Optimal sequential state discrimination between two mixed quantum states

Min Namkung* and Younghun Kwon†
Department of Applied Physics, Hanyang University, Ansan, Kyunggi-Do 425-791, South Korea
(Received 12 April 2017; published 18 August 2017)

Recently, sequential state discrimination, as a quantum-key distribution protocol, has been proposed for multiple receivers. A previous study [J. A. Bergou *et al.*, Phys. Rev. Lett. **111**, 100501 (2013)] showed that every receiver could successfully perform a sequential state discrimination of two pure states with identical prior probabilities. In this study, we extend the sequential state discrimination to mixed states with arbitrary prior probability. First, we analytically obtain the condition of the receiver's optimal measurement. In addition, we show that the optimal probability for every receiver to share the mixed state prepared by the sender is not zero. Furthermore, we compare the sequential state discrimination to the strategies of quantum reproducing and quantum broadcasting. We find that there are cases in which, unlike that of the pure state, the sequential state discrimination of mixed states shows a better performance than the other strategies.

DOI: 10.1103/PhysRevA.96.022318

I. INTRODUCTION

Quantum state discrimination is one of the important research areas in quantum information processing [1,2]. In quantum state discrimination, the receiver only knows the prior probabilities of quantum states prepared by a sender. In order to obtain information of those states, the receiver should perform a measurement on those states. The result of the measurement can be either inconclusive or conclusive. When an inconclusive result is obtained, the receiver cannot obtain any information on the quantum states prepared by a sender. If a conclusive result is found, the receiver can obtain information on those quantum states, which cannot always be perfect [3]. When the strategy of unambiguous state discrimination is applied, a conclusive result of the receiver always provides information on the quantum state without error [4–7]. This implies that unambiguous state discrimination may play an important role in the protocols of quantum-key distribution [8].

Recently, Bergou *et al.* [9] proposed *sequential state discrimination*, which is a strategy for multiple receivers to discriminate a quantum state prepared by a sender when a classical communication is prohibited among receivers. By applying the strategy of unambiguous state discrimination to the receivers, they obtain the success probability of sequential state discrimination of two nonorthogonal pure states with identical prior probabilities. In this case, all of the receivers discriminate the two pure states. Pang *et al.* [10] found a larger success probability for the same situation, considered in Ref. [9], when every receiver discriminates only one of the two pure states. Also, sequential state discrimination was experimentally realized [11]. However, the condition for the receiver's optimal measurement of sequential state discrimination has not been found yet.

In this study, we extend the strategy of sequential state discrimination to mixed states. Furthermore, in our study, prior probability can be arbitrary. First, we consider the condition of the receiver's optimal measurements for the sequential state discrimination of two mixed states. Using the condition, we show that the success probability of the sequential state discrimination of mixed states for multiple receivers is not zero. This implies that multiple receivers can share the mixed states of a sender. In the case of mixed states with identical eigenvalues [12,13] and prior probabilities, we analytically determine the optimal measurement condition for receivers. In this study, we consider the sequential state discrimination of a rank-2 mixed state, which naturally includes the rank-1 state (pure state). Our approach can be extended to the sequential state discrimination of mixed states with arbitrary rank. In addition, we compare our strategy of sequential state discrimination to the other strategies, which include quantum reproducing and quantum broadcasting [14,15]. We show that there are cases in which sequential state discrimination of mixed states is better than the other strategies, which implies that sequential state discrimination of mixed states can be an effective strategy for state discrimination among multiple parties.

II. SCENARIO OF SEQUENTIAL STATE DISCRIMINATION

Quantum state discrimination is often performed between two parties [16,17]. Suppose that two parties consist of a sender, Alice, and a receiver, Bob. With a prior probability q_i, Alice prepares a quantum state ρ_i out of the quantum ensembles $\{\rho_1, \rho_2, \ldots, \rho_n\}$. Bob performs a measurement on the state prepared by Alice, using a positive operator valued measurement (POVM). If the strategy of quantum state discrimination is a minimum error discrimination [18], the result of Bob's measurement is conclusive. When Bob's measurement is allowed to be inconclusive and any two quantum states of quantum ensembles $\{\rho_1, \rho_2, \ldots, \rho_n\}$ do not have an identical support, Bob can use an unambiguous discrimination strategy [19,20]. In the case of unambiguous discrimination strategy, when Bob's result is conclusive, Bob can always trust his result. If the quantum state of a quantum ensemble $\{\rho_1, \rho_2, \ldots, \rho_n\}$ is not orthogonal, Bob obtains the probability of an inconclusive result. In fact, unambiguous discrimination can be used for quantum-key distribution. The way of applying unambiguous discrimination to quantum-key distribution can be understood in the following manner. When

*mslab.nk@gmail.com
†yyhkwon@hanyang.ac.kr

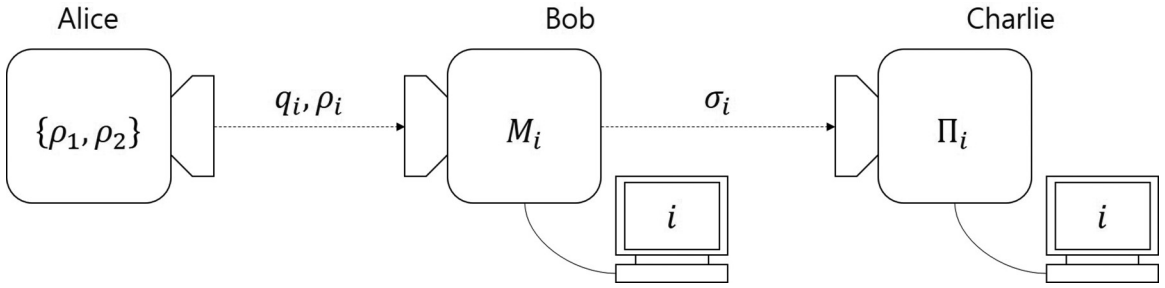

FIG. 1. Sequential state discrimination of Bob and Charlie. First, Alice prepares a quantum state ρ_i with prior probability q_i and sends it to Bob. By a nonoptimal POVM $\{M_i\}$, Bob performs unambiguous discrimination on Alice's quantum state. If Bob correctly discriminates the quantum state of Alice, Bob sends his postmeasurement state σ_i to Charlie. Then, Charlie discriminates σ_i, with an optimal POVM.

Alice prepares a quantum state out of nonorthogonal quantum states and sends it to Bob, if Bob performs unambiguous discrimination, Bob's conclusive result does not contain any error. Bob tells Alice whether his measurement succeeded or failed. In this way, they can establish a key. However, if Eve intervenes between Alice and Bob, eavesdropper Eve causes an error. When Eve's measurement fails, she should guess which state Alice prepares, which causes an error between the state Alice prepares and the state Bob receives.

In Ref. [9], by applying the unambiguous discrimination strategy, they proposed a sequential state discrimination. Here, let us explain the scenario of sequential state discrimination among a sender Alice and two receivers Bob and Charlie, which is expressed in Fig. 1. Alice prepares a quantum state ρ_i, with a prior probability q_i. Bob performs a measurement on the quantum state ρ_i, prepared by Alice, with POVM $\{M_0, M_1, \ldots, M_n\}$. Note that Bob does not inform Charlie of his result. Therefore, Charlie should read Alice's state ρ_i by measuring the postmeasurement state σ_i, which is the state after the measurement of Bob. In order to do this, Charlie measures σ_i with POVM $\{\Pi_0, \Pi_1, \ldots, \Pi_n\}$, where Π_0 ($\Pi_i \neq 0$) produces an inconclusive (conclusive) result. The probability for Bob and Charlie to obtain the correct result becomes

$$P_{s,\mathrm{seq}}^{(B,C)} = \sum_{i=1}^{n} q_i \mathrm{Tr}[\rho_i M_i]\mathrm{Tr}[\sigma_i \Pi_i]. \tag{1}$$

If Bob performs an optimal unambiguous discrimination on Alice's state ρ_i, because the post-measurement state σ_i has an identical support space, Charlie cannot discriminate the state σ_i without an error [21]. Therefore, Bob should use a nonoptimal measurement for Alice's state ρ_i. Meanwhile, the last receiver Charlie should perform the optimal POVM. Therefore, optimal sequential state discrimination can be obtained by the POVM that maximizes Eq. (1).

