Upper and lower bounds on optimal success probability of quantum state discrimination with and without inconclusive results

Kenji Nakahira,[1] Tsuyoshi Sasaki Usuda,[1,2] and Kentaro Kato[1]

[1]*Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University, Machida, Tokyo 194-8610, Japan*

[2]*School of Information Science and Technology, Aichi Prefectural University, Nagakute, Aichi 480-1198, Japan*

(Received 29 September 2017; published 8 January 2018)

We propose upper and lower bounds on the maximum success probability for discriminating given quantum states. The proposed upper bound is obtained from a suboptimal solution to the dual problem of the corresponding optimal state discrimination problem. We also give a necessary and sufficient condition for the upper bound to achieve the maximum success probability; the proposed lower bound can be obtained from this condition. It is derived that a slightly modified version of the proposed upper bound is tighter than that proposed by Qiu *et al.* [Phys. Rev. A **81**, 042329 (2010)]. Moreover, we propose upper and lower bounds on the maximum success probability with a fixed rate of inconclusive results. The performance of the proposed bounds is evaluated through numerical experiments.

DOI: 10.1103/PhysRevA.97.012103

I. INTRODUCTION

Discrimination of quantum states is a basic and important problem in the field of quantum information theory. The objective of this work is to distinguish between a given finite set of known quantum states as well as possible. As is well known, no measurement can discriminate perfectly between nonorthogonal states; thus, the problem is to find a measurement that minimizes or maximizes a certain optimality criterion. Since the pioneering work of Helstrom, Holevo, and Yuen *et al.* [1–3], quantum state discrimination problems with several criteria have been widely investigated.

The success probability is one of the most used criteria for discriminating quantum states. A quantum measurement maximizing the success probability, which is called a minimum-error measurement, has been widely investigated. However, closed-form analytical expressions for minimum-error measurements have only been obtained in some particular cases (e.g., Refs. [4–10]). Another criterion is based on the inconclusive probability; a quantum measurement maximizing the success probability with a fixed failure (i.e., inconclusive) probability which is called an optimal inconclusive measurement, has also been investigated [11–13]. A minimum-error measurement and an unambiguous measurement that maximizes the success probability can be regarded as special cases of optimal inconclusive measurements. Obtaining an optimal inconclusive measurement is generally a more difficult task than obtaining a minimum-error measurement. In fact, closed-form analytical expressions for optimal inconclusive measurements are only known for very special cases (e.g., Refs. [14–18]). Instead of analytical approaches, we can use numerical methods. It is known that the design of an optimal success probabilities can be treated as a positive semidefinite programming problems [19]. In many cases, an optimal value can be computed in polynomial time by well-known algorithms for solving semidefinite programs such with interior point methods. However, in large-scale problems, these methods require the vast amount of calculation.

Instead of computing an exact optimal success probabilities, several previous studies have given its upper and/or lower bounds [20–28]. These methods are especially useful for large-scale problems of which it is hard to compute an exact value within feasible time; for example, in Ref. [25], bounds are effectively used for comparing optimal success probabilities with different optical states. In the case of minimum-error measurements, Qiu *et al.* compared some of these upper bounds with each other, and derived another upper bound [27], which improves some upper bounds in some cases. In contrast, the square root measurement (SRM, also called the pretty good measurement) is well known as a suboptimal measurement of the success probability criterion; the success probability of the SRM is a good lower bound on the optimal one. In the case of optimal inconclusive measurements, an upper bound on the optimal success probability for binary quantum states has been derived by Sugimoto *et al.* [28].

In the present study, some upper and lower bounds on the success probabilities of minimum-error and optimal inconclusive measurements are derived. The approach to this derivation exploits the fact that the optimal success probabilities are upper bounded by suboptimal solutions to the dual problems of optimal state discrimination problems. We also present a necessary and sufficient condition for this upper bound to be attainable, from which the proposed lower bound can be obtained. In the case of minimum-error measurements, we show that a slightly modified version of the proposed bound is tighter than Qiu *et al.*'s upper bound. We also evaluate the performance of the proposed bounds through numerical experiments. These experiments show that, on average, the proposed upper and lower bounds for minimum-error measurements are, respectively, tighter than Qiu *et al.*'s upper bound and the lower bound given by the success probabilities of the SRMs. The performance of the proposed upper and lower bounds for optimal inconclusive measurements is also evaluated, which demonstrates that, on average, the proposed upper bound is tighter than Sugimoto *et al.*'s one in the case of binary quantum states.

II. MINIMUM-ERROR AND OPTIMAL INCONCLUSIVE MEASUREMENTS

We consider discrimination between M quantum states represented by a set of density operators $\{\hat{\sigma}_m\}_{m\in\mathcal{I}_M}$ with prior probabilities $\{\xi_m\}_{m\in\mathcal{I}_M}$, where $\mathcal{I}_k = \{0,1,\ldots,k-1\}$. $\hat{\sigma}_m$ satisfies $\hat{\sigma}_m \geqslant 0$ and $\mathrm{Tr}\hat{\sigma}_m = 1$, where $\hat{A} \geqslant 0$, $\hat{A} \geqslant \hat{B}$, and $\hat{A} \leqslant \hat{B}$, respectively, denote that $\hat{A}$, $\hat{A}-\hat{B}$, and $\hat{B}-\hat{A}$ are positive semidefinite. To simplify notation, let $\hat{\rho}_m = \xi_m\hat{\sigma}_m$, which we refer to as a quantum state. We can easily verify $\hat{\rho}_m \geqslant 0$, $\mathrm{Tr}\hat{\rho}_m = \xi_m > 0$ for any $m \in \mathcal{I}_M$, and $\sum_{m=0}^{M-1}\mathrm{Tr}\hat{\rho}_m = 1$. A set of quantum states, $\rho = \{\hat{\rho}_m\}_{m\in\mathcal{I}_M}$, is referred to 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 $\{\hat{\rho}_m\}$.

Let us consider a quantum measurement that may return an inconclusive answer, which can be described by a positive operator-valued measure (POVM) with $M+1$ detection operators, $\Pi = \{\hat{\Pi}_m\}_{m\in\mathcal{I}_{M+1}}$. The detection operator $\hat{\Pi}_m$ with $m \in \mathcal{I}_M$ corresponds to identification of the state $\hat{\rho}_m$, while $\hat{\Pi}_M$ corresponds to the inconclusive answer. It is assumed without loss of generality that $\hat{\Pi}_m$ is on $\mathcal{H}$ for any $m \in \mathcal{I}_{M+1}$. Let $\mathcal{M}$ be the entire set of POVMs on $\mathcal{H}$ each of which consists of $M+1$ detection operators; then any $\Pi \in \mathcal{M}$ satisfies

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

where $\hat{1}$ is the identity operator on $\mathcal{H}$.

The success probability, $P_{\mathrm{C}}(\Pi)$, the error probability, $P_{\mathrm{E}}(\Pi)$, and the inconclusive probability, $P_{\mathrm{I}}(\Pi)$, of a POVM Π can be represented as

$$\begin{aligned} P_{\mathrm{C}}(\Pi) &= \sum_{m=0}^{M-1}\mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_m), \\ P_{\mathrm{E}}(\Pi) &= \sum_{m=0}^{M-1}\sum_{\substack{k=0 \\ (m\neq k)}}^{M-1}\mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_k), \\ P_{\mathrm{I}}(\Pi) &= \sum_{m=0}^{M-1}\mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_M) = \mathrm{Tr}(\hat{G}\hat{\Pi}_M), \end{aligned} \tag{2}$$

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

$$\hat{G} = \sum_{m=0}^{M-1}\hat{\rho}_m. \tag{3}$$

The sum of these probabilities is one,

$$P_{\mathrm{C}}(\Pi) + P_{\mathrm{E}}(\Pi) + P_{\mathrm{I}}(\Pi) = 1, \tag{4}$$

for any $\Pi \in \mathcal{M}$.

An optimal inconclusive measurement Π with the inconclusive probability of p $(0 \leqslant p \leqslant 1)$ is a measurement maximizing the success probability $P_{\mathrm{C}}(\Pi)$ under the constraint that $P_{\mathrm{I}}(\Pi) = p$; i.e., it is an optimal solution to the following optimization problem:

$$\begin{aligned} \mathrm{P}:\quad &\text{maximize} \quad P_{\mathrm{C}}(\Pi) \\ &\text{subject to} \quad \Pi \in \mathcal{M}_p \end{aligned} \tag{5}$$

with a POVM Π, where $\mathcal{M}_p$ is the entire set of POVMs, $\Pi \in \mathcal{M}$, satisfying $P_{\mathrm{I}}(\Pi) = p$. In particular, an optimal solution with $p = 0$ is called a minimum-error measurement, which always satisfies $\hat{\Pi}_M = 0$. Let Q_p be the optimal value of problem P,

$$Q_p = \max_{\Pi\in\mathcal{M}_p} P_{\mathrm{C}}(\Pi). \tag{6}$$

Also, let $Q = Q_0$, which is equal to the success probability of a minimum-error measurement.

Problem P is semidefinite programming, and its dual problem can be represented as [12]

$$\begin{aligned} \mathrm{DP}:\quad &\text{minimize} \quad \mathrm{Tr}\hat{Z} - ap \\ &\text{subject to} \quad \hat{Z} \in \mathcal{S}_a \end{aligned} \tag{7}$$

with a positive semidefinite operator $\hat{Z}$ on $\mathcal{H}$ and $a \in \mathbf{R}_+$, where $\mathbf{R}_+$ is the entire set of nonnegative real numbers, and $\mathcal{S}_a$ is expressed as

$$\mathcal{S}_a = \{\hat{Z}\colon \hat{Z} \geqslant \hat{\rho}_m(\forall m \in \mathcal{I}_M), \hat{Z} \geqslant a\hat{G}\}. \tag{8}$$

The optimal value of problem DP is equal to that of problem P: Q_p [12]. The following inequality thus holds:

$$\mathrm{Tr}\hat{Z} - ap \geqslant Q_p,\ \forall a \in \mathbf{R}_+, \hat{Z} \in \mathcal{S}_a. \tag{9}$$

Similarly, the dual problem with $p = 0$ is represented as [19]

$$\begin{aligned} \mathrm{DP_{me}}:\quad &\text{minimize} \quad \mathrm{Tr}\hat{X} \\ &\text{subject to} \quad \hat{X} \in \mathcal{S}_0 \end{aligned} \tag{10}$$

with a positive semidefinite operator $\hat{X}$. As in Eq. (9), we have

$$\mathrm{Tr}\hat{X} \geqslant Q,\ \forall \hat{X} \in \mathcal{S}_0. \tag{11}$$

III. BOUNDS ON SUCCESS PROBABILITY OF MINIMUM-ERROR MEASUREMENT

A. Preparation

Let the spectral decomposition of a Hermitian operator $\hat{A}$ be $\hat{A} = \sum_n \lambda_n\hat{E}_n$, where λ_n is an eigenvalue of $\hat{A}$, and $\hat{E}_n$ is the corresponding projection operator. Let $\hat{A}_+$ be

$$\hat{A}_+ = \sum_{\lambda_n>0}\lambda_n\hat{E}_n. \tag{12}$$

Also, let $\underline{P_+}(\hat{A})$ and $\overline{P_+}(\hat{A})$, respectively, be

$$\underline{P_+}(\hat{A}) = \sum_{\lambda_n>0}\hat{E}_n, \overline{P_+}(\hat{A}) = \sum_{\lambda_n\geqslant 0}\hat{E}_n. \tag{13}$$

In other words, $\underline{P_+}(\hat{A})$ is the projection operator onto the support space of $\hat{A}_+$, and $\overline{P_+}(\hat{A})$ is the projection operator onto the kernel of $(-\hat{A})_+$. From Eq. (13), $\overline{P_+}(\hat{A}) \geqslant \underline{P_+}(\hat{A})$ obviously holds.

In preparation for subsequent subsections, we show the following lemma.

