ISSN 2186-6570

Examples of deriving sequential measurements maximizing average success probabilities

Kenji Nakahira*, Kentaro Kato

Quantum Information Science Research Center,
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.7, No.1, 5-10, 2017

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.7 No.1 : 5–10 (2017)

Examples of deriving sequential measurements maximizing average success probabilities

Kenji Nakahira*, Kentaro Kato
Quantum Information Science Research Center,
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610 Japan
E-mail: *nakahira@lab.tamagawa.ac.jp

***Abstract*—A sequential measurement (SM) for distinguishing between bipartite quantum states shared by Alice and Bob is considered. We provide two new examples in which SMs maximizing the average success probabilities can be obtained using techniques described in Refs. [arXiv quant-ph/1706.02125v2],[arXiv quant-ph/1707.04736v1]. The first example demonstrates that there exists a set of product states that can be exactly distinguished by an SM from Bob to Alice, while the average success probability of any SM from Alice to Bob is almost zero. The second one shows a set of product states that can be exactly distinguished by local operations and classical communication, while the average success probability of any SM is almost zero, regardless of the direction of communication. These examples might be useful to provide a new method for secure data communication and/or storage.**

I. Introduction

Local discrimination of quantum states has been intensively investigated in quantum information theory in recent years. A measurement realized by local operations and one-way classical communication (one-way LOCC), also called a sequential measurement (SM), is one of the most interesting measurements. SMs are relatively easy to implement in a wide range of physical systems, but, in general, the ability of the best SM to discriminate between quantum states is strictly less than that of the best global measurement. In the 1990s, several works have been reported to analyze the performance of an SM in the Bayes criterion and the mutual information criterion [1]–[8]. After that, many studies have been carried out to evaluate the discrimination performance of SMs in various quantum state sets (e.g., [9]–[20]). However, they have not been investigated systematically; for example, either the dual problem of the problem of finding an SM maximizing the average success probability, which we call an optimal SM in this paper, or necessary and sufficient conditions for an SM to be optimal have not been addressed, whereas those for an optimal global measurement have already been derived in the 1970s [21]–[23].

More recently, a necessary and sufficient condition for an SM to be optimal has been provided by Croke *et al.* [24]. Also, the authors and their co-worker have derived the dual problem for an optimal SM and other necessary and sufficient conditions for an optimal SM [25], [26]. This paper deals only with the problem of finding an SM maximizing the average success probability, while Ref. [26] deals with a more general problem applicable to various criteria (e.g., the Bayes criterion, the Neyman Pearson criterion, and the minimax criterion).

In this paper, we provide two new examples in which optimal SMs can be obtained using methods of Refs. [25], [26]. These examples involve two sets of bipartite product states shared by Alice and Bob. The first one can be exactly distinguished by an SM from Bob to Alice, while the average success probability of any SM from Alice to Bob is almost zero. The second one can also be exactly distinguished by LOCC, while the average success probability of any SM, regardless of the direction of communication, is almost zero. Note that Ref. [27] shows that there can be nonignorable gaps in performance between such measurements. Hence, in the first example, the gap between the average success probabilities of an optimal SM and an optimal LOCC measurement is almost one, while, in the second example, the gap between the average success probabilities of an optimal LOCC measurement and an optimal global measurement is almost one. These extremely large gaps might be useful to provide a new method for secure data communication and/or storage.

In Sections II and III, we first briefly recall the primal and dual problems of obtaining an optimal SM and some its properties, which is described in Refs. [25], [26]. Then, in Section IV, we provide two examples in which optimal SMs can be obtained.

II. Optimal sequential measurement

A. Sequential measurement

We begin with some definitions and notation. We consider a composite system, $\mathcal{H}_{\mathrm{AB}} = \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$, where A and B respectively refer to the subsystems of Alice and Bob. For each $k \in \{\mathrm{A}, \mathrm{B}, \mathrm{AB}\}$, let $\mathcal{S}_k$ and $\mathcal{S}_k^+$ be, respectively, the entire sets of Hermitian operators and positive semidefinite operators on $\mathcal{H}_k$, and $\hat{1}_k$ be the identity operators on $\mathcal{H}_k$. $\hat{x} \geq 0$ with a Hermitian operator $\hat{x}$ denotes that $\hat{x}$ is positive semidefinite. Similarly, $\hat{x} \geq \hat{y}$ means $\hat{x} - \hat{y} \geq 0$. Let $\mathcal{I}_N \coloneqq \{0, 1, \cdots, N-1\}$.

In an SM from Alice to Bob, Alice first performs a measurement, which is represented by a positive operator

valued measure (POVM) $\{\hat{A}_j\}_j$ with $\hat{A}_j \in \mathcal{S}_{\rm A}^+$, and sends the measurement result j to Bob. Then, Bob performs a measurement $\{\hat{B}_m^{(j)}\}_{m\in\mathcal{I}_M}$ with $\hat{B}_m^{(j)} \in \mathcal{S}_{\rm B}^+$, which depends on j. The outcome of his measurement, $m \in \mathcal{I}_M$, represents the result of the SM.