III. FORMULATION OF MIXED-STATE SEQUENTIAL STATE DISCRIMINATION

In the sequential state discrimination, if the probability of Eq. (1) is larger than zero, there is a chance for Bob and Charlie to obtain the information of Alice's quantum state. Reference [9] demonstrated that when Alice prepared an ensemble of pure quantum states $\{|\psi_1\rangle, |\psi_2\rangle\}$ with identical prior probabilities, Bob and Charlie could share Alice's quantum state with a nonzero probability.

In this article, we extend the result of Ref. [9], which considers only pure states, to that of mixed states. Furthermore, we consider the situation in which Alice prepares an ensemble of mixed quantum states with arbitrary prior probabilities. Now, let us assume that Alice prepares an ensemble of two mixed quantum states $\{\rho_1, \rho_2\}$ with a prior probability q_i, where $i = 1,2$. The two mixed state of Alice lie in four-dimensional Hilbert space and ρ_i has a spectral decomposition as follows:

$$\begin{aligned} \rho_1 &= r_1 |r_1\rangle \langle r_1| + \bar{r}_1 |\bar{r}_1\rangle \langle \bar{r}_1|, \\ \rho_2 &= r_2 |r_2\rangle \langle r_2| + \bar{r}_2 |\bar{r}_2\rangle \langle \bar{r}_2|. \end{aligned} \tag{2}$$

Here, $\{|r_i\rangle, |\bar{r}_i\rangle\}$ is an orthonormal basis of ρ_i. In the orthonormal basis $\{|r_i\rangle, |\bar{r}_i\rangle\}$ ($i = 1,2$), they fulfill the relations $\langle r_1|r_2\rangle = c$, $\langle \bar{r}_1|\bar{r}_2\rangle = \bar{c}$ and $\langle r_1|\bar{r}_2\rangle = \langle r_2|\bar{r}_1\rangle = 0$ [20]. $\{r_i, \bar{r}_i\}$ are the eigenvalues of ρ_i, satisfying $r_i + \bar{r}_i = 1$. When both $|c|$ and $|\bar{c}|$ are not one, the supports of ρ_1 and ρ_2 do not coincide. In this case, there is a POVM of Bob that can discriminate ρ_1 and ρ_2 without error. The rank of the quantum states of Alice can be up to two. Therefore, the POVM of Bob becomes

$$\begin{aligned} M_1 &= \alpha_1 |\alpha_1\rangle \langle \alpha_1| + \bar{\alpha}_1 |\bar{\alpha}_1\rangle \langle \bar{\alpha}_1|, \\ M_2 &= \alpha_2 |\alpha_2\rangle \langle \alpha_2| + \bar{\alpha}_2 |\bar{\alpha}_2\rangle \langle \bar{\alpha}_2|, \\ M_0 &= \mathcal{I} - M_1 - M_2, \end{aligned} \tag{3}$$

where $\{|\alpha_i\rangle, |\bar{\alpha}_i\rangle\}$ is an orthonormal basis of M_i ($i = 1,2$). α_i and $\bar{\alpha}_i$ are non-negative real numbers, with the condition $0 \leqslant \alpha_i, \bar{\alpha}_i \leqslant 1$. Bob's POVM in Eq. (3) fulfills the properties (B1) $M_i \geqslant 0$ ($\forall i \in \{0,1,2\}$), (B2) $M_0 + M_1 + M_2 = \mathcal{I}$, and (B3) $\mathrm{Tr}[\rho_i M_j] = 0$ ($\forall i \in \{1,2\}$ such that $i \neq j$). (B1) is the positive-semidefinite condition and (B2) is the completeness condition. (B3) implies that Bob can discriminate Alice's state without error. When $\{|\alpha_i\rangle, |\bar{\alpha}_i\rangle\}$ has orthogonal properties such as $|\alpha_i\rangle \perp |r_j\rangle$ and $|\bar{\alpha}_i\rangle \perp |\bar{r}_j\rangle$ ($\forall i, j \in \{1,2\}, i \neq j$), the POVM of Eq. (3) fulfills property (B3). If each of $|c|$ and $|\bar{c}|$ are less than one, there exists $\{|\alpha_i\rangle, |\bar{\alpha}_i\rangle\}$ that satisfies the orthogonal properties. When $M_0 = \mathcal{I} - M_1 - M_2$ is a positive-semidefinite operator, (B1) and (B2) hold simultaneously and Bob's POVM should satisfy [19]

$$\begin{aligned} \alpha_1\alpha_2(1 - |c|^2) - \alpha_1 - \alpha_2 + 1 > 0, \\ \bar{\alpha}_1\bar{\alpha}_2(1 - |\bar{c}|^2) - \bar{\alpha}_1 - \bar{\alpha}_2 + 1 > 0. \end{aligned} \tag{4}$$

The derivation of this condition can be found in Appendix A. The inequalities of Eq. (4) are strict inequalities. If

the left-hand side of Eq. (4) becomes zero, Bob's POVM performs an optimal discrimination on Alice's mixed state. Then, Charlie will not be able to obtain any information about Alice's quantum states. In order to consider the postmeasurement state of Bob σ_i, we should consider the Kraus operator $\{K_0, K_1, K_2\}$, corresponding to Bob's POVM [22]. For $i = 1,2$, the Kraus operator K_i satisfying $M_i = K_i^\dagger K_i$ can be determined by a singular-value decomposition. The Kraus operator we use in this paper is the special form corresponding to Bob's POVM [23,24]. Since in four-dimensional Hilbert space the number of 2-rank mixed states that Charlie can discriminate without error is two, we can consider the special Kraus operator. Meanwhile, the Kraus operator K_0 corresponding to M_0 maps the support of ρ_i to the support of σ_i [9]. In Appendix B, we prove the existence of the operator K_0. Using these operators, the postmeasurement state of Bob σ_i becomes

$$\sigma_i = \frac{K_i \rho_i K_i^\dagger}{\mathrm{Tr}[K_i \rho_i K_i^\dagger]} \equiv s_i \left|s_i\right\rangle \left\langle s_i\right| + \bar{s}_i \left|\bar{s}_i\right\rangle \left\langle \bar{s}_i\right|, \tag{5}$$

where $\{|s_i\rangle, |\bar{s}_i\rangle\}$ are the orthonormal bases of σ_i and satisfy $\langle s_1|s_2\rangle = c'$, $\langle \bar{s}_1|\bar{s}_2\rangle = \bar{c}'$, $\langle s_1|\bar{s}_2\rangle = \langle s_2|\bar{s}_1\rangle = 0$. Here, $\{s_i, \bar{s}_i\}$ are the eigenvalues of σ_i with the property $s_i + \bar{s}_i = 1$. In Appendix B, we demonstrate that $|c| < |c'|$ and $|\bar{c}| < |\bar{c}'|$. These inequalities imply that Bob obtains information about Alice's state. When Bob uses a nonoptimal POVM, $|c'|$ and $|\bar{c}'|$ are less than one. In this case, Charlie can obtain information about Alice's state ρ_i from the postmeasurement state of Bob σ_i. As the postmeasurement state of Bob σ_i can be described by rank-2 density matrices, Charlie's POVM can be given by

$$\begin{aligned} \Pi_1 &= \beta_1 \left|\beta_1\right\rangle \left\langle \beta_1\right| + \bar{\beta}_1 \left|\bar{\beta}_1\right\rangle \left\langle \bar{\beta}_1\right|, \\ \Pi_2 &= \beta_2 \left|\beta_2\right\rangle \left\langle \beta_2\right| + \bar{\beta}_2 \left|\bar{\beta}_2\right\rangle \left\langle \bar{\beta}_2\right|, \\ \Pi_0 &= \mathcal{I} - \Pi_1 - \Pi_2. \end{aligned} \tag{6}$$

