Rapid Communications Editors' Suggestion

Perfect discrimination of nonorthogonal quantum states with posterior classical partial information

Seiseki Akibue,[*] Go Kato,[†] and Naoki Marumo[‡]

NTT Communication Science Laboratories, NTT Corporation 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa 243-0124, Japan

(Received 25 November 2018; published 8 February 2019)

The indistinguishability of nonorthogonal pure states lies at the heart of quantum information processing. Although the indistinguishability reflects the impossibility of measuring complementary physical quantities by a single measurement, we demonstrate that the distinguishability can be perfectly retrieved simply with the help of posterior classical partial information. We demonstrate this by showing an ensemble of nonorthogonal pure states such that a state randomly sampled from the ensemble can be perfectly identified by a single measurement with the help of postprocessing of the measurement outcomes and additional partial information about the sampled state, i.e., the label of the subensemble from which the state is sampled. When an ensemble consists of two subensembles, we show that the perfect distinguishability of the ensemble with the help of postprocessing can be restated as a matrix-decomposition problem. Furthermore, we give the analytical solution for the problem when both subensembles consist of two states.

DOI: 10.1103/PhysRevA.99.020102

I. INTRODUCTION

The existence of nonorthogonal pure states is a peculiar feature of quantum mechanics. Indeed, an ensemble of them is neither perfectly cloned [1,2] nor perfectly distinguishable [3–7]. This is in contrast to classical theories, which assume that any ensemble of distinct pure states, each of which is not a probabilistic mixture of different states, is perfectly distinguishable in principle. While the nonorthogonality of pure states has its origin purely in quantum mechanics, we investigate its classical aspect in this Rapid Communication.

From a practical point of view, the indistinguishability of nonorthogonal pure states restricts our ability to transmit information [8]; conversely, it enables extremely secure designs of banknotes [9] and secret key distribution [10]. For example, in the quantum key distribution (QKD) protocol proposed in Ref. [10], a secret bit is encoded in a basis randomly chosen from two complementary bases, $\mathbb{S}^{(A)} = (|0\rangle, |1\rangle)$ and $\mathbb{S}^{(B)} = (|+\rangle, |-\rangle)$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. An eavesdropper cannot intercept the secret bit perfectly if she does not know which basis is used since a state in $\mathbb{S}^{(A)}$ and that in $\mathbb{S}^{(B)}$ are nonorthogonal. Moreover, even if she is informed of the label of the chosen basis, $X \in \{A, B\}$, after the quantum state encoding the secret bit is destroyed by her measurement, she cannot intercept the secret bit perfectly owing to the complementarity of measurement: The accurate measurement of one physical quantity entails an inaccurate measurement of another complementary quantity (see Fig. 1). Thus, it seems that a state randomly sampled from nonorthogonal pure states cannot be identified perfectly even if classical partial information about the sampled state is available after measurement of the state is performed.

Contrary to such an intuition, in this Rapid Communication, we show that such classical partial information is sometimes sufficient for accomplishing perfect discrimination of nonorthogonal pure states. Suppose that a state is randomly sampled from an ensemble of pure states $\mathbb{S}$ consisting of two *a priori* known subensembles $\mathbb{S}^{(A)}$ and $\mathbb{S}^{(B)}$. First, we give an example of a pair of subensembles $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ such that $\mathbb{S}$ is an ensemble of nonorthogonal pure states but the sampled state can be perfectly identified by the classical postprocessing of the measurement outcomes with the label of the subensemble, $X \in \{A, B\}$, from which the state is sampled. Second, we investigate a standard pair $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$, which is trivially distinguishable by postprocessing. Third, we give the necessary conditions for $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ to be perfectly distinguishable by postprocessing. The conditions imply that the first example we gave can be considered as a maximally nonorthogonal distinguishable pair in the smallest Hilbert space. Finally, we show that the perfect distinguishability with the help of postprocessing can be restated as a matrix-decomposition problem, and also give the analytical solution for the problem when $|\mathbb{S}^{(A)}| = |\mathbb{S}^{(B)}| = 2$. The result also implies that every perfectly distinguishable pair with the help of postprocessing can be embedded in a larger Hilbert space as a standard pair.

Note that the state discrimination with the help of postprocessing has been investigated in Refs. [11–13], motivated by the analysis of quantum cryptographic protocols. In Refs. [11,12], the optimal discrimination of basis states (or their probabilistic mixtures) was investigated, where perfect discrimination is impossible in general. In Ref. [13], further investigations concerning the optimal measurement for imperfect state discrimination were done. In contrast, we focus on the perfect discrimination of general pure states in this Rapid Communication.

II. DEFINITIONS

We consider a quantum system represented by finite-dimensional Hilbert space $\mathcal{H}$. The two *a priori* known

[*] seiseki.akibue.rb@hco.ntt.co.jp

[†] go.kato.gm@hco.ntt.co.jp

[‡] naoki.marumo.ec@hco.ntt.co.jp

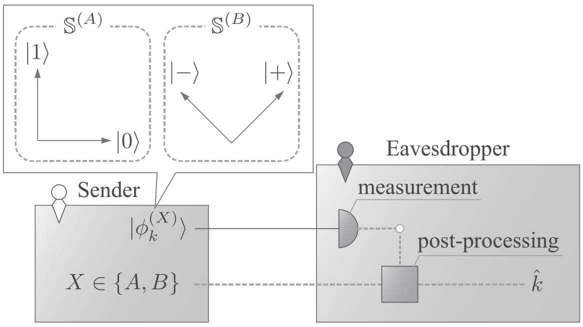

FIG. 1. Indistinguishability of nonorthogonal pure states in a QKD-like protocol. First, the sender randomly chooses label $X \in \{A, B\}$ and encodes his secret bit in a basis state of $\mathbb{S}^{(X)}$. Second, the eavesdropper intercepts the state transmitted from the sender and measures it. She cannot identify the transmitted state perfectly even if she can process her measurement outcomes with label X.

