Finding optimal measurements with inconclusive results using the problem of minimum error discrimination

Kenji Nakahira
Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Kanagawa 244-0817, Japan
and Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, Machida, Tokyo 194-8610, Japan

Tsuyoshi Sasaki Usuda
School of Information Science and Technology, Aichi Prefectural University, Nagakute, Aichi 480-1198, Japan
and Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, Machida, Tokyo 194-8610, Japan

Kentaro Kato
Quantum Communication Research Center, Quantum ICT Research Institute, Tamagawa University, Machida, Tokyo 194-8610, Japan
(Received 21 December 2014; published 24 February 2015)

We propose an approach for finding an optimal measurement for quantum state discrimination that maximizes the probability of correct detection with a fixed rate of inconclusive results. In our approach, we obtain the optimal measurement by solving the problem of finding a measurement that maximizes the weighted sum of the probability of correct detection and that of inconclusive results. We show that this problem can be reduced to the widely studied problem of finding a minimum error measurement for a certain state set, which maximizes the probability of correct detection without inconclusive results. As an application of our approach, we show how to solve the problem of finding an optimal measurement for qubit states with a fixed rate of inconclusive results.

DOI: 10.1103/PhysRevA.91.022331 PACS number(s): 03.67.Hk

I. INTRODUCTION

Quantum state discrimination is one of the fundamental problems in quantum information theory. The goal of this task is to distinguish between a given finite set of known states with given prior probabilities as well as possible. If the given states are not orthogonal, then perfect discrimination between them is impossible. Therefore, the problem is to find a measurement that minimizes or maximizes a certain optimality criterion. Since the basic framework of quantum state discrimination was established by the pioneering work of Helstrom, Holevo, and Yuen *et al.* [1–3], several optimization strategies have been proposed, such as Bayes strategy [1–3], Neymann-Pearson strategy [2], mutual information strategy [1], and minimax strategy [4].

A measurement maximizing the correct probability, which is called a minimum error measurement, has been well investigated. Necessary and sufficient conditions for a minimum error measurement have been formulated [1–3,5]. Closed-form analytical expressions for minimum error measurements have also been derived for some cases (see, e.g., [6–9]). In another strategy, we can consider a measurement that can achieve error-free, i.e., unambiguous, discrimination at the expense of allowing for a certain rate of inconclusive results [10–12]. An unambiguous measurement that maximizes the correct probability, which is called an optimal unambiguous measurement, has been investigated, and closed-form analytical expressions have been obtained for some cases (see, e.g., [13–16]). The use of an optimal unambiguous measurement can be a more efficient eavesdropping strategy on quantum cryptosystems [17,18].

Minimum error measurements and optimal unambiguous measurements can be interpreted as special cases of optimal inconclusive measurements (OIMs), which maximize the correct probability with a fixed failure, i.e., inconclusive, probability [19–21]. An OIM can be expected to guarantee that the correct probability is higher than that of an optimal unambiguous measurement while maintaining a sufficiently low error probability. Note that a measurement that maximizes the correct probability where a certain fixed error probability is allowed, which we call an optimal error margin measurement (OEM), has also been investigated [22–24]. An OEM has a close relationship with an OIM [25,26]. Although necessary and sufficient conditions for an OIM have been derived [20,21,27], obtaining an OIM is generally a more difficult task than obtaining a minimum error measurement or an optimal unambiguous measurement. In fact, closed-form analytical expressions of OIMs are not known except for some particular cases [25,26,28].

In this paper, we propose an approach for finding an OIM. In Sec. III, we present our approach, where we consider the problem of maximizing an objective function that is the weighted sum of the correct and inconclusive probabilities. We first obtain a measurement maximizing the objective function, which we call a modified optimal inconclusive measurement (MOIM), and then find a corresponding OIM. We show that the problem of finding an MOIM can be reduced to the problem of finding a minimum error measurement for a certain state set, and thus is relatively easy to solve. Moreover, we clarify the relationship between an MOIM and an OIM as well as an OEM. In Sec. IV, we show how to solve the problem of finding an MOIM and an OIM for qubit states.

II. OPTIMAL INCONCLUSIVE MEASUREMENT (OIM)

Let us consider discrimination between M quantum states represented by density operators $\tilde{\rho}_m$ $(m \in \mathcal{I}_M)$ with prior probabilities ξ_m, where $\mathcal{I}_k = \{0,1,\ldots,k-1\}$. $\tilde{\rho}_m$ satisfies $\tilde{\rho}_m \geqslant 0$ and $\mathrm{Tr}\,\tilde{\rho}_m = 1$, where $\hat{A} \geqslant 0$ and $\hat{A} \geqslant \hat{B}$ respectively denote that $\hat{A}$ and $\hat{A}-\hat{B}$ are positive semidefinite. Also, let $\hat{\rho}_m=\xi_m\tilde{\rho}_m$. $\hat{\rho}_m$ satisfies $\hat{\rho}_m \geqslant 0$, $\mathrm{Tr}\hat{\rho}_m=\xi_m>0$ for any m, and $\sum_{m=0}^{M-1}\mathrm{Tr}\hat{\rho}_m=1$. We refer to a set of quantum states, $\rho=\{\hat{\rho}_m : m\in\mathcal{I}_M\}$, as a quantum state set. Let $\mathcal{H}$ be the state space of ρ, which is the Hilbert space spanned by the supports of the operators $\{\hat{\rho}_m\}$.

A quantum measurement that may return an inconclusive answer can be described by a positive operator-valued measure (POVM) with $M+1$ detection operators, $\Pi=\{\hat{\Pi}_m : m\in\mathcal{I}_{M+1}\}$. We assume without loss of generality that each detection operator $\hat{\Pi}_m$ is on $\mathcal{H}$. Let $\mathcal{M}$ be the entire set of POVMs on $\mathcal{H}$ that consist of $M+1$ detection operators. Each $\Pi\in\mathcal{M}$ satisfies

$$\hat{\Pi}_m \geqslant 0, \quad \forall m\in\mathcal{I}_{M+1},$$
$$\sum_{m=0}^{M}\hat{\Pi}_m=\hat{1}, \tag{1}$$

where $\hat{1}$ is the identity operator on $\mathcal{H}$. The detection operator $\hat{\Pi}_m$ $(m\in\mathcal{I}_M)$ corresponds to identification of the state $\hat{\rho}_m$, while $\hat{\Pi}_M$ corresponds to the inconclusive answer.

The correct probability, $P_{\mathrm{C}}(\Pi)$, and the error probability, $P_{\mathrm{E}}(\Pi)$, can be expressed as

$$P_{\mathrm{C}}(\Pi)=\sum_{m=0}^{M-1}\mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_m),$$
$$P_{\mathrm{E}}(\Pi)=\sum_{\substack{m=0\\(m\neq k)}}^{M-1}\sum_{k=0}^{M-1}\mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_k). \tag{2}$$

The inconclusive probability, $P_{\mathrm{I}}(\Pi)$, can be represented as

$$P_{\mathrm{I}}(\Pi)=\sum_{m=0}^{M-1}\mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_M)=\mathrm{Tr}(\hat{G}\hat{\Pi}_M), \tag{3}$$

where $\hat{G}$ is the Gram operator of ρ expressed as

$$\hat{G}=\sum_{m=0}^{M-1}\hat{\rho}_m. \tag{4}$$

$P_{\mathrm{C}}(\Pi)+P_{\mathrm{E}}(\Pi)+P_{\mathrm{I}}(\Pi)=1$ always holds for any $\Pi\in\mathcal{M}$.

An OIM is a measurement maximizing the correct probability $P_{\mathrm{C}}(\Pi)$ under the constraint that $P_{\mathrm{I}}(\Pi)=p\in\mathbf{R}_{[0,1]}$, where $\mathbf{R}_{[a,b]}$ is the entire set of real numbers x satisfying $a\leqslant x\leqslant b$. Thus an OIM is an optimal solution of the following problem:

$$\begin{aligned}&\text{maximize} && \mathrm{P_C}(\Pi)\\ &\text{subject to} && \Pi\in\mathcal{M}_p,\end{aligned} \tag{5}$$

where $\mathcal{M}_p$ is the entire set of POVMs $\Pi\in\mathcal{M}$ satisfying $P_{\mathrm{I}}(\Pi)=p$. An optimal solution of the following problem is a minimum error measurement:

$$\begin{aligned}&\text{maximize} && \mathrm{P_C}(\Pi)\\ &\text{subject to} && \Pi\in\mathcal{M}.\end{aligned} \tag{6}$$

We can easily verify that a minimum error measurement satisfies $\hat{\Pi}_M=0$, which means $P_{\mathrm{I}}(\Pi)=0$. Thus a minimum error measurement is a special case of an OIM, which satisfies $p=0$. A measurement maximizing $P_{\mathrm{C}}(\Pi)$ under the constraint that $P_{\mathrm{E}}(\Pi)=0$ is an optimal unambiguous measurement. Now, let p_{u} be the inconclusive probability for an optimal unambiguous measurement. Then, an optimal unambiguous measurement can be regarded as a special case of an OIM, which satisfies $p=p_{\mathrm{u}}$.