We can also understand this SM in a different way [25]. Each of Bob's POVM is uniquely labeled by an index ω; let $\{\hat{B}_m^{(\omega)}\}_{m\in\mathcal{I}_M}$ be his POVM indexed by ω. Let Ω be the entire set of all possible values of ω. Alice first performs a continuous measurement $\hat{A} = \{\hat{A}(\omega)\}_{\omega\in\Omega}$ with $\hat{A}(\omega) \in \mathcal{S}_{\rm A}^+$ to determine which measurement Bob performs, and then sends the measurement result ω to him. Bob performs the corresponding measurement $\{\hat{B}_m^{(\omega)}\}_{m\in\mathcal{I}_M}$ with $\hat{B}_m^{(\omega)} \in \mathcal{S}_{\rm B}^+$ and obtains the final result m. Let $\mathcal{M}_{\rm A}$ be the entire set of all Alice's POVMs. Any SM is expressed by a function of $\hat{A} \in \mathcal{M}_{\rm A}$, which is denoted as $\{\hat{\Pi}_m^{(\hat{A})}\}_{m\in\mathcal{I}_M}$ with

$$\hat{\Pi}_m^{(\hat{A})} \;:=\; \int_\Omega \hat{A}(d\omega) \otimes \hat{B}_m^{(\omega)}. \tag{1}$$

B. Discrimination problem

Let us consider the problem of discriminating a set of M quantum states, $\{\tilde{\rho}_m\}_{m\in\mathcal{I}_M}$. Each density operator $\tilde{\rho}_m \geq 0$ has unit trace, i.e., $\mathrm{Tr}\,\tilde{\rho}_m = 1$. We refer to $\{\hat{\rho}_m = \xi_m\tilde{\rho}_m\}_{m\in\mathcal{I}_M}$ as a quantum state set, which denotes $\{\tilde{\rho}_m\}_{m\in\mathcal{I}_M}$ with prior probabilities $\{\xi_m\}_{m\in\mathcal{I}_M}$, We can easily verify that $\hat{\rho}_m \geq 0$, $\mathrm{Tr}\,\hat{\rho}_m > 0$ for any m, and $\sum_m \mathrm{Tr}\,\hat{\rho}_m = 1$ hold.

The average success probability with an SM $\{\hat{\Pi}_m^{(\hat{A})}\}_{m\in\mathcal{I}_M}$ is defined as

$$P_{\rm S}(\hat{A}) \;:=\; \sum_{m\in\mathcal{I}_M} \mathrm{Tr}\left[\hat{\rho}_m\hat{\Pi}_m^{(\hat{A})}\right]. \tag{2}$$

The problem of obtaining an optimal SM is formulated as

$$\begin{array}{lll} \mathrm{P}: & \text{maximize} & P_{\rm S}(\hat{A}) \\ & \text{subject to} & \hat{A} \in \mathcal{M}_{\rm A} \end{array} \tag{3}$$

with variable $\hat{A}$. Let $P_{\rm S}^\star$ and $\hat{A}^\star$ be respectively the optimal value and an optimal solution to Problem P. There may be more than one optimal solution. $P_{\rm S}(\hat{A}^\star) = P_{\rm S}^\star$ obviously holds. We can easily see that Problem P is a convex programming problem.

C. Dual problem

We will get the dual problem of Problem P. Let

$$\begin{aligned} \mathcal{X} \;&:=\; \left\{\hat{X} \in \mathcal{S}_{\rm A} : \hat{X} \geq \hat{\sigma}_\omega,\ \forall\omega \in \Omega\right\}, \\ \hat{\sigma}_\omega \;&:=\; \mathrm{Tr}_{\rm B} \sum_{m\in\mathcal{I}_M} \hat{\rho}_m\hat{B}_m^{(\omega)}. \end{aligned} \tag{4}$$

Then, we have that for any $\hat{A} \in \mathcal{M}_{\rm A}$ and $\hat{X} \in \mathcal{X}$,

$$\begin{aligned} P_{\rm S}(\hat{A}) \;&=\; \sum_{m\in\mathcal{I}_M} \mathrm{Tr}\left[\hat{\rho}_m\hat{\Pi}_m^{(\hat{A})}\right] \\ &=\; \mathrm{Tr}\int_\Omega \hat{\sigma}_\omega\hat{A}(d\omega) \\ &\leq\; \mathrm{Tr}\,\hat{X}\int_\Omega \hat{A}(d\omega) \;=\; \mathrm{Tr}\,\hat{X}, \end{aligned} \tag{5}$$

where the second line follows from Eqs. (1) and (4). This implies that we can consider the following dual problem:

$$\begin{array}{lll} \mathrm{DP}: & \text{minimize} & \mathrm{Tr}\,\hat{X} \\ & \text{subject to} & \hat{X} \in \mathcal{X} \end{array}$$

with variable $\hat{X}$. From Eq. (5), $\mathrm{Tr}\,\hat{X} \geq P_{\rm S}^\star$ holds for any $\hat{X} \in \mathcal{X}$. Let $\hat{X}^\star$ be an optimal solution to Problem DP; then, we can derive that $\mathrm{Tr}\,\hat{X}^\star = P_{\rm S}^\star$ holds [25]. Problem DP is also a convex programming problem.

Unfortunately, Problems P and DP are much more difficult to solve than the well-known primal and dual problems for finding an optimal global measurement (e.g., [21]), which is not limited to an SM. The reason is that, in the former problems, since Ω is not countable (e.g., it is difficult to decide whether $\hat{X}$ is in $\mathcal{X}$ or not). However, we can obtain an analytical (or numerical) solution to Problems P and DP in some cases.