ensembles of distinguishable pure states are described by indexed sets of orthonormal vectors, $\mathbb{S}^{(X)} = (|\phi_k^{(X)}\rangle \in \mathcal{H})_{k\in\mathbb{K}^{(X)}}$ $(X \in \{A, B\})$, where $\mathbb{K}^{(X)} = \{0, 1, \dots, |\mathbb{S}^{(X)}| - 1\}$ for $X \in \{A, B\}$. We suppose that the state of $\mathcal{H}$ is randomly sampled from ensemble $\mathbb{S}$ consisting of $\mathbb{S}^{(A)}$ and $\mathbb{S}^{(B)}$.

The measurement performed on $\mathcal{H}$ is described by a positive-operator-valued measure (POVM) over a finite set Ω [3], $(M_\omega \in P(\mathcal{H}))_{\omega\in\Omega}$, such that $\sum_{\omega\in\Omega} M_\omega = I$, where $P(\mathcal{H})$ and I represent the set of positive semidefinite operators and the identity operator on $\mathcal{H}$, respectively. After the measurement, the label of the subensemble, $X \in \{A, B\}$, from which the state is sampled is received, and one processes the measurement outcome ω and X to guess k as $\hat{k} = f^{(X)}(\omega)$, where $f^{(X)} : \Omega \to \mathbb{K}^{(X)}$ for $X \in \{A, B\}$.

Thus, the pair $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing if and only if there exist POVM $(M_\omega)_{\omega\in\Omega}$ and postprocessing $(f^{(X)})_{X\in\{A,B\}}$ such that

$$\forall X \in \{A, B\},\ \forall k \in \mathbb{K}^{(X)},\ \sum_{\omega\in f^{(X)-1}(k)} \langle\phi_k^{(X)}|M_\omega|\phi_k^{(X)}\rangle = 1. \quad (1)$$

Note that a more general postprocessing including probabilistic processing does not change the condition for perfect distinguishability [11–13].

III. MEASUREMENT TABLE

If $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing, we can construct a measurement table representing the POVM and classical postprocessing. The measurement table is POVM over $\mathbb{K} := \mathbb{K}^{(A)} \times \mathbb{K}^{(B)}$, $(M_{ab})_{(a,b)\in\mathbb{K}}$ such that

$$M_{ab} = \sum_{\omega\in\mathbf{f}^{-1}((a,b))} M_\omega, \quad (2)$$

where $\mathbf{f}(\omega) = (f^{(A)}(\omega), f^{(B)}(\omega))$. We can verify that $(M_{ab})_{(a,b)\in\mathbb{K}}$ is a valid POVM, i.e., it is an indexed set of positive semidefinite operators and the sum of the elements is the identity operator. Equation (1) implies that

$$\left(\forall a \in \mathbb{K}^{(A)},\ \sum_{b\in\mathbb{K}^{(B)}} \langle\phi_a^{(A)}|M_{ab}|\phi_a^{(A)}\rangle = 1\right)$$
$$\wedge\left(\forall b \in \mathbb{K}^{(B)},\ \sum_{a\in\mathbb{K}^{(A)}} \langle\phi_b^{(B)}|M_{ab}|\phi_b^{(B)}\rangle = 1\right), \quad (3)$$

or equivalently,

$$\left[\forall\{a, a'|a \neq a'\} \subseteq \mathbb{K}^{(A)}, \forall b \in \mathbb{K}^{(B)}, |\phi_{a'}^{(A)}\rangle \in \ker(M_{ab})\right]$$
$$\wedge\left[\forall\{b, b'|b \neq b'\} \subseteq \mathbb{K}^{(B)}, \forall a \in \mathbb{K}^{(A)}, |\phi_{b'}^{(B)}\rangle \in \ker(M_{ab})\right]. \quad (4)$$

TABLE I. Measurement table to distinguish $\mathbb{S}^{(A)} = (|0+1\rangle, |0-1\rangle)$ and $\mathbb{S}^{(B)} = (|0+2\rangle, |0-2\rangle)$, where $|0+1+2\rangle$ represents the normalized state $\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$. We can easily check that (M_{ab}) is a valid POVM and satisfies Eq. (4).

	$\lvert 0+2\rangle$	$\lvert 0-2\rangle$
$\lvert 0+1\rangle$	$M_{00} = \left[\frac{\sqrt{3}}{2}\lvert 0+1+2\rangle\right]$	$M_{01} = \left[\frac{\sqrt{3}}{2}\lvert 0+1-2\rangle\right]$
$\lvert 0-1\rangle$	$M_{10} = \left[\frac{\sqrt{3}}{2}\lvert 0-1+2\rangle\right]$	$M_{11} = \left[\frac{\sqrt{3}}{2}\lvert 0-1-2\rangle\right]$

Conversely, if there exists a measurement table satisfying Eqs. (3) or (4) for $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$, it is perfectly distinguishable by postprocessing. We give an example of a measurement table which perfectly distinguishes an ensemble of nonorthogonal pure states in Table I, where we use the notation $[|\psi\rangle] = [\psi] := |\psi\rangle\langle\psi|$.