An OEM is a measurement maximizing $P_{\mathrm{C}}(\Pi)$ under the constraint that $P_{\mathrm{E}}(\Pi)\leqslant\gamma$, for a given $\gamma\in\mathbf{R}_{[0,1]}$. γ is referred to as an error margin. Any OEM Π is an OIM with the inconclusive probability of $p=P_{\mathrm{I}}(\Pi)$, and any OIM Π' is an OEM with the error probability of $\gamma=P_{\mathrm{E}}(\Pi')$ [25,26]. Let $\tilde{\gamma}$ be the error probability of a minimum error measurement. Then, the error probability of an OEM with the error margin of γ is $\min(\gamma,\tilde{\gamma})$ [26]. Therefore, an OEM is an optimal solution of the following problem:

$$\begin{aligned}&\text{maximize} && \mathrm{P_C}(\Pi)\\ &\text{subject to} && \Pi\in\mathcal{M}^{(\mathrm{e})}_{\min(\gamma,\tilde{\gamma})},\end{aligned} \tag{7}$$

where $\mathcal{M}^{(\mathrm{e})}_{\gamma}$ is the entire set of POVMs $\Pi\in\mathcal{M}$ satisfying $P_{\mathrm{E}}(\Pi)=\gamma$.

The problem of Eq. (5) is a semidefinite programming, and its dual problem can be represented as [20]

$$\begin{aligned}&\text{minimize} && \mathrm{Tr}\hat{Z}-\mathrm{ap}\\ &\text{subject to} && \hat{Z}\geqslant\hat{\rho}_m(\forall m\in\mathcal{I}_M), \quad \hat{Z}\geqslant a\hat{G},\end{aligned} \tag{8}$$

where $\hat{Z}$ is a semidefinite positive operator on $\mathcal{H}$ and a is a real number. Similarly, the dual problem of the problem of Eq. (6) is represented as [5]

$$\begin{aligned}&\text{minimize} && \mathrm{Tr}\hat{X}\\ &\text{subject to} && \hat{X}\geqslant\hat{\rho}_m(\forall m\in\mathcal{I}_M),\end{aligned} \tag{9}$$

where $\hat{X}$ is a semidefinite positive operator on $\mathcal{H}$.

III. MODIFIED OPTIMAL INCONCLUSIVE MEASUREMENT (MOIM)

It is generally harder to find an OIM with the inconclusive probability $p>0$ than a minimum error measurement. We can see that the main reason is that an optimal solution of Eq. (5), Π, must satisfy $P_{\mathrm{I}}(\Pi)=p$ for a given p. Indeed, because of this constraint, we must find not only $\hat{Z}$ but also a when we try to find an optimal solution of Eq. (8). Similarly, due to the constraint of $P_{\mathrm{E}}(\Pi)=\gamma$, it is hard to find an OEM in many cases as well as an OIM. In this section, we first consider another optimization problem without these constraints. We next discuss the relationships between this problem and optimal problems for finding an OIM and an OEM. Using these relationships, we can obtain an OIM and an OEM from an MOIM.

A. Problem formulation

Let us consider the following problem:

$$\begin{aligned}&\text{maximize} && \mathrm{P_C}(\Pi)+\alpha\mathrm{P_I}(\Pi)\\ &\text{subject to} && \Pi\in\mathcal{M},\end{aligned} \tag{10}$$

where $\alpha\in\mathbf{R}$ is a constant ($\mathbf{R}$ is the entire set of real numbers). We call an optimal solution of Eq. (10) an MOIM and also call α an inconclusive degree. Equation (10) is identical to

Eq. (6) when $\alpha \leqslant 0$, since an optimal solution Π must satisfy $P_{\rm I}(\Pi) = 0$, i.e., $\hat{\Pi}_M = 0$, in this case. If α can be expressed as $\alpha = 1 - \epsilon$ with a sufficiently small $\epsilon > 0$, then an optimal solution of Eq. (10) is an optimal unambiguous measurement, if it exists. Moreover, in the case of $\alpha \geqslant 1$, the POVM $\Pi = \{\hat{\Pi}_m = 0 (\forall m \in \mathcal{I}_M), \hat{\Pi}_M = \hat{1}\}$ is an optimal solution of Eq. (10). Indeed, since $P_{\rm C}(\Pi) + P_{\rm I}(\Pi) \leqslant 1$ and $P_{\rm I}(\Pi) \leqslant 1$, we find that

$$P_{\rm C}(\Pi) + \alpha P_{\rm I}(\Pi) \leqslant 1 + (\alpha - 1) P_{\rm I}(\Pi) \leqslant \alpha, \qquad (11)$$

where the equalities hold when $P_{\rm I}(\Pi) = 1$.

The following proposition claims that an MOIM is equivalent to a minimum error measurement for a certain state set.

Proposition 1. An MOIM for ρ is equivalent to a minimum error measurement for $\rho' = \{\hat{\rho}'_m : m \in \mathcal{I}_{M+1}\}$, with

$$\begin{aligned} \hat{\rho}'_m &= \hat{\rho}_m/(1+\alpha), \quad m \in \mathcal{I}_M, \\ \hat{\rho}'_M &= \alpha \hat{G}/(1+\alpha), \end{aligned} \qquad (12)$$

where $\hat{G}$ is defined by Eq. (4).

Note that $1/(1+\alpha)$ in Eq. (12) is a normalizing constant such that $\sum_{m=0}^{M} {\rm Tr}\hat{\rho}'_m = 1$.

Proof. The objective function in Eq. (10) can be represented as

$$\begin{aligned} P_{\rm C}(\Pi) + \alpha P_{\rm I}(\Pi) &= \sum_{m=0}^{M-1} {\rm Tr}(\hat{\rho}_m \hat{\Pi}_m) + {\rm Tr}(\alpha \hat{G} \hat{\Pi}_M) \\ &= (1+\alpha) \sum_{m=0}^{M} {\rm Tr}(\hat{\rho}'_m \hat{\Pi}_m). \end{aligned} \qquad (13)$$

Thus, maximizing $P_{\rm C}(\Pi) + \alpha P_{\rm I}(\Pi)$ is equivalent to maximizing the correct probability for ρ', that is, $\sum_{m=0}^{M} {\rm Tr}(\hat{\rho}'_m \hat{\Pi}_m)$. ■

Since the dual problem of finding a minimum error measurement is Eq. (9), from Proposition 1, the dual problem of Eq. (10) can be obtained by minimizing ${\rm Tr}\hat{X}$ subject to $\hat{X} \geqslant \hat{\rho}'_m$ $(m \in \mathcal{I}_{M+1})$. Now, let $\hat{Z} = (1+\alpha)\hat{X}$; then this problem can be expressed by

$$\begin{aligned} &\text{minimize} \quad {\rm Tr}\hat{Z} \\ &\text{subject to} \quad \hat{Z} \geqslant \hat{\rho}_m (\forall m \in \mathcal{I}_M), \quad \hat{Z} \geqslant \alpha \hat{G}. \end{aligned} \qquad (14)$$

We call $\hat{Z}$ the Lagrange operator of this problem. Equation (14) is somewhat similar to Eq. (8). However, α in Eq. (14) is a given constant, while a in Eq. (8) is an unknown variable.

It is easier to obtain an MOIM than an OIM or an OEM in general, since the constraint in Eq. (10) is less restrictive. Indeed, an OIM and an OEM must satisfy $P_{\rm I}(\Pi) = p$ and $P_{\rm E}(\Pi) = \min(\gamma, \tilde{\gamma})$, respectively. We will show the relationships between the problem of Eq. (10) and optimal problems for finding an OIM and an OEM in Secs. III B and III C.