Lemma 1. Let $\hat{A}$ and $\hat{B}$ be positive semidefinite operators. We consider the following optimization problem:

$$\begin{aligned} &\text{minimize} \quad \mathrm{Tr}\hat{Y} \\ &\text{subject to} \quad \hat{Y} \geqslant \hat{A}, \hat{Y} \geqslant \hat{B} \end{aligned} \tag{14}$$

with a variable $\hat{Y}$. Also, let $\hat{Y}^\star = \hat{B} + (\hat{A} - \hat{B})_+$; accordingly, $\hat{Y}^\star$ is the optimal solution to problem (14). In addition, any operator $\hat{\Phi}$ with $\hat{1} \geqslant \hat{\Phi} \geqslant 0$ satisfies

$$\mathrm{Tr}\hat{Y}^\star \geqslant \mathrm{Tr}(\hat{A}\hat{\Phi}) + \mathrm{Tr}[\hat{B}(\hat{1} - \hat{\Phi})]. \tag{15}$$

The equality in Eq. (15) holds if and only if

$$\overline{P_+}(\hat{A} - \hat{B}) \geqslant \hat{\Phi} \geqslant \underline{P_+}(\hat{A} - \hat{B}). \tag{16}$$

Proof. The case of $\mathrm{Tr}(\hat{A} + \hat{B}) = 0$, i.e., $\hat{A} = \hat{B} = 0$, is obvious, so we concentrate on $\mathrm{Tr}(\hat{A} + \hat{B}) \neq 0$. Let $c = 1/\mathrm{Tr}(\hat{A} + \hat{B})$, $\hat{\rho}_A = c\hat{A}$, $\hat{\rho}_B = c\hat{B}$, and $\hat{X} = c\hat{Y}$; then problem (14) can be reformulated as

$$\begin{aligned} &\text{minimize} && \mathrm{Tr}\hat{X} \\ &\text{subject to} && \hat{X} \geqslant \hat{\rho}_A, \hat{X} \geqslant \hat{\rho}_B. \end{aligned} \tag{17}$$

This is the dual problem of the problem of obtaining a minimum-error measurement for a binary quantum state set $\{\hat{\rho}_A, \hat{\rho}_B\}$. Thus, the optimal solution is $\hat{X}^\star = \hat{\rho}_B + (\hat{\rho}_A - \hat{\rho}_B)_+$ (e.g., Ref. [29]). Moreover, for any operator $\hat{\Phi}$ with $\hat{1} \geqslant \hat{\Phi} \geqslant 0$, $\{\hat{\Phi}, \hat{1} - \hat{\Phi}\}$ is a POVM for a binary quantum state set; thus, it follows that

$$\mathrm{Tr}\hat{X}^\star \geqslant \mathrm{Tr}(\hat{\rho}_A\hat{\Phi}) + \mathrm{Tr}[\hat{\rho}_B(\hat{1} - \hat{\Phi})]. \tag{18}$$

Dividing this equation by c gives Eq. (15). Obviously, the equality in (15) holds if and only if $\{\hat{\Phi}, \hat{1} - \hat{\Phi}\}$ is a minimum-error measurement, i.e., (16) holds [29]. ■

B. Proposed upper bound

According to Eq. (11), for any feasible solution to problem $\mathrm{DP_{me}}$, $\hat{X} \in \mathcal{S}_0$, Q is upper bounded by $\mathrm{Tr}\hat{X}$. Here we consider obtaining a suboptimal solution to problem $\mathrm{DP_{me}}$ by using Lemma 1. For $m \in \mathcal{I}_{M-1}$, the following optimization problem is considered:

$$\begin{aligned} &\text{minimize} && \mathrm{Tr}\hat{X}'_{m+1} \\ &\text{subject to} && \hat{X}'_{m+1} \geqslant \hat{\rho}_{m+1}, \hat{X}'_{m+1} \geqslant \hat{X}_m \end{aligned} \tag{19}$$

with a positive semidefinite operator $\hat{X}'_{m+1}$, where $\hat{X}_0 = \hat{\rho}_0$, and $\hat{X}_{m+1}$ ($m \in \mathcal{I}_{M-1}$) is an optimal solution to problem (19). We derive an upper bound on Q, namely, $\overline{Q} = \mathrm{Tr}\hat{X}_{M-1}$. According to Lemma 1, the optimal solution to problem (19) is expressed as $\hat{X}_{m+1} = \hat{X}_m + (\hat{\rho}_{m+1} - \hat{X}_m)_+$. The proposed upper bound $\overline{Q}$ can thus be expressed as

$$\begin{aligned} \overline{Q} &= \mathrm{Tr}\hat{X}_{M-1}, \\ \hat{X}_0 &= \hat{\rho}_0, \\ \hat{X}_{m+1} &= \hat{X}_m + (\hat{\rho}_{m+1} - \hat{X}_m)_+, \ \ m \in \mathcal{I}_{M-1}. \end{aligned} \tag{20}$$

We can easily show that Q is upper bounded by $\overline{Q}$:

Theorem 2. $\overline{Q} \geqslant Q$.

Proof. From the constraint of problem (19), it is clear that $\hat{X}_{M-1} \geqslant \hat{X}_m \geqslant \hat{\rho}_m$ holds for any $m \in \mathcal{I}_M$. Thus, $\hat{X}_{M-1} \in \mathcal{S}_0$ also holds, which gives $\overline{Q} \geqslant Q$ from Eq. (11). ■

Remark 3. For a set of binary states, $\overline{Q} = Q$ holds.

Proof. Since $\hat{X}_1 = \hat{\rho}_0 + (\hat{\rho}_1 - \hat{\rho}_0)_+$ is the optimal solution to problem $\mathrm{DP_{me}}$, $\overline{Q} = \mathrm{Tr}\hat{X}_1 = Q$ holds. ■

In Ref. [27], Qiu *et al.* proposed an upper bound on Q, denoted as $\overline{Q}^{\mathrm{Qiu}}$, expressed as

$$\begin{aligned} \overline{Q}^{\mathrm{Qiu}} &= \min_{k \in \mathcal{I}_M} \overline{Q}^{\mathrm{Qiu}}(k), \\ \overline{Q}^{\mathrm{Qiu}}(k) &= \xi_k + \sum_{\mathcal{I}_M \ni m \neq k} \mathrm{Tr}(\hat{\rho}_m - \hat{\rho}_k)_+. \end{aligned} \tag{21}$$

Note that $\overline{Q}^{\mathrm{Qiu}}$ is identical to $1 - L_4$ in Ref. [27]. $\overline{Q}^{\mathrm{Qiu}}(k)$ is equivalent to $\overline{Q}^{\mathrm{Qiu}}(0)$ after permuting $\hat{\rho}_0$ and $\hat{\rho}_k$. Here we give a slightly modified version of $\overline{Q}$, denoted as $\overline{Q}'$, and show $\overline{Q}' \leqslant \overline{Q}^{\mathrm{Qiu}}$. $\overline{Q}'$ is defined as

$$\overline{Q}' = \min_{k \in \mathcal{I}_M} \overline{Q}(k), \tag{22}$$

where $\overline{Q}(k)$ is $\overline{Q}$ obtained from Eq. (20) after permuting $\hat{\rho}_0$ and $\hat{\rho}_k$. Since $\overline{Q}(k) \geqslant Q$ holds for any $k \in \mathcal{I}_M$, Q is obviously upper bounded by $\overline{Q}'$. Moreover, from $\overline{Q}(0) = \overline{Q}$, $\overline{Q}' \leqslant \overline{Q}$ holds. The following proposition also holds:

Proposition 4. $\overline{Q}' \leqslant \overline{Q}^{\mathrm{Qiu}}$.

Proof. It suffices to show $\overline{Q}(k) \leqslant \overline{Q}^{\mathrm{Qiu}}(k)$ for any $k \in \mathcal{I}_M$. Since $\overline{Q}(k) \leqslant \overline{Q}^{\mathrm{Qiu}}(k)$ is equivalent to $\overline{Q}(0) \leqslant \overline{Q}^{\mathrm{Qiu}}(0)$ for the quantum state set that is obtained by permutation of $\hat{\rho}_0$ and $\hat{\rho}_k$, it is only necessary to show $\overline{Q}(0) \leqslant \overline{Q}^{\mathrm{Qiu}}(0)$ for any quantum state set. Since $\hat{X}_m \geqslant \hat{\rho}_0$ gives $\hat{\rho}_{m+1} - \hat{\rho}_0 \geqslant \hat{\rho}_{m+1} - \hat{X}_m$ for any $m \in \mathcal{I}_{M-1}$, from Lemma 10 in Appendix A,

$$\mathrm{Tr}(\hat{\rho}_{m+1} - \hat{\rho}_0)_+ \geqslant \mathrm{Tr}(\hat{\rho}_{m+1} - \hat{X}_m)_+ \tag{23}$$

is obtained. Therefore, Eqs. (20) and (21) give

$$\begin{aligned} \overline{Q}(0) &= \mathrm{Tr}\hat{\rho}_0 + \sum_{m=0}^{M-2} \mathrm{Tr}(\hat{\rho}_{m+1} - \hat{X}_m)_+ \\ &\leqslant \xi_0 + \sum_{m=0}^{M-2} \mathrm{Tr}(\hat{\rho}_{m+1} - \hat{\rho}_0)_+ = \overline{Q}^{\mathrm{Qiu}}(0). \end{aligned} \tag{24}$$

■

C. Attainability of proposed upper bound

A necessary and sufficient condition for the proposed upper bound to achieve the optimal success probability is provided by the following theorem:

Theorem 5. $\overline{Q} = Q$ holds if and only if $\{\hat{E}_k\}_{k=1}^{M-1}$ exists such that

$$\begin{aligned} \overline{P_+}[\hat{A}_k(\hat{X}_{k-1} - \hat{\rho}_k)\hat{A}_k^\dagger] &\geqslant \hat{E}_k \\ &\geqslant \underline{P_+}[\hat{A}_k(\hat{X}_{k-1} - \hat{\rho}_k)\hat{A}_k^\dagger], \\ &\quad k \in \{1, \ldots, M-1\}, \end{aligned} \tag{25}$$

and

$$\begin{aligned} \hat{A}_m(\hat{X}_{m-1} - \hat{\rho}_m)_+\hat{A}_m^\dagger &= [\hat{A}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{A}_m^\dagger]_+, \\ &\quad m \in \{1, 2, \ldots, M-2\}, \end{aligned} \tag{26}$$

where

$$\hat{A}_m = \begin{cases} \hat{E}_{m+1}^{\frac{1}{2}}\hat{E}_{m+2}^{\frac{1}{2}} \cdots \hat{E}_{M-1}^{\frac{1}{2}}, & 0 \leqslant m < M-1, \\ \hat{1}, & m = M-1. \end{cases} \tag{27}$$

Proof. In preparation for the proof, a set of operators, $\Pi = \{\hat{\Pi}_m\}_{m\in\mathcal{I}_M}$, is defined as

$$\hat{\Pi}_m = \begin{cases} |\hat{A}_m|^2 - |\hat{A}_{m-1}|^2, & 1 \leqslant m \leqslant M-1, \\ |\hat{A}_0|^2, & m = 0, \end{cases} \quad (28)$$

where $|\hat{A}| = (\hat{A}^\dagger \hat{A})^{1/2}$. For any $\{\hat{E}_k\}_{k=1}^{M-1}$ with $\hat{1} \geqslant \hat{E}_k \geqslant 0$,

$$\sum_{m=0}^{M-1} \hat{\Pi}_m = |\hat{A}_{M-1}|^2 = \hat{1},$$
$$\hat{\Pi}_m = \hat{A}_m^\dagger(\hat{1} - \hat{E}_m)\hat{A}_m \geqslant 0, \ 1 \leqslant m \leqslant M-1,$$
$$\hat{\Pi}_0 = |\hat{A}_0|^2 \geqslant 0 \quad (29)$$

holds. The second line of Eq. (29) follows from $|\hat{A}_{m-1}|^2 = \hat{A}_m^\dagger \hat{E}_m \hat{A}_m$, which is given by Eq. (27). Thus, Π is a POVM. On the contrary, for any POVM $\Pi = \{\hat{\Pi}_m\}$, $\{\hat{E}_k\}_{k=1}^{M-1}$ exists such that $\hat{1} \geqslant \hat{E}_k \geqslant 0$ and Eq. (28) hold (see Appendix B).