Here, $\{|\beta_i\rangle, |\bar{\beta}_i\rangle\}$ are the orthonormal bases of $\Pi_i (i = 1,2)$. β_i and $\bar{\beta}_i$ are non-negative real numbers with the property $0 \leqslant \beta_i, \bar{\beta}_i \leqslant 1$. The POVM of Eq. (6) should satisfy (C1) $\Pi_i \geqslant 0$ $(\forall i \in \{0,1,2\})$, (C2) $\Pi_0 + \Pi_1 + \Pi_2 = \mathcal{I}$, and (C3) $\mathrm{Tr}[\sigma_i \Pi_j] = 0$ $(\forall i, j \in \{1,2\}$ such that $i \neq j)$. (C3) is the condition that Charlie can be confident of his results. When the postmeasurement state of Bob σ_i fulfills $|c'|, |\bar{c}'| < 1$, there exists a POVM with property (C3). When $\Pi_0 = \mathcal{I} - \Pi_1 - \Pi_2$ is positive semidefinite, the inconclusive result of Charlie is obtained by Π_0. Then, Charlie's POVM $\{\Pi_0, \Pi_1, \Pi_2\}$ satisfies (C1) and (C2), providing the conditions

$$\begin{aligned} \beta_1\beta_2(1 - |c'|^2) - \beta_1 - \beta_2 + 1 = 0, \\ \bar{\beta}_1\bar{\beta}_2(1 - |\bar{c}'|^2) - \bar{\beta}_1 - \bar{\beta}_2 + 1 = 0. \end{aligned} \tag{7}$$

Note that the conditions of Charlie's POVM are given by equality, unlike Bob's condition. This implies that Charlie's POVM performs an optimal measurement on the postmeasurement state of Bob σ_i. Therefore, the postmeasurement states of Charlie share the same support, which implies that any other party cannot obtain information about Alice's state ρ_i, from the postmeasurement states of Charlie. The optimal success probability of Bob and Charlie becomes $P_{s,\mathrm{seq}}^{(B,C)} = f(\alpha_1^{\mathrm{opt}}, \alpha_2^{\mathrm{opt}}) + \bar{f}(\bar{\alpha}_1^{\mathrm{opt}}, \bar{\alpha}_2^{\mathrm{opt}})$, where $(\alpha_1^{\mathrm{opt}}, \alpha_2^{\mathrm{opt}})$ and $(\bar{\alpha}_1^{\mathrm{opt}}, \bar{\alpha}_2^{\mathrm{opt}})$ are given as follows:

$$(\alpha_1^{\mathrm{opt}}, \alpha_2^{\mathrm{opt}}) \in \left\{(\alpha_1^\star, \alpha_2^\star), \left(\frac{1}{1+|c|}, 0\right), \left(0, \frac{1}{1+|c|}\right)\right\}, \tag{8}$$

$$(\bar{\alpha}_1^{\mathrm{opt}}, \bar{\alpha}_2^{\mathrm{opt}}) \in \left\{(\bar{\alpha}_1^\star, \bar{\alpha}_2^\star), \left(\frac{1}{1+|\bar{c}|}, 0\right), \left(0, \frac{1}{1+|\bar{c}|}\right)\right\}. \tag{9}$$

Here, $(\alpha_1^{\mathrm{opt}}, \alpha_2^{\mathrm{opt}})$ and $(\bar{\alpha}_1^{\mathrm{opt}}, \bar{\alpha}_2^{\mathrm{opt}})$ satisfy the following conditions:

$$\begin{aligned} \alpha_2^\star &= \frac{\alpha_1^\star\{1 - \alpha_1^\star(1-|c|^2)\}^3}{x + \alpha_1^\star(1-|c|^2)\{1 - \alpha_1^\star(1-|c|^2)\}^3}, \; x = |c|^2 \frac{q_2 r_2}{q_1 r_1}, \\ \alpha_1^\star &= \frac{\alpha_2^\star\{1 - \alpha_2^\star(1-|c|^2)\}^3}{y + \alpha_2^\star(1-|c|^2)\{1 - \alpha_2^\star(1-|c|^2)\}^3}, \; y = |c|^2 \frac{q_1 r_1}{q_2 r_2}, \\ \bar{\alpha}_2^\star &= \frac{\bar{\alpha}_1^\star\{1 - \bar{\alpha}_1^\star(1-|\bar{c}|^2)\}^3}{\bar{x} + \bar{\alpha}_1^\star(1-|\bar{c}|^2)\{1 - \bar{\alpha}_1^\star(1-|\bar{c}|^2)\}^3}, \; \bar{x} = |\bar{c}|^2 \frac{q_2 \bar{r}_2}{q_1 \bar{r}_1}, \\ \bar{\alpha}_1^\star &= \frac{\bar{\alpha}_2^\star\{1 - \bar{\alpha}_2^\star(1-|\bar{c}|^2)\}^3}{\bar{y} + \bar{\alpha}_2^\star(1-|\bar{c}|^2)\{1 - \bar{\alpha}_2^\star(1-|\bar{c}|^2)\}^3}, \; \bar{y} = |\bar{c}|^2 \frac{q_1 \bar{r}_1}{q_2 \bar{r}_2}, \end{aligned} \tag{10}$$

$$\begin{aligned} \alpha_2^\star &\leqslant \frac{\alpha_1^\star\{1 - \alpha_1^\star(1-|c|^2)\}}{x + \alpha_1^\star(1-|c|^2)\{1 - \alpha_1^\star(1-|c|^2)\}}, \; x = |c|^2 \frac{q_2 r_2}{q_1 r_1}, \\ \alpha_1^\star &\leqslant \frac{\alpha_2^\star\{1 - \alpha_2^\star(1-|c|^2)\}}{y + \alpha_2^\star(1-|c|^2)\{1 - \alpha_2^\star(1-|c|^2)\}}, \; y = |c|^2 \frac{q_1 r_1}{q_2 r_2}, \\ \bar{\alpha}_2^\star &\leqslant \frac{\bar{\alpha}_1^\star\{1 - \bar{\alpha}_1^\star(1-|\bar{c}|^2)\}}{\bar{x} + \bar{\alpha}_1^\star(1-|\bar{c}|^2)\{1 - \bar{\alpha}_1^\star(1-|\bar{c}|^2)\}}, \; \bar{x} = |\bar{c}|^2 \frac{q_2 \bar{r}_2}{q_1 \bar{r}_1}, \\ \bar{\alpha}_1^\star &\leqslant \frac{\bar{\alpha}_2^\star\{1 - \bar{\alpha}_2^\star(1-|\bar{c}|^2)\}}{\bar{y} + \bar{\alpha}_2^\star(1-|\bar{c}|^2)\{1 - \bar{\alpha}_2^\star(1-|\bar{c}|^2)\}}, \; \bar{y} = |\bar{c}|^2 \frac{q_1 \bar{r}_1}{q_2 \bar{r}_2} \end{aligned} \tag{11}$$

(see Appendix C for a detailed derivation of the optimization). If two mixed states of Alice are symmetric and are prepared with equal prior probability, the optimal success probability can be found, as summarized in Table I. Note that there exists a POVM of Bob and Charlie, not being a null operator, that provides a success probability of sequential state discrimination. It is different from the case of sequential state discrimination of the pure state [9]. In sequential state discrimination of a pure state, there is a case that optimal POVM has a null element [10]. However, in sequential state discrimination of a mixed state, POVM without a null element can obtain an optimal success probability, which can be useful in quantum-key distribution. This is because in a quantum-key distribution protocol one should discriminate every quantum state. This implies that Bob and Charlie can always share the mixed state prepared by Alice, with a nonzero probability, which is one of the main results of our study. Our approach for mixed states naturally includes the case of sequential state discrimination of the pure state. It is because a pure state can be thought of as a special case in which the eigenvalues of two rank-2 mixed states are zero and one. Furthermore, by considering an example, we will show that in the case of the same fidelity, if a sender encodes a message onto mixed states rather than pure states, the receivers Bob and Charlie may share the Alice's message with a higher success probability. In addition, it will be shown that unlike the pure state, when a sender prepares the mixed state, there

TABLE I. Optimal success probability of Bob and Charlie in terms of $|c|$ and $|\bar{c}|$. Here, $|c| = |\langle r_1|r_2\rangle|$ and $|\bar{c}| = |\langle \bar{r}_1|\bar{r}_2\rangle|$ denote the overlap of two mixed states ρ_1,ρ_2 which Alice prepares. Here, the optimal success probability is obtained when the two mixed states are prepared with identical prior probabilities, and the optimal success probability can be categorized into four cases, in terms of $|c|$ and $|\bar{c}|$.

