} L_3^{+}\big) \quad \mathrm{Tr}\big(\sigma^{\otimes 2} K_1^{+}\big) \quad \mathrm{Tr}\big(\sigma^{\otimes 2} K_3^{-}\big) \quad \mathrm{Tr}\big(\sigma^{\otimes 2} L_3^{-}\big)\big)^T,$$
$$w = (w_1 \quad w_2 \quad w_3 \quad w_4 \quad w_5)^T,$$

and define a 5×5 matrix M by

$$M = \frac{1}{15}\begin{pmatrix} 3 & -9 & 0 & 0 & 0 \\ 0 & 15 & 0 & 0 & 0 \\ 0 & 0 & 15 & 0 & 0 \\ -5 & 0 & -5 & 5 & -15 \\ 0 & 0 & 0 & 0 & 15 \end{pmatrix} \quad \text{as the inverse of} \quad \begin{pmatrix} 5 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 5 & 3 & 1 & 3 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $v' = M^T \cdot v$ and $w' = M^{-1} \cdot w$. Each quantity in (34) is an entry of w', and the power of the test in theorem 4 is given as $v^T \cdot w = v'^T \cdot w'$. When each entry of v' is non-negative, the maximum of $v'^T \cdot w'$ is attained by maximizing w'. From (33), (A.1) and (A.2), there is θ_0 such that v' is non-negative. Therefore, if (34) is maximized, then the power of the test is maximized. □

Let $\mathrm{pt}_C(X)$ be the partial transpose of an operator X on a subsystem C, for example, $\mathrm{pt}_{A_1 \otimes B_1}(X)$ is given by

$$\mathrm{pt}_{A_2 B_2}(X) = \sum_{0 \leqslant i,j,k,l \leqslant 1} I_{A_1 B_1} \otimes |i\rangle_{A_2} |j\rangle_{B_2} \langle k|_{A_2} \langle l|_{B_2} X I_{A_1 B_1} \otimes |i\rangle_{A_2} |j\rangle_{B_2} \langle k|_{A_2} \langle l|_{B_2},$$

where $I_{A_2 B_2}$ is the identity on $A_2 \otimes B_2$.

Lemma 2 (For theorem 4)**.** *If* $T = \{T_0, T_1\}$ *is samplewise-local then* $w_2 = w_5$.

Proof. The samplewise-locality of T implies that $\mathrm{pt}_{A_2 \otimes B_2}(T_1)$ is positive, in particular,

$$R = \begin{pmatrix} \langle u|\mathrm{pt}_{A_2\otimes B_2}(T_1)|u\rangle & \langle u|\mathrm{pt}_{A_2\otimes B_2}(T_1)|v\rangle \\ \langle v|\mathrm{pt}_{A_2\otimes B_2}(T_1)|u\rangle & \langle v|\mathrm{pt}_{A_2\otimes B_2}(T_1)|v\rangle \end{pmatrix} = \begin{pmatrix} 0 & -\frac{5\sqrt{-1}}{6\sqrt{3}}(w_2 - w_5) \\ \frac{5\sqrt{-1}}{6\sqrt{3}}(w_2 - w_5) & \frac{17w_1 + 9w_3 + w_4}{27} \end{pmatrix}$$

should be positive where

$$|u\rangle = \big|\phi_{AB}^0\big\rangle_1 \big|\phi_{AB}^0\big\rangle_2, \qquad |v\rangle = \frac{5\big|\phi_{AB}^1\big\rangle_1\big|\phi_{AB}^1\big\rangle_2 - \big|\phi_{AB}^2\big\rangle_1\big|\phi_{AB}^2\big\rangle_2 - \big|\phi_{AB}^3\big\rangle_1\big|\phi_{AB}^3\big\rangle_2}{3\sqrt{3}}.$$

Since $\det(R) = -25/108(w_2 - w_5)^2 \geqslant 0$ holds, $w_2 = w_5$. □

Lemma 3 (For theorem 4)**.** *If* $T = \{T_0, T_1\}$ *is* AB*-local then*

$$0 \leqslant \frac{10w_1 + 6w_2 - w_3}{12} \leqslant 1, \tag{A.3}$$

$$0 \leqslant \frac{w_3 + 2(w_4 + w_5)}{4} \leqslant 1. \tag{A.4}$$

Proof. The AB-locality of T implies that $\mathrm{pt}_{B_1 \otimes B_2}(T_0) = \mathrm{pt}_{B_1 \otimes B_2}(I - T_1)$ is positive. The first result (A.3) is obtained since

$$\frac{1}{2}\big(\langle 0_{A_1} 1_{B_1} 0_{A_2} 1_{B_2}| - \langle 1_{A_1} 0_{B_1} 1_{A_2} 0_{B_2}|\big)\mathrm{pt}_{B_1 \otimes B_2}(T_1)\big(|0_{A_1} 1_{B_1} 0_{A_2} 1_{B_2}\rangle - |1_{A_1} 0_{B_1} 1_{A_2} 0_{B_2}\rangle\big)$$
$$= \frac{10 w_1 + 6 w_2 - w_3}{12}.$$