III. Properties of optimal sequential measurements

A. Conditions for optimal sequential measurements

We first show necessary and sufficient conditions for an optimal SM.

Theorem 1 (Theorem 2 of Ref. [26]) For any $\hat{A} \in \mathcal{M}_{\rm A}$, the following statements are all equivalent.

(1) $\hat{A}$ is an optimal solution to Problem P.
(2) The following holds with an optimal solution, $\hat{X}^\star$, to Problem DP:

$$(\hat{X}^\star - \hat{\sigma}_\omega)\hat{A}(\omega) \;=\; 0, \quad \forall\omega \in \Omega. \tag{6}$$

(3) There exists $\hat{X}^\star \in \mathcal{X}$ satisfying Eq. (6).
(4) The following holds:

$$\int_\Omega \hat{\sigma}_{\omega'}\hat{A}(d\omega') \;\geq\; \hat{\sigma}_\omega, \quad \forall\omega \in \Omega. \tag{7}$$

Equation (6) implies that, for any $\omega \in \Omega$, supp $\hat{A}(\omega)$ is in the kernel of $\hat{X}^\star - \hat{\sigma}_\omega$. If $\hat{A}$ is discrete-valued (i.e., $\hat{A}(\omega) \neq 0$ holds for $\omega \in \Omega$ only if ω is in at most countable set $\{\omega_n\}_n$), then Eq. (7) can be rewritten as

$$\sum_n \hat{\sigma}_{\omega_n}\hat{A}(\omega_n) \;\geq\; \hat{\sigma}_\omega, \quad \forall\omega \in \Omega, \tag{8}$$

which is equivalent to Eq. (19) of Ref. [24] [1].

B. Symmetric property

We next show that if a given state set has a certain symmetry, then there exist optimal solutions to Problems P and DP with the same type of symmetry. This fact is useful to obtain an analytical (or numerical) expression of an optimal solution.

We use group theory to exploit the symmetric properties of quantum states. Let $\mathcal{G}$ be a group with at least two

[1] Although a continuous-valued POVM might be optimal, there always exists an optimal solution to Problem P with a finite number of outcomes [25] if $\mathcal{H}_{\rm A}$ is finite dimensional.

elements and $e \in \mathcal{G}$ be its identity element. Suppose that the following statements hold:

(1) There exists a map $\pi_g : \mathcal{I}_M \to \mathcal{I}_M$, for each $m \in \mathcal{I}_M$, such that $\pi_{gh}(m) = \pi_g[\pi_h(m)]$ $(g, h \in \mathcal{G})$ and $\pi_e(m) = m$ hold.
(2) For any $g \in \mathcal{G}$, there exists a unitary (or anti-unitary) operator $\hat{U}_g$ on $\mathcal{H}_{\rm AB}$ written by $\hat{U}_g = \hat{V}_g \otimes \hat{W}_g$ with unitary (or anti-unitary) operators $\hat{V}_g$ on $\mathcal{H}_{\rm A}$ and $\hat{W}_g$ on $\mathcal{H}_{\rm B}$. Moreover, $\hat{V}_{gh} = \hat{V}_g \hat{V}_h$ and $\hat{W}_{gh} = \hat{W}_g \hat{W}_h$ hold for any $g, h \in \mathcal{G}$. (Note that this gives $\hat{V}_e = \hat{1}_{\rm A}$ and $\hat{W}_e = \hat{1}_{\rm B}$.)

For any $g \in \mathcal{G}$, let $\eta_g : \Omega \to \Omega$ be a map satisfying

$$\hat{B}_m^{[\eta_g(\omega)]} = \hat{W}_g \hat{B}^{(\omega)}_{\pi_g^{-1}(m)} \hat{W}_g^\dagger, \quad \forall g \in \mathcal{G}, m \in \mathcal{I}_M, \omega \in \Omega, \tag{9}$$

where π_g^{-1} is the inverse map of π_g.

Note that all of the following maps can be regarded as group actions: $m \mapsto \pi_g(m)$, $\hat{Q}^{(\rm A)} \mapsto \hat{V}_g \hat{Q}^{(\rm A)} \hat{V}_g^\dagger$ $(\hat{Q}^{(\rm A)} \in \mathcal{S}_{\rm A})$, $\hat{Q}^{(\rm B)} \mapsto \hat{W}_g \hat{Q}^{(\rm B)} \hat{W}_g^\dagger$ $(\hat{Q}^{(\rm B)} \in \mathcal{S}_{\rm B})$, $\hat{Q} \mapsto \hat{U}_g \hat{Q} \hat{U}_g^\dagger$ $(\hat{Q} \in \mathcal{S}_{\rm AB})$, and $\omega \mapsto \eta_g(\omega)$ [2].

The following theorem holds.