	$\lvert c\rvert \leqslant 3-2\sqrt{2}$	$\lvert c\rvert > 3-2\sqrt{2}$
$\lvert\bar{c}\rvert \leqslant 3-2\sqrt{2}$	$P_{\text{seq}}^{(B,C)} = r(1-\sqrt{\lvert\bar{c}\rvert})^2 + \bar{r}(1-\sqrt{\lvert\bar{c}\rvert})^2$	$P_{\text{seq}}^{(B,C)} = 0.5r(1-\lvert c\rvert)^2 + \bar{r}(1-\sqrt{\lvert\bar{c}\rvert})^2$
$\lvert\bar{c}\rvert > 3-2\sqrt{2}$	$P_{\text{seq}}^{(B,C)} = r(1-\sqrt{\lvert c\rvert})^2 + 0.5\bar{r}(1-\lvert\bar{c}\rvert)^2$	$P_{\text{seq}}^{(B,C)} = 0.5r(1-\lvert c\rvert)^2 + 0.5\bar{r}(1-\lvert\bar{c}\rvert)^2$

are cases in which the sequential state discrimination strategy shows a better performance than the other strategies, such as quantum reproducing and quantum broadcasting.

In fact, our approach can be extended to sequential state discrimination of the rank-N mixed state ($N \geqslant 1$), as Bob's POVM element M_0 corresponding to the inconclusive result consists of the two-dimensional block matrix. This can be seen in Appendix A.

As explained in Table I, it is clear that if Alice prepares two symmetric mixed states, receivers can share the mixed state of Alice, by sequential state discrimination. When the two mixed states are not symmetric, the optimal sequential state discrimination is explained in the following example.

Example. Alice prepares a mixed state out of the two mixed states ρ_1,ρ_2 with equal prior probabilities,

$$\begin{aligned}\rho_1 &= 0.2\,|0\rangle\langle 0| + 0.8\,|1\rangle\langle 1|,\\ \rho_2 &= 0.14(0.10\,|0\rangle + 0.995\,|2\rangle)(0.10\,\langle 0| + 0.995\,\langle 2|)\\ &\quad + 0.86(0.15\,|1\rangle + 0.989\,|3\rangle)(0.15\,\langle 1| + 0.989\,\langle 3|). \quad (12)\end{aligned}$$

As we can see, ρ_1 and ρ_2 are not symmetric. Because $|c| = 0.1$ and $|\bar{c}| = 0.15$, there exists a POVM with which Bob can discriminate ρ_1 and ρ_2 without error:

$$\begin{aligned}M_1 &= \alpha_1(0.995\,|0\rangle - 0.1\,|2\rangle)(0.995\,\langle 0| - 0.1\,\langle 2|)\\ &\quad + \bar{\alpha}_1(0.989\,|1\rangle - 0.15\,|3\rangle)(0.989\,\langle 1| - 0.15\,\langle 3|),\\ M_2 &= \alpha_2\,|2\rangle\langle 2| + \bar{\alpha}_2\,|3\rangle\langle 3|, \quad (13)\end{aligned}$$

where $(\alpha_1,\alpha_2) = (0.7850, 0.5568)$ satisfies Eqs. (10) and (11). Among the three candidates of optimal points {(0.7850, 0.5568),(0,0.9091),(0.9091,0)} (see Fig. 2), the first one provides the largest value of f. Therefore, $(\alpha_1^{\text{opt}},\alpha_2^{\text{opt}}) = (0.7850,0.5568)$ is the optimal point of f. Meanwhile, $(\bar{\alpha}_1,\bar{\alpha}_2) = (0.5854,0.6643)$ fulfills Eqs. (10) and (11). Among the three candidates of optimal points {(0.5854,0.6643), (0.8695,0),(0,0.8695)} (see Fig. 2), the first one produces the largest value of $\bar{f}$ and $(\bar{\alpha}_1^{\text{opt}},\bar{\alpha}_2^{\text{opt}}) = (0.5854,0.6643)$ is the optimal point of $\bar{f}$. Therefore, the optimal success probability of Bob and Charlie becomes $f(0.7850,0.5568) + \bar{f}(0.5854,0.6643) = 0.45242$. Then, the Kraus operators of Bob become $K_1 = \sqrt{0.7850}\,|0\rangle\,(0.995\,\langle 0| - 0.1\,\langle 2|) + \sqrt{0.5854}\,|1\rangle\,(0.989\,\langle 1| - 0.15\,\langle 3|)$, $K_2 = \sqrt{0.5568}(0.316\,|0\rangle + 0.949\,|2\rangle)\,\langle 2| + \sqrt{0.6643}(0.387\,|1\rangle + 0.922\,|3\rangle)\,\langle 3|$ (see Appendix B). Charlie's POVM to discriminate σ_1,σ_2 without error becomes

$$\begin{aligned}\Pi_1 &= \beta_1(0.949\,|0\rangle - 0.316\,|2\rangle)(0.949\,\langle 0| - 0.316\,\langle 2|)\\ &\quad + \bar{\beta}_1(0.922\,|1\rangle - 0.387\,|3\rangle)(0.922\,\langle 1| - 0.387\,\langle 3|),\\ \Pi_2 &= \beta_2\,|2\rangle\langle 2| + \bar{\beta}_2\,|3\rangle\langle 3|, \quad (14)\end{aligned}$$

where $\beta_1,\beta_2,\bar{\beta}_1,\bar{\beta}_2$ are determined automatically if Bob's POVM is fixed. The fidelity [25] of two mixed states in this example is 0.1411. For the pure states with the same fidelity, the optimal success probability becomes 0.3989, which is less value than that of the mixed states with the same fidelity. It implies that our proposal using mixed states is more effective in quantum-key distribution than that of pure states. In the case of the same fidelity, if Alice encodes a message onto mixed states rather than pure states, Bob and Charlie can share the Alice's message with a higher success probability.

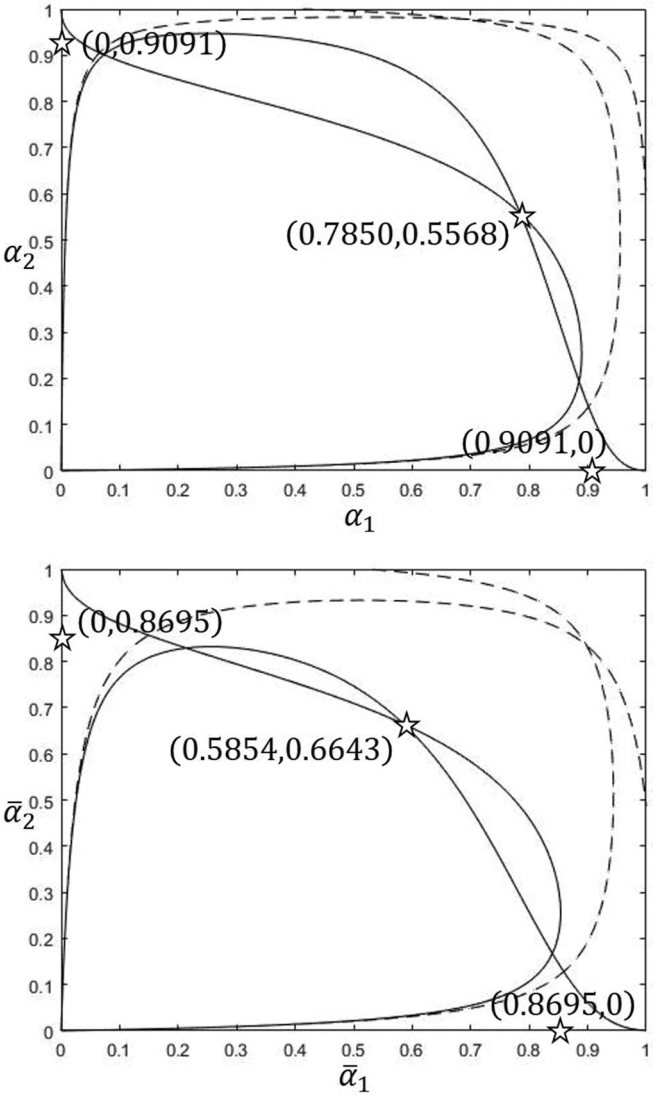

FIG. 2. Bob's POVM condition that optimizes sequential state discrimination. The solid lines display the points satisfying Eq. (10). The dotted lines display the points satisfying the equality condition of Eq. (11).