IV. STANDARD PAIR

We define a standard pair, $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)}) = ((|\Phi_a^{(A)}\rangle)_{a\in\mathbb{K}^{(A)}}, (|\Phi_b^{(B)}\rangle)_{b\in\mathbb{K}^{(B)}})$, which is trivially distinguishable by postprocessing as follows.

Definition 1. For $\mathbb{S} \subseteq \mathcal{Y}$, where $\mathcal{Y} = \mathbb{C}^{|\mathbb{K}|}$ is a Hilbert space spanned by the orthonormal basis $\{|ab\rangle\}_{(a,b)\in\mathbb{K}}$, $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is called a standard pair if their elements are represented by

$$|\Phi_a^{(A)}\rangle = \sum_b \alpha_{ab}|ab\rangle \wedge |\Phi_b^{(B)}\rangle = \sum_a \beta_{ab}|ab\rangle, \quad (5)$$

where $\sum_b |\alpha_{ab}|^2 = 1$ and $\sum_a |\beta_{ab}|^2 = 1$.

We can easily verify that the standard pair is perfectly distinguishable by the measurement table $(M_{ab} = |ab\rangle\langle ab|)$. In addition to the standard pair, we can verify that if $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ can be embedded in a larger Hilbert space as a standard pair, it is also perfectly distinguishable by postprocessing, as stated in the following proposition.

Proposition 1. Let the reduced Hilbert space of $\mathcal{H}$ be $\mathcal{X} := \mathrm{span}(\mathbb{S})$. If there exists isometry $V : \mathcal{X} \to \mathcal{Y}$ such that $((V|\phi_a^{(A)}\rangle), (V|\phi_b^{(B)}\rangle))$ is a standard pair, $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing.

Note that if $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by the measurement table (M_{ab}) consisting of rank-r operators with $r \leqslant 1$, it can always be embedded in a larger Hilbert space as a standard pair by using Naimark's extension as follows: Let $M_{ab} = |\tilde{\psi}_{ab}\rangle\langle\tilde{\psi}_{ab}|$, where $|\tilde{\psi}_{ab}\rangle \in \mathcal{H}$ is an unnor-

TABLE II. Corresponding standard pair $((V|\phi_a^{(A)}\rangle), (V|\phi_b^{(B)}\rangle))$ of $((|\phi_a^{(A)}\rangle), (|\phi_b^{(B)}\rangle))$ defined in Table I, where $V = \sum_{a,b} |ab\rangle\langle\tilde{\psi}_{ab}|$, $|\tilde{\psi}_{00}\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle)$, $|\tilde{\psi}_{01}\rangle = \frac{1}{2}(|0\rangle + |1\rangle - |2\rangle)$, $|\tilde{\psi}_{10}\rangle = \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle)$, and $|\tilde{\psi}_{11}\rangle = \frac{1}{2}(|0\rangle - |1\rangle - |2\rangle)$. A measurement table distinguishing the standard pair is also shown in the table.

	$\|+0\rangle$	$\|+1\rangle$
$\|0+\rangle$	$\|00\rangle\langle 00\|$	$\|01\rangle\langle 01\|$
$\|1+\rangle$	$\|10\rangle\langle 10\|$	$\|11\rangle\langle 11\|$

malized state. Define isometry $V = \sum_{(a,b)\in\mathbb{K}} |ab\rangle\langle\tilde{\psi}_{ab}|$. Then $((V|\phi_a^{(A)}\rangle), (V|\phi_b^{(B)}\rangle))$ is a standard pair. We give an example of the corresponding extension of Table I in Table II.

In general, we cannot assume that a measurement table consists of rank-r operators with $r \leqslant 1$. For example, it is not obvious whether the perfectly distinguishable pair given in Table III can be embedded in a larger Hilbert space as a standard pair. However, in Sec. VI, we show that every perfectly distinguishable pair can be embedded as a standard pair.

V. NECESSARY CONDITIONS

We show two propositions regarding the necessary conditions for perfect distinguishability with the help of postprocessing. Since $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ given in Table I saturates both conditions, it can be considered as a maximally nonorthogonal pair in the smallest Hilbert space.

Proposition 2. If $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing and any pair of a state in $\mathbb{S}^{(A)}$ and a state in $\mathbb{S}^{(B)}$ is nonorthogonal, the dimension of $\mathcal{H}$ must satisfy $\dim\mathcal{H} \geqslant |\mathbb{S}^{(A)}| + |\mathbb{S}^{(B)}| - 1$.

Proof. If either $|\mathbb{S}^{(A)}|$ or $|\mathbb{S}^{(B)}|$ is 1, the statement is trivial. Thus, we assume $|\mathbb{S}^{(A)}| \geqslant 2$ and $|\mathbb{S}^{(B)}| \geqslant 2$.

It is enough to show that for any perfectly distinguishable $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$, the following two conditions cannot be satisfied simultaneously:

1. $\forall a \in \mathbb{K}^{(A)}, \forall c \in \{0,1\}, \langle\phi_a^{(A)}|\phi_c^{(B)}\rangle \neq 0$,
2. $\forall c \in \{0,1\}, |\phi_c^{(B)}\rangle \in \mathrm{span}(\mathbb{S}^{(A)} \cup \mathbb{S}^{(B)c})$, where $\mathbb{S}^{(B)c} = \mathbb{S}^{(B)} \setminus (|\phi_0^{(B)}\rangle, |\phi_1^{(B)}\rangle)$.