B. Relationship with an OIM

In this subsection, we derive the relationship between an MOIM and an OIM by showing the relationship between the inconclusive degree α in Eq. (10) and the inconclusive probability p in Eq. (5).

Let us define $P_{\rm C}^\circ(p)$ as

$$P_{\rm C}^\circ(p) = \begin{cases} \max_{\Pi \in \mathcal{M}_p} P_{\rm C}(\Pi), & p \in \mathbf{R}_{[0,1]}, \\ -\infty, & \text{otherwise}, \end{cases} \qquad (15)$$

that is, $P_{\rm C}^\circ(p)$ is the correct probability of an OIM Π with $P_{\rm I}(\Pi) = p$ in the case of $p \in \mathbf{R}_{[0,1]}$; otherwise, $P_{\rm C}^\circ(p) = -\infty$. We also define $F(\alpha)$ as

$$F(\alpha) = \max_{\Pi \in \mathcal{M}} P_{\rm C}(\Pi) + \alpha P_{\rm I}(\Pi), \qquad (16)$$

which is equivalent to the optimal value of the objective function in Eq. (10). Then, the following theorem holds.

Theorem 2. $P_{\rm C}^\circ(p)$ is concave and $F(\alpha)$ is convex. $F(\alpha)$ is the Legendre transformation of $-P_{\rm C}^\circ(p)$ and vice versa.

Proof. First, we show that $P_{\rm C}^\circ(p)$ is concave. According to the definition of $P_{\rm C}^\circ(p)$, it suffices to show that $P_{\rm C}^\circ(p)$ is concave in the range of $p \in \mathbf{R}_{[0,1]}$. Let Π and Π' be respectively OIMs with $P_{\rm I}(\Pi) = p \in \mathbf{R}_{[0,1]}$ and $P_{\rm I}(\Pi') = p' \in \mathbf{R}_{[0,1]}$. Also, let $Q = \{(\hat{\Pi}_m + \hat{\Pi}'_m)/2 : m \in \mathcal{I}_{M+1}\}$. We can easily verify that Q is a POVM satisfying

$$\begin{aligned} P_{\rm C}(Q) &= [P_{\rm C}(\Pi) + P_{\rm C}(\Pi')]/2 = [P_{\rm C}^\circ(p) + P_{\rm C}^\circ(p')]/2, \\ P_{\rm I}(Q) &= (p + p')/2. \end{aligned} \qquad (17)$$

From the definition of $P_{\rm C}^\circ(p)$, $P_{\rm C}^\circ[P_{\rm I}(Q)] \geqslant P_{\rm C}(Q)$ must hold. Thus we have that for any $p, p' \in \mathbf{R}_{[0,1]}$,

$$P_{\rm C}^\circ[(p+p')/2] \geqslant [P_{\rm C}^\circ(p) + P_{\rm C}^\circ(p')]/2, \qquad (18)$$

which means that $P_{\rm C}^\circ(p)$ is concave in the range of $p \in \mathbf{R}_{[0,1]}$.

Next, we show that $F(\alpha)$ is the Legendre transformation of $-P_{\rm C}^\circ(p)$. From Eq. (16), we obtain

$$\begin{aligned} F(\alpha) &= \max_{\Pi \in \mathcal{M}} P_{\rm C}(\Pi) + \alpha P_{\rm I}(\Pi) \\ &= \max_{p \in \mathbf{R}_{[0,1]}} \max_{\Pi \in \mathcal{M}_p} P_{\rm C}(\Pi) + \alpha p \\ &= \max_{p \in \mathbf{R}_{[0,1]}} P_{\rm C}^\circ(p) + \alpha p, \end{aligned} \qquad (19)$$

where the third line follows from Eq. (15). This means that $F(\alpha)$ is the Legendre transformation of $-P_{\rm C}^\circ(p)$.

Since $F(\alpha)$ is the Legendre transformation of the convex function $-P_{\rm C}^\circ(p)$, $F(\alpha)$ is convex and $-P_{\rm C}^\circ(p)$ is the Legendre transformation of $F(\alpha)$ [29]. ■

We will also show that $F(\alpha) = F(0)$ holds at least in the range of $\alpha \leqslant 1/M$, and $F(\alpha) = \alpha$ holds with $\alpha \geqslant 1$. From Eq. (16), $F(0)$ is equivalent to the correct probability of a minimum error measurement, that is, $F(0) = P_{\rm C}^\circ(0)$. Let $\hat{X}$ be an optimal solution of Eq. (9), which is the dual problem for obtaining a minimum error measurement. Then, ${\rm Tr}\hat{X} = P_{\rm C}^\circ(0)$ holds. Since $\hat{X} \geqslant \hat{\rho}_m$ holds for any $m \in \mathcal{I}_M$, we have that for any $\alpha \leqslant 1/M$,

$$\hat{X} - \alpha \hat{G} \geqslant \hat{X} - \frac{\hat{G}}{M} = \frac{1}{M} \sum_{m=0}^{M-1} (\hat{X} - \hat{\rho}_m) \geqslant 0. \qquad (20)$$

Therefore, $\hat{X}$ is also an optimal solution of Eq. (9), which yields $F(\alpha) = {\rm Tr}\hat{X} = F(0)$ for any $\alpha \leqslant 1/M$. Moreover, $F(\alpha) = \alpha$ holds for any $\alpha \geqslant 1$, since Eq. (11) holds and the equalities hold when $P_{\rm I}(\Pi) = 1$.

We also show another proof that $-P_{\rm C}^\circ(p)$ is the Legendre transformation of $F(\alpha)$ using the optimization problems of

Eqs. (5) and (10) and their duals. Let $\hat{Z}(\alpha)$ be an optimal solution of Eq. (14) as a function of α. The minimum value of the objective function in Eq. (8), which can be represented as $\min_{a\in\mathbf{R}} \mathrm{Tr}\hat{Z}(a) - ap$, is equivalent to $P_{\rm C}^{\circ}(p)$, since Eq. (8) is the dual problem of Eq. (5). [Note that Eq. (5) has a feasible solution only if $p \in \mathbf{R}_{[0,1]}$. However, we can see that $\min_{a\in\mathbf{R}} \mathrm{Tr}\hat{Z}(a) - ap = -\infty = P_{\rm C}^{\circ}(p)$ holds even if $p \notin \mathbf{R}_{[0,1]}$.] In contrast, since Eq. (14) is the dual problem of Eq. (10), we have $\mathrm{Tr}\hat{Z}(a) = F(a)$. Thus we obtain

$$P_{\rm C}^{\circ}(p) = \min_{a\in\mathbf{R}} F(a) - ap. \tag{21}$$

The right-hand side equals the Legendre transformation of $F(a)$ multiplied by -1.

Next, we discuss the relationship between an MOIM and an OIM. $-P_{\rm C}^{\circ}(p)$ is convex and thus semi-differentiable. Let $\alpha^-(p)$ and $\alpha^+(p)$ be the left and right derivatives of $-P_{\rm C}^{\circ}(p)$ at p, respectively. We show the following proposition.

Proposition 3. There exist the following relationships between an MOIM and an OIM.

(1) An MOIM Π° with the inconclusive degree α is an OIM with the inconclusive probability of $P_{\rm I}(\Pi^{\circ})$.

(2) An OIM with the inconclusive probability of $p \in \mathbf{R}_{[0,1]}$ is an MOIM with any inconclusive degree α satisfying $\alpha^-(p) \leqslant \alpha \leqslant \alpha^+(p)$.

Proof. (1) Let Π' be an OIM with the inconclusive probability of $P_{\rm I}(\Pi^{\circ})$, i.e., $P_{\rm I}(\Pi') = P_{\rm I}(\Pi^{\circ})$. Since Π° is an MOIM, $P_{\rm C}(\Pi^{\circ}) + \alpha P_{\rm I}(\Pi^{\circ}) \geqslant P_{\rm C}(\Pi') + \alpha P_{\rm I}(\Pi')$ holds, which gives $P_{\rm C}(\Pi^{\circ}) \geqslant P_{\rm C}(\Pi')$. Thus Π° is also an OIM with the inconclusive probability of $P_{\rm I}(\Pi^{\circ})$.