In the following, $\{\hat{E}_k\}$ satisfying $\hat{1} \geqslant \hat{E}_k \geqslant 0$ $(1 \leqslant k \leqslant M-1)$ and its corresponding POVM Π, defined by Eq. (28), are considered. From Lemma 13 in Appendix A and $\hat{X}_m = \hat{X}_{m-1} + (\hat{\rho}_m - \hat{X}_{m-1})_+$, it follows that for any m with $1 \leqslant m \leqslant M-1$,

$$\begin{aligned} &\mathrm{Tr}(\hat{A}_m \hat{X}_m \hat{A}_m^\dagger) \\ &\geqslant \mathrm{Tr}[\hat{A}_m \hat{\rho}_m \hat{A}_m^\dagger (\hat{1} - \hat{E}_m)] + \mathrm{Tr}(\hat{A}_m \hat{X}_{m-1} \hat{A}_m^\dagger \hat{E}_m) \\ &= \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}_m) + \mathrm{Tr}(\hat{A}_{m-1} \hat{X}_{m-1} \hat{A}_{m-1}^\dagger), \end{aligned} \quad (30)$$

where the last line follows from $\hat{A}_m^\dagger(\hat{1} - \hat{E}_m)\hat{A}_m = \hat{\Pi}_m$ and $\hat{A}_m^\dagger \hat{E}_m \hat{A}_m = |\hat{A}_{m-1}|^2$. Using Eq. (30) recursively for $m = M-1, M-2, \ldots, 1$ yields

$$\begin{aligned} \overline{Q} &= \mathrm{Tr}\hat{X}_{M-1} \\ &\geqslant \sum_{m=1}^{M-1} \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}_m) + \mathrm{Tr}(\hat{\rho}_0 |\hat{A}_0|^2) \\ &= \sum_{m=0}^{M-1} \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}_m) = P_{\mathrm{C}}(\Pi). \end{aligned} \quad (31)$$

First, we prove the sufficiency of Theorem 5. Assume $\overline{Q} = Q$. $\Pi = \{\hat{\Pi}_m\}$ is taken as a minimum-error measurement. $\hat{E}_m$ is chosen to satisfy $\hat{1} \geqslant \hat{E}_m \geqslant 0$ and Eqs. (27) and (28). Then, from $\overline{Q} = Q = P_{\mathrm{C}}(\Pi)$, the equality in Eq. (31) holds, implying that the equality in Eq. (30) holds for any $m \in \{M-1, M-2, \ldots, 1\}$. Therefore, according to Lemma 13, Eqs. (25) and (26) hold.

Next, we prove the necessity of Theorem 5. Assume that $\{\hat{E}_k\}_{k=1}^{M-1}$ exists such that Eqs. (25) and (26) hold. Also, let $\Pi = \{\hat{\Pi}_m\}$ be the POVM defined by Eq. (28). According to Lemma 13, the equality in Eq. (30) holds for any $m \in \{M-1, M-2, \ldots, 1\}$; thus, the equality in Eq. (31), $\overline{Q} = P_{\mathrm{C}}(\Pi)$, holds. From $\overline{Q} \geqslant Q \geqslant P_{\mathrm{C}}(\Pi)$, $\overline{Q} = Q$ therefore also holds. ∎

$\hat{e}_m$ and $\hat{a}_m$ are defined as

$$\hat{e}_m = \overline{P_+}[\hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{a}_m^\dagger],$$
$$\hat{a}_m = \begin{cases} \hat{e}_{m+1}\hat{e}_{m+2}\cdots\hat{e}_{M-1}, & 0 \leqslant m < M-1, \\ \hat{1}, & m = M-1. \end{cases} \quad (32)$$

Note that if $\hat{E}_m = \hat{e}_m$, then $\hat{A}_m = \hat{a}_m$. The following corollary (proof in Appendix C) holds:

Corollary 6. Assume that, for any m with $1 \leqslant m \leqslant M-1$,

$$\mathrm{supp}[\hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{a}_m^\dagger] = \mathrm{supp}\, \hat{a}_m \hat{X}_m \hat{a}_m^\dagger. \quad (33)$$

Then $\overline{Q} = Q$ holds if and only if

$$\hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)_+ \hat{a}_m^\dagger = [\hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{a}_m^\dagger]_+,$$
$$m \in \{1,2,\ldots,M-2\}. \quad (34)$$

D. Proposed lower bound

The proof of Theorem 5 shows that if $\overline{Q} = Q$, then the POVM $\{\hat{\Pi}_m\}_{m\in\mathcal{I}_M}$ of Eq. (28), which is obtained from the corresponding $\{\hat{E}_k\}_{k=1}^{M-1}$, is a minimum-error measurement. In particular, substituting $\hat{E}_k = \hat{e}_k$ gives that the POVM $\Pi^\circ = \{\hat{\Pi}_m^\circ\}_{m\in\mathcal{I}_M}$ defined as

$$\hat{\Pi}_m^\circ = \begin{cases} |\hat{a}_m|^2 - |\hat{a}_{m-1}|^2, & 0 < m \leqslant M-1, \\ |\hat{a}_0|^2, & m = 0, \end{cases} \quad (35)$$

where $\hat{e}_m$ and $\hat{a}_m$ are given by Eq. (32). is also a minimum-error measurement when $\overline{Q} = Q$. Exploiting this fact, we propose a lower bound on Q, denoted as $\underline{Q}$, expressed as

$$\underline{Q} = P_{\mathrm{C}}(\Pi^\circ) = \sum_{m=0}^{M-1} \mathrm{Tr}(\hat{\rho}_m \hat{\Pi}_m^\circ). \quad (36)$$

Since Π° is a POVM, $\underline{Q} \leqslant Q$ obviously holds. The SRM $\Pi^{\mathrm{SRM}} = \{\hat{\Pi}_m^{\mathrm{SRM}}\}_{m\in\mathcal{I}_M}$, which is defined as

$$\hat{\Pi}_m^{\mathrm{SRM}} = \hat{G}^{-\frac{1}{2}}\hat{\rho}_m\hat{G}^{-\frac{1}{2}}, \quad (37)$$

is well known as a good approximation to a minimum-error measurement. We will show in numerical experiments in Sec. VI that $\underline{Q}$ tends to be closer to Q than the success probability of the SRM.

IV. BOUNDS ON SUCCESS PROBABILITY OF OPTIMAL INCONCLUSIVE MEASUREMENT

A. Proposed upper bound

The arguments presented in the previous section can be extended to optimal inconclusive measurements as follows. Assume that a suboptimal solution, $\hat{X}^\circ$, to problem $\mathrm{DP}_{\mathrm{me}}$ for a quantum state set ρ is given. In this paper, let $\hat{X}^\circ = \hat{X}_{M-1}$, which is defined by Eq. (20). Note that if an optimal solution $\hat{X}^\star$ to problem $\mathrm{DP}_{\mathrm{me}}$ is given, then $\hat{X}^\circ = \hat{X}^\star$ can be used instead of $\hat{X}^\circ = \hat{X}_{M-1}$. A suboptimal solution to problem DP can be obtained by solving the following optimization problem:

$$\begin{aligned} &\text{minimize} && \mathrm{Tr}\hat{Z} - ap \\ &\text{subject to} && \hat{Z} \in \mathcal{Z}_a \end{aligned} \quad (38)$$

with a positive semidefinite operator $\hat{Z}$ on $\mathcal{H}$ and $a \in \mathbf{R}_+$, where

$$\mathcal{Z}_a = \{\hat{Z} : \hat{Z} \geqslant a\hat{G}, \hat{Z} \geqslant \hat{X}^\circ\}. \quad (39)$$

Indeed, from $\hat{X}^\circ \in \mathcal{S}_0$, $\hat{Z} \in \mathcal{S}_a$ holds for any $\hat{Z} \in \mathcal{Z}_a$; i.e., $\hat{Z}$ is a feasible solution to problem DP. Accordingly, Q_p is upper bounded by the optimal value of problem (38). Let

$$s(a) = \min_{\hat{Z} \in \mathcal{Z}_a} \mathrm{Tr}\hat{Z} - ap; \tag{40}$$

then the optimal value of problem (38) is equal to $\min_{a \in \mathbf{R}_+} s(a)$. Lemma 1 indicates that $\mathrm{Tr}\hat{Z} \geqslant \mathrm{Tr}\hat{X}^\circ + \mathrm{Tr}(a\hat{G} - \hat{X}^\circ)_+$ holds for any $\hat{Z} \in \mathcal{Z}_a$ and the equality holds when $\hat{Z} = \hat{X}^\circ + (a\hat{G} - \hat{X}^\circ)_+$. Thus, we have

$$s(a) = \mathrm{Tr}\hat{X}^\circ + \mathrm{Tr}(a\hat{G} - \hat{X}^\circ)_+ - ap. \tag{41}$$

Since it is difficult to obtain the optimal value, $\min_{a \in \mathbf{R}_+} s(a)$, of problem (38) in general, we consider computing the minimum $s(a)$ for several values of a as a suboptimal solution. We propose an upper bound on Q_p, denoted as $\overline{Q_p}$, expressed as

$$\overline{Q_p} = \min\left\{1 - p, \min_{a \in \mathcal{A}} s(a)\right\}, \tag{42}$$

where $\mathcal{A} \subseteq \mathbf{R}_+$ is a set of candidates for a. Note that, from Eq. (4), $Q_p \leqslant 1 - p$ always holds, and Eq. (42) guarantees that $\overline{Q_p}$ does not exceed $1 - p$. It is expected that $\overline{Q_p}$ can be effectively obtained by adaptively selecting appropriate candidates.

Theorem 7. $\overline{Q_p} \geqslant Q_p$.

Proof. Since the case of $\overline{Q_p} = 1 - p$ is obvious, we assume $\overline{Q_p} < 1 - p$. Recall that $\hat{Z} \in \mathcal{S}_a$ holds for any $\hat{Z} \in \mathcal{Z}_a$. Thus, Eqs. (9) and (40) give

$$s(a) = \min_{\hat{Z} \in \mathcal{Z}_a} \mathrm{Tr}\hat{Z} - ap \geqslant \min_{\hat{Z} \in \mathcal{S}_a} \mathrm{Tr}\hat{Z} - ap \geqslant Q_p. \tag{43}$$

Therefore, from Eq. (42), we have

$$\overline{Q_p} = \min_{a \in \mathcal{A}} s(a) \geqslant Q_p. \tag{44}$$

■

Algorithm 1 shows an example of computing $\overline{Q_p}$. We will provide a concrete algorithm on how to initialize and update a in Sec. IV C.

Algorithm 1 An example of computing $\overline{Q_p}$.

Input: $\{\hat{\rho}_m\}_{m \in \mathcal{I}_M}, p$
1: Let $\hat{X}^\circ = \hat{X}_{M-1}$, where $\hat{X}_{M-1}$ is given by Eq. (20)
2: $\overline{Q_p} \leftarrow 1 - p$
3: Initialize a
4: **for** $j \leftarrow 1,2,\ldots$ **do**
5: Compute $s(a)$ from Eq. (41)
6: $\overline{Q_p} \leftarrow \min\{\overline{Q_p}, s(a)\}$
7: Update a
8: **end for**
Output: $\overline{Q_p}$

B. Properties of $s(a)$

To appropriately update a in Algorithm 1, the properties of $s(a)$ should be well understood. The following proposition shows some of the properties (proof in Appendix D):

Proposition 8. Let $\lambda_{\max}(\hat{A})$ and $\lambda_{\min}(\hat{A})$ be the maximum and minimum eigenvalues of a positive semidefinite operator $\hat{A}$, respectively. $s(a)$ satisfies the following conditions:

(1) If $a \leqslant \lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$, then $s(a) = \mathrm{Tr}\hat{X}^\circ - ap$ holds. Also, $1/M \leqslant \lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$ holds.

(2) If $a \geqslant \lambda_{\max}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$, then $s(a) = a(1-p)$ holds.

(3) $s(a)$ is convex with respect to a.

Note that since $\hat{G}$ is a positive definite operator on $\mathcal{H}$, $\hat{G}^{-1/2}$ exists.