If $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable, we can find a measurement table (M_{ab}). If the second condition is satisfied, we can find the following decompositions:

$$\big|\phi_c^{(B)}\big\rangle = \sum_{a\in\mathbb{K}^{(A)}} \alpha_{ac}\big|\phi_a^{(A)}\big\rangle + \sum_{b\geqslant 2} \beta_{bc}\big|\phi_b^{(B)}\big\rangle \tag{6}$$

for $c \in \{0,1\}$. Since Eq. (4) implies $M_{a,1-c}|\phi_c^{(B)}\rangle = 0$, we obtain

$$\forall a \in \mathbb{K}^{(A)},\ \forall c \in \{0,1\},\ \alpha_{ac}M_{a,1-c}\big|\phi_a^{(A)}\big\rangle = 0. \tag{7}$$

If the first condition is satisfied, since Eq. (4) guarantees $\langle\phi_a^{(A)}|M_{ac}|\phi_c^{(B)}\rangle = \langle\phi_a^{(A)}|\phi_c^{(B)}\rangle \neq 0$, we obtain

$$\forall a \in \mathbb{K}^{(A)},\ \forall c \in \{0,1\},\ \alpha_{ac}M_{ac}\big|\phi_a^{(A)}\big\rangle \neq 0, \tag{8}$$

which leads us to a contradiction. ■

TABLE III. Measurement table to distinguish $\mathbb{S}^{(A)} = (|1+2\rangle, |3+4\rangle)$ and $\mathbb{S}^{(B)} = (|0+3\rangle, |2+4\rangle)$.

	$\|0+3\rangle$	$\|2+4\rangle$
$\|1+2\rangle$	$\|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|2\rangle\langle 2\|$
$\|3+4\rangle$	$\|3\rangle\langle 3\|$	$\|4\rangle\langle 4\|$

This proposition shows that the retrieval of the perfect distinguishability of such nonorthogonal pure states appears only with $d(\geqslant 3)$-dimensional Hilbert space.

Proposition 3. If $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing, then $\min\{|\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle|^2\}_{(a,b)\in\mathbb{K}} \leqslant \frac{1}{|\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|}$.

Proof. Let (M_{ab}) be a measurement table distinguishing $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$. By using the Cauchy-Schwartz inequality, arithmetic mean (AM)-geometric mean (GM) inequality, Eq. (3), and Eq. (4), we can derive the following inequality:

$$\begin{aligned}\prod_{ab} \big|\big\langle\phi_a^{(A)}\big|\phi_b^{(B)}\big\rangle\big|^2 &= \prod_{ab} \big|\big\langle\phi_a^{(A)}\big|M_{ab}\big|\phi_b^{(B)}\big\rangle\big|^2\\ &\leqslant \prod_{ab} \big\langle\phi_a^{(A)}\big|M_{ab}\big|\phi_a^{(A)}\big\rangle\big\langle\phi_b^{(B)}\big|M_{ab}\big|\phi_b^{(B)}\big\rangle\\ &\leqslant \left(\sum_{ab}\frac{\big\langle\phi_a^{(A)}\big|M_{ab}\big|\phi_a^{(A)}\big\rangle}{|\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|}\right)^{|\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|}\\ &\quad\times\left(\sum_{ab}\frac{\big\langle\phi_b^{(B)}\big|M_{ab}\big|\phi_b^{(B)}\big\rangle}{|\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|}\right)^{|\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|}\\ &= |\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|^{-|\mathbb{S}^{(A)}||\mathbb{S}^{(B)}|}.\end{aligned} \tag{9}$$

This completes the proof. ■

This proposition shows that there does not exist a perfectly distinguishable pair each of whose pairwise overlap $|\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle|$ is strictly larger than the pair given in Table I.

Note that we did not assume that the perfectly distinguishable pair can be embedded as a standard pair in the proofs. This allows us to apply these propositions to a more general setting as discussed in Sec. VII.

VI. PERFECT DISTINGUISHABILITY AS A MATRIX DECOMPOSITION

We show that perfect distinguishability with the help of postprocessing can be restated as a matrix-decomposition problem, and give the analytical solution for the problem in the case of $|\mathbb{S}^{(A)}| = |\mathbb{S}^{(B)}| = 2$. This result also implies that any perfectly distinguishable pair with the help of postprocessing can be embedded in a larger Hilbert space as a standard pair (see Table IV). The main theorem uses Lemma 1 followed by two definitions about linear algebra.

Definition 2. The set of matrices that can be decomposed into the elementwise product of a right stochastic matrix and left one is defined by

$$\bar{\mathcal{D}}(n,m) := \{P \in L(\mathbb{R}^m, \mathbb{R}^n) | P = A \circ B\}, \tag{10}$$

where $\circ$ represents the elementwise product, $L(\mathbb{R}^m, \mathbb{R}^n)$ represents the set of $n \times m$ matrices, and A and B are a right stochastic matrix and a left one, respectively.

TABLE IV. Corresponding standard pair $((V|\phi_a^{(A)}\rangle), (V|\phi_b^{(B)}\rangle))$ of $((|\phi_a^{(A)}\rangle), (|\phi_b^{(B)}\rangle))$ defined in Table III, where $V = \sum_{ab} |ab\rangle\langle\psi_{ab}|$, where $|\psi_{00}\rangle = \frac{1}{2\sqrt{5}}(-|0\rangle + 4|1\rangle + |2\rangle + |3\rangle - |4\rangle)$, $|\psi_{01}\rangle = \frac{1}{2\sqrt{3}}(|0\rangle + 3|2\rangle - |3\rangle + |4\rangle)$, $|\psi_{10}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle)$, and $|\psi_{11}\rangle = \frac{1}{\sqrt{6}}(-|0\rangle + |3\rangle + 2|4\rangle)$.