(2) Let $\Pi^{\bullet}$ be an OIM with the inconclusive probability of p. Let us consider an MOIM with the inconclusive degree α satisfying $\alpha^-(p) \leqslant \alpha \leqslant \alpha^+(p)$. Since $-P_{\rm C}^{\circ}(p)$ is convex, the tangent line to the function $-P_{\rm C}^{\circ}(p)$ with slope α passes through the contact point $[p, -P_{\rm C}^{\circ}(p)]$ (the tangent line may have another contact point). Thus, from Eq. (19), we find that

$$\begin{aligned} F(\alpha) &= \max_{p'\in\mathbf{R}_{[0,1]}} P_{\rm C}^{\circ}(p') + \alpha p' \\ &= P_{\rm C}^{\circ}(p) + \alpha p \\ &= P_{\rm C}(\Pi^{\bullet}) + \alpha P_{\rm I}(\Pi^{\bullet}). \end{aligned} \tag{22}$$

Therefore, $\Pi^{\bullet}$ is an MOIM with the inconclusive degree α. ∎

Here we say that p corresponds to α if there exists an OIM Π with the inconclusive probability p such that Π is also an MOIM with the inconclusive degree α. We also say that α corresponds to p if there exists an MOIM Π with the inconclusive degree α such that Π is also an OIM with the inconclusive probability p. From statement (2) of Proposition 3, p corresponds to all α satisfying $\alpha^-(p) \leqslant \alpha \leqslant \alpha^+(p)$. This implies that p corresponds to plural α when $\alpha^-(p) \neq \alpha^+(p)$. In contrast, α corresponds to all p such that $p^-(\alpha) \leqslant p \leqslant p^+(\alpha)$, where $p^-(\alpha)$ and $p^+(\alpha)$ are respectively the left and right derivatives of $F(\alpha)$ at α, which means that α may correspond to plural p.

Typical behavior of $P_{\rm C}^{\circ}(p)$ and $F(\alpha)$ is shown in Fig. 1(a), which is only illustrative and does not relate to any specific discrimination problem. In this example, $P_{\rm C}^{\circ}(p)$ is linear in the ranges of $0 \leqslant p \leqslant p_1$ and $p_2 \leqslant p \leqslant 1$ and is strictly concave

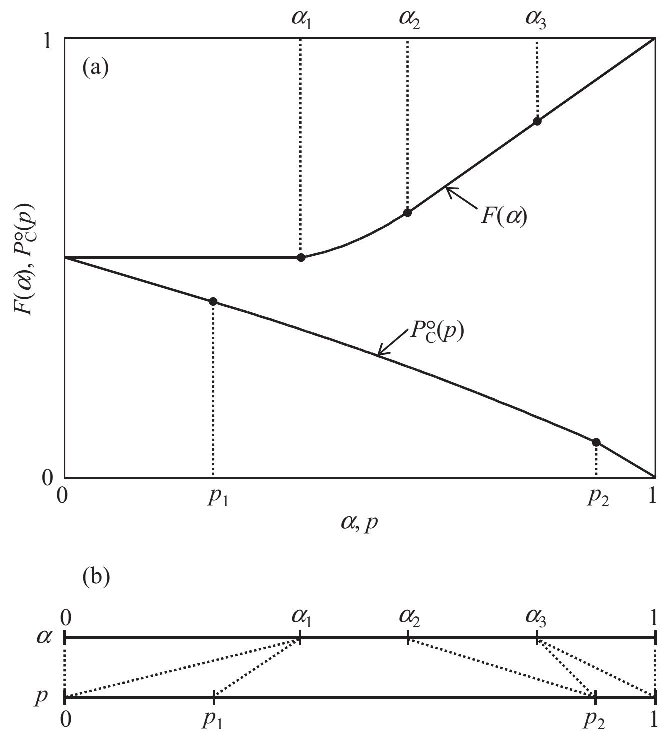

FIG. 1. Typical behavior of $P_{\rm C}^{\circ}(p)$ and $F(\alpha)$.

in the range of $p_1 < p < p_2$. $P_{\rm C}^{\circ}(p)$ is differentiable in the ranges of $0 < p < 1$ except at $p = p_2$. $F(\alpha)$, which is the Legendre transformation of $-P_{\rm C}^{\circ}(p)$, is linear in the ranges of $\alpha \leqslant \alpha_1$ and $\alpha \geqslant \alpha_2$ and is strictly convex in the range of $\alpha_1 < \alpha < \alpha_2$. $F(\alpha)$ is differentiable except at $\alpha = \alpha_1$ and $\alpha = \alpha_3$. Figure 1(b) depicts the correspondence between α and p in this example. This figure shows that, for example, any α with $0 \leqslant \alpha < \alpha_1$ corresponds to $p = 0$, and $\alpha = \alpha_1$ corresponds to any p with $0 \leqslant p \leqslant p_1$. $p = 0$ also corresponds to any α with $0 \leqslant \alpha \leqslant \alpha_1$. p at which $P_{\rm C}^{\circ}(p)$ is not differentiable (i.e., $p = 0$, p_2, and 1) corresponds to plural α. α at which $F(\alpha)$ is not differentiable (i.e., $\alpha = \alpha_1, \alpha_3$) corresponds to plural p. α with $\alpha_1 < \alpha < \alpha_2$ and p with $p_1 < p < p_2$ have one-to-one correspondence.

C. Relationship with an OEM

In a similar way as in the previous subsection, we can also derive the relationship between an MOIM and an OEM. Let us define $P_{\rm C}^{\circ({\rm e})}(\gamma)$ as

$$P_{\rm C}^{\circ({\rm e})}(\gamma) = \begin{cases} \max_{\Pi\in\mathcal{M}_\gamma^{({\rm e})}} P_{\rm C}(\Pi), & \gamma \in \mathbf{R}_{[0,1]}, \\ -\infty, & \text{otherwise}. \end{cases} \tag{23}$$

$P_{\rm C}^{\circ({\rm e})}(\gamma)$ is the correct probability of an OEM with the error margin γ in the case of $\gamma \in \mathbf{R}_{[0,\bar{\gamma}]}$. In the case of $\gamma \in \mathbf{R}_{[\bar{\gamma},1]}$, $P_{\rm C}^{\circ({\rm e})}(\gamma) = 1 - \gamma$ holds since the inconclusive probability is zero. We also define $F^{({\rm e})}(\beta)$ as

$$F^{({\rm e})}(\beta) = (1-\beta)F\left(-\frac{\beta}{1-\beta}\right) + \beta, \tag{24}$$

where $F(\alpha)$ is the function defined by Eq. (16). We can derive the following theorem.

Theorem 4. $P_{\rm C}^{\circ({\rm e})}(\gamma)$ is concave and $F^{({\rm e})}(\beta)$ is convex. $F^{({\rm e})}(\beta)$ is the Legendre transformation of $-P_{\rm C}^{\circ({\rm e})}(\gamma)$ and vice versa.

Proof. We can prove this theorem in a similar way to the proof of Theorem 2. First, we show that $P_{\rm C}^{\circ({\rm e})}(\gamma)$ is concave. According to the definition of $P_{\rm C}^{\circ({\rm e})}(\gamma)$, it suffices to show that $P_{\rm C}^{\circ({\rm e})}(\gamma)$ is concave in the range of $\gamma \in \mathbf{R}_{[0,1]}$. Let $\Pi \in \mathcal{M}_\gamma^{({\rm e})}$ and $\Pi' \in \mathcal{M}_{\gamma'}^{({\rm e})}$ be OEMs for $\gamma,\gamma' \in \mathbf{R}_{[0,1]}$.

Also, let $Q = \{(\hat\Pi_m + \hat\Pi'_m)/2 : m \in \mathcal{I}_{M+1}\}$. We can easily see that Q is a POVM satisfying

$$P_{\rm C}(Q) = \left[P_{\rm C}^{\circ({\rm e})}(\gamma) + P_{\rm C}^{\circ({\rm e})}(\gamma')\right]/2,$$
$$P_{\rm E}(Q) = (\gamma + \gamma')/2. \tag{25}$$

From the definition of $P_{\rm C}^{\circ({\rm e})}(\gamma)$, $P_{\rm C}^{\circ({\rm e})}[P_{\rm E}(Q)] \geqslant P_{\rm C}(Q)$ must hold. Thus we have that for any $\gamma,\gamma' \in \mathbf{R}_{[0,1]}$,

$$P_{\rm C}^{\circ({\rm e})}[(\gamma+\gamma')/2] \geqslant \left[P_{\rm C}^{\circ({\rm e})}(\gamma) + P_{\rm C}^{\circ({\rm e})}(\gamma')\right]/2, \tag{26}$$

which means that $P_{\rm C}^{\circ({\rm e})}(\gamma)$ is concave in the range of $\gamma \in \mathbf{R}_{[0,1]}$.