Theorem 2 (Theorem 4 of Ref. [26]) Suppose that a state set $\{\hat{\rho}_m\}_{m \in \mathcal{I}_M}$ satisfies

$$\hat{U}_g \hat{\rho}_m \hat{U}_g^\dagger = \hat{\rho}_{\pi_g(m)}, \quad \forall g \in \mathcal{G}, m \in \mathcal{I}_M. \tag{10}$$

Then, there exists an optimal solution $\hat{A}^\star$ to Problem P such that

$$\hat{V}_g \hat{A}^\star(\omega) \hat{V}_g^\dagger = \hat{A}^\star[\eta_g(\omega)], \quad \forall g \in \mathcal{G}, \omega \in \Omega. \tag{11}$$

Moreover, there exists an optimal solution $\hat{X}^\star$ to Problem DP such that

$$\hat{V}_g \hat{X}^\star \hat{V}_g^\dagger = \hat{X}^\star, \quad \forall g \in \mathcal{G}. \tag{12}$$

It follows that if Eq. (11) holds, then $\hat{\Pi}^{(\hat{A}^\star)}$ has the following symmetry:

$$\hat{U}_g \hat{\Pi}_m^{(\hat{A}^\star)} \hat{U}_g^\dagger = \hat{\Pi}^{(\hat{A}^\star)}_{\pi_g(m)}. \tag{13}$$

Problems P and DP clearly remain in convex programming problems even if we restrict the solution domains from $\mathcal{M}_{\rm A}$ to $\{\hat{A} \in \mathcal{M}_{\rm A} : \hat{V}_g \hat{A}(\omega) \hat{V}_g^\dagger = \hat{A}[\eta_g(\omega)], \ \forall g \in \mathcal{G}\}$ and from $\mathcal{X}$ to $\{\hat{X} \in \mathcal{X} : \hat{V}_g \hat{X} \hat{V}_g^\dagger = \hat{X}, \ \forall g \in \mathcal{G}\}$, respectively.

IV. Examples

Now, we provide two examples of deriving closed-form analytical expressions for optimal SMs.

[2] In Ref. [26], these maps are denoted as the same symbol, i.e., "$g\circ$".

A. Example 1

Our first example demonstrates that there exists a set of product states that can be exactly distinguished by an SM from Bob to Alice, while the average success probability of any SM from Alice to Bob is almost zero. Let us consider an SM from Alice to Bob for K^2 states $\{\hat{\rho}_{m,k}\}_{m,k \in \mathcal{I}_K}$, where

$$\begin{aligned} \hat{\rho}_{m,k} &:= \frac{1}{K^2} |\psi_{m,k}\rangle \langle \psi_{m,k}|, \\ |\psi_{m,k}\rangle &:= |a_k^{(m)}\rangle \otimes |m\rangle, \end{aligned} \tag{14}$$

and K is prime. $\{|m\rangle\}_{m \in \mathcal{I}_K}$ is an orthonormal basis (ONB) in $\mathcal{H}_{\rm B}$ with $\dim \mathcal{H}_{\rm B} = K$. For each $m \in \mathcal{I}_K$, $\{|a_k^{(m)}\rangle\}_{k \in \mathcal{I}_K}$ is also an ONB in $\mathcal{H}_{\rm A}$ with $\dim \mathcal{H}_{\rm A} = K$. A set of ONBs $\{|a_k^{(m)}\rangle\}_{m,k \in \mathcal{I}_K}$ constitutes so-called mutually unbiased bases (MUB) [28], which satisfy $|\langle a_k^{(m)} | a_{k'}^{(m')} \rangle| = 1/\sqrt{K}$ $(\forall k, k' \in \mathcal{I}_K)$ for any distinct $m, m' \in \mathcal{I}_K$. In the case of $K = 2$, an analytical expression for an optimal SM has been derived in Ref. [10]. In what follows, we will provide an analytical solution for $K \geq 3$.

The MUB basis vectors $\{|a_k^{(m)}\rangle\}_{m,k \in \mathcal{I}_K}$ can be chosen to be eigenstates of generalized Pauli operators. Generalized Pauli operators $\hat{S}_{\rm X}$ and $\hat{S}_{\rm Z}$ are expressed by

$$\begin{aligned} \hat{S}_{\rm X} &:= \sum_{n \in \mathcal{I}_K} |n \oplus 1\rangle \langle n|, \\ \hat{S}_{\rm Z} &:= \sum_{n \in \mathcal{I}_K} \tau^n |n\rangle \langle n|, \end{aligned} \tag{15}$$

where $\tau := \exp(2\pi\sqrt{-1}/K)$, $\{|n\rangle\}_{n \in \mathcal{I}_K}$ is an ONB in $\mathcal{H}_{\rm A}$, and $\oplus$ is the addition modulo K. We choose $|a_k^{(m)}\rangle$, without loss of generality, such that the ONB $\{|a_k^{(m)}\rangle\}_{k \in \mathcal{I}_K}$ is the eigenbasis of the operator $\hat{S}_{\rm X} \hat{S}_{\rm Z}^m$ for each $m \in \mathcal{I}_K$ (see, e.g., [29]).