	$\lvert 10\rangle$	$\left(\sqrt{\frac{2}{3}}\lvert 0\rangle + \sqrt{\frac{1}{3}}\lvert 1\rangle\right)\lvert 1\rangle$
$\lvert 0\rangle\left(\sqrt{\frac{5}{8}}\lvert 0\rangle + \sqrt{\frac{3}{8}}\lvert 1\rangle\right)$	$\lvert 00\rangle\langle 00\rvert$	$\lvert 01\rangle\langle 01\rvert$
$\lvert 1\rangle\left(\sqrt{\frac{1}{4}}\lvert 0\rangle + \sqrt{\frac{3}{4}}\lvert 1\rangle\right)$	$\lvert 10\rangle\langle 10\rvert$	$\lvert 11\rangle\langle 11\rvert$

Definition 3. The set of elementwise positive matrices in $\bar{\mathcal{D}}(n, m)$ is defined by

$$\mathcal{D}(n, m) := \{P \in \bar{\mathcal{D}}(n, m) | P > 0\}. \qquad (11)$$

Note that $\bar{\mathcal{D}}(n, m)$ is the closure of $\mathcal{D}(n, m)$, and the matrix inequalities such as $P > 0$ and $P \geqslant Q$ represent elementwise inequalities such as $P_{ij} > 0$ and $P_{ij} \geqslant Q_{ij}$ for all i and j.

Lemma 1. If $n \geqslant 2$ and $m \geqslant 2$, the following statement holds: For any $P \in \bar{\mathcal{D}}(n, m)$ and for any $Q \in L(\mathbb{R}^m, \mathbb{R}^n)$,

$$0 \leqslant Q \leqslant P \Rightarrow Q \in \bar{\mathcal{D}}(n, m). \qquad (12)$$

Proof. First, we show that it is sufficient to prove

$$\forall P \in \mathcal{D}(n, m),\ \forall Q,\ 0 < Q \leqslant P \Rightarrow Q \in \mathcal{D}(n, m). \qquad (13)$$

Assume Eq. (13) holds. Since $\bar{\mathcal{D}}(n, m)$ is the closure of $\mathcal{D}(n, m)$, for any $P \in \bar{\mathcal{D}}(n, m)$ and for any $\delta > 0$, there exists $P' \in \mathcal{D}(n, m)$ such that $|P - P'| < \delta$. For any $Q \in L(\mathbb{R}^m, \mathbb{R}^n)$ such that $0 \leqslant Q \leqslant P$, we define $Q' \in L(\mathbb{R}^m, \mathbb{R}^n)$ as

$$Q'_{ij} = \begin{cases} Q_{ij} & (0 < Q_{ij} \leqslant P'_{ij}), \\ P'_{ij} & (Q_{ij} > P'_{ij}), \\ \min\{\delta, P'_{ij}\} & (Q_{ij} = 0). \end{cases} \qquad (14)$$

Since $0 < Q' \leqslant P'$, $Q' \in \mathcal{D}(n, m)$ by using Eq. (13). Note that for any $\epsilon > 0$, there exists sufficiently small $\delta > 0$ such that $|Q - Q'| < \epsilon$. Thus, $Q \in \bar{\mathcal{D}}(n, m)$.

Second, we show that it is sufficient to prove

$$\forall P \in \mathcal{D}(2, 2),\ \forall Q,\ 0 < Q \leqslant P \Rightarrow Q \in \mathcal{D}(2, 2). \qquad (15)$$

Note that for proving Eq. (13), it is sufficient to prove for any $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$ and for any $\delta \in (0, 1]$,

$$\forall P \in \mathcal{D}(n, m),\ P \circ T_\delta^{(ij)} \in \mathcal{D}(n, m), \qquad (16)$$

where $T_\delta^{(ij)}$ is the $n \times m$ matrix, all of whose elements are 1 except for the (i, j) element, which is set to δ. Assume Eq. (15) holds. For any $P \in \mathcal{D}(n, m)$ and for any $T_\delta^{(ij)}$, pick up their arbitrary 2×2 submatrices $P[2]$ and $T_\delta^{(ij)}[2]$ containing the (i, j) element. (There exist such submatrices since we assume $n \geqslant 2$ and $m \geqslant 2$.) Letting $P = A \circ B$, the corresponding submatrices $A[2]$ and $B[2]$ satisfy $P[2] = A[2] \circ B[2]$. Define the right stochastic matrix $\tilde{A}[2]$ and left one $\tilde{B}[2]$ by

$$\tilde{A}[2] := A[2] \circ \begin{pmatrix} \frac{1}{A[2]_{1*}} & \frac{1}{A[2]_{1*}} \\ \frac{1}{A[2]_{2*}} & \frac{1}{A[2]_{2*}} \end{pmatrix}, \qquad (17)$$

$$\tilde{B}[2] := B[2] \circ \begin{pmatrix} \frac{1}{B[2]_{*1}} & \frac{1}{B[2]_{*2}} \\ \frac{1}{B[2]_{*1}} & \frac{1}{B[2]_{*2}} \end{pmatrix}, \qquad (18)$$