Next, we show that $F^{({\rm e})}(\beta)$ is the Legendre transformation of $-P_{\rm C}^{\circ({\rm e})}(\gamma)$. From Eqs. (16), (23), and (24), we obtain

$$\begin{aligned} F^{({\rm e})}(\beta) &= \max_{\Pi\in\mathcal{M}}(1-\beta)\left[P_{\rm C}(\Pi) - \frac{\beta}{1-\beta}P_{\rm I}(\Pi)\right] + \beta \\ &= \max_{\Pi\in\mathcal{M}}(1-\beta)P_{\rm C}(\Pi) - \beta P_{\rm I}(\Pi) + \beta \\ &= \max_{\Pi\in\mathcal{M}} P_{\rm C}(\Pi) + \beta P_{\rm E}(\Pi) \\ &= \max_{\gamma\in\mathbf{R}_{[0,1]}}\max_{\Pi\in\mathcal{M}_\gamma^{({\rm e})}} P_{\rm C}(\Pi) + \beta\gamma \\ &= \max_{\gamma\in\mathbf{R}_{[0,1]}} P_{\rm C}^{\circ({\rm e})}(\gamma) + \beta\gamma. \end{aligned} \tag{27}$$

Thus $F^{({\rm e})}(\beta)$ is the Legendre transformation of $-P_{\rm C}^{\circ({\rm e})}(\gamma)$.

Since $-P_{\rm C}^{\circ({\rm e})}(\gamma)$ is convex, $F^{({\rm e})}(\beta)$ is also convex, and thus $-P_{\rm C}^{\circ({\rm e})}(\gamma)$ is the Legendre transformation of $F^{({\rm e})}(\beta)$ [29]. ■

IV. MOIM FOR QUBIT STATES

Deconinck *et al.* show a method for finding a minimum error measurement for qubit states using the dual problem and the Bloch sphere representation of qubits [30]. In this section, we extend their method to an MOIM for qubit states. An OIM with any inconclusive probability can be obtained from an MOIM, as described in the previous section. We also consider an MOIM and an OIM for a three mirror symmetric state set, as an example.

A. Geometric representation

Let us consider a qubit state set $\rho = \{\hat\rho_m : m \in \mathcal{I}_M\}$. $\hat\rho_m$ can be expressed as

$$\hat\rho_m = \tfrac{1}{2}(\xi_m \hat1 + \vec\rho_m\cdot\vec\sigma), \tag{28}$$

where $\xi_m = {\rm Tr}\hat\rho_m$ and $\vec\rho_m \in \mathbf{R}^3$. $\vec\sigma = (\hat\sigma_x,\hat\sigma_y,\hat\sigma_z)$ are the Pauli matrices. We denote the expression of Eq. (28), which is called the Bloch sphere representation, as $\hat\rho_m \sim (\xi_m,\vec\rho_m)$. $(\xi_m,\vec\rho_m) \in \mathbf{R}^4$ holds. Similarly, an optimal solution of Eq. (14), $\hat Z$, and the operator $\alpha\hat G$ can be written as

$$\hat Z = \tfrac{1}{2}(Z_t\hat1 + \vec Z\cdot\vec\sigma), \quad Z_t = {\rm Tr}\hat Z,$$
$$\alpha\hat G = \tfrac{1}{2}(\alpha\hat1 + \alpha\vec G\cdot\vec\sigma), \quad \vec G = \sum_{m=0}^{M-1}\vec\rho_m, \tag{29}$$

that is, $\hat Z \sim (Z_t,\vec Z) \in \mathbf{R}^4$ and $\alpha\hat G \sim (\alpha,\alpha\vec G) \in \mathbf{R}^4$.

Let us define

$$\mathcal{C}(\hat B) = \{(t,\vec r) : |t - B_t| \geqslant |\vec r - \vec B|\},$$
$$\mathcal{C}_-(\hat B) = \mathcal{C}(\hat B)\cap\{(t,\vec r) : t \leqslant B_t\}, \tag{30}$$
$$\mathcal{C}_+(\hat B) = \mathcal{C}(\hat B)\cap\{(t,\vec r) : t \geqslant B_t\}$$

for an operator $\hat B \geqslant 0$, where $\hat B \sim (B_t,\vec B)$. $\mathcal{C}(\hat B)$ can be interpreted as the light cone of $(B_t,\vec B)$. Similarly, $\mathcal{C}_-(\hat B)$ and $\mathcal{C}_+(\hat B)$ can respectively be interpreted as the past and future light cones. For any $\hat A \geqslant 0$, $\hat Z \geqslant \hat A$ is equivalent to $(A_t,\vec A) \in \mathcal{C}_-(\hat Z)$, where $\hat A \sim (A_t,\vec A)$ [30]. Thus the optimization problem of Eq. (14) can be rewritten as the following conic quadratic program for $\hat Z \sim (Z_t,\vec Z)$:

$$\begin{aligned} &\text{minimize} \quad Z_t \\ &\text{subject to} \quad (\xi_m,\vec\rho_m) \in \mathcal{C}_-(\hat Z)(\forall m \in \mathcal{I}_M), \\ &\qquad\qquad\quad (\alpha,\alpha\vec G) \in \mathcal{C}_-(\hat Z). \end{aligned} \tag{31}$$

In the same way as in Ref. [30], we represent each state $\hat\rho_m \sim (\xi_m,\vec\rho_m)(m \in \mathcal{I}_M)$ by a three-dimensional ball (denoted as $\mathcal{B}_m$) with center $\vec\rho_m$ and radius $\xi_m - \xi_{\rm min}$, where $\xi_{\rm min} = \min_{m\in\mathcal{I}_M}\xi_m$. We also represent $\alpha\hat G \sim (\alpha,\alpha\vec G)$ by a ball (denoted as $\mathcal{B}_M$) with center $\alpha\vec G$ and radius $\alpha - \xi_{\rm min}$ (if $\alpha < \xi_{\rm min}$, then $\mathcal{B}_M$ is the empty set). A ball $\mathcal{B}_m$ with $m \in \mathcal{I}_M$ (or $\mathcal{B}_M$) is the intersection of the past light cone $\mathcal{C}_-(\hat\rho_m)$ [or $\mathcal{C}_-(\alpha\hat G)$] and the hyperplane with time coordinate equal to $\xi_{\rm min}$.

The problem of Eq. (31) can also be rewritten as the following proposition.

Proposition 5. We consider an MOIM with the inconclusive degree α for a qubit state set $\rho = \{\hat\rho_m : m \in \mathcal{I}_M\}$. Let $\mathcal{B}_m$ $(m \in \mathcal{I}_M)$ and $\mathcal{B}_M$ be balls in $\mathbf{R}^3$ corresponding to $\hat\rho_m$ and $\alpha\hat G$, respectively. Also, let $\mathcal{B}_Z$ be the ball of minimum radius R and center $\vec Z$ that includes all of the $M+1$ balls $\mathcal{B}_m$ $(m \in \mathcal{I}_{M+1})$, i.e., $\mathcal{B}_m \cap \mathcal{B}_Z = \mathcal{B}_m$ for any $m \in \mathcal{I}_{M+1}$. Then, $\hat Z$ expressed by $\hat Z \sim (R + \xi_{\rm min},\vec Z)$ is an optimal solution of Eq. (14), where $\xi_{\rm min} = \min_{m\in\mathcal{I}_M}\xi_m$. Note that this proposition implies that if $\alpha \leqslant \xi_{\rm min}$, then the problem of finding an MOIM is equivalent to that of finding a minimum error measurement, since $\mathcal{B}_M$ is the empty set. This agrees with the fact that $F(\alpha) = F(0)$ holds in the range of $\alpha \leqslant \xi_{\rm min} \leqslant 1/M$, as described in Sec. III B. Proposition 5 is somewhat different from Proposition 1 of Ref. [30], where $\mathcal{B}_m$ is the intersection of the future cone $\mathcal{C}_+(\hat\rho_m)$ and the hyperplane with time coordinate equal to $\max_{m\in\mathcal{I}_M}\xi_m$. When we consider an MOIM, our expression is simpler than that in Ref. [30], where the expression should be changed when $\alpha > \max_{m\in\mathcal{I}_M}\xi_m$.