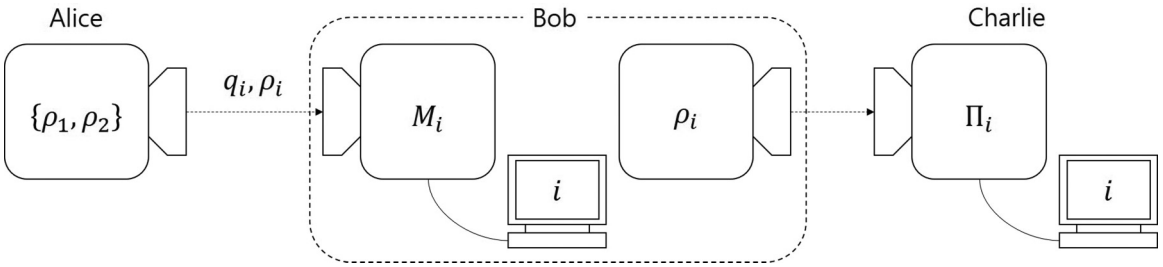

FIG. 3. Quantum reproducing scenario of Bob and Charlie for a quantum state prepared by Alice. Bob performs the optimal POVM $\{M_i\}$ on quantum state ρ_i prepared by Alice with prior probability q_i. If Bob correctly discriminates Alice's quantum state, he reproduces ρ_i and sends it to Charlie. Using an optimal POVM, Charlie discriminates the quantum state ρ_i received by Bob. When Bob's measurement fails to discriminate Alice's mixed state, Bob informs Charlie of the fact that his measurement fails.

IV. COMPARISON WITH OTHER SCENARIOS

In this section, we compare the sequential state discrimination strategy with the other strategies. The first strategy is considered in Ref. [9], which can be called quantum reproducing (see Fig. 3). However, the difference between this and our strategy is that Alice uses mixed states. First, Alice prepares a quantum state out of $\{\rho_1, \rho_2\}$ with the same prior probabilities and sends it to Bob [the spectral decomposition of the two mixed states is identical to Eq. (2)]. When Bob succeeds at discriminating Alice's mixed state without error, Bob produces Alice's mixed state and sends it to Charlie. Charlie may discriminate the mixed state sent by Bob without error. When Bob's measurement fails to discriminate Alice's mixed state, Bob informs Charlie of the fact that his measurement fails. In this strategy, Bob and Charlie should use an optimal POVM. The probability that Bob and Charlie can successfully share Alice's mixed state ρ_i becomes

$$P^{(B,C)}_{s,\text{reproduce}} = (1 - \sqrt{r_1 r_2}|c| - \sqrt{\bar{r}_1 \bar{r}_2}|\bar{c}|)^2. \tag{15}$$

The other strategy is that Bob broadcasts Alice's mixed state with a probability [14] (see Fig. 4). The broadcast strategy is to transform the initial state ρ_i into the ρ satisfying $\text{Tr}_B \rho = \text{Tr}_C \rho = \rho_i$. If Alice's state is pure, the broadcast strategy is identical to quantum cloning. When Bob successfully broadcasts Alice's state ρ_i, Bob and Charlie can share ρ. Bob and Charlie perform an optimal POVM on their partial state. When Bob's measurement fails to discriminate Alice's mixed state, Bob informs Charlie of the fact that his measurement fails. In this broadcast strategy, the probability that Bob and Charlie can find ρ_i can be given by [15]

$$P^{(B,C)}_{s,\text{broad}} = \min\left\{\frac{1}{1+|c|}, \frac{1}{1+|\bar{c}|}\right\}(1 - \sqrt{r_1 r_2}|c| - \sqrt{\bar{r}_1 \bar{r}_2}|\bar{c}|)^2. \tag{16}$$

The detailed calculation can be found in Appendix D. Here, let us compare the sequential state discrimination strategy with the other strategies described above. We should note that unlike the pure state, when Alice prepares the mixed state, there are cases in which the sequential state discrimination strategy shows a better performance than the other strategies. As a first example, let us consider $\rho_1 = 0.5\,|0\rangle\langle 0| + 0.5\,|3\rangle\langle 3|$ and $\rho_2 = 0.5(0.7317\,|0\rangle + 0.6816\,|2\rangle)(0.7317\,\langle 0| + 0.6816\,\langle 2|) + 0.5\,|1\rangle\langle 1|$. If a sender prepares one of these states with identical prior probabilities, we have $P^{(B,C)}_{s,\text{seq}} = 0.51799$, $P^{(B,C)}_{s,\text{broad}} = 0.2322$, and $P^{(B,C)}_{s,\text{reproduce}} = 0.40214$. Therefore, $P^{(B,C)}_{s,\text{seq}}$ is larger than $P^{(B,C)}_{s,\text{broad}}$ ($P^{(B,C)}_{s,\text{reproduce}}$) by 0.28577 (0.11585). The second example is the quantum system with $\rho_1 = 0.3\,|0\rangle\langle 0| + 0.7\,|1\rangle\langle 1|$ and $\rho_2 = 0.3(0.09109\,|0\rangle + 0.9958\,|2\rangle)(0.09109\,\langle 0| + 0.9958\,\langle 2|) + 0.7(0.8639\,|1\rangle + 0.5036\,|3\rangle)(0.8639\,\langle 1| + 0.5036\,\langle 3|)$. When the prior probabilities are identical, we have $P^{(B,C)}_{s,\text{seq}} = 0.15272$, $P^{(B,C)}_{s,\text{broad}} = 0.07263$, and $P^{(B,C)}_{s,\text{reproduce}} = 0.13538$. Therefore, $P^{(B,C)}_{s,\text{seq}}$ is larger than $P^{(B,C)}_{s,\text{broad}}$ ($P^{(B,C)}_{s,\text{reproduce}}$) by 0.08009 (0.01734). This fact implies that the sequential state discrimination strategy can be the better strategy for mixed states, which differs in the case of the pure state [9].

V. CONCLUSION

In our study, we extended the sequential state discrimination of pure states to that of mixed states with arbitrary prior probabilities. First, we obtained the success probability and optimal measurement of receivers Bob and Charlie, for a rank-2 mixed state prepared by Alice. The condition of eigenvalues for an optimal POVM was found by a high-order algebraic equation. In order to find an optimal POVM, we had to solve the high-order algebraic equation, which can be determined numerically. When the rank-2 mixed states have identical eigenvalues and prior probabilities, the solution to the algebraic equation could be obtained analytically, which implies the existence of an analytic optimal solution. By the optimal POVM condition, we could show that Bob and Charlie could share the rank-2 mixed state, prepared by Alice, with a nonzero probability. In fact, our approach can be extended to a rank-N mixed state. In addition, we compared our strategy of sequential state discrimination to the cases of quantum reproducing and quantum broadcasting. We found that unlike the pure-state case, the sequential state discrimination of mixed states may be better than the other strategies.

In fact, we assumed that the support spaces of the two mixed states should not be overlapped. As the unambiguous state discrimination of two mixed states with an arbitrary support space is not yet solved, it is difficult to handle the sequential state discrimination of arbitrary mixed states [26–28]. In the future, we will study the sequential state discrimination for mixed states with an arbitrary support space.

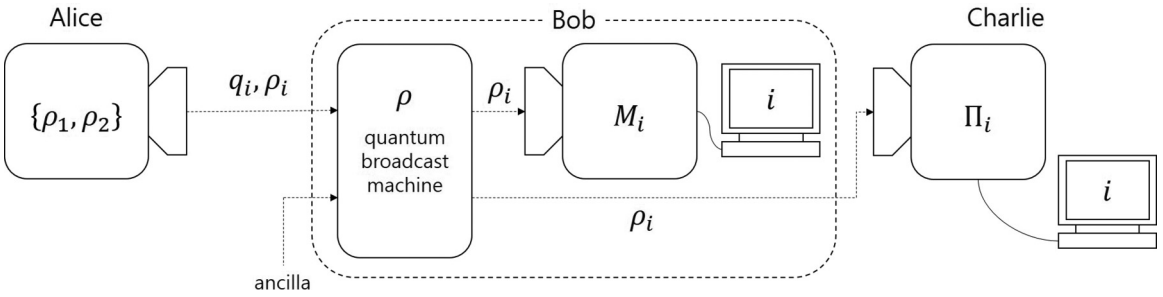

FIG. 4. Quantum broadcasting scenario of Bob and Charlie for a quantum state prepared by Alice. Bob broadcasts a quantum state ρ_i prepared by Alice with prior probability q_i. When Bob succeeds at broadcasting it, Bob can share the bipartite state ρ with Charlie. Then, Bob and Charlie perform an optimal POVM on the partial state. When Bob's measurement fails to discriminate Alice's mixed state, Bob informs Charlie of the fact that his measurement fails.