First, we obtain an optimal solution $\hat{X}^\star$ to Problem DP. Let $\mathcal{G}$ be the group generated by $\hat{S}_{\rm X}$ and $\hat{S}_{\rm Z}$ (i.e., the entire set of unitary operators expressed as the multiplication of finite number of elements in $\{\hat{S}_{\rm X}, \hat{S}_{\rm Z}, \hat{S}_{\rm X}^\dagger, \hat{S}_{\rm Z}^\dagger\}$). For each $g \in \mathcal{G}$, the unitary operators $\hat{V}_g$ and $\hat{W}_g$ is set to $\hat{V}_g := g$ and $\hat{W}_g := \hat{1}_{\rm B}$, and $\hat{U}_g := \hat{V}_g \otimes \hat{W}_g = g \otimes \hat{1}_{\rm B}$. We can easily verify that $\{\hat{\rho}_{m,k}\}_{m,k \in \mathcal{I}_K}$ satisfies Eq. (10) with appropriate maps $\{\pi_g\}_{g \in \mathcal{G}}$. Therefore, from Theorem 2, there exists an optimal solution $\hat{X}^\star$ to Problem DP such that $\hat{S}_{\rm X} \hat{X}^\star \hat{S}_{\rm X}^\dagger = \hat{X}^\star = \hat{S}_{\rm Z} \hat{X}^\star \hat{S}_{\rm Z}^\dagger$, i.e., $\hat{X}^\star$ commutes with $\hat{S}_{\rm X}$ and $\hat{S}_{\rm Z}$. On the other hand, since $\hat{S}_{\rm X}$ and $\hat{S}_{\rm Z}$ do not share any eigenvector, any operator commuting with $\hat{S}_{\rm X}$ and $\hat{S}_{\rm Z}$ is proportional to $\hat{1}_{\rm A}$. Thus, we have $\hat{X}^\star = c^\star \hat{1}_{\rm A}$ with a constant $c^\star$. Substituting this into Problem DP, we obtain the following problem

$$\begin{aligned} &\text{minimize} && c \\ &\text{subject to} && c\hat{1}_{\rm A} \geq \hat{\sigma}_\omega, \quad \forall \omega \in \Omega \end{aligned} \tag{16}$$

with variable c, whose optimal value is $c^\star$. Thus, it follows that $c^\star$ equals the maximum of the largest eigen-

values of $\hat{\sigma}_\omega$, which gives

$$c^\star \;=\; \max\{\langle\phi|\hat{\sigma}_\omega|\phi\rangle : |\phi\rangle \in \mathcal{H}_{\rm A}, \langle\phi|\phi\rangle = 1, \omega \in \Omega\}. \tag{17}$$

$c^\star$ can be derived from this equation as follows. Substituting Eq. (14) into Eq. (4), we have

$$\hat{\sigma}_\omega \;=\; \frac{1}{K^2}\sum_{m,k\in\mathcal{I}_K} p^{(\omega)}_{m,k}\,|a^{(m)}_k\rangle\langle a^{(m)}_k|, \tag{18}$$

where

$$p^{(\omega)}_{m,k} \;:=\; \langle m|\hat{B}^{(\omega)}_{m,k}|m\rangle \tag{19}$$

and $\{\hat{B}^{(\omega)}_{m,k}\}_{m,k\in\mathcal{I}_K}$ is the POVM on $\mathcal{H}_{\rm B}$ corresponding to $\omega \in \Omega$. From Eq. (18), we have that for any normal vector $|\phi\rangle \in \mathcal{H}_{\rm A}$,

$$\begin{aligned}\langle\phi|\hat{\sigma}_\omega|\phi\rangle &= \frac{1}{K^2}\sum_{m,k\in\mathcal{I}_K} p^{(\omega)}_{m,k}\left|\langle\phi|a^{(m)}_k\rangle\right|^2\\ &\le \frac{1}{K^2}\sum_{m,k\in\mathcal{I}_K} p^{(\omega)}_{m,k}\left|\langle\phi|a^{(m)}_{\kappa(m)}\rangle\right|^2\\ &\le \frac{1}{K^2}\sum_{m\in\mathcal{I}_K}\left|\langle\phi|a^{(m)}_{\kappa(m)}\rangle\right|^2\\ &= \frac{1}{K^2}\langle\phi|\hat{\Gamma}|\phi\rangle,\end{aligned} \tag{20}$$

where $\kappa(m)$ is a function of m such that

$$\kappa(m) \;\in\; \operatorname*{argmax}_{k\in\mathcal{I}_K}|\langle\phi|a^{(m)}_k\rangle|, \quad \forall m \in \mathcal{I}_K \tag{21}$$

and

$$\hat{\Gamma} \;:=\; \sum_{m\in\mathcal{I}_K}|a^{(m)}_{\kappa(m)}\rangle\langle a^{(m)}_{\kappa(m)}|. \tag{22}$$

The third line of Eq. (20) follows from $\sum_{k\in\mathcal{I}_K} p^{(\omega)}_{m,k} \le \langle m|\hat{1}_{\rm B}|m\rangle = 1$, which is given by $\sum_{k\in\mathcal{I}_K}\hat{B}^{(\omega)}_{m,k} \le \hat{1}_{\rm B}$.

Due to the symmetry of the states, we can here assume $\kappa(m) = 0$ for each $m \in \mathcal{I}_K$ without loss of generality. It is known that, in the case when $K \ge 3$ is prime, $|a^{(m)}_k\rangle$ can be expressed as (e.g., [29])

$$|a^{(m)}_k\rangle \;=\; \frac{1}{\sqrt{K}}\sum_{n\in\mathcal{I}_K}\tau^{-kn+mn(n-1)/2}|n\rangle. \tag{23}$$

Substituting Eq. (23) into Eq. (22), and with some algebra, we can obtain

$$\hat{\Gamma} \;=\; \left|\frac{K+1}{2}\right\rangle\left\langle\frac{K+1}{2}\right| + 2\sum_{m\in\mathcal{I}_{(K-1)/2}}|\nu_m\rangle\langle\nu_m|, \tag{24}$$

where $|\nu_m\rangle$ is the normal vector defined by

$$|\nu_m\rangle \;:=\; \begin{cases}(|0\rangle+|1\rangle)/\sqrt{2}, & m=0,\\ (|m+1\rangle+|K-m\rangle)/\sqrt{2}, & m>0.\end{cases} \tag{25}$$