From Proposition 5, we can find a Lagrange operator $\hat Z$ of an MOIM for a qubit state set using a geometric representation. An MOIM Π can be derived from $\hat Z$ in the same way as in Ref. [30]. The detection operator $\hat\Pi_m$ satisfies $\hat\Pi_m \neq 0$ only if the past light cone $\mathcal{C}_-(\hat Z)$ includes $\hat\rho_m$ on its boundary [30].

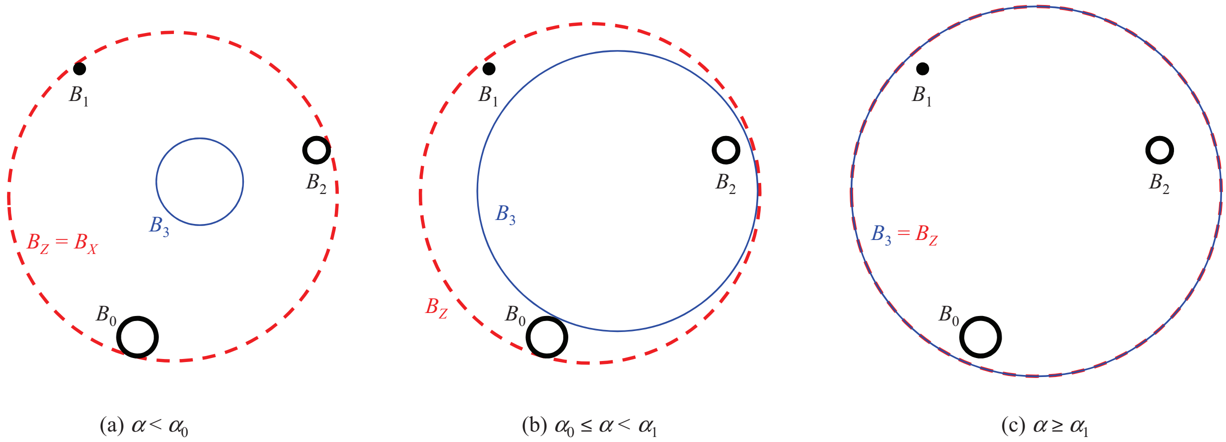

FIG. 2. (Color online) Example of a geometric representation for the problem of finding an MOIM for a three qubit state set $\rho = \{\hat{\rho}_m : m \in \mathcal{I}_3\}$ (projected on the two-dimensional plane that includes the centers of three balls $\mathcal{B}_0$, $\mathcal{B}_1$, and $\mathcal{B}_2$). $\mathcal{B}_m$ $(m \in \mathcal{I}_3)$ (in black), $\mathcal{B}_3$ (blue), and $\mathcal{B}_Z$ (red, dashed) respectively correspond to $\hat{\rho}_m$, $\alpha\hat{G}$, and $\hat{Z}$. (a) $\mathcal{B}_3$ is not tangent to $\mathcal{B}_Z$. (b) $\mathcal{B}_3$ is tangent to $\mathcal{B}_Z$ and $\mathcal{B}_3 \neq \mathcal{B}_Z$. (c) $\mathcal{B}_3 = \mathcal{B}_Z$.

Note again that an OIM and an error margin measurement can respectively be derived from Theorems 2 and 4 once we find an MOIM.

Here we consider a three qubit state set $\rho = \{\hat{\rho}_m : m \in \mathcal{I}_3\}$. We can restrict ourselves to the two-dimensional plane that includes the centers of three balls $\mathcal{B}_0$, $\mathcal{B}_1$, and $\mathcal{B}_2$. Note that this plane also includes the center of the ball $\mathcal{B}_3$ since $\vec{G} = \sum_{m=0}^{2} \vec{\rho}_m$ holds. Figure 2 shows $\mathcal{B}_m$ $(m \in \mathcal{I}_3)$ (in black), $\mathcal{B}_3$ (blue), and $\mathcal{B}_Z$ (red, dashed). The radius of $\mathcal{B}_3$ increases as α increases. Let $\mathcal{B}_X$ be the minimum circle including three balls $\mathcal{B}_0, \mathcal{B}_1$, and $\mathcal{B}_2$. $\mathcal{B}_X$ corresponds to the Lagrange operator $\hat{X}$ of a minimum error measurement. Also, let α_0 be the inconclusive degree α such that $\mathcal{B}_3$ satisfies $\mathcal{B}_3 \subset \mathcal{B}_X$ and is tangent to $\mathcal{B}_X$. Let α_1 be the minimum α such that $\mathcal{B}_3$ includes three balls $\mathcal{B}_0$, $\mathcal{B}_1$, and $\mathcal{B}_2$. In the case of $\alpha < \alpha_0$, since $\mathcal{B}_X$ includes $\mathcal{B}_3$, $\mathcal{B}_Z = \mathcal{B}_X$ holds [Fig. 2(a)]. In the case of $\alpha_0 \leqslant \alpha < \alpha_1$, $\mathcal{B}_Z$ is tangent to $\mathcal{B}_3$ and increases as α increases [Fig. 2(b)]. In the case of $\alpha \geqslant \alpha_1$, since $\mathcal{B}_3$ is the minimum ball that includes four balls $\mathcal{B}_m$ $(m \in \mathcal{I}_4)$, $\mathcal{B}_Z = \mathcal{B}_3$ holds [Fig. 2(c)].

In the case of $M \geqslant 4$, we can also consider a similar geometric representation as that of Ref. [30]. Deconinck *et al.* show an efficient algorithm for finding a minimum error measurement for a qubit state set with any M [30]. This algorithm can be applied to find an MOIM since, from Proposition 1, this problem can be reduced to the problem of finding a minimum error measurement.

B. Example of three mirror symmetric state set

We consider the problem of finding an MOIM for a three state set $\rho = \{\hat{\rho}_m : m \in \mathcal{I}_3\}$ that has certain symmetries. Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis and assume that ρ_m can be expressed as

$$\begin{aligned} \rho_0 &= (1-2\xi)[\eta_0 \hat{1} + (1-\eta_0)\,|0\rangle], \\ \rho_1 &= \xi[\eta_1 \hat{1} + (1-\eta_1)(\cos\theta\,|0\rangle + \sin\theta\,|1\rangle)], \\ \rho_2 &= \xi[\eta_1 \hat{1} + (1-\eta_1)(\cos\theta\,|0\rangle - \sin\theta\,|1\rangle)], \end{aligned} \tag{32}$$

where $\xi \in \mathbf{R}_{[0,1/2]}$, $\eta_k \in \mathbf{R}_{[0,1]}(k \in \{0,1\})$, and $\theta \in \mathbf{R}$. Assume $\sin\theta \neq 0$. We call such a state set a three mirror symmetric state set, which is a slight generalization of that described in Ref. [31]. Indeed, in the case in which $\hat{\rho}_m$ is a pure state for any $m \in \mathcal{I}_3$, i.e., $\eta_0 = \eta_1 = 0$, our definition is the same as that in Ref. [31]. Let $\vec{\rho}_m = (x_m, y_m, z_m)$. We can easily find that $x_0 = y_0 = y_1 = y_2 = 0$, $z_0 \geqslant 0$, $x_2 = -x_1 \neq 0$, $z_2 = z_1$, and $\xi_2 = \xi_1$. Thus a set of three balls $\{\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2\}$ is symmetric about the plane $x = 0$, and their centers are on the plane $y = 0$. Moreover, $\vec{G}$ can be represented as $\vec{G} = (0,0,G_z)$, where $G_z = z_0 + 2z_1$.

Assume that we know the Lagrange operator of a minimum error measurement, $\hat{X} \sim (X_t, \vec{X})$ [i.e., an optimal solution of Eq. (9)], which can be obtained using the method described in Ref. [30]. Using $(X_t, \vec{X})$, we will find the Lagrange operator of an MOIM, $\hat{Z} \sim (Z_t, \vec{Z})$, with any inconclusive degree α. From the symmetries of ρ, $\vec{X}$ and $\vec{Z}$ can respectively be represented as $\vec{X} = (0,0,X_z)$ and $\vec{Z} = (0,0,Z_z)$.