ACKNOWLEDGMENTS

We thank Donghoon Ha and Jihwan Kim for their insightful discussions. This work is supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (NRF2015R1D1A1A01060795) and Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. R0190-15-2028, PSQKD).

APPENDIX A: DERIVATION OF BOB AND CHARLIE'S POVM CONDITION

Here, we derive the POVM conditions of Bob and Charlie, which are described in Eqs. (4) and (7). First, we show that POVM conditions of Bob are given by the inequalities of Eq. (4). From Eq. (3) and completeness condition (B2), we can write the POVM element M_0 of Bob,

$$\begin{aligned} M_0 &= \mathcal{I} - \alpha_1 |\alpha_1\rangle\langle\alpha_1| - \alpha_2 |\alpha_2\rangle\langle\alpha_2| \\ &\quad - \bar{\alpha}_1 |\bar{\alpha}_1\rangle\langle\bar{\alpha}_1| - \bar{\alpha}_2 |\bar{\alpha}_2\rangle\langle\bar{\alpha}_2| \\ &= (\mathcal{I}' - \alpha_1 |\alpha_1\rangle\langle\alpha_1| - \alpha_2 |\alpha_2\rangle\langle\alpha_2|) \\ &\quad \oplus (\bar{\mathcal{I}}' - \bar{\alpha}_1 |\bar{\alpha}_1\rangle\langle\bar{\alpha}_1| - \bar{\alpha}_2 |\bar{\alpha}_2\rangle\langle\bar{\alpha}_2|). \end{aligned} \tag{A1}$$

Here, $\mathcal{I}'(\bar{\mathcal{I}}')$ is an identity matrix of space spanned by $|\alpha_1\rangle$ and $|\alpha_2\rangle$ ($|\bar{\alpha}_1\rangle$ and $|\bar{\alpha}_2\rangle$). The space spanned by $|\alpha_1\rangle$ and $|\alpha_2\rangle$ is orthogonal to the space spanned by $|\bar{\alpha}_1\rangle$ and $|\bar{\alpha}_2\rangle$. Therefore, the last term of Eq. (A1) contains the direct sum "$\oplus$." M_0 consists of the block matrix $M_0', \bar{M}_0'$. Then, we have $M_0 = M_0' \oplus \bar{M}_0'$. The condition that M_0 is positive semidefinite is equivalent to the condition that the two block matrices $M_0', \bar{M}_0'$ are positive semidefinite. M_0' and $\bar{M}_0'$ have identical forms. Therefore, if the condition that M_0' can be positive semidefinite is obtained, we can find the condition for $\bar{M}_0'$. As $|r_1\rangle \perp |\alpha_2\rangle$ according to (B3), when $|r_1\rangle = [1\ \ 0]^T$ and $|\alpha_2\rangle = [0\ \ 1]^T$, M_0' can be written as

$$M_0' = \begin{bmatrix} 1 - \alpha_1(1 - |c|) & \alpha_1 c\sqrt{1 - |c|^2} \\ \alpha_1 c^* \sqrt{1 - |c|^2} & 1 - \alpha_1 |c|^2 - \alpha_2 \end{bmatrix}. \tag{A2}$$

Similarly, we obtain $\bar{M}_0'$,

$$\bar{M}_0' = \begin{bmatrix} 1 - \bar{\alpha}_1(1 - |\bar{c}|) & \bar{\alpha}_1 \bar{c}\sqrt{1 - |\bar{c}|^2} \\ \bar{\alpha}_1 c^* \sqrt{1 - |\bar{c}|^2} & 1 - \bar{\alpha}_1 |\bar{c}|^2 - \bar{\alpha}_2 \end{bmatrix}. \tag{A3}$$

From (A2), the condition for $M_0' \geqslant 0$ becomes

$$\alpha_1\alpha_2(1 - |c|^2) - \alpha_1 - \alpha_2 + 1 \geqslant 0. \tag{A4}$$

Similarly, the condition for $\bar{M}_0' \geqslant 0$ can be determined as

$$\bar{\alpha}_1\bar{\alpha}_2(1 - |\bar{c}|^2) - \bar{\alpha}_1 - \bar{\alpha}_2 + 1 \geqslant 0. \tag{A5}$$

However, as the POVM of Bob is not optimal, Eqs. (A4) and (A5) become strict inequalities. The condition for the POVM of Charlie can be obtained. However, as the POVM of Charlie is optimal, the condition for the POVM of Charlie becomes strict equalities.

APPENDIX B: STRUCTURE OF K_0 AND FORM OF $c', \bar{c}'$

Here, we obtain the Kraus operator K_0, corresponding to the POVM element M_0 of Bob. When K_0 is given in the following form, K_0 maps the support space of ρ_i to that of σ_i:

$$\begin{aligned} K_0 &= (\sqrt{\gamma_1}\,|s_1\rangle\langle\alpha_1| + \sqrt{\gamma_2}\,|s_2\rangle\langle\alpha_2|) \\ &\quad \oplus (\sqrt{\bar{\gamma}_1}\,|\bar{s}_1\rangle\langle\bar{\alpha}_1| + \sqrt{\bar{\gamma}_2}\,|\bar{s}_2\rangle\langle\bar{\alpha}_2|) \\ &\equiv K_0' \oplus \bar{K}_0'. \end{aligned} \tag{B1}$$

Now, let us find $\gamma_1, \gamma_2, \bar{\gamma}_1, \bar{\gamma}_2$ satisfying $M_0 = K_0^\dagger K_0$. Here, we introduce the following theorem.

Theorem 1. Two $n \times n$ matrices A, B are equal iff $\langle x| A |y\rangle = \langle x| B |y\rangle$ for elements $|x\rangle, |y\rangle$ obtained from the linear independent basis $\{|a\rangle, |b\rangle, |c\rangle, \dots\}$.

If $M_0' = K_0'^\dagger K_0'$ and $\bar{M}_0' = \bar{K}_0'^\dagger \bar{K}_0'$ are satisfied, we have $M_0 = K_0^\dagger K_0$. When $|r_1\rangle$ and $|r_2\rangle$ ($|\bar{r}_1\rangle$ and $|\bar{r}_2\rangle$) are linearly independent, the supports of ρ_1 and ρ_2 are not identical. From Theorem 1, we find the conditions that give $M_0' = K_0'^\dagger K_0'$, $\bar{M}_0' = \bar{K}_0'^\dagger \bar{K}_0'$:

$$\begin{aligned} 1 - \alpha_1(1 - |c|^2) &= \gamma_1(1 - |c|^2), \\ 1 - \alpha_2(1 - |c|^2) &= \gamma_2(1 - |c|^2), \\ c &= \sqrt{\gamma_1\gamma_2}(1 - |c|^2)c', \\ 1 - \bar{\alpha}_1(1 - |\bar{c}|^2) &= \bar{\gamma}_1(1 - |\bar{c}|^2), \\ 1 - \bar{\alpha}_2(1 - |\bar{c}|^2) &= \bar{\gamma}_2(1 - |\bar{c}|^2), \\ \bar{c} &= \sqrt{\bar{\gamma}_1\bar{\gamma}_2}(1 - |\bar{c}|^2)\bar{c}'. \end{aligned} \tag{B2}$$

From Eq. (B2), we obtain $c,\bar{c}'$:

$$c' = \frac{c}{\sqrt{\{1-\alpha_1(1-|c|^2)\}\{1-\alpha_2(1-|c|^2)\}}},$$
$$\bar{c}' = \frac{\bar{c}}{\sqrt{\{1-\bar{\alpha}_1(1-|\bar{c}|^2)\}\{1-\bar{\alpha}_2(1-|\bar{c}|^2)\}}}. \tag{B3}$$

The conditions that $c',\bar{c}'$ of Eq. (B3) satisfy $|c'|,|\bar{c}'| \leqslant 1$ are Eqs. (A4) and (A5) of Appendix A. In other words, the fact that the postmeasurement states σ_1,σ_2 do not have identical support spaces is equivalent to the condition that the POVM of Bob is not optimal.