The following proposition also holds (proof in Appendix E):

Proposition 9. Let $\tilde{p}(a) = \mathrm{Tr}[\hat{G}\underline{P_+}(a\hat{G} - \hat{X}^\circ)]$ and $\tilde{p}^+(a) = \mathrm{Tr}[\hat{G}\overline{P_+}(a\hat{G} - \hat{X}^\circ)]$; then the following conditions hold:

(1) If $a < a'$, then $\tilde{p}^+(a) \leqslant \tilde{p}(a')$ holds. In addition, $\tilde{p}(a)$ and $\tilde{p}^+(a)$ monotonically increase with respect to a.

(2) a minimizes $s(a)$ if and only if $\tilde{p}(a) \leqslant p \leqslant \tilde{p}^+(a)$ holds.

C. Algorithm for computing proposed upper bound

Propositions 8 and 9 are useful to update a in Algorithm 1. For example, since $\tilde{p}(a)$ monotonically increases with respect to a, as stated in Proposition 9, a should be updated to a larger value if $\tilde{p}(a) < p$ or the smaller value if $\tilde{p}(a) > p$.

A concrete example of Algorithm 1 is shown in Algorithm 2. Let $a^\star \in \mathrm{argmin}_a\, s(a)$. When initializing and updating a, Algorithm 2 exploits Propositions 8 and 9. In steps 4 and 7, a_L and a_R are respectively initialized to $\lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$ and $\lambda_{\max}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2}) + \epsilon$, where ϵ is a sufficiently small positive number. Accordingly, since $a_\mathrm{L}\hat{G} - \hat{X}^\circ \leqslant 0$ and $a_\mathrm{R}\hat{G} - \hat{X}^\circ \geqslant \epsilon\hat{G}$ hold [see Eqs. (D1) and (D3) in Appendix D], $\tilde{p}(a_\mathrm{L}) = 0$ and $\tilde{p}(a_\mathrm{R}) = 1$ hold. Thus, from $\tilde{p}(a_\mathrm{L}) \leqslant p \leqslant \tilde{p}(a_\mathrm{R})$ and Proposition 9, $a_\mathrm{L} \leqslant a^\star \leqslant a_\mathrm{R}$ holds. In step 11, an estimated $a^\star$, i.e., a, is computed on the assumption that $\tilde{p}(a')$ is well approximated as linear in $a_\mathrm{L} \leqslant a' \leqslant a_\mathrm{R}$; such a satisfies $a_\mathrm{L} \leqslant a \leqslant a_\mathrm{R}$. In steps 14–18, a is substituted into a_L if $\tilde{p}(a) \leqslant p$ (i.e., $a \leqslant a^\star$); otherwise, a is substituted into a_R. As a result, steps 10–19 guarantee that a_L and a_R satisfy $a_\mathrm{L} \leqslant a^\star \leqslant a_\mathrm{R}$ and are closer to $a^\star$ than those in the previous iteration. The iteration process in Algorithm 2 stops after a

Algorithm 2 Concrete example of computing $\overline{Q_p}$.

Input: $\{\hat{\rho}_m\}_{m \in \mathcal{I}_M}, p$
1: Let $\hat{X}^\circ = \hat{X}_{M-1}$, where $\hat{X}_{M-1}$ is given by Eq. (20)
2: $\overline{Q_p} \leftarrow 1 - p$
3: /* Initialize a_L */
4: $a_\mathrm{L} \leftarrow \lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$
5: $\overline{Q_p} \leftarrow \min\{\overline{Q_p}, \mathrm{Tr}\hat{X}^\circ - a_\mathrm{L}p\}$
6: /* Initialize a_R */
7: $a_\mathrm{R} \leftarrow \lambda_{\max}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2}) + \epsilon$
8: $\overline{Q_p} \leftarrow \min\{\overline{Q_p}, a_\mathrm{R}(1-p)\}$
9: /* Iterate */
10: **for** $j \leftarrow 1,2,\ldots,J$ **do**
11: $a \leftarrow [[\tilde{p}(a_\mathrm{R}) - p]a_\mathrm{L} + [p - \tilde{p}(a_\mathrm{L})]a_\mathrm{R}]/[\tilde{p}(a_\mathrm{R}) - \tilde{p}(a_\mathrm{L})]$
12: Compute $s(a)$ using Eq. (41)
13: $\overline{Q_p} \leftarrow \min\{\overline{Q_p}, s(a)\}$
14: **if** $\tilde{p}(a) \leqslant p$ **then**
15: $a_\mathrm{L} \leftarrow a$
16: **else**
17: $a_\mathrm{R} \leftarrow a$
18: **end if**
19: **end for**
Output: $\overline{Q_p}$

fixed number of iterations; alternatively, it may continue until certain stopping criteria (e.g., the difference between a_L and a_R

is sufficiently small) are met. It is obvious that the difference between $\overline{Q_p}$ and Q_p monotonically decreases as the number of iterations, J, increases.

D. Attainability of proposed upper bound

A necessary and sufficient condition for $\overline{Q_p} = Q_p$ is determined as follows. First, $a^\star$ is taken as the optimal solution of a in problem DP. Then we consider solving the following optimization problem:

$$\begin{aligned} &\text{minimize} \quad \mathrm{Tr}\,\hat{Z} \\ &\text{subject to} \quad \hat{Z} \in \mathcal{S}_{a^\star} \end{aligned} \tag{45}$$

with $\hat{Z}$. Since the optimal value of problem DP is Q_p, the optimal value of problem (45) is $Q_p + a^\star p$. Comparing Eqs. (10) and (45) indicates that Eq. (45) can be regarded as the problem of finding the success probability of a minimum-error measurement for the set of $M+1$ quantum states $\rho' = \{c\hat{\rho}_m\}_{m\in\mathcal{I}_{M+1}}$, with $\hat{\rho}_M = a^\star \hat{G}$, where $c = 1/(1+a^\star)$ is a constant such that $\sum_{m\in\mathcal{I}_{M+1}} \mathrm{Tr}(c\hat{\rho}_m) = 1$. Therefore, Theorem 5 and Corollary 6 can be applied in the case of optimal inconclusive measurements.

E. Proposed lower bound

It is easy to extend the discussion in Sec. III D to optimal inconclusive measurements. Assume that a_L and a_R satisfying $\tilde{p}(a_\mathrm{L}) \leqslant p \leqslant \tilde{p}(a_\mathrm{R})$ are given (such a_L and a_R can be obtained from Algorithm 2). $\Pi^{(a)} = \{\hat{\Pi}_m^{(a)}\}_{m\in\mathcal{I}_{M+1}}$ is defined as

$$\begin{aligned} \hat{\Pi}_m^{(a)} &= \begin{cases} \left|\hat{a}_m^{(a)}\right|^2 - \left|\hat{a}_{m-1}^{(a)}\right|^2, & 0 < m \leqslant M, \\ \left|\hat{a}_0^{(a)}\right|^2, & m = 0, \end{cases} \\ \hat{a}_m^{(a)} &= \begin{cases} \hat{e}_{m+1}^{(a)}\hat{e}_{m+2}^{(a)}\cdots\hat{e}_M^{(a)}, & 0 \leqslant m < M, \\ \hat{1}, & m = M, \end{cases} \\ \hat{e}_m^{(a)} &= \begin{cases} \overline{P_+}[\hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{a}_m^\dagger], & 0 < m \leqslant M-1, \\ \overline{P_+}(\hat{X}_{M-1} - a\hat{G}), & m = M. \end{cases} \end{aligned} \tag{46}$$

Therefore, as discussed in Sec. III D, it is clear that $\Pi^{(a)}$ is a POVM. In addition, since

$$\begin{aligned} \hat{\Pi}_M^{(a)} &= \left|\hat{a}_M^{(a)}\right|^2 - \left|\hat{a}_{M-1}^{(a)}\right|^2 = \hat{1} - \overline{P_+}(\hat{X}_{M-1} - a\hat{G}) \\ &= \underline{P_+}(a\hat{G} - \hat{X}_{M-1}) \end{aligned} \tag{47}$$

holds, the inconclusive probability of the POVM $\Pi^{(a)}$ can be formulated as

$$\mathrm{Tr}\big(\hat{G}\hat{\Pi}_M^{(a)}\big) = \mathrm{Tr}[\hat{G}\underline{P_+}(a\hat{G} - \hat{X}_{M-1})] = \tilde{p}(a). \tag{48}$$

Let us consider the POVM $\Pi^\bullet = \{\hat{\Pi}_m^\bullet\}_{m\in\mathcal{I}_{M+1}}$, where $\Pi^\bullet$ is defined as

$$\hat{\Pi}_m^\bullet = \frac{[\tilde{p}(a_\mathrm{R}) - p]\hat{\Pi}_m^{(a_\mathrm{L})} + [p - \tilde{p}(a_\mathrm{L})]\hat{\Pi}_m^{(a_\mathrm{R})}}{\tilde{p}(a_\mathrm{R}) - \tilde{p}(a_\mathrm{L})} \tag{49}$$

if $\tilde{p}(a_\mathrm{R}) \neq \tilde{p}(a_\mathrm{L})$, $\hat{\Pi}_m^\bullet = \hat{\Pi}_m^{(a_\mathrm{L})}$ otherwise. It is easy to verify that $P_\mathrm{I}(\Pi^\bullet) = p$ holds. We use the success probability of $\Pi^\bullet$, $P_\mathrm{C}(\Pi^\bullet)$, as a lower bound on Q_p, denoted as $\underline{Q_p}$; i.e., $\underline{Q_p}$ is given by

$$\underline{Q_p} = P_\mathrm{C}(\Pi^\bullet) = \sum_{m=0}^{M-1} \mathrm{Tr}(\hat{\rho}_m\hat{\Pi}_m^\bullet). \tag{50}$$

From $P_\mathrm{I}(\Pi^\bullet) = p$, $\underline{Q_p} \leqslant Q_p$ obviously holds.

V. COMPUTATIONAL COMPLEXITY

In this section, we discuss the computational complexity of computing the proposed bounds.

First, the computational complexity of computing $\overline{Q}$ and $\underline{Q}$ is investigated. With regard to $\overline{Q}$, which is computed from Eq. (20), the major computational cost is computing $(\hat{\rho}_{m+1} - \hat{X}_m)_+$. It can be derived by computing the eigenvalues and their corresponding eigenvectors of $\hat{\rho}_{m+1} - \hat{X}_m$ and then using Eq. (12). Let $N = \dim\mathcal{H}$. The computation of the eigenvalues and eigenvectors generally takes $O(N^3)$ time, which indicates that the time complexity required by computing $\overline{Q}$ is $O[(M-1)N^3]$. {Similarly, the time complexity of computing $\overline{Q}'$ in Eq. (22) is $O[M(M-1)N^3]$.} In contrast, the computation of $\overline{Q}^{\mathrm{Qiu}}$ in Eq. (21) requires $O[M(M-1)N^3]$ time, which is $O(M)$ times longer than that for computing $\overline{Q}$. Although $\overline{Q}$ is not always tighter than $\overline{Q}^{\mathrm{Qiu}}$, the numerical results presented in the next section demonstrate that $\overline{Q} < \overline{Q}^{\mathrm{Qiu}}$ holds on average. With regard to $\underline{Q}$, it is assumed that X_m ($m \in \mathcal{I}_M$) in Eq. (20) is given; from Eqs. (32) and (36), the major computational cost is computing $\overline{P_+}(\cdot)$ and operator multiplication. Both of them generally require $O(N^3)$ time, and thus the computation of $\underline{Q}$ takes $O[(M-1)N^3]$. Note that Ref. [30] provides a method of computing the eigenvalues and eigenvectors of $\hat{\rho}_{m+1} - \hat{X}_m$ from those of a corresponding $(\mathrm{rank}\,\hat{\rho}_{m+1} + \mathrm{rank}\,\hat{X}_m)$-dimensional square matrix; this method can reduce the cost of computing $\overline{Q}$ and $\underline{Q}$ if $\mathrm{rank}\,\hat{\rho}_{m+1} + \mathrm{rank}\,\hat{X}_m$ is smaller than N.