For simplicity, we only consider the case in which a minimum error measurement Π satisfies $\hat{\Pi}_m \neq 0$ $(\forall m \in \mathcal{I}_3)$; otherwise, we can also find $\hat{Z}$ in the same way as described below. We can use Eq. (31) to compute $\hat{Z}$ as well as Proposition 5. Figure 3 shows the Bloch sphere representation of ρ in the cross section of the two-dimensional plane $x = y = 0$. Note that $\hat{\rho}_0$ is on the plane $x = y = 0$, while $\hat{\rho}_1$ or $\hat{\rho}_2$ is not.

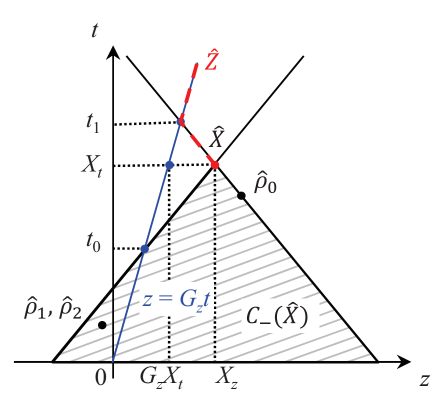

FIG. 3. (Color online) Bloch sphere representation of a three mirror symmetric state set in the cross section of the two-dimensional plane $x = y = 0$ (in the case of $X_z \geqslant G_z X_t$).

Since $\hat{\Pi}_m \neq 0$ ($\forall m \in \mathcal{I}_3$), the past light cone $\mathcal{C}_-(\hat{X})$, which is indicated by hatched shading in Fig. 3, includes $\hat{\rho}_0$, $\hat{\rho}_1$, and $\hat{\rho}_2$ on its boundary. Moreover, since $\alpha\hat{G} \sim (\alpha,(0,0,G_z\alpha))$, $\alpha\hat{G}$ is on the line $x = y = 0$, $z = G_z t$ (in blue). Let us denote the t coordinates of the two cross-points on $x = y = 0$ between the line $z = G_z t$ and the boundary of the cone $\mathcal{C}(\hat{X})$ as t_0 and t_1 ($t_0 \leqslant t_1$), which are the solutions of the following equation:

$$|t - X_t| = |G_z t - X_z|. \tag{33}$$

In the case of $\alpha \leqslant t_0$, since $\mathcal{C}_-(\hat{X})$ includes $\alpha\hat{G}$, $\hat{X} \geqslant \alpha\hat{G}$ holds. Thus $\hat{Z} = \hat{X}$ holds in this case. In the case of $\alpha > t_0$, the way of computing $\hat{Z}$ depends on whether $X_z \geqslant G_z X_t$ or not.

1. *Case of $X_z \geqslant G_z X_t$*

First, we consider the case of $\alpha > t_0$ and $X_z \geqslant G_z X_t$. We can see that $\hat{Z} \sim (Z_t,\vec{Z})$ is the point of minimum Z_t such that $\mathcal{C}_-(\hat{Z})$ includes $\hat{\rho}_0$ and $\alpha\hat{G}$ since such $\mathcal{C}_-(\hat{Z})$ also includes $\hat{\rho}_1$ and $\hat{\rho}_2$. If $\alpha > t_1$, then since $\mathcal{C}_-(\alpha\hat{G})$ includes $\hat{\rho}_0$, $\hat{Z} = \alpha\hat{G}$ holds. If $t_0 < \alpha \leqslant t_1$, then since $\hat{\rho}_0$ and $\alpha\hat{G}$ are tangent to $\mathcal{C}_-(\hat{Z})$, $\hat{Z}$ is on the cross section of the boundaries of the future light cones $\mathcal{C}_+(\hat{\rho}_0)$ and $\mathcal{C}_+(\alpha\hat{G})$. It follows that $\hat{Z}$ is also on the boundaries of $\mathcal{C}_+(\hat{X})$. The trajectory of $\hat{Z}$ is shown in Fig. 3 in red dashed line. After some algebra, $\hat{Z}$ can be written as follows:

$$(Z_t,Z_z) = \begin{cases} (X_t,X_z), & \alpha \leqslant t_0, \\ (Z_t(\alpha),Z_z(\alpha)), & t_0 < \alpha \leqslant t_1, \\ (\alpha,\alpha G_z), & \text{otherwise}, \end{cases}$$
$$Z_t(\alpha) = X_t + \frac{\alpha - t_0}{t_1 - t_0}(t_1 - X_t), \tag{34}$$
$$Z_z(\alpha) = X_z + \frac{\alpha - t_0}{t_1 - t_0}(t_1 G_z - X_z).$$

From Theorem 2, the correct probability of an OIM, $P_{\mathrm{C}}^{\circ}(p)$, can be obtained by performing the Legendre transformation of $F(\alpha) = Z_t$, which is given by Eq. (34), with respect to α followed by multiplying -1. $P_{\mathrm{C}}^{\circ}(p)$ can be expressed by

$$P_{\mathrm{C}}^{\circ}(p) = \begin{cases} -t_0 p + X_t, & 0 \leqslant p \leqslant p_0, \\ -t_1 p + t_1, & p_0 < p \leqslant 1, \end{cases}$$
$$p_0 = \frac{t_1 - X_t}{t_1 - t_0}. \tag{35}$$

The correct probability of an OEM, $P_{\mathrm{C}}^{\circ(\mathrm{e})}(\gamma)$, can also be obtained by performing the Legendre transformation of $F^{(\mathrm{e})}(\beta)$ of Eq. (24) with $F(\alpha) = Z_t$ followed by multiplying -1.

2. *Case of $X_z < G_z X_t$*

Next, we consider the case of $\alpha > t_0$ and $X_z < G_z X_t$. Since $\mathcal{C}_-(\alpha\hat{G})$ includes $\hat{\rho}_0$, if $\mathcal{C}_-(\hat{Z})$ includes $\alpha\hat{G}$, then $\mathcal{C}_-(\hat{Z})$ also includes $\hat{\rho}_0$. Thus $\hat{Z} \sim (Z_t,\vec{Z})$ is the point of minimum Z_t such that $\mathcal{C}_-(\hat{Z})$ includes $\hat{\rho}_1$, $\hat{\rho}_2$, and $\alpha\hat{G}$. Moreover, $\hat{Z} = \alpha\hat{G}$ holds if $\alpha \geqslant \alpha_1$, where α_1 is the minimum inconclusive degree α such that $\mathcal{C}_-(\alpha\hat{G})$ includes $\hat{\rho}_1$ and $\hat{\rho}_2$.

We now consider the case of $t_0 < \alpha < \alpha_1$. Figure 4 shows $\mathcal{B}_m$ ($m \in \mathcal{I}_4$) and $\mathcal{B}_Z$ in the cross section of the plane $(y,t) = (0,\xi_{\min})$.

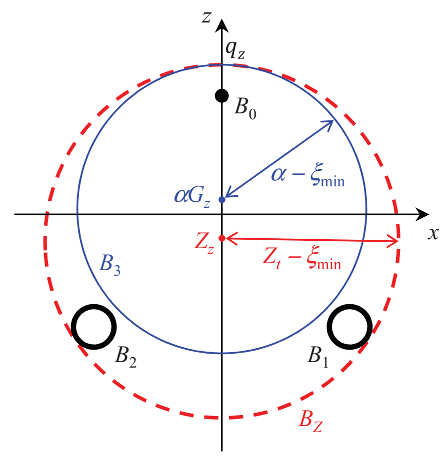

FIG. 4. (Color online) Bloch sphere representation of a three mirror symmetric state set in the cross section of the plane $(y,t) = (0,\xi_{\min})$ (in the case of $X_z < G_z X_t$).