where $A[2]_{i*} = A[2]_{i1} + A[2]_{i2}$ and $B[2]_{*j} = B[2]_{1j} + B[2]_{2j}$. Since $0 < \tilde{A}[2] \circ \tilde{B}[2] \circ T_\delta^{(ij)}[2] \leqslant \tilde{A}[2] \circ \tilde{B}[2]$, there exists a right stochastic matrix $\tilde{A}'[2]$ and left one $\tilde{B}'[2]$ satisfying $\tilde{A}'[2] \circ \tilde{B}'[2] = \tilde{A}[2] \circ \tilde{B}[2] \circ T_\delta^{(ij)}[2]$ by using Eq. (15). Define elementwise positive 2×2 matrices $A'[2]$ and $B'[2]$ by

$$A'[2] := \tilde{A}'[2] \circ \begin{pmatrix} A[2]_{1*} & A[2]_{1*} \\ A[2]_{2*} & A[2]_{2*} \end{pmatrix}, \qquad (19)$$

$$B'[2] := \tilde{B}'[2] \circ \begin{pmatrix} B[2]_{*1} & B[2]_{*2} \\ B[2]_{*1} & B[2]_{*2} \end{pmatrix}. \qquad (20)$$

Since $A'[2] \circ B'[2] = P[2] \circ T_\delta^{(ij)}[2]$ and A (B) whose submatrix $A[2]$ ($B[2]$) is replaced by $A'[2]$ ($B'[2]$) preserves the sum of elements in each row (column), i.e., a right (left) stochastic matrix, Eq. (16) is proven.

Third, we prove Eq. (15) by explicitly analyzing $\mathcal{D}(2, 2)$. By definition, $P \in \mathcal{D}(2, 2)$ if and only if $P > 0$ and there exist real numbers $A_{21}, A_{22}, B_{11}, B_{12}$, and $A_{11} \in (P_{11}, 1 - P_{12})$ such that

$$\begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix} = \begin{pmatrix} A_{11} & 1 - A_{11} \\ A_{21} & A_{22} \end{pmatrix} \circ \begin{pmatrix} B_{11} & B_{12} \\ 1 - B_{11} & 1 - B_{12} \end{pmatrix} \qquad (21)$$

and $A_{21} + A_{22} = 1$. Note that two conditions $A_{11} \in (P_{11}, 1 - P_{12})$ and $P > 0$ are necessary and sufficient for two matrices on the right-hand side of Eq. (21) to be elementwise positive. Under the two conditions, $A_{21} + A_{22}$ can be regarded as a function of A_{11} defined by

$$f(A_{11}) = \frac{P_{21}}{1 - \frac{P_{11}}{A_{11}}} + \frac{P_{22}}{1 - \frac{P_{12}}{1 - A_{11}}}. \qquad (22)$$

Thus, $P \in \mathcal{D}(2, 2)$ if and only if $P > 0$ and there exists a real number $x \in (P_{11}, 1 - P_{12})$ such that $f(x) = 1$. If $P_{11} < 1 - P_{12}$, f is an unbounded convex function $[\lim_{x \searrow P_{11}} f(x) = \lim_{x \nearrow 1 - P_{12}} f(x) = \infty]$ with a global minimum $f(x^*)$, where $x^* = \lambda P_{11} + (1 - \lambda)(1 - P_{12})$ and $\lambda = \frac{\sqrt{P_{12}P_{22}}}{\sqrt{P_{11}P_{21}} + \sqrt{P_{12}P_{22}}}$. By straightforward calculation, $P \in \mathcal{D}(2, 2)$ if and only if

$$\begin{aligned} &(P > 0) \wedge (P_{11} + P_{12} < 1) \\ &\quad \wedge \left[P_{11}^c P_{22}^c + P_{12}^c P_{21}^c - 2(P_{11}P_{12}P_{21}P_{22})^{\frac{1}{2}} \geqslant 1\right], \end{aligned} \qquad (23)$$

where $P_{ij}^c = 1 - P_{ij}$. This implies Eq. (15). ■

Theorem 1. Assume $|\mathbb{S}^{(A)}| \geqslant 2$ and $|\mathbb{S}^{(B)}| \geqslant 2$. The following three conditions are equivalent:

1. $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing.

2. A standard pair $((|\Phi_a^{(A)}\rangle), (|\Phi_b^{(B)}\rangle))$ exists such that $\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle = \langle\Phi_a^{(A)}|\Phi_b^{(B)}\rangle$ for all $(a, b) \in \mathbb{K}$.

3. $P \in \bar{\mathcal{D}}(|\mathbb{S}^{(A)}|, |\mathbb{S}^{(B)}|)$, where $P_{ab} = |\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle|^2$.

Proof. "2 ⇒ 1" is shown by using Lemma 2 in Appendix A, and Proposition 1. "3 ⇒ 2" is shown by taking the standard pair with the following amplitudes:

$$\alpha_{ab} = e^{-i\theta(a,b)}\sqrt{A_{ab}}, \quad \beta_{ab} = \sqrt{B_{ab}}, \qquad (24)$$

where $e^{i\theta(a,b)}|\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle| = \langle\phi_a^{(A)}|\phi_b^{(B)}\rangle$ and $P = A \circ B$.