Equation (24) indicates that the largest eigenvalue of $\hat{\Gamma}$ is 2, and thus, from Eq. (20), the maximum value of $\langle\phi|\hat{\sigma}_\omega|\phi\rangle$ is $\frac{2}{K^2}$, which gives $c^\star = \frac{2}{K^2}$ (i.e., $\hat{X}^\star = \frac{2}{K^2}\hat{1}_{\rm A}$). Therefore, we obtain [3]

$$P^\star_{\rm S} \;=\; {\rm Tr}\hat{X}^\star \;=\; \frac{2}{K}. \tag{26}$$

Next, we obtain an optimal SM. From Eq. (6), if $\hat{A}(\omega) \neq 0$, then at least one of the eigenvalues of $\hat{X}^\star - \hat{\sigma}_\omega \ge 0$ is zero; i.e., $\hat{\sigma}_\omega$ has the eigenvalue $\frac{2}{K^2}$. This implies that the equality in Eq. (20) holds when $|\phi\rangle = |u\rangle$, where $|u\rangle$ is a normalized eigenvector corresponding to the largest eigenvalue of $\hat{\sigma}_\omega$. We consider the case $p^{(\omega)}_{m,k} = \delta_{k,\kappa(m)}$ ($\delta_{m,n}$ is the Kronecker delta), where $\kappa(m)$ satisfies Eq. (21) with $|\phi\rangle = |u\rangle$, which is sufficient for the equality in Eq. (20) with $|\phi\rangle = |u\rangle$. In this case, $\hat{B}^{(\omega)}_{m,k}$ can be expressed as

$$\hat{B}^{(\omega)}_{m,k} \;=\; \delta_{k,\kappa(m)}|m\rangle\langle m|. \tag{27}$$

We can easily verify that $\hat{A}(\omega)$ written by the following form:

$$\hat{A}(\omega) \;=\; \gamma|u\rangle\langle u| \tag{28}$$

with $\gamma > 0$ satisfies Eq. (6). These conditions help us to find an optimal SM.

Let $\kappa(m) = t \oplus ms$ $(s, t \in \mathcal{I}_K)$ and $\omega_{s,t} \in \Omega$ be the corresponding index; then, Eq. (27) gives

$$\hat{B}^{(\omega_{s,t})}_{m,k} \;=\; \delta_{k,t\oplus ms}|m\rangle\langle m|. \tag{29}$$

From Eq. (18), we have

$$\hat{\sigma}_{\omega_{s,t}} \;=\; \frac{1}{K^2}\sum_{m\in\mathcal{I}_K}|a^{(m)}_{t\oplus ms}\rangle\langle a^{(m)}_{t\oplus ms}|. \tag{30}$$

The following is a normalized eigenvector corresponding to the largest eigenvalue, $\frac{2}{K^2}$, of $\hat{\sigma}_{\omega_{s,t}}$:

$$|u_{s,t}\rangle \;:=\; \frac{1}{\sqrt{2K}}\sum_{j\in\mathcal{I}_K}\tau^{js(s+1)/2}|a^{(j)}_{t\oplus js}\rangle. \tag{31}$$

In this case, we can see that Eq. (21) holds with $|\phi\rangle = |u\rangle$. We choose $\hat{A}^\star$ such that

$$\hat{A}^\star(\omega_{s,t}) \;:=\; \frac{1}{K}|u_{s,t}\rangle\langle u_{s,t}| \tag{32}$$

and $\hat{A}^\star(\omega) := 0$ when $\omega \in \Omega$ is not in $\{\omega_{s,t} : s, t \in \mathcal{I}_K\}$. We can easily verify $\sum_{s,t\in\mathcal{I}_K}\hat{A}^\star(\omega_{s,t}) = \hat{1}_{\rm A}$, and thus, $\hat{A}^\star$ is a POVM on $\mathcal{H}_{\rm A}$ with K^2 outcomes $\{\omega_{s,t}\}_{s,t\in\mathcal{I}_K}$. Since Eq. (6) with $\hat{A} = \hat{A}^\star$ holds, from Theorem 1, $\hat{A}^\star$ is an optimal solution to Problem P. Substituting Eqs. (29) and (32) into Eq. (1), the corresponding optimal SM $\{\hat{\Pi}^{(\hat{A}^\star)}_{m,k}\}_{m,k\in\mathcal{I}_K}$ can be expressed by

$$\begin{aligned}\hat{\Pi}^{(\hat{A}^\star)}_{m,k} &= \sum_{s,t\in\mathcal{I}_K}\left(\frac{1}{K}|u_{s,t}\rangle\langle u_{s,t}|\right)\otimes\left(\delta_{k,t\oplus ms}|m\rangle\langle m|\right)\\ &= \frac{1}{K}\sum_{s\in\mathcal{I}_K}|u_{s,k\ominus ms}\rangle\langle u_{s,k\ominus ms}|\otimes|m\rangle\langle m|,\end{aligned} \tag{33}$$

[3] If $K = 2$, then Eq. (23) does not hold. However, we can apply the same technique to this case and obtain $\hat{X}^\star = (\frac{1}{4} + \frac{1}{4\sqrt{2}})\hat{1}_{\rm A}$. This yields $P^\star_{\rm S} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$, which is consistent with the result in Ref. [10].

where $\ominus$ denotes the subtraction modulo K.