Next, the computational complexity of computing $\overline{Q_p}$ and $\underline{Q_p}$ is investigated. With regard to $\overline{Q_p}$, which is computed by Algorithm 2, the major computational cost is computing the following values: (a) $\hat{X}^\circ$ in step 1, (b) $\lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$ in step 4 and $\lambda_{\max}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$ in step 7, and (c) $s(a)$ in step 12 and $\tilde{p}(a)$ in step 14. Since the computational complexities of computing the $(-1/2)$-th power of an operator, operator multiplication, and the eigenvalues and eigenvectors are all $O(N^3)$, the computations of values (a)–(c) above respectively require $O[(M-1)N^3]$, $O(N^3)$, and $O(JN^3)$ times. Therefore, the total computational complexity of computing $\overline{Q_p}$ is roughly $O[(M+J)N^3]$; in particular, in the case of $M \gg J$, it is close to that of computing $\overline{Q}$. With regard to $\underline{Q_p}$, we can make a similar discussion of $\underline{Q}$. Assume that X_m ($m \in \mathcal{I}_M$) in Eq.(20) is given. From Eqs. (46), (49), and (50), the major computational cost is computing $\overline{P_+}(\cdot)$ and operator multiplication, both of which generally take $O(N^3)$ time. Thus, the total computational complexity of $\underline{Q_p}$ is $O(MN^3)$.

We can compute the exact optimal solution using algorithms for solving semidefinite programs such with interior point methods. CSDP [31] is a widely used semidefinite programming solver implementing a primal-dual interior point method. We here assume that N^2 is much larger than M and J, which is satisfied in many practical cases; then CSDP takes $O(N^6)$ time for a single iteration [31]. Thus, we can say that our method, which takes $O(N^3)$ time (for constant M and J), significantly decreases the amount of calculation compared to CSDP. Note that efficient numerical algorithms for obtaining exact optimal solutions are presented [32,33], which take $O(N^3)$ time for a single iteration. However, these algorithms require many iterations to converge (e.g., several hundreds or thousands). Note that, although we observed in many experiments that these algorithms converge to exact solutions, they are not proved to converge, except for a particular case.

VI. NUMERICAL EXAMPLES

We discuss the accuracy of the proposed bounds on the success probabilities of minimum-error and optimal inconclusive measurements through numerical examples as follows.

One hundred sets of randomly generated M quantum states, $\rho = \{\hat{\rho}_m = \xi_m \hat{\sigma}_m\}_{m\in\mathcal{I}_M}$ with rank $\hat{\rho}_m = R$ $(m \in \mathcal{I}_M)$, where M and R are parameters, were used in these examples. More precisely, for each m, the density operator $\hat{\sigma}_m$ was computed by $\hat{\sigma}_m = \hat{U}_m \hat{D}_m \hat{U}_m^\dagger$, where $\hat{U}_m$ is a unitary operator picked uniformly at random from the Haar measure and $\hat{D}_m$ is a diagonal operator with rank R. The nonzero diagonal elements, $\{d_{m,k}\}_{k\in\mathcal{I}_R}$, of $\hat{D}_m$ were chosen independently and uniformly at random between 0 and 1, and were normalized to sum to 1. The prior probabilities, $\{\xi_m\}_{m\in\mathcal{I}_M}$, were also uniformly randomly selected. In the case of optimal inconclusive measurements, the inconclusive probability, p, was uniformly randomly selected in the range from 0 to 0.2. It was observed in preliminary experiments that our results were robust to variations in the underlying distribution. We computed the optimal success probability Q_p and the upper $(\overline{Q}_p)$ and lower $(\underline{Q}_p)$ bounds defined by Eqs. (42) and (50). Note that $\overline{Q}_p$ and $\underline{Q}_p$ are respectively equal to $\overline{Q}$ in Eq. (20) and $\underline{Q}$ in Eq. (36) when $p = 0$. The average relative errors, defined as $|\overline{Q}_p - Q_p|/Q_p$ or $|\underline{Q}_p - Q_p|/Q_p$, are depicted.

It should be mentioned that, in additional experiments (not shown), we also computed $\overline{Q}'$ in Eq. (22) and observed that the relative errors were somewhat smaller than those in the case of $\overline{Q}$. Since the value of $\overline{Q}$ depends on the labeling of the M quantum states, the bound can be further optimized by considering all possible permutations of the set of quantum states. However, the naive implementation has time complexity $O[M!(M-1)N^3]$, which is excessively high when M is large. Therefore, developing an effective and efficient labeling method may be interesting for further research.

A. Case of minimum-error measurements

Figure 1 shows the average relative errors of the proposed upper bound, $\overline{Q}$, and Qiu *et al.*'s upper bound, $\overline{Q}^{\mathrm{Qiu}}$. We observed that, at least in the range of $3 \leqslant M \leqslant 9$ and $R \leqslant 9$, the average relative error of $\overline{Q}$ is more than eight times smaller than that of $\overline{Q}^{\mathrm{Qiu}}$, while $\overline{Q} < \overline{Q}^{\mathrm{Qiu}}$ is not guaranteed for each quantum state set. It also shows that the average relative error of $\overline{Q}$ increases gradually with increasing M, while that of $\overline{Q}^{\mathrm{Qiu}}$ increases rapidly. Note that, in the case of $M = 2$, the average relative errors of $\overline{Q}$ and $\overline{Q}^{\mathrm{Qiu}}$ are always zero.

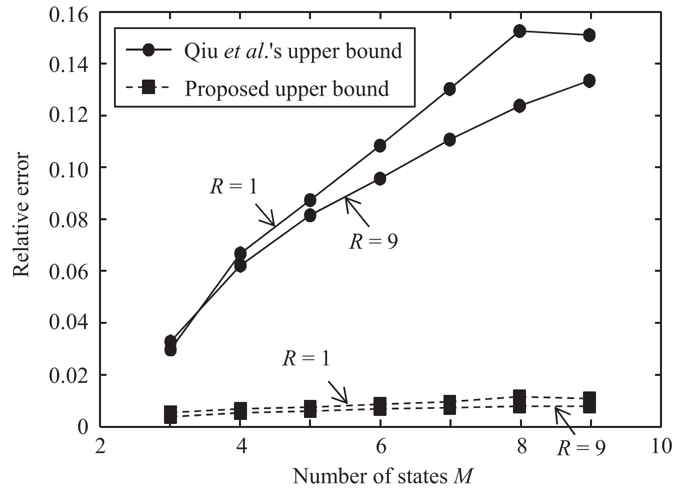

FIG. 1. Average relative errors of upper bounds, $\overline{Q}$, on the success probability of minimum-error measurements for M quantum states.

Figure 2 shows the average relative errors of the proposed lower bound, $\underline{Q}$, and the success probability of the SRM; the former is more than 5.8 times smaller than the latter.

B. Case of optimal inconclusive measurements

Figure 3 shows the average relative errors of $\overline{Q}_p$ with $J = 2$ and 3 in the case of binary state sets. It also shows the upper bound proposed by Sugimoto *et al.* [28], which is based on the fidelity between the binary states. In the case of $R = 1$, the analytical expression of the optimal value, Q_p, is given [28,34]; Sugimoto *et al.*'s upper bound exploits this expression, and achieves Q_p when $R = 1$. Although the proposed upper bound has a nonzero error when $R = 1$, at least in the range of $2 \leqslant M \leqslant 9$, the average relative error of $\overline{Q}_p$ is more than three times smaller than that of Sugimoto *et al.*'s upper bound.

Figures 4 and 5, respectively, show the average relative errors of the proposed upper and lower bounds, $\overline{Q}_p$ and $\underline{Q}_p$, in the case of $M \geqslant 3$. It shows that the average relative error increases gradually with increasing M. In each case, we

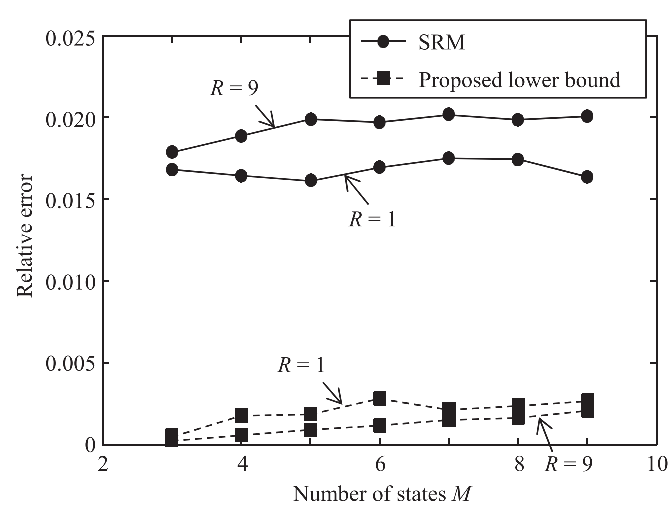

FIG. 2. Average relative errors of lower bounds, $\underline{Q}$, on the success probability of minimum-error measurements for M quantum states.

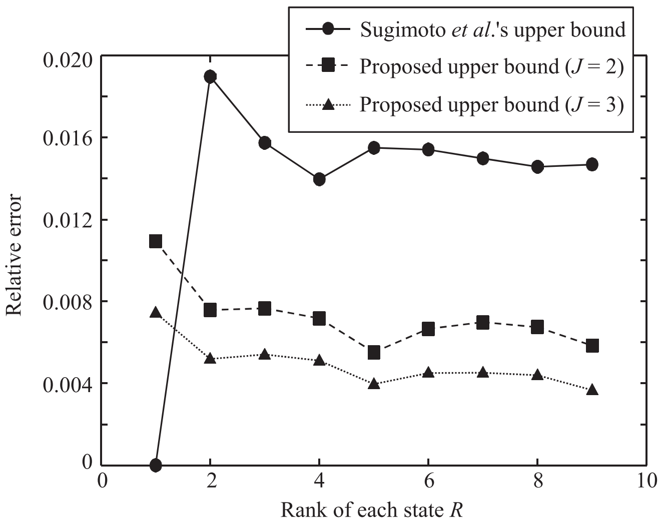

FIG. 3. Average relative errors of upper bounds, $\overline{Q_p}$, on the success probability of optimal inconclusive measurements for binary quantum state sets (i.e., $M = 2$).

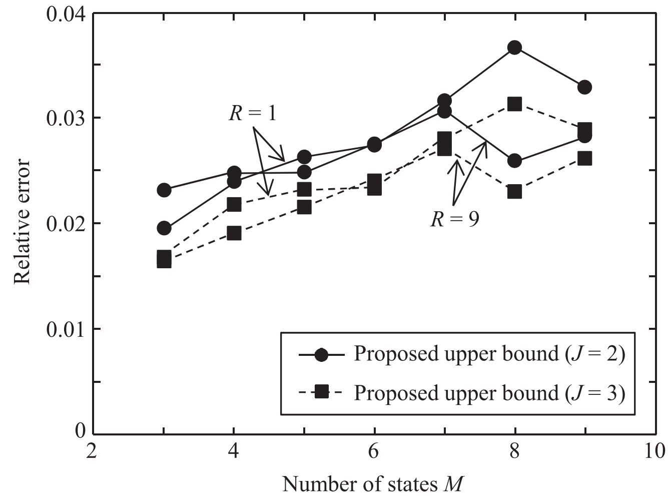

FIG. 5. Average relative errors of lower bounds, $\underline{Q_p}$, on the success probability of optimal inconclusive measurements for $M \geqslant 3$ quantum states.

observed that at least in the range of $M \leqslant 9$ and $R \leqslant 9$ the average relative error is less than 0.037 and 0.032 with $J = 2$ and 3, respectively.

VII. CONCLUSION

We proposed upper and lower bounds on the success probabilities of minimum-error and optimal inconclusive measurements. The proposed upper bounds are suboptimal solutions to the dual problems of the optimal state discrimination problems. The proposed lower bounds are obtained from the success probabilities of POVMs corresponding to suboptimal solutions to the dual problems. Numerical examples show that, on average, the proposed upper and lower bounds for minimum-error measurements are, respectively, tighter than Qiu *et al.*'s upper bound and the lower bound given by the success probabilities of the SRMs. The performance of the proposed upper and lower bounds for optimal inconclusive measurements is also evaluated, which demonstrates that, on average, the proposed upper bound is tighter than Sugimoto *et al.*'s one in the case of binary quantum states.