We show "1 ⇒ 3" in the following. If $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable, there exists a measurement table

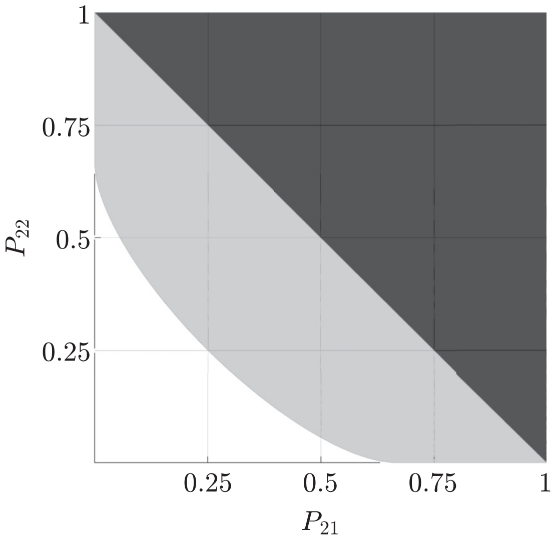

FIG. 2. The region of (P_{21}, P_{22}) for perfectly distinguishable $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ with the help of postprocessing when $P_{11} = P_{12} = 1/4$, shown by the white region. The example shown in Table I resides on the boundary of perfectly distinguishable pairs. Note that since $\mathbb{S}^{(B)}$ is an indexed set of orthonormal vectors, (P_{21}, P_{22}) cannot be in the dark gray region for any $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$.

(M_{ab}). Equation (3) guarantees that $A_{ab} = \langle\phi_a^{(A)}|M_{ab}|\phi_a^{(A)}\rangle$ and $B_{ab} = \langle\phi_b^{(B)}|M_{ab}|\phi_b^{(B)}\rangle$ are a right stochastic matrix and left one, respectively. Using Eq. (4) and the Cauchy-Schwartz inequality, we obtain

$$\left|\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle\right|^2 = \left|\langle\phi_a^{(A)}|M_{ab}|\phi_b^{(B)}\rangle\right|^2 \leqslant A_{ab}B_{ab}, \tag{25}$$

which implies condition 3 by using Lemma 1. ■

We can derive the following criteria for perfect distinguishability as a corollary of Theorem 1 (see Fig. 2).

Corollary 1. Assume $|\mathbb{S}^{(A)}| = |\mathbb{S}^{(B)}| = 2$. Let the 2×2 matrix P be $P_{ab} = |\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle|^2$. Then, $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ is perfectly distinguishable by postprocessing if and only if P satisfies

$$P^c_{11}P^c_{22} + P^c_{12}P^c_{21} - 2(P_{11}P_{12}P_{21}P_{22})^{\frac{1}{2}} \geqslant 1, \tag{26}$$

where $P^c_{ij} = 1 - P_{ij}$.

A proof is straightforward by using Eq. (23) and the fact that $\bar{\mathcal{D}}(2, 2)$ is the closure of $\mathcal{D}(2, 2)$. Note that similar criteria for larger sets can be analytically obtained via a similar derivation of Eq. (23).

VII. RELATED PAST WORK

The investigation of a perfectly distinguishable tuple $((\mathbb{S}^{(n)} = (|\phi_k^{(n)}\rangle)_{k\in\mathbb{K}^{(n)}})_{n=1}^{N}$ with the help of postprocessing of the measurement outcomes with label n is related to the mean king's problem (MKP) [14–19]. The MKP consists of three steps: First, a player prepares a composite system $\mathcal{H} \otimes \mathcal{R}$. Second, the mean king performs a randomly chosen projective measurement on subsystem $\mathcal{H}$. Third, the player tries to guess the king's measurement outcome by postprocessing of her own measurement outcomes obtained by measuring $\mathcal{H} \otimes \mathcal{R}$ and the label of the measurement chosen by the king. The main issue in the MKP—understanding the ensemble of the king's measurement whose outcome can be perfectly identified by the player—has led to the development of several important concepts in quantum mechanics, including a mutually unbiased basis [20,21] and a weak value [22].

It is known that even for noncommuting projective measurements which inevitably produce nonorthogonal pure states for distinct outcomes in the third step, the player can still identify the king's outcome perfectly with the help of postprocessing. Thus, the retrieval of the perfect distinguishability of nonorthogonal pure states can be partially understood by using the result of the MKP. However, since the king cannot prepare general nonorthogonal pure states in $\mathcal{H} \otimes \mathcal{R}$ by interacting only with the subsystem $\mathcal{H}$, a full understanding of the phenomenon cannot be obtained via the MKP. On the other hand, in many cases, it is enough for the player to prepare the maximally entangled state in the first step of the MKP [14,16–19,21]. In such cases, the only nontrivial part of the problem is whether the nonorthogonal pure states produced in the third step are perfectly distinguishable with the help of postprocessing. Therefore, the investigation of a perfectly distinguishable tuple $(\mathbb{S}^{(n)})_{n=1}^{N}$ with the help of postprocessing extracts an intriguing structure from the MKP as a simpler problem, which would deepen our understanding of the MKP and lead us to key concepts in quantum mechanics.

As a first step toward the general case, we have investigated the case of $N = 2$. Note that the three propositions we have shown hold for general N, which could be a guide to a further investigation for the general case.

VIII. CONCLUSION

We have investigated a perfectly distinguishable pair of ensembles of pure states $(\mathbb{S}^{(A)}, \mathbb{S}^{(B)})$ with the help of postprocessing, and have shown that such a pair can always be embedded in a larger Hilbert space as a corresponding standard pair. The distinguishability has been shown to be completely determined by whether a matrix whose elements consist of $|\langle\phi_a^{(A)}|\phi_b^{(B)}\rangle|^2$ can be decomposed into the element-wise product of two types of stochastic matrices. By using the result, we also gave a complete characterization of perfectly distinguishable pairs when $|\mathbb{S}^{(A)}| = |\mathbb{S}^{(B)}| = 2$. Furthermore, we gave the necessary conditions for N-tuple $(\mathbb{S}^{(n)})_{n=1}^{N}$ to be perfectly distinguishable by postprocessing.