We now compare the performances of SMs from Alice to Bob and the other way around. From Eq. (26), the average success probability, $P_{\mathrm{S}}^{\star}$, of an optimal SM from Alice to Bob converges to zero if K goes to infinity. This behavior is substantially different from that in the case of an SM from Bob to Alice, of which the maximum average success probability is exactly one regardless of K. Indeed, in this case, Bob first measures in the $\{|m\rangle\}_{m\in\mathcal{I}_K}$ basis, and sends the result m to Alice. She then measures in the corresponding $\{|a_k^{(m)}\rangle\}_{k\in\mathcal{I}_K}$ basis. We can regard $|a_k^{(m)}\rangle$ as a quantum state in which the classical message k is encrypted with the classical key m. If the communication from Bob to Alice is allowed, then Bob can completely specify the key m and sends it to Alice. In this case, she can correctly decrypt the message k. However, if not allowed, Alice cannot fully decrypt k.

B. Example 2

In our second example, we show a set of product states that can be exactly distinguished by two-way LOCC, while the average success probability of any SM, regardless of the direction of communication, is almost zero. Let us consider the following K^3 states $\{\hat{\rho}'_{m,k,l}\}_{m,k,l\in\mathcal{I}_K}$:

$$\begin{aligned}\hat{\rho}'_{m,k,l} &:= \frac{1}{K^3}\,|\psi'_{m,k,l}\rangle\langle\psi'_{m,k,l}|\,,\\ |\psi'_{m,k,l}\rangle &:= |a_k^{(m)}\rangle\otimes[|m\rangle\otimes|a_l^{(k)}\rangle],\end{aligned}\tag{34}$$

where $|a_k^{(m)}\rangle\in\mathcal{H}_{\mathrm{A}}$ and $|m\rangle\otimes|a_l^{(k)}\rangle\in\mathcal{H}_{\mathrm{B},1}\otimes\mathcal{H}_{\mathrm{B},2}=\mathcal{H}_{\mathrm{B}}$ are respectively states in Alice's and Bob's subsystems. $\mathcal{H}_{\mathrm{A}}$, $\mathcal{H}_{\mathrm{B},1}$, and $\mathcal{H}_{\mathrm{B},2}$ are all K-dimensional. $|a_k^{(m)}\rangle$ and $|m\rangle$ are the same as the above-mentioned one; i.e., $\{|m\rangle\}_{m\in\mathcal{I}_K}$ is an ONB in a Hilbert space $\mathcal{H}_{\mathrm{B},1}$, and a set of $\{|a_k^{(m)}\rangle\}_{k\in\mathcal{I}_K}$ constitutes MUB in $\mathcal{H}_{\mathrm{A}}$ or $\mathcal{H}_{\mathrm{B},2}$. In this example, it can be interpreted that the classical message k is encrypted with the classical key m, and the message l is encrypted with the key k. Thus, if LOCC with two rounds of communication (i.e., Bob $\to$ Alice $\to$ Bob) is allowed, then these states are perfectly distinguishable, while they cannot be perfectly distinguished if restricted to an SM.

We consider an SM from Alice to Bob and another from Bob to Alice. In the former case (i.e., Alice $\to$ Bob), to determine m and k as accurately as possible, they perform an optimal SM on the state $|a_k^{(m)}\rangle\otimes|m\rangle\in\mathcal{H}_{\mathrm{A}}\otimes\mathcal{H}_{\mathrm{B},1}$ in the same way as the first example. If they correctly identify k, then Bob can perfectly get l by subsequently measuring in the $\{|a_l^{(k)}\rangle\}_{l\in\mathcal{I}_K}$ basis in $\mathcal{H}_{\mathrm{B},2}$. In the latter case (i.e., Bob $\to$ Alice), Bob can get m without disturbing the global state $|a_k^{(m)}\rangle\otimes|m\rangle\otimes|a_l^{(k)}\rangle$ by simply measuring in the $\{|m\rangle\}_{m\in\mathcal{I}_K}$ basis in $\mathcal{H}_{\mathrm{B},1}$. After that, they must discriminate between the pure states $\{|a_k^{(m)}\rangle\otimes|a_l^{(k)}\rangle\}\}_{k,l\in\mathcal{I}_K}$ with fixed m, which can be regarded as the same states as those given by $\{|\psi_{m,k}\rangle\}_{m,k\in\mathcal{I}_K}$ of Eq. (14). Thus, an optimal SM for these states can be obtained in the same way as the first example. In the both cases, it follows that the maximum average success probability is $\frac{2}{K}$ (i.e., identical to $P_{\mathrm{S}}^{\star}$ of Eq. (26)), which converges to zero if K goes to infinity. The analytical expressions of optimal SMs are also obtained in the same way as the first example.

V. Conclusion

Two examples were provided in which optimal SMs can be obtained using the methods of Refs. [25], [26]. These examples demonstrate that the dual problem for an optimal SM and its properties derived in these references are useful for obtaining an analytical expression of an optimal SM. We showed that there is a quantum state set in which the gap between the average success probabilities of an optimal SM and an optimal LOCC measurement is almost one, and that there is another quantum state set in which the gap between the average success probabilities of an optimal LOCC measurement and an optimal global measurement is almost one.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number JP17H07115.