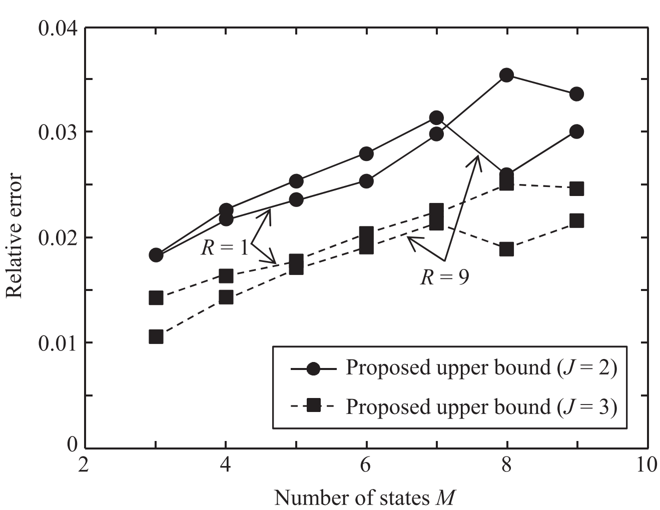

FIG. 4. Average relative errors of upper bounds, $\overline{Q_p}$, on the success probability of optimal inconclusive measurements for $M \geqslant 3$ quantum states.

ACKNOWLEDGMENTS

We are grateful to O. Hirota of Tamagawa University for support. This work was supported by JSPS KAKENHI Grants No. JP17H07115 and No. JP16H04367.

APPENDIX A: LEMMAS ON HERMITIAN OPERATORS

Let $\lambda_0(\hat{H}) \geqslant \lambda_1(\hat{H}) \geqslant \cdots \geqslant \lambda_{N-1}(\hat{H})$ be the ordered eigenvalues of an N-dimensional Hermitian operator $\hat{H}$.

Lemma 10. $\mathrm{Tr}\,\hat{A}_+ \geqslant \mathrm{Tr}\,\hat{B}_+$ holds for any Hermitian operators $\hat{A}$ and $\hat{B}$ with $\hat{A} \geqslant \hat{B}$, where the equality holds if and only if $\hat{A}_+ = \hat{B}_+$.

Proof. First, we show $\mathrm{Tr}\,\hat{A}_+ \geqslant \mathrm{Tr}\,\hat{B}_+$. Let N be the dimension of the space on which $\hat{A}$ and $\hat{B}$ act. Since $\hat{A} \geqslant \hat{B}$, $\sum_{n=0}^{k} \lambda_n(\hat{A}) \geqslant \sum_{n=0}^{k} \lambda_n(\hat{B})$ holds for any $k \in \mathcal{I}_N$ [35]. In contrast, for any N-dimensional Hermitian operator $\hat{H}$, the following can be easily obtained:

$$\mathrm{Tr}\,\hat{H}_+ \geqslant \sum_{n=0}^{k} \lambda_n(\hat{H}), \quad \forall k \in \mathcal{I}_N. \tag{A1}$$

Therefore, it follows that

$$\mathrm{Tr}\,\hat{A}_+ \geqslant \sum_{n=0}^{t-1} \lambda_n(\hat{A}) \geqslant \sum_{n=0}^{t-1} \lambda_n(\hat{B}) = \mathrm{Tr}\,\hat{B}_+, \tag{A2}$$

where t is the number of positive eigenvalues of $\hat{B}$.

Next, we show that $\hat{A}_+ = \hat{B}_+$ holds if $\mathrm{Tr}\,\hat{A}_+ = \mathrm{Tr}\,\hat{B}_+$ (the converse is obvious). Let $\hat{P} = \underline{P_+}(\hat{B})$. From $\hat{A}_+ \geqslant \hat{A}$, $\hat{A}_+ \geqslant \hat{B}$ holds. Premultiplying and postmultiplying $\hat{A}_+ \geqslant \hat{B}$ with $\hat{P}$

yields $\hat{P}\hat{A}_+\hat{P} \geqslant \hat{B}_+$. Thus, we have

$$\mathrm{Tr}\hat{A}_+ \geqslant \mathrm{Tr}(\hat{A}_+^{1/2}\hat{P}\hat{A}_+^{1/2}) = \mathrm{Tr}(\hat{P}\hat{A}_+\hat{P}) \geqslant \mathrm{Tr}\hat{B}_+ = \mathrm{Tr}\hat{A}_+, \tag{A3}$$

where the first inequality follows from $\hat{A}_+ \geqslant \hat{A}_+^{1/2}\hat{P}\hat{A}_+^{1/2}$, which is obtained from $\hat{1} \geqslant \hat{P}$. From Eq. (A3), $\mathrm{Tr}\hat{A}_+ = \mathrm{Tr}(\hat{P}\hat{A}_+\hat{P})$ holds. It thus follows that $\mathrm{supp}\hat{A}_+ \subseteq \mathrm{supp}\hat{P}$, $\hat{A}_+ = \hat{P}\hat{A}_+\hat{P}$, which gives $\hat{A}_+ \geqslant \hat{B}_+$. Since $\mathrm{Tr}(\hat{A}_+ - \hat{B}_+) = 0$, $\hat{A}_+ - \hat{B}_+ = 0$ holds. ■

Lemma 11. For any Hermitian operators $\hat{A}$ and $\hat{B}$, $\mathrm{Tr}\hat{A}_+ + \mathrm{Tr}\hat{B}_+ \geqslant \mathrm{Tr}(\hat{A}+\hat{B})_+$ holds.

Proof. $\hat{A}_+ \geqslant \hat{A}$ and $\hat{B}_+ \geqslant \hat{B}$ gives $\hat{A}_+ + \hat{B}_+ \geqslant \hat{A}+\hat{B}$. Thus, from Lemma 10, we have

$$\mathrm{Tr}\hat{A}_+ + \mathrm{Tr}\hat{B}_+ = \mathrm{Tr}(\hat{A}_+ + \hat{B}_+)_+ \geqslant \mathrm{Tr}(\hat{A}+\hat{B})_+. \tag{A4}$$

■

Lemma 12. For any Hermitian operator $\hat{A}$ and $\hat{B}$ with $\hat{A} \geqslant \hat{B}$,

$$\mathrm{Tr}[(\hat{A}-\hat{B})\underline{P_+}(\hat{A})] \geqslant \mathrm{Tr}[(\hat{A}-\hat{B})\overline{P_+}(\hat{B})]. \tag{A5}$$

Proof. Let us consider the following optimization problem:

$$\begin{aligned} &\text{maximize} && \mathrm{Tr}(\hat{C}\hat{\Phi}) \\ &\text{subject to} && \hat{1} \geqslant \hat{\Phi} \geqslant 0, \end{aligned} \tag{A6}$$

where $\hat{C}$ is a Hermitian operator. It is clear that $\hat{\Phi} = \underline{P_+}(\hat{C})$ and $\hat{\Phi} = \overline{P_+}(\hat{C})$ are optimal solutions to this problem. Substituting $\hat{C} = \hat{A}$ and $\hat{C} = \hat{B}$, respectively, into problem (A6) gives

$$\begin{aligned} \mathrm{Tr}[\hat{A}\underline{P_+}(\hat{A})] &\geqslant \mathrm{Tr}[\hat{A}\overline{P_+}(\hat{B})], \\ \mathrm{Tr}[\hat{B}\underline{P_+}(\hat{A})] &\leqslant \mathrm{Tr}[\hat{B}\overline{P_+}(\hat{B})]. \end{aligned} \tag{A7}$$

Therefore, Eq. (A5) holds. ■

Lemma 13. For any operator $\hat{A}$ and any positive semidefinite operators $\hat{\rho}$, $\hat{X}$, and $\hat{E}$ with $\hat{1} \geqslant \hat{E} \geqslant 0$,

$$\begin{aligned} &\mathrm{Tr}[\hat{A}[\hat{X} + (\hat{\rho}-\hat{X})_+]\hat{A}^\dagger] \\ &\geqslant \mathrm{Tr}[\hat{A}\hat{\rho}\hat{A}^\dagger(\hat{1}-\hat{E}) + \hat{A}\hat{X}\hat{A}^\dagger\hat{E}]. \end{aligned} \tag{A8}$$

The equality holds if and only if

$$\hat{A}(\hat{X}-\hat{\rho})_+\hat{A}^\dagger = [\hat{A}(\hat{X}-\hat{\rho})\hat{A}^\dagger]_+, \tag{A9}$$

$$\overline{P_+}[\hat{A}(\hat{X}-\hat{\rho})\hat{A}^\dagger] \geqslant \hat{E} \geqslant \underline{P_+}[\hat{A}(\hat{X}-\hat{\rho})\hat{A}^\dagger]. \tag{A10}$$

Proof. It follows that

$$\begin{aligned} &\mathrm{Tr}[\hat{A}[\hat{X} + (\hat{\rho}-\hat{X})_+]\hat{A}^\dagger] \\ &= \mathrm{Tr}[\hat{A}[\hat{\rho} + (\hat{X}-\hat{\rho})_+]\hat{A}^\dagger] \\ &\geqslant \mathrm{Tr}[\hat{A}\hat{\rho}\hat{A}^\dagger + (\hat{A}\hat{X}\hat{A}^\dagger - \hat{A}\hat{\rho}\hat{A}^\dagger)_+] \\ &\geqslant \mathrm{Tr}[\hat{A}\hat{\rho}\hat{A}^\dagger(\hat{1}-\hat{E}) + \hat{A}\hat{X}\hat{A}^\dagger\hat{E}], \end{aligned} \tag{A11}$$

where the second line follows from $\hat{X} + (\hat{\rho}-\hat{X})_+ = \hat{\rho} + (\hat{X}-\hat{\rho})_+$. The third line follows from Lemma 10 by substituting $\hat{A}(\hat{X}-\hat{\rho})_+\hat{A}^\dagger$ and $\hat{A}(\hat{X}-\hat{\rho})\hat{A}^\dagger$ for $\hat{A}$ and $\hat{B}$, respectively. Note that $\hat{A}(\hat{X}-\hat{\rho})_+\hat{A}^\dagger \geqslant \hat{A}(\hat{X}-\hat{\rho})\hat{A}^\dagger$ holds from $(\hat{X}-\hat{\rho})_+ \geqslant \hat{X}-\hat{\rho}$. The fourth line follows from Lemma 1. From Lemmas 1 and 10, the equality in Eq. (A11) holds if and only if Eqs. (A9) and (A10) hold. ■

Lemma 14. For any positive semidefinite operators $\hat{A}$ and $\hat{B}$ with $\mathrm{supp}\hat{A} \subseteq \mathrm{supp}\hat{B}$ and any operator $\hat{C}$, $\mathrm{supp}(\hat{C}\hat{A}\hat{C}^\dagger) \subseteq \mathrm{supp}(\hat{C}\hat{B}\hat{C}^\dagger)$ holds. Moreover, if $\mathrm{supp}\hat{A} = \mathrm{supp}\hat{B}$, then $\mathrm{supp}(\hat{C}\hat{A}\hat{C}^\dagger) = \mathrm{supp}(\hat{C}\hat{B}\hat{C}^\dagger)$ holds.

Proof. $\mathrm{supp}\hat{A} \subseteq \mathrm{supp}\hat{B}$ gives $\mathrm{Ker}\hat{A} \supseteq \mathrm{Ker}\hat{B}$. We obtain

$$\begin{aligned} |x\rangle \in \mathrm{Ker}(\hat{C}\hat{B}\hat{C}^\dagger) &\Longrightarrow \hat{B}^{\frac{1}{2}}\hat{C}^\dagger|x\rangle = 0 \\ &\Longrightarrow \hat{C}^\dagger|x\rangle \in \mathrm{Ker}\hat{B} \\ &\Longrightarrow \hat{C}^\dagger|x\rangle \in \mathrm{Ker}\hat{A} \\ &\Longrightarrow \hat{A}^{\frac{1}{2}}\hat{C}^\dagger|x\rangle = 0 \\ &\Longrightarrow |x\rangle \in \mathrm{Ker}(\hat{C}\hat{A}\hat{C}^\dagger), \end{aligned} \tag{A12}$$

which indicates $\mathrm{Ker}(\hat{C}\hat{A}\hat{C}^\dagger) \supseteq \mathrm{Ker}(\hat{C}\hat{B}\hat{C}^\dagger)$, i.e., $\mathrm{supp}(\hat{C}\hat{A}\hat{C}^\dagger) \subseteq \mathrm{supp}(\hat{C}\hat{B}\hat{C}^\dagger)$. If $\mathrm{supp}\hat{A} = \mathrm{supp}\hat{B}$, then, from $\mathrm{supp}\hat{A} \subseteq \mathrm{supp}\hat{B}$ and $\mathrm{supp}\hat{A} \supseteq \mathrm{supp}\hat{B}$, $\mathrm{supp}(\hat{C}\hat{A}\hat{C}^\dagger) = \mathrm{supp}(\hat{C}\hat{B}\hat{C}^\dagger)$ obviously holds. ■

APPENDIX B: SUPPLEMENT OF THEOREM 5

Let $\hat{P}_{\hat{X}}$ be the projection operator onto the support space of a positive semidefinite operator $\hat{X}$; i.e., $\hat{P}_{\hat{X}} = \underline{P_+}(\hat{X})$.