The second result (A.4) is obtained since

$$\frac{1}{2}\big(\langle 0_{A_1} 0_{B_1} 0_{A_2} 0_{B_2}| - \langle 1_{A_1} 1_{B_1} 1_{A_2} 1_{B_2}|\big)\mathrm{pt}_{B_1 \otimes B_2}(T_1)\big(|0_{A_1} 0_{B_1} 0_{A_2} 0_{B_2}\rangle - |1_{A_1} 1_{B_1} 1_{A_2} 1_{B_2}\rangle\big)$$
$$= \frac{w_3 + 2(w_4 + w_5)}{4}.$$

□

Lemma 4 (For theorem 4)**.** *If $T = \{T_0, T_1\}$ is AB-local and samplewise local then*

$$\tfrac{3}{4}(w_2 + w_5) \leqslant 1.$$

Proof. The AB-locality and samplewise locality of T implies that $\mathrm{pt}_{B_2}(T_0) = \mathrm{pt}_{B_2}(I - T_1)$ is positive. Since

$$\langle \phi^0_{AB}|_1 \langle \phi^2_{AB}|_2 \mathrm{pt}_{B_2}(T_1) |\phi^0_{AB}\rangle_1 |\phi^2_{AB}\rangle_2 = \tfrac{3}{4}(w_2 + w_5),$$

we have the result. □

Lemma 5 (For theorem 5)**.** *In theorem 5, the type 2 error probability of the test is uniformly minimized if $3w_1 + 2w_2$ and w_2 are simultaneously minimized.*

Proof. Define column vectors v and w by

$$v = \big(\mathrm{Tr}\big(\sigma^{\otimes 2}\big(K_5^+ + K_1^+ + K_3^-\big)\big) \quad \mathrm{Tr}\big(\sigma^{\otimes 2}\big(L_3^+ + L_3^-\big)\big)\big)^T,$$
$$w = (w_1 \quad w_2)^T,$$

and define a 2×2 matrix M by

$$M = \frac{1}{3}\begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix} \quad \text{as the inverse of} \quad \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}.$$

Let $v' = M^T \cdot v$ and $w' = M^{-1} \cdot w$. The power of the test in theorem 5 is given as $v^T \cdot w = v'^T \cdot w'$. If each entry of v' is non-negative, the maximum of $v'^T \cdot w'$ is attained by maximizing w'. From (42), v' is non-negative. Therefore, if $3w_1 + 2w_2$ and w_2 are simultaneously minimized, the type 2 error probability is minimized. □

References

[1] Barbieri M, De Martini F, Di Nepi G, Mataloni P, D'Ariano G M and Macchiavello C 2003 *Phys. Rev. Lett.* **91** 227901
[2] Bennett C, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[3] Bennett C and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[4] Brown L D, Hwang J. T. G and Munk A 1997 *Ann. Stat.* **25** 2345–67
[5] D'Ariano G M, Macchiavello C and Paris M G A 2003 *Phys. Rev.* A **67** 042310
[6] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[7] Fulton W and Harris J 1991 *Representation Theory: A First Course* (New York: Springer)

[8] Goodman R and Wallach N R 1998 *Representations and Invariants of the Classical Groups* (Cambridge: Cambridge University Press)
[9] Gühne O, Hyllus P, Brus D, Ekert A, Lewenstein M, Macchiavello C and Sanpera A 2002 *Phys. Rev.* A **66** 062305
[10] Hayashi M 2002 *J. Phys. A: Math. Gen.* **35** 10759–73
[11] Hayashi M 2005 *Asymptotic Theory of Quantum Statistical Inference: Selected Papers* (Singapore: World Scientific)
[12] Hayashi M in preparation
[13] Hayashi M 2006 *Quantum Information: An Introduction* (Berlin: Springer)
[14] Hayashi M, Markham D, Murao M, Owari M and Virmani S 2006 *Phys. Rev. Lett.* **96** 040501
[15] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)
[16] Hiai F and Petz D 1991 *Commun. Math. Phys.* **143** 99–114
[17] Holevo A S 1982 *Probabilistic and Statistical Aspects of Quantum Theory* (Amsterdam: North-Holland)
[18] Horodecki M, Horodecki P and Horodecki R 1996 *Phys. Lett.* A **223** 1
[19] Lehmann E L 1986 *Testing Statistical Hypotheses* 2nd edn (New York: Wiley)
[20] Lewenstein M, Kraus B, Cirac J I and Horodecki P 2000 *Phys. Rev.* A **62** 052310
[21] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[22] Rains E M 1999 *Phys. Rev.* A **60** 173
[23] Rains E M 2001 *IEEE Trans. Inf. Theory* **47** 2921
[24] Terhal B M 2000 *Phys. Lett.* A **271** 319
[25] Ogawa T and Nagaoka H 2000 *IEEE Trans. Inf. Theory* **46** 2428–33
[26] Owari M and Hayashi M 2006 *Phys. Rev.* A **74** 032108
[27] Virmani S and Plenio M B 2003 *Phys. Rev.* A **67** 062308