References

[1] D. Brody and B. Meister, "Minimum decision cost for quantum ensembles," *Phys. Rev. Lett.*, vol. 76, pp. 1–5, 1996.

[2] M. Ban, K. Yamazaki, and O. Hirota, "Accessible information in combined and sequential quantum measurementson a binary-state signal," *Phys. Rev. A*, vol. 55, no. 1, p. 22, 1997.

[3] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "A demonstration of superadditivity in the classical capacity of a quantum channel," *Phys. Lett. A*, vol. 236, no. 1, pp. 1–4, 1997.

[4] ——, "Quantum channels showing superadditivity in classical capacity," *Phys. Rev. A*, vol. 58, no. 1, p. 146, 1998.

[5] M. Sasaki, T. Sasaki-Usuda, M. Izutsu, and O. Hirota, "Realization of a collective decoding of code-word states," *Phys. Rev. A*, vol. 58, no. 1, p. 159, 1998.

[6] M. Osaki, O. Hirota, and M. Ban, "The maximum mutual information without coding for binary quantum-state signals," *Journal of Modern Optics*, vol. 45, no. 2, pp. 269–282, 1998.

[7] T. S. Usuda, I. Takumi, M. Hata, and O. Hirota, "Minimum error detection of classical linear code sending through a quantum channel," *Phys. Lett. A*, vol. 256, pp. 104–108, 1999.

[8] O. Hirota, "A foundation of quantum channels with super additiveness for shannon information," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, no. 4-5, pp. 401–423, 2000.

[9] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, "Local distinguishability of multipartite orthogonal quantum states," *Phys. Rev. Lett.*, vol. 85, no. 23, p. 4972, 2000.

[10] B. Groisman and L. Vaidman, "Nonlocal variables with product-state eigenstates," *J. Phys. A: Math. Gen.*, vol. 34, no. 35, p. 6881, 2001.

[11] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, "Optimal local discrimination of two multipartite pure states," *Phys. Lett. A*, vol. 288, no. 2, pp. 62–68, 2001.

[12] Y.-X. Chen and D. Yang, "Optimal conclusive discrimination of two nonorthogonal pure product multipartite states through local operations," *Phys. Rev. A*, vol. 64, no. 6, p. 064303, 2001.

[13] J. Walgate and L. Hardy, "Nonlocality, asymmetry, and distinguishing bipartite states," *Phys. Rev. Lett.*, vol. 89, no. 14, p. 147901, 2002.

[14] Y.-X. Chen and D. Yang, "Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communications," *Phys. Rev. A*, vol. 65, no. 2, p. 022320, 2002.

[15] H. Fan, "Distinguishability and indistinguishability by local operations and classical communication," *Phys. Rev. Lett.*, vol. 92, no. 17, p. 177905, 2004.
[16] A. Acín, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia, "Multiple-copy two-state discrimination with individual measurements," *Phys. Rev. A*, vol. 71, no. 3, p. 032338, 2005.
[17] M. Nathanson, "Distinguishing bipartitite orthogonal states using locc: Best and worst cases," *J. Math. Phys.*, vol. 46, no. 6, p. 062103, 2005.
[18] Z. Ji, H. Cao, and M. Ying, "Optimal conclusive discrimination of two states can be achieved locally," *Phys. Rev. A*, vol. 71, no. 3, p. 032323, 2005.
[19] S. Bandyopadhyay, S. Ghosh, and G. Kar, "Locc distinguishability of unilaterally transformable quantum states," *New J. Phys.*, vol. 13, no. 12, p. 123013, 2011.
[20] Z.-C. Zhang, Q.-Y. Wen, F. Gao, G.-J. Tian, and T.-Q. Cao, "One-way locc indistinguishability of maximally entangled states," *Quant. Inf. Proc.*, vol. 13, no. 3, pp. 795–804, 2014.
[21] A. S. Holevo, "Statistical decision theory for quantum systems," *J. Multivar. Anal.*, vol. 3, pp. 337–394, 1973.
[22] H. P. Yuen, K. S. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 125–134, 1975.
[23] C. W. Helstrom, *Quantum detection and estimation theory*. Academic Press, 1976.
[24] S. Croke, S. M. Barnett, and G. Weir, "Optimal sequential measurements for bipartite state discrimination," *Phys. Rev. A*, vol. 95, p. 052308, May 2017.
[25] K. Nakahira, K. Kato, and T. S. Usuda, "Optimal discrimination of optical coherent states cannot always be realized by interfering with coherent light, photon counting, and feedback," *arXiv preprint quant-ph/1706.02125v2*, 2017.
[26] ——, "Generalized bipartite quantum state discrimination problems with sequential measurements," *arXiv preprint quant-ph/1707.04736v1*, 2017.
[27] S. Croke and S. M. Barnett, "Difficulty of distinguishing product states locally," *Phys. Rev. A*, vol. 95, no. 1, p. 012337, 2017.
[28] I. Ivonovic, "Geometrical description of quantal state determination," *J. Phys. A: Math. Gen.*, vol. 14, no. 12, p. 3241, 1981.
[29] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," *Int. J. Quant. Inf.*, vol. 8, no. 4, pp. 535–640, 2010.