For any POVM $\Pi = \{\hat{\Pi}_m\}_{m\in\mathcal{I}_M}$, define $\hat{E}_m$ as

$$\hat{E}_m = (\hat{A}_m^-)^\dagger\left(\sum_{k=0}^{m-1}\hat{\Pi}_k\right)\hat{A}_m^-, \quad m \in \{1,2,\ldots,M-1\}, \tag{B1}$$

where $\hat{A}_m$ is defined as Eq. (27), and $\hat{A}^-$ denotes the Moore-Penrose inverse operator of $\hat{A}$. Now we show that Eq. (28) and $\hat{1} \geqslant \hat{E}_m \geqslant 0$ hold.

First, we show Eq. (28). From $\hat{A}_m^-\hat{A}_m = \hat{P}_{|\hat{A}_m|}$, we have that for any $m \in \mathcal{I}_{M-1}$,

$$|\hat{A}_m|^2 = \hat{A}_{m+1}^\dagger\hat{E}_{m+1}\hat{A}_{m+1} = \hat{P}_{|\hat{A}_{m+1}|}\left(\sum_{k=0}^{m}\hat{\Pi}_k\right)\hat{P}_{|\hat{A}_{m+1}|}, \tag{B2}$$

where the first equality follows from Eq. (27). Using Eq. (B2), we can show

$$|\hat{A}_m|^2 = \sum_{k=0}^{m}\hat{\Pi}_k, \forall m \in \mathcal{I}_M \tag{B3}$$

by induction as follows. The case of $m = M-1$ is obvious. Assume that Eq. (B3) holds when $m = t+1$ with $t \in \mathcal{I}_{M-1}$; we have

$$\begin{aligned} \mathrm{supp}\hat{P}_{|\hat{A}_{t+1}|} = \mathrm{supp}|\hat{A}_{t+1}|^2 &= \mathrm{supp}\left(\sum_{k=0}^{t+1}\hat{\Pi}_k\right) \\ &\supseteq \mathrm{supp}\left(\sum_{k=0}^{t}\hat{\Pi}_k\right), \end{aligned} \tag{B4}$$

which yields $\hat{P}_{|\hat{A}_{t+1}|}(\sum_{k=0}^{t}\hat{\Pi}_k)\hat{P}_{|\hat{A}_{t+1}|} = \sum_{k=0}^{t}\hat{\Pi}_k$. Thus, Eq. (B3) also holds when $m = t$. Equation (28) is readily obtained from Eq. (B3).

Next, we show $\hat{1} \geqslant \hat{E}_m \geqslant 0$. $\hat{E}_m \geqslant 0$ obviously holds, so we only need to show $\hat{1} \geqslant \hat{E}_m$. From Eq. (28), $|\hat{A}_{m-1}|^2 \leqslant |\hat{A}_m|^2$ holds. Premultiplying and postmultiplying $|\hat{A}_{m-1}|^2 \leqslant |\hat{A}_m|^2$ with $(\hat{A}_m^-)^\dagger$ and $\hat{A}_m^-$, respectively, and using $\hat{A}_m\hat{A}_m^- =$

$\hat{P}_{\hat{A}\hat{A}^\dagger}$, we have that for any m with $1 \leqslant m \leqslant M-1$,

$$\begin{aligned}\hat{E}_m &= (\hat{A}_m^-)^\dagger |\hat{A}_{m-1}|^2 \hat{A}_m^- \leqslant (\hat{A}_m^-)^\dagger |\hat{A}_m|^2 \hat{A}_m^- \\ &= (\hat{A}_m \hat{A}_m^-)^\dagger (\hat{A}_m \hat{A}_m^-) = \hat{P}_{\hat{A}\hat{A}^\dagger} \leqslant \hat{1}.\end{aligned} \tag{B5}$$

APPENDIX C: PROOF OF COROLLARY 6

The necessity is obvious from Theorem 5. We prove the sufficiency as follows. Assume $\overline{Q} = Q$. We choose $\{\hat{E}_k\}_{k=1}^{M-1}$ satisfying Eqs. (25) and (26) (such $\{\hat{E}_k\}_{k=1}^{M-1}$ exists from Theorem 5). To show Eq. (34), it is sufficient to show that the following equations hold for any m with $1 \leqslant m \leqslant M-1$:

$$\hat{A}_m(\hat{X}_{m-1} - \hat{\rho}_m)_+ \hat{A}_m^\dagger = \hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)_+ \hat{a}_m^\dagger, \tag{C1}$$

$$\hat{A}_m(\hat{X}_{m-1} - \hat{\rho}_m) \hat{A}_m^\dagger = \hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m) \hat{a}_m^\dagger, \tag{C2}$$

where $\hat{A}_m$ is defined by Eq. (27). $(\hat{X}_{m-1} - \hat{\rho}_m)_+$, $\hat{X}_{m-1}$, and $\hat{\rho}_m$ are positive semidefinite operators whose support spaces are subspaces of $\mathrm{supp}\hat{X}_m$. Thus, if

$$\hat{A}_m \hat{x} \hat{A}_m^\dagger = \hat{a}_m \hat{x} \hat{a}_m^\dagger, \quad \forall \hat{x} \geqslant 0 \text{ such that } \mathrm{supp}\,\hat{x} \subseteq \mathrm{supp}\hat{X}_m \tag{C3}$$

for any m with $1 \leqslant m \leqslant M-1$, then substituting $(\hat{X}_{m-1} - \hat{\rho}_m)_+$, $\hat{X}_{m-1}$, and $\hat{\rho}_m$ into x in Eq. (C3) gives Eqs. (C1) and (C2). Therefore, it suffices to show that Eq. (C3) holds for any m with $1 \leqslant m \leqslant M-1$.

In preparation for proving it, we show that if Eq. (C3) holds for a certain m with $1 \leqslant m \leqslant M-1$, then we have that for any Hermitian operator $\hat{y}$ with $\mathrm{supp}\hat{y} \subseteq \mathcal{R}_m$,

$$\hat{E}_m^{\frac{1}{2}} \hat{y} \hat{E}_m^{\frac{1}{2}} = \hat{e}_m \hat{y} \hat{e}_m, \tag{C4}$$

where $\mathcal{R}_m = \mathrm{supp}(\hat{a}_m \hat{X}_m \hat{a}_m^\dagger)$. Let $\hat{T}_m = \hat{a}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{a}_m^\dagger$; then, from Eq. (33), we have $\mathcal{R}_m = \mathrm{supp}\hat{T}_m$. Let $\underline{\hat{e}_m} = \underline{P_+}(\hat{T}_m)$. Recall $\hat{e}_m = \overline{P_+}(\hat{T}_m)$. For any $\hat{e}$ with $\hat{e}_m \geqslant \hat{e} \geqslant \underline{\hat{e}_m}$, $\mathrm{supp}\Delta\hat{e} \subseteq \mathrm{Ker}\hat{T}_m$ holds, where $\Delta\hat{e} = \hat{e} - \underline{\hat{e}_m}$, which indicates $\mathrm{supp}\Delta\hat{e}$ is perpendicular to $\mathcal{R}_m$. Thus, for any Hermitian operator $\hat{y}$ with $\mathrm{supp}\hat{y} \subseteq \mathcal{R}_m$, from $\Delta\hat{e}\hat{y} = \hat{y}\Delta\hat{e} = 0$, we obtain

$$\hat{e}\hat{y}\hat{e} = (\underline{\hat{e}_m} + \Delta\hat{e})\hat{y}(\underline{\hat{e}_m} + \Delta\hat{e}) = \underline{\hat{e}_m}\hat{y}\underline{\hat{e}_m}. \tag{C5}$$

In contrast, m satisfying Eq. (C3) also satisfies Eq. (C2), which yields $\hat{e}_m = \overline{P_+}[\hat{A}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{A}_m^\dagger]$ and $\underline{\hat{e}_m} = \underline{P_+}[\hat{A}_m(\hat{X}_{m-1} - \hat{\rho}_m)\hat{A}_m^\dagger]$. Accordingly, from Eq. (25), $\hat{e}_m \geqslant \hat{E}_m \geqslant \underline{\hat{e}_m}$ holds; thus, $\hat{e}_m^{\frac{1}{2}} \geqslant \hat{E}_m^{\frac{1}{2}} \geqslant \underline{\hat{e}_m}^{\frac{1}{2}}$ holds. From $\hat{e}_m^{\frac{1}{2}} = \hat{e}_m$ and $\underline{\hat{e}_m}^{\frac{1}{2}} = \underline{\hat{e}_m}$, this gives $\hat{e}_m \geqslant \hat{E}_m^{\frac{1}{2}} \geqslant \underline{\hat{e}_m}$. Therefore, substituting $\hat{e} = \hat{e}_m$ and $\hat{e} = \hat{E}_m^{\frac{1}{2}}$ into Eq. (C5) gives

$$\hat{E}_m^{\frac{1}{2}} \hat{y} \hat{E}_m^{\frac{1}{2}} = \underline{\hat{e}_m}\hat{y}\underline{\hat{e}_m} = \hat{e}_m \hat{y} \hat{e}_m, \tag{C6}$$

i.e., Eq. (C4) holds.

We prove Eq. (C3) for any m with $1 \leqslant m \leqslant M-1$ by induction on m. This is obvious for $m = M-1$, since $\hat{A}_{M-1} = \hat{a}_{M-1} = \hat{1}$ holds. Assume that, for a certain $m = k+1 \leqslant M-1$, Eq. (C3) holds. For any $\hat{x} \geqslant 0$ with $\mathrm{supp}\hat{x} \subseteq \mathrm{supp}\hat{X}_k$, we obtain

$$\begin{aligned}\hat{A}_k \hat{x} \hat{A}_k^\dagger &= \hat{E}_{k+1}^{\frac{1}{2}} \hat{A}_{k+1} \hat{x} \hat{A}_{k+1}^\dagger \hat{E}_{k+1}^{\frac{1}{2}} \\ &= \hat{E}_{k+1}^{\frac{1}{2}} \hat{a}_{k+1} \hat{x} \hat{a}_{k+1}^\dagger \hat{E}_{k+1}^{\frac{1}{2}} \\ &= \hat{e}_{k+1} \hat{a}_{k+1} \hat{x} \hat{a}_{k+1}^\dagger \hat{e}_{k+1} \\ &= \hat{a}_k \hat{x} \hat{a}_k^\dagger,\end{aligned} \tag{C7}$$

where the second line follows from $\mathrm{supp}\hat{x} \subseteq \mathrm{supp}\hat{X}_k \subseteq \mathrm{supp}\hat{X}_{k+1}$ and Eq. (C3) with $m = k+1$. The third line follows from $\mathrm{supp}(\hat{a}_{k+1}\hat{x}\hat{a}_{k+1}^\dagger) \subseteq \mathrm{supp}(\hat{a}_{k+1}\hat{X}_{k+1}\hat{a}_{k+1}^\dagger) = \mathcal{R}_{k+1}$, which is obtained by $\mathrm{supp}\hat{x} \subseteq \mathrm{supp}\hat{X}_{k+1}$ and Lemma 14, and from Eq. (C4) with $m = k+1$ and $\hat{y} = \hat{a}_{k+1}\hat{x}\hat{a}_{k+1}^\dagger$. Therefore, Eq. (C3) holds for $m = k$. ■

APPENDIX D: PROOF OF PROPOSITION 8

(1) We have

$$\begin{aligned}\lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2}) \geqslant a &\iff \hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2} \geqslant a\hat{1} \\ &\iff \hat{X}^\circ \geqslant a\hat{G}.\end{aligned} \tag{D1}$$

From Eq. (41), $s(a) = \mathrm{Tr}\hat{X}^\circ - ap$ holds when $\hat{X}^\circ \geqslant a\hat{G}$. Moreover, $\hat{X}^\circ \geqslant \hat{\rho}_m$ for any $m \in \mathcal{I}_M$ gives

$$\hat{X}^\circ - \frac{\hat{G}}{M} = \frac{1}{M}\sum_{m=0}^{M-1}(\hat{X}^\circ - \hat{\rho}_m) \geqslant 0. \tag{D2}$$

Thus, from Eq. (D1) with $a = 1/M$, $1/M \leqslant \lambda_{\min}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2})$.