The ball $\mathcal{B}_Z$ is tangent to $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$. Let us denote the maximum z coordinate of the points in the ball $\mathcal{B}_3$ as q_z. Since the ball $\mathcal{B}_3$ has radius $\alpha - \xi_{\min}$ and center $(x,z) = (0,\alpha G_z)$, $q_z = \alpha(1 + G_z) - \xi_{\min}$ holds. Since q_z is also the maximum z coordinate of the points in the ball $\mathcal{B}_Z$, the radius of the ball $\mathcal{B}_Z$, $Z_t - \xi_{\min}$, is equal to $q_z - Z_z$. Thus Z_t can be expressed using Z_z as

$$Z_t = q_z - Z_z + \xi_{\min} = \alpha(1 + G_z) - Z_z. \tag{36}$$

Here we will compute Z_z. Since $\mathcal{B}_Z$ is tangent to $\mathcal{B}_1$, the distance between the center of $\mathcal{B}_Z$, i.e., $(x,z) = (0,Z_z)$, and the center of $\mathcal{B}_1$, i.e., $(x,z) = (x_1,z_1)$, is equivalent to the difference between the radiuses of $\mathcal{B}_Z$ and $\mathcal{B}_1$, i.e., $Z_t - \xi_1$, which yields

$$\sqrt{x_1^2 + (z_1 - Z_z)^2} = Z_t - \xi_1. \tag{37}$$

Substituting Eq. (36) into Eq. (37) and solving Z_z yields

$$Z_z = \frac{x_1^2 + z_1^2 - [\alpha(1 + G_z) - \xi_1]^2}{2[z_1 - \alpha(1 + G_z) + \xi_1]}. \tag{38}$$

Using Eqs. (36) and (38), we can compute $\hat{Z} \sim (Z_t,\vec{Z})$ for $t_0 < \alpha < \alpha_1$.

In the same way as in the case of $X_z \geqslant G_z X_t$, the analytical expression of $P_{\mathrm{C}}^{\circ}(p)$ can be obtained by performing the Legendre transformation of Z_t with respect to α followed by multiplying -1, although it is somewhat complicated (here we do not show it explicitly). The correct probability of an OEM, $P_{\mathrm{C}}^{\circ(\mathrm{e})}(\gamma)$, can also be obtained in the same way.

Figure 5(a) depicts an example of $P_{\mathrm{C}}^{\circ}(p)$ and $F(\alpha)$ in the case of $\xi = 1/3$, $\eta_0 = \eta_1 = 0$, and $\theta = 0.26\pi$. In this case, $t_0 \sim 0.52$ and $\alpha_1 \sim 0.74$ hold. $F(\alpha) = X_t \sim 0.67$ in the range of $0 \leqslant \alpha \leqslant t_0$ and $F(\alpha) = \alpha$ in the range of $\alpha \geqslant \alpha_1$. $P_{\mathrm{C}}^{\circ}(p)$ is linear in the ranges of $0 \leqslant p \leqslant p_1$ and $p_2 \leqslant p \leqslant 1$, where $p_1 = p^+(t_0) \sim 0.06$ and $p_2 = p^-(\alpha_1) \sim 0.48$ [$p^-(\alpha)$ and $p^+(\alpha)$ are respectively the left and right derivatives of $F(\alpha)$]. $P_{\mathrm{C}}^{\circ}(p)$ is strictly concave in the range of $p_1 < p < p_2$. Figure 5(b) shows the correspondence between α and p, which indicates that $\alpha = t_0$ corresponds to any p with $0 \leqslant p \leqslant p_1$, and $\alpha = \alpha_1$ corresponds to any p with $p_2 \leqslant p \leqslant 1$.

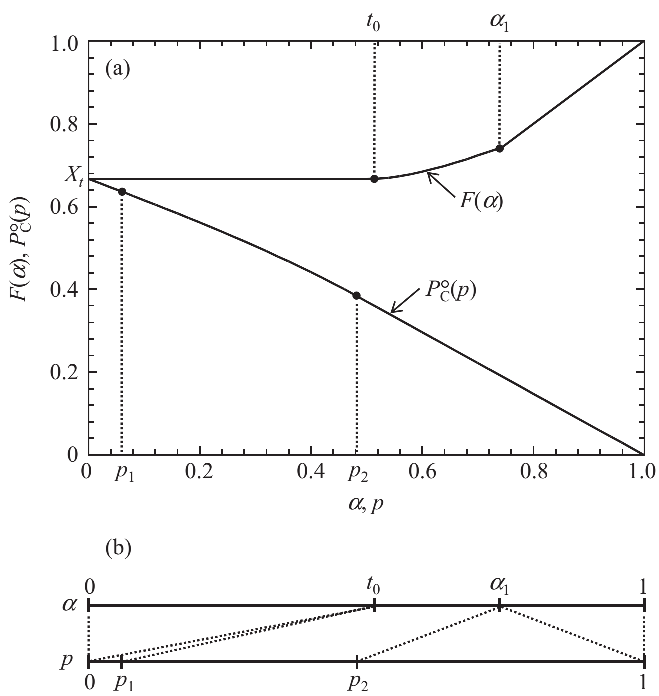

FIG. 5. $P^{\circ}_{\mathrm{C}}(p)$ and $F(\alpha)$ for a three mirror symmetric state set with $\xi = 1/3$, $\eta_0 = \eta_1 = 0$, and $\theta = 0.26\pi$, which satisfies $X_z < G_z X_t$.

α with $t_0 < \alpha < \alpha_1$ and p with $p_1 < p < p_2$ have one-to-one correspondence.

V. CONCLUSION

We proposed an approach for finding an optimal inconclusive measurement (OIM). In our approach, we first obtain a modified optimal inconclusive measurement (MOIM), which maximizes the weighted sum of the correct and inconclusive probabilities, and then find a corresponding OIM. We showed that the problem of finding an MOIM can be reduced to the problem of finding a minimum error measurement for a certain state set. We also showed that the correct probabilities of an OIM and an optimal error margin measurement can be derived by performing the Legendre transformation of the maximum weighted sum of the correct and inconclusive probabilities. It follows from these results that an OIM with any inconclusive probability can be obtained if an MOIM with any inconclusive degree is computed. We finally showed how to solve the problem of finding an OIM for qubit states.

ACKNOWLEDGMENTS

We are grateful to O. Hirota of Tamagawa University and J. Tyson for support. T.S.U. was supported (in part) by JSPS KAKENHI (Grant No. 24360151).

[1] A. S. Holevo, J. Multivar. Anal. **3**, 337 (1973).
[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[3] H. P. Yuen, K. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theor. **21**, 125 (1975).
[4] O. Hirota and S. Ikehara, Trans. IECE Jpn. **E65**, 627 (1982).
[5] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theor. **49**, 1007 (2003).
[6] V. P. Belavkin, Stochastics **1**, 315 (1975).
[7] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[8] T. S. Usuda, I. Takumi, M. Hata, and O. Hirota, Phys. Lett. A **256**, 104 (1999).
[9] Y. C. Eldar and G. D. Forney, Jr., IEEE Trans. Inf. Theor. **47**, 858 (2001).
[10] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[11] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[12] A. Peres, Phys. Lett. A **128**, 19 (1988).
[13] Y. C. Eldar, IEEE Trans. Inf. Theor. **49**, 446 (2003).
[14] U. Herzog, Phys. Rev. A **75**, 052309 (2007).
[15] M. Kleinmann, H. Kampermann, and D. Bruß, J. Math. Phys. **51**, 032201 (2010).
[16] J. A. Bergou, U. Futschik, and E. Feldman, Phys. Rev. Lett. **108**, 250502 (2012).
[17] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[18] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).
[19] A. Chefles and S. M. Barnett, J. Mod. Opt. **45**, 1295 (1998).
[20] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).
[21] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).
[22] M. A. P. Touzel, R. B. A. Adamson, and A. M. Steinberg, Phys. Rev. A **76**, 062314 (2007).
[23] A. Hayashi, T. Hashimoto, and M. Horibe, Phys. Rev. A **78**, 012333 (2008).
[24] H. Sugimoto, T. Hashimoto, M. Horibe, and A. Hayashi, Phys. Rev. A **80**, 052322 (2009).
[25] U. Herzog, Phys. Rev. A **86**, 032314 (2012).
[26] K. Nakahira, T. S. Usuda, and K. Kato, Phys. Rev. A **86**, 032316 (2012).
[27] K. Nakahira and T. S. Usuda, Phys. Rev. A **87**, 012308 (2013).
[28] E. Bagan, R. Muñoz-Tapia, G. A. Olivares-Renteria, and J. A. Bergou, Phys. Rev. A **86**, 040303 (2012).
[29] J.-B. Hiriart-Urruty and C. Lemaréchal, *Fundamentals of Convex Analysis* (Springer-Verlag, New York, 2001).
[30] M. E. Deconinck and B. M. Terhal, Phys. Rev. A **81**, 062304 (2010).
[31] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter, Phys. Rev. A **65**, 052308 (2002).