APPENDIX C: OPTIMIZATION OF SEQUENTIAL STATE DISCRIMINATION

In this section, we optimize the probability that Bob and Charlie perform sequential state discrimination successfully in terms of the POVM. First of all, the probability is given by $P_{s,\mathrm{seq}}^{(B,C)} = f + \bar{f}$. Here, f and $\bar{f}$ are

$$f = (1-|c|^2)(1-|c'|^2)(q_1 r_1 \alpha_1\beta_1 + q_2 r_2 \alpha_2\beta_2),$$
$$\bar{f} = (1-|\bar{c}|^2)(1-|\bar{c}'|^2)(q_1 \bar{r}_1 \bar{\alpha}_1\bar{\beta}_1 + q_2 r_2 \bar{\alpha}_2\bar{\beta}_2). \tag{C1}$$

Note that $\alpha_i,\bar{\alpha}_i,\beta_i,\bar{\beta}_i$ are parameters of the POVM. Here, we obtain the conditions of $\alpha_i,\bar{\alpha}_i,\beta_i,\bar{\beta}_i$, which can optimize f and $\bar{f}$ of Eq. (C1), as follows:

$$\begin{aligned}
&\alpha_1\alpha_2(1-|c|^2) - \alpha_1 - \alpha_2 + 1 > 0,\\
&\bar{\alpha}_1\bar{\alpha}_2(1-|\bar{c}|^2) - \bar{\alpha}_1 - \bar{\alpha}_2 + 1 > 0,\\
&\beta_1\beta_2(1-|c|^2) - \beta_1 - \beta_2 + 1 = 0,\\
&\bar{\beta}_1\bar{\beta}_2(1-|\bar{c}|^2) - \bar{\beta}_1 - \bar{\beta}_2 + 1 = 0.
\end{aligned} \tag{C2}$$

According to Eqs. (C1) and (C2), α_i,β_i and $\bar{\alpha}_i,\bar{\beta}_i$ consist of independent constraints. Therefore, the optimization of $P_s^{(B,C)}$, being the success probability of sequential state discrimination, can be rewritten as

$$\begin{aligned}
&\text{maximize} \quad f\\
&\text{subject to} \quad \alpha_1\alpha_2(1-|c|^2) - \alpha_1 - \alpha_2 + 1 > 0,\\
&\qquad\qquad \beta_1\beta_2(1-|c|^2) - \beta_1 - \beta_2 + 1 = 0.
\end{aligned} \tag{C3}$$

The optimization of $\bar{f}$ is understood similarly. The parameters $|c'|,|\bar{c}'|$, related to the postmeasurement state of Bob σ_i, depend on $\alpha_i,\bar{\alpha}_i$ (see Appendix B). Now, let us find the conditions of $\beta_i,\bar{\beta}_i$ for optimizing f. From (8), we can express f as $f = \Lambda_1\beta_1 + \Lambda_2\beta_2$, where $\Lambda_1 = (1-|c|^2)(1-|c'|^2)q_1 r_1\alpha_1$ and $\Lambda_2 = (1-|c|^2)(1-|c'|^2)q_2 r_2\alpha_2$ are independent of (β_1,β_2). As Λ_1 and Λ_2 are non-negative, (β_1,β_2), which is tangential of f and the equality of Eq. (7) and exists in the regions of $0 \leqslant \beta_1 \leqslant 1$ and $0 \leqslant \beta_2 \leqslant 1$, is an optimal point of f (see Fig. 5). The conditions of Bob's POVM, satisfying the above conditions, become

$$\alpha_2 \leqslant \frac{\alpha_1\{1-\alpha_1(1-|c|^2)\}}{x+\alpha_1(1-|c|^2)\{1-\alpha_1(1-|c|^2)\}}, \quad x = |c|^2\frac{q_2 r_2}{q_1 r_1},$$
$$\alpha_1 \leqslant \frac{\alpha_2\{1-\alpha_2(1-|c|^2)\}}{y+\alpha_2(1-|c|^2)\{1-\alpha_2(1-|c|^2)\}}, \quad y = |c|^2\frac{q_1 r_1}{q_2 r_2}. \tag{C4}$$

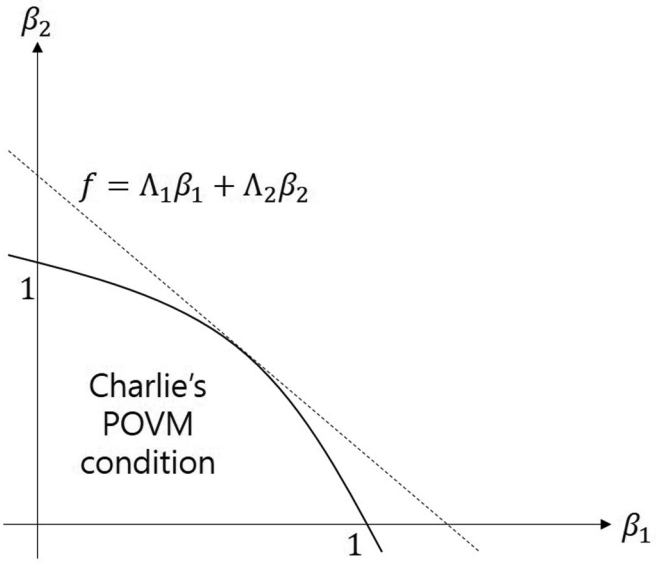

FIG. 5. Geometric condition for Charlie's optimal POVM. If in $0 \leqslant \beta_1,\beta_2 \leqslant 1$, the line $f = \Lambda_1\beta_1 + \Lambda_2\beta_2$ becomes a tangent to the boundary of the set satisfying Charlie's POVM condition, Charlie's POVM is optimal.

Considering the tangential point of f and equality of Eq. (7), f is a function of (α_1,α_2), $f(\alpha_1,\alpha_2)$. In order to examine a local maximum of $f(\alpha_1,\alpha_2)$ in the region satisfying Eq. (C4), we find $(\alpha_1^\star,\alpha_2^\star)$, where the gradient of $f(\alpha_1,\alpha_2)$ is a zero vector. $(\alpha_1^\star,\alpha_2^\star)$ fulfills the following conditions:

$$\alpha_2^\star = \frac{\alpha_1^\star\{1-\alpha_1^\star(1-|c|^2)\}^3}{x+\alpha_1^\star(1-|c|^2)\{1-\alpha_1^\star(1-|c|^2)\}^3}, \quad x = |c|^2\frac{q_2 r_2}{q_1 r_1},$$
$$\alpha_1^\star = \frac{\alpha_2^\star\{1-\alpha_2^\star(1-|c|^2)\}^3}{y+\alpha_2^\star(1-|c|^2)\{1-\alpha_2^\star(1-|c|^2)\}^3}, \quad y = |c|^2\frac{q_1 r_1}{q_2 r_2}. \tag{C5}$$

If Bob's POVM does not satisfy Eq. (C4), (β_1,β_2) of optimizing f is (1,0) or (0,1). When $(\beta_1,\beta_2) = (1,0)$, f has an optimal point at $\alpha_2 = 0$ and f becomes a single-valued function $f(\alpha_1,0)$. $f(\alpha_1,0)$ has a maximum value at $\alpha_1 = 1/(1+|c|)$. Similarly, if $(\beta_1,\beta_2) = (0,1)$, f has an optimal point at $\alpha_1 = 0$ and f becomes a single-valued function of α_2, $f(0,\alpha_2)$. $f(0,\alpha_2)$ has a maximum value at $\alpha_2 = 1/(1+|c|)$. Therefore, the optimal point for f, $(\alpha_1^{\mathrm{opt}},\alpha_2^{\mathrm{opt}})$, becomes

$$(\alpha_1^{\mathrm{opt}},\alpha_2^{\mathrm{opt}}) \in \left\{(\alpha_1^\star,\alpha_2^\star),\left(\frac{1}{1+|c|},0\right),\left(0,\frac{1}{1+|c|}\right)\right\}. \tag{C6}$$