(2) We have

$$\begin{aligned}a \geqslant \lambda_{\max}(\hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2}) &\iff a\hat{1} \geqslant \hat{G}^{-1/2}\hat{X}^\circ\hat{G}^{-1/2} \\ &\iff a\hat{G} \geqslant \hat{X}^\circ.\end{aligned} \tag{D3}$$

Thus, $a\hat{G} - \hat{X}^\circ \geqslant 0$. From Eq. (41) and $\mathrm{Tr}\hat{G} = 1$, we have

$$s(a) = \mathrm{Tr}\hat{X}^\circ + \mathrm{Tr}(a\hat{G} - \hat{X}^\circ) - ap = a(1-p). \tag{D4}$$

(3) For any t with $0 \leqslant t \leqslant 1$ and $a, a' \in \mathbf{R}_+$, substituting $\hat{A} = t(a\hat{G} - \hat{X}^\circ)$ and $\hat{B} = (1-t)(a'\hat{G} - \hat{X}^\circ)$ into Lemma 11 gives

$$\begin{aligned}&t\mathrm{Tr}(a\hat{G} - \hat{X}^\circ)_+ + (1-t)\mathrm{Tr}(a'\hat{G} - \hat{X}^\circ)_+ \\ &\quad \geqslant \mathrm{Tr}[[ta + (1-t)a']\hat{G} - \hat{X}^\circ]_+,\end{aligned} \tag{D5}$$

where we use $\hat{A} + \hat{B} = [ta + (1-t)a']\hat{G} - \hat{X}^\circ$. Therefore, from Eq. (41), $ts(a) + (1-t)s(a') \geqslant s[ta + (1-t)a']$ obviously holds; i.e., $s(a)$ is convex. ■

APPENDIX E: PROOF OF PROPOSITION 9

Let $\hat{\Phi}_a = \underline{P_+}(a\hat{G} - \hat{X}^\circ)$ and $\hat{\Phi}_a^+ = \overline{P_+}(a\hat{G} - \hat{X}^\circ)$; then, $\tilde{p}(a) = \mathrm{Tr}(\hat{G}\hat{\Phi}_a)$ and $\tilde{p}^+(a) = \mathrm{Tr}(\hat{G}\hat{\Phi}_a^+)$ hold.

(1) For any $a, a' \in \mathbf{R}_+$ with $a < a'$, we have

$$(a' - a)\mathrm{Tr}(\hat{G}\hat{\Phi}_{a'}) \geqslant (a' - a)\mathrm{Tr}(\hat{G}\hat{\Phi}_a^+), \tag{E1}$$

which follows from substituting $\hat{A} = a'\hat{G} - \hat{X}^\circ$ and $\hat{B} = a\hat{G} - \hat{X}^\circ$ into Lemma 12. Dividing both sides of Eq. (E1) by $a' - a$ yields $\tilde{p}(a') \geqslant \tilde{p}^+(a)$. In contrast, since $\tilde{p}(b) \leqslant \tilde{p}^+(b)$ for any $b \in \mathbf{R}_+$, we obtain

$$\tilde{p}(a) \leqslant \tilde{p}^+(a) \leqslant \tilde{p}(a') \leqslant \tilde{p}^+(a'), \tag{E2}$$

which indicates that $\tilde{p}(a)$ and $\tilde{p}^+(a)$ monotonically increase with respect to a.

(2) First, we show $\tilde{p}(a^\star) \leqslant p \leqslant \tilde{p}^+(a^\star)$, where $a^\star \in \mathrm{argmin}_a\, s(a)$. The dual problem of problem (38) is expressed as (see Ref. [36])

$$\begin{aligned} &\text{maximize} \quad \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})] \\ &\text{subject to} \quad \hat{1} \geqslant \hat{\Phi} \geqslant 0, \mathrm{Tr}(\hat{G}\hat{\Phi}) = p. \end{aligned} \tag{E3}$$

Let $\hat{\Phi}^\star$ be an optimal solution to problem (E3). Since the optimal value of problem (38), $s(a^\star)$, is equivalent to the optimal value of problem (E3), we have

$$\begin{aligned} s(a^\star) &= \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi}^\star)] \\ &= \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi}^\star)] + \mathrm{Tr}(a\hat{G}\hat{\Phi}^\star) - ap, \end{aligned} \tag{E4}$$

where the second line follows from $\mathrm{Tr}(\hat{G}\hat{\Phi}^\star) = p$. In contrast, $s(a) + ap$ is equivalent to the optimal value of problem (14) with $\hat{A} = a\hat{G}$ and $\hat{B} = \hat{X}^\circ$. Thus, from Eq. (15), we have that for any operator $\hat{\Phi}$ with $\hat{1} \geqslant \hat{\Phi} \geqslant 0$:

$$s(a) + ap \geqslant \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})] + \mathrm{Tr}(a\hat{G}\hat{\Phi}). \tag{E5}$$

From Lemma 1, if the equality in Eq. (E5) holds, then $\hat{\Phi}_a^+ \geqslant \hat{\Phi} \geqslant \hat{\Phi}_a$ holds. Thus, Eq. (E4) gives $\hat{\Phi}_{a^\star}^+ \geqslant \hat{\Phi}^\star \geqslant \hat{\Phi}_{a^\star}$. Multiplying both sides by $\hat{G}$ and taking the trace gives $\tilde{p}(a^\star) \leqslant p \leqslant \tilde{p}^+(a^\star)$.

Next assume that $\tilde{p}(a) \leqslant p \leqslant \tilde{p}^+(a)$; we show that a minimizes $s(a)$. Since problem (E3) is the dual problem of problem (38), we have that for any operator $\hat{\Phi}$ with $\hat{1} \geqslant \hat{\Phi} \geqslant 0$ and $\mathrm{Tr}(\hat{G}\hat{\Phi}) = p$,

$$s(a) \geqslant s(a^\star) \geqslant \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})]. \tag{E6}$$

Thus, to prove that a minimizes $s(a)$, $s(a) = s(a^\star)$, it suffices to find $\hat{\Phi}$ with $\hat{1} \geqslant \hat{\Phi} \geqslant 0$ and $\mathrm{Tr}(\hat{G}\hat{\Phi}) = p$ such that $s(a) = \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})]$. We show that $\hat{\Phi} = c\hat{\Phi}_a + (1-c)\hat{\Phi}_a^+$ is such a value, where $c = 1$ if $\tilde{p}(a) = \tilde{p}^+(a)$; otherwise, $c = [\tilde{p}^+(a) - p]/[\tilde{p}^+(a) - \tilde{p}(a)]$. Note that c obviously satisfies $0 \leqslant c \leqslant 1$. It is easily seen that $\hat{1} \geqslant \hat{\Phi} \geqslant 0$ and $\mathrm{Tr}(\hat{G}\hat{\Phi}) = p$ hold. From $\hat{\Phi}_a^+ \geqslant \hat{\Phi}_a$, $\hat{\Phi}_a^+ \geqslant \hat{\Phi} \geqslant \hat{\Phi}_a$ holds. Substituting $\hat{A} = a\hat{G}$ and $\hat{B} = \hat{X}^\circ$ into Lemma 1 and using Eq. (15) gives

$$\begin{aligned} \mathrm{Tr}\hat{X}^\circ + \mathrm{Tr}(a\hat{G} - \hat{X}^\circ)_+ &= \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})] + \mathrm{Tr}(a\hat{G}\hat{\Phi}) \\ &= \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})] + ap, \end{aligned} \tag{E7}$$

where the second line follows from $\mathrm{Tr}(\hat{G}\hat{\Phi}) = p$. Therefore, from Eq. (41), $s(a) = \mathrm{Tr}[\hat{X}^\circ(\hat{1} - \hat{\Phi})]$ holds. ■

[1] A. S. Holevo, J. Multivar. Anal. **3**, 337 (1973).
[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, San Diego, 1976).
[3] H. P. Yuen, K. S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **21**, 125 (1975).
[4] V. P. Belavkin, Stochastics **1**, 315 (1975).
[5] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[6] T. S. Usuda, I. Takumi, M. Hata, and O. Hirota, Phys. Lett. A **256**, 104 (1999).
[7] S. M. Barnett, Phys. Rev. A **64**, 030303 (2001).
[8] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter, Phys. Rev. A **65**, 052308 (2002).
[9] C. L. Chou and L. Y. Hsu, Phys. Rev. A **68**, 042305 (2003).
[10] Y. C. Eldar and G. D. Forney Jr., IEEE Trans. Inf. Theory **47**, 858 (2001).
[11] A. Chefles and S. M. Barnett, J. Mod. Opt. **45**, 1295 (1998).
[12] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).
[13] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).
[14] U. Herzog, Phys. Rev. A **86**, 032314 (2012).
[15] K. Nakahira, T. S. Usuda, and K. Kato, Phys. Rev. A **86**, 032316 (2012).
[16] E. Bagan, R. Muñoz-Tapia, G. A. Olivares-Renteria, and J. A. Bergou, Phys. Rev. A **86**, 040303 (2012).
[17] K. Nakahira, T. S. Usuda, and K. Kato, Phys. Rev. A **91**, 022331 (2015).
[18] U. Herzog, Phys. Rev. A **91**, 042338 (2015).
[19] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theory **49**, 1007 (2003).
[20] P. Hayden, D. Leung, and G. Smith, Phys. Rev. A **71**, 062339 (2005).
[21] A. Montanaro, Commun. Math. Phys. **273**, 619 (2007).
[22] M. Hayashi, A. Kawachi, and H. Kobayashi, Quantum Inf. Comput. **8**, 0345 (2008).
[23] A. Montanaro, in *2008 IEEE Information Theory Workshop* (IEEE, New York, 2008), pp. 378–380.
[24] D. Qiu, Phys. Rev. A **77**, 012328 (2008).
[25] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, Phys. Rev. Lett. **101**, 253601 (2008).
[26] J. Tyson, J. Math. Phys. **50**, 032106 (2009).
[27] D. Qiu and L. Li, Phys. Rev. A **81**, 042329 (2010).
[28] H. Sugimoto, T. Hashimoto, M. Horibe, and A. Hayashi, Phys. Rev. A **80**, 052322 (2009).
[29] C. W. Helstrom, J. Stat. Phys. **1**, 231 (1969).
[30] G. Cariolaro and A. Vigato, in *Information Theory Workshop (ITW), 2011 IEEE* (IEEE, New York, 2011), pp. 242–246.
[31] B. Borchers, Optim. Methods Softw. **11**, 613 (1999).
[32] K. Nakahira, K. Kato, and T. S. Usuda, Phys. Rev. A **91**, 012318 (2015).
[33] K. Nakahira, T. S. Usuda, and K. Kato, IEEE Trans. Inf. Theory **63**, 7845 (2017).
[34] K. Nakahira and T. S. Usuda, Phys. Rev. A **86**, 052323 (2012).
[35] A. W. Marshall, I. Olkin, and B. Arnold, *Inequalities: Theory of Majorization and Its Applications* (Springer Science & Business Media, New York, 2010).
[36] K. Nakahira, K. Kato, and T. S. Usuda, Phys. Rev. A **91**, 052304 (2015).