ACKNOWLEDGMENTS

We are greatly indebted to S. Tani, Y. Takeuchi, Y. Takahashi, T. Ikuta, H. Yamasaki, A. Soeda, M. Murao, T. Morimae, R. Salazar, and T. Heinosaari for their valuable discussions.

APPENDIX : EXISTENCE OF ISOMETRY

We prove the following lemma used in the proof of Theorem 1.

Lemma 2. If $(|\psi_i\rangle \in \mathcal{H})_{i\in\mathbb{I}}$ and $(|\Psi_i\rangle \in \mathcal{H}')_{i\in\mathbb{I}}$ satisfy $\langle\psi_i|\psi_j\rangle = \langle\Psi_i|\Psi_j\rangle$ for all $i, j \in \mathbb{I}$, there exists isometry V :

$\tilde{\mathcal{H}} \to \mathcal{H}'$ such that $V|\psi_i\rangle = |\Psi_i\rangle$ for all $i \in \mathbb{I}$, where $\tilde{\mathcal{H}} = \mathrm{span}(\{|\psi_i\rangle\}_{i\in\mathbb{I}})$ and $\mathbb{I}$ is a finite set.

Proof. Take a basis of $\tilde{\mathcal{H}}$ as $\{|\psi_i\rangle\}_{i\in\tilde{\mathbb{I}}}$, where $\tilde{\mathbb{I}} \subseteq \mathbb{I}$. Define linear operator $V : \tilde{\mathcal{H}} \to \mathcal{H}'$ as $V|\psi_i\rangle = |\Psi_i\rangle$ for all $i \in \tilde{\mathbb{I}}$. We can easily check that V is an isometry since it does not change the inner product of the basis, i.e., $\langle\psi_i|V^\dagger V|\psi_j\rangle = \langle\Psi_i|\Psi_j\rangle = \langle\psi_i|\psi_j\rangle$ for all $i, j \in \tilde{\mathbb{I}}$.

Let an orthonormal basis of $\tilde{\mathcal{H}}$ be $(|\tilde{\psi}_i\rangle)_{i\in\tilde{\mathbb{I}}}$. We can verify that an indexed set of vectors $(|\tilde{\Psi}_i\rangle)_{i\in\tilde{\mathbb{I}}}$ defined by $|\tilde{\Psi}_i\rangle = \sum_{j\in\tilde{\mathbb{I}}} \alpha_{ij}|\Psi_j\rangle$ is also orthonormal, where α_{ij} satisfies $|\tilde{\psi}_i\rangle = \sum_{j\in\tilde{\mathbb{I}}} \alpha_{ij}|\psi_j\rangle$. Take arbitrary $j \in \mathbb{I} \setminus \tilde{\mathbb{I}}$ and let $|\psi_j\rangle = \sum_{i\in\tilde{\mathbb{I}}} \beta_i|\psi_i\rangle$.

Since $\langle\tilde{\psi}_k|\psi_i\rangle = \langle\tilde{\Psi}_k|\Psi_i\rangle$ for all $k \in \tilde{\mathbb{I}}$ and $i \in \mathbb{I}$,

$$\forall k \in \tilde{\mathbb{I}}, \quad \langle\tilde{\Psi}_k|\left(\sum_{i\in\tilde{\mathbb{I}}} \beta_i|\Psi_i\rangle\right) = \langle\tilde{\psi}_k|\psi_j\rangle = \langle\tilde{\Psi}_k|\Psi_j\rangle. \quad \text{(A1)}$$

Since $\langle\Psi_j|\Psi_j\rangle = \langle\psi_j|\psi_j\rangle$, $|\Psi_j\rangle = \sum_{i\in\tilde{\mathbb{I}}} \beta_i|\Psi_i\rangle$, which shows $V|\psi_j\rangle = |\Psi_j\rangle$ for all $j \in \mathbb{I} \setminus \tilde{\mathbb{I}}$. ■

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[2] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[3] C. W. Helstrom, J. Stat. Phys. **1**, 231 (1969).

[4] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[5] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[6] A. Peres, Phys. Lett. A **128**, 19 (1988).

[7] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, Phys. Rev. Lett. **96**, 070401 (2006).

[8] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

[9] S. Wiesner, SIGACT News **15**, 78 (1983).

[10] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).

[11] M. A. Ballester, S. Wehner, and A. Winter, IEEE Trans. Inf. Theory **54**, 4183 (2008).

[12] D. Gopal and S. Wehner, Phys. Rev. A **82**, 022326 (2010).

[13] C. Carmeli, T. Heinosaari, and A. Toigo, Phys. Rev. A **98**, 012126 (2018).

[14] L. Vaidman, Y. Aharonov, and D. Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).

[15] S. Ben-Menahem, Phys. Rev. A **39**, 1621 (1989).

[16] Y. Aharanov and B. G. Englert, J. Phys. Sci. **56**, 16 (2001).

[17] M. Horibe, A. Hayashi, and T. Hashimoto, Phys. Rev. A **71**, 032337 (2005).

[18] G. Kimura, H. Tanaka, and M. Ozawa, Phys. Rev. A **73**, 050301 (2006).

[19] M. Reimpell and R. F. Werner, Phys. Rev. A **75**, 062334 (2007).

[20] J. Schwinger, Proc. Natl. Acad. Sci. USA **46**, 570 (1960).

[21] B. G. Englert and Y. Aharanov, Phys. Lett. A **284**, 1 (2001).

[22] Y. Aharonov, D. Z. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351 (1988).