In the same way, we can obtain the optimal condition of $\bar{f}$,

$$(\bar{\alpha}_1^{\mathrm{opt}},\bar{\alpha}_2^{\mathrm{opt}}) \in \left\{(\bar{\alpha}_1^\star,\bar{\alpha}_2^\star),\left(\frac{1}{1+|\bar{c}|},0\right),\left(0,\frac{1}{1+|\bar{c}|}\right)\right\}. \tag{C7}$$

From Eq. (C7), the equality condition for $(\bar{\alpha}_1^\star,\bar{\alpha}_2^\star)$ becomes

$$\bar{\alpha}_2^\star = \frac{\bar{\alpha}_1^\star\{1-\bar{\alpha}_1^\star(1-|\bar{c}|^2)\}^3}{\bar{x}+\bar{\alpha}_1^\star(1-|\bar{c}|^2)\{1-\bar{\alpha}_1^\star(1-|\bar{c}|^2)\}^3}, \quad \bar{x}=|\bar{c}|^2\frac{q_2\bar{r}_2}{q_1\bar{r}_1},$$
$$\bar{\alpha}_1^\star = \frac{\bar{\alpha}_2^\star\{1-\bar{\alpha}_2^\star(1-|\bar{c}|^2)\}^3}{\bar{y}+\bar{\alpha}_2^\star(1-|\bar{c}|^2)\{1-\bar{\alpha}_2^\star(1-|\bar{c}|^2)\}^3}, \quad \bar{y}=|\bar{c}|^2\frac{q_1\bar{r}_1}{q_2\bar{r}_2}. \tag{C8}$$

When Alice prepares mixed states with arbitrary prior probability, it is difficult to determine $(\alpha_1^\star,\alpha_2^\star)$ and $(\bar{\alpha}_1^\star,\bar{\alpha}_2^\star)$ in an analytic manner. However, if Alice prepares a symmetric mixed state (that is, the case of identical eigenvalues) [13] with the same prior probabilities, we obtain $\alpha_1^\star=\alpha_2^\star=(1-\sqrt{|c|})/(1-|c|^2)$ and $\bar{\alpha}_1^\star=\bar{\alpha}_2^\star=(1-\sqrt{|\bar{c}|})/(1-|\bar{c}|^2)$. Furthermore, we find $f(1/(1+|c|),0)=f(0,1/(1+|c|))$ and $\bar{f}(1/(1+|\bar{c}|),0)=\bar{f}(0,1/(1+|\bar{c}|))$.

APPENDIX D: OPTIMIZING SUCCESS PROBABILITY OF QUANTUM BROADCASTING

Here, we obtain the probability that one of the mixed states $\{\rho_1,\rho_2\}$ prepared by Alice can be broadcast correctly. The necessary and sufficient conditions that the quantum broadcast can be performed can be found in the following theorem.

Theorem 2. Suppose that a bipartite state ρ satisfies $\mathrm{Tr}_B\rho=\mathrm{Tr}_A\rho=\rho_i$, where ρ_i is one of Alice's two quantum states $\{\rho_1,\rho_2\}$. Then, if a square matrix $\Phi\equiv X-\sqrt{\Gamma}Y\sqrt{\Gamma}$ is positive semidefinite, Bob and Charlie can share ρ with the probability t_i. Here, $\sqrt{\Gamma}=\mathrm{diag}\{\sqrt{t_1},\sqrt{t_1},\sqrt{t_2},\sqrt{t_2}\}$ and X,Y are defined by [15]

$$X=\begin{bmatrix}\langle r_1|r_1\rangle & \langle r_1|\bar{r}_1\rangle & \langle r_1|r_2\rangle & \langle r_1|\bar{r}_2\rangle\\ \langle \bar{r}_1|r_1\rangle & \langle \bar{r}_1|\bar{r}_1\rangle & \langle \bar{r}_1|r_2\rangle & \langle \bar{r}_1|\bar{r}_2\rangle\\ \langle r_2|r_1\rangle & \langle r_2|\bar{r}_1\rangle & \langle r_2|r_2\rangle & \langle r_2|\bar{r}_2\rangle\\ \langle \bar{r}_2|r_1\rangle & \langle \bar{r}_2|\bar{r}_1\rangle & \langle \bar{r}_2|r_2\rangle & \langle \bar{r}_2|\bar{r}_2\rangle\end{bmatrix},$$
$$Y=\begin{bmatrix}\langle r_1|r_1\rangle^2 & \langle r_1|\bar{r}_1\rangle^2 & \langle r_1|r_2\rangle^2 & \langle r_1|\bar{r}_2\rangle^2\\ \langle \bar{r}_1|r_1\rangle^2 & \langle \bar{r}_1|\bar{r}_1\rangle^2 & \langle \bar{r}_1|r_2\rangle^2 & \langle \bar{r}_1|\bar{r}_2\rangle^2\\ \langle r_2|r_1\rangle^2 & \langle r_2|\bar{r}_1\rangle^2 & \langle r_2|r_2\rangle^2 & \langle r_2|\bar{r}_2\rangle^2\\ \langle \bar{r}_2|r_1\rangle^2 & \langle \bar{r}_2|\bar{r}_1\rangle^2 & \langle \bar{r}_2|r_2\rangle^2 & \langle \bar{r}_2|\bar{r}_2\rangle^2\end{bmatrix}. \tag{D1}$$

In this study, we assume $t_1=t_2\equiv t$. From this, we obtain the condition that Φ is positive semidefinite,

$$(1-t)\pm c(1-tc)\geqslant 0,$$
$$(1-t)\pm \bar{c}(1-t\bar{c})\geqslant 0. \tag{D2}$$

The left side of Eq. (D2) show the four eigenvalues of Φ. Here, we assumed that $c,\bar{c}$ are real because the phases of $c,\bar{c}$ are irrelevant. t, satisfying the inequalities of Eq. (D2), fulfills $t\leqslant\min\{1/(1+c),1/(1+\bar{c})\}$.

[1] S. J. van Enk, Phys. Rev. A **66**, 042313 (2002).
[2] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. Lett. **90**, 257901 (2003).
[3] C. W. Helstrom, *Quantum Detection and Estimation* (Academic, New York, 1976).
[4] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[5] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[6] A. Peres, Phys. Lett. A **128**, 19 (1988).
[7] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[8] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[9] J. A. Bergou, E. Feldman, and M. Hillery, Phys. Rev. Lett. **111**, 100501 (2013).
[10] C.-Q. Pang, F.-L. Zhang, L.-F. Xu, M.-L. Liang, and J.-L. Chen, Phys. Rev. A **88**, 052331 (2013).
[11] M. A. Solis-Prosser, P. Gonzalez, J. Fuenzalida, S. Gomez, G. B. Xavier, A. Delgado, and G. Lima, Phys. Rev. A **94**, 042309 (2016).
[12] P. Raynal and N. Lutkenhaus, Phys. Rev. A **76**, 052322 (2007).
[13] U. Herzog, Phys. Rev. A **75**, 052309 (2007).
[14] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[15] L. Li, D. Qiu, L. Li, L. Wu, and X. Zou, J. Phys. A: Math. Theor. **42**, 175302 (2009).
[16] J. A. Bergou, J. Phys: Conf. Ser. **84**, 012001 (2007).
[17] S. Croke, Adv. Opt. Photon. **1**, 238 (2009).
[18] J. Bae, New J. Phys. **15**, 073037 (2013).
[19] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).
[20] U. Herzog and J. A. Bergou, Phys. Rev. A **71**, 050301(R) (2005).
[21] P. Raynal, N. Lutkenhaus, and S. J. van Enk, Phys. Rev. A **68**, 022308 (2003).
[22] M. A. Nielson and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2010).
[23] In general, a POVM element can be expressed as $M_i=\sum_j K_{ij}^\dagger K_{ij}$, using Kraus operator K_i.
[24] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Wiley, New York, 1991).
[25] R. Josza, J. Mod. Opt **41**, 2315 (1994).
[26] Y. C. Eldar, M. Stojnic, and B. Hassibi, Phys. Rev. A **69**, 062318 (2004).
[27] M. Kleinmann, H. Kampermann, and D. Bruß, Phys. Rev. A **81**, 020304(R) (2010).
[28] L. Li, Phys. Rev. A **86**, 032320 (2012).