entropy

Article

Uniqueness of Minimax Strategy in View of Minimum Error Discrimination of Two Quantum States

Jihwan Kim, Donghoon Ha and Younghun Kwon *

Department of Applied Physics, Hanyang University, Ansan, Kyunggi-Do 425-791, Korea

* Correspondence: yyhkwon@hanyang.ac.kr

Received: 28 May 2019; Accepted: 6 July 2019; Published: 9 July 2019

Abstract: This study considers the minimum error discrimination of two quantum states in terms of a two-party zero-sum game, whose optimal strategy is a minimax strategy. A minimax strategy is one in which a sender chooses a strategy for a receiver so that the receiver may obtain the minimum information about quantum states, but the receiver performs an optimal measurement to obtain guessing probability for the quantum ensemble prepared by the sender. Therefore, knowing whether the optimal strategy of the game is unique is essential. This is because there is no alternative if the optimal strategy is unique. This paper proposes the necessary and sufficient condition for an optimal strategy of the sender to be unique. Also, we investigate the quantum states that exhibit the minimum guessing probability when a sender's minimax strategy is unique. Furthermore, we show that a sender's minimax strategy and a receiver's minimum error strategy cannot be unique if one can simultaneously diagonalize two quantum states, with the optimal measurement of the minimax strategy. This implies that a sender can confirm that the optimal strategy of only a single side (a sender or a receiver but not both of them) is unique by preparing specific quantum states.

Keywords: quantum state discrimination; quantum minimax; uniqueness of strategy; guessing probability

1. Introduction

Quantum information processing can be achieved by discriminating quantum states, where classical information is encoded. Quantum states which are orthogonal to each other can be perfectly distinguishable. However, non-orthogonal quantum states cannot be perfectly discriminated. Therefore, one needs to have a discrimination strategy for non-orthogonal quantum states, and there are various strategies [1–4] such as minimum error discrimination (MD) [4–7], unambiguous discrimination [8–12], maximum confidence discrimination [13], and discrimination of fixed rate inconclusive result [14–18]. Unambiguous discrimination is a strategy where there is no error in the conclusive result by allowing an inconclusive result. Maximum confidence is a strategy where one maximizes the confidence of a conclusive result. Discrimination of fixed rate inconclusive result is a strategy where one may fix the rate of an inconclusive result. Among these strategies, the MD strategy can conclusively discriminate quantum states with a prior probability.

The MD strategy is employed for quantum states with a given prior probability, and the quantum states are optimally measured. MD strategy is that one maximizes the probability that the result of measurement of a receiver correctly points out the quantum state that a sender transmitted when only a conclusive result is permitted. The maximum probability is called guessing probability. One can investigate the behavior of MD in terms of a prior probability when quantum states are given.

Because the guessing probability is obtained based on prior probability, a change in prior probability results in different guessing probabilities, which implies that prior probabilities can be considered as a strategy of a sender. Even though one has discussed the uniqueness of measurement strategy in discrimination of two quantum states, the strategy of preparation such as a prior probability, which can be a strategy of a sender, has not been discussed in terms of identical guessing probability and optimal measurement strategy.

Quantum minimax approach is obtained by applying the minimax approach of a statistical decision to quantum state discrimination. Von Neumann, the inventor of game theory, showed that there exists a solution to the minimax problem when sender and receiver can choose a finite number of strategies in a two-person zero-sum game. Wald proved that the necessary and sufficient condition to the existence of a solution to the minimax problem is that the set of strategy for sender and receiver is countable [19]. Hirota and Ikehara discussed quantum minimax theorem, using the fact that the set of measurement strategy satisfies compactness [20]. They suggested the necessary and sufficient condition for minimax strategy in quantum state discrimination.

Further, by mean value theorem D'Ariano showed that there exists a quantum minimax strategy for two quantum state discrimination and provided a sufficient condition for the strategy [21]. However, in spite of these studies, the necessary and sufficient condition for uniqueness of minimax strategy in two quantum state discrimination is not known yet. Even more, the uniqueness of minimax strategy in two quantum state discrimination is not understood in terms of sender's strategy, which is a selection of prior probability.

This study investigates a two-person zero-sum game where the payoff is defined by the correct probability of two quantum states [19–22]. The optimal strategy of the game is a minimax strategy, where the minimax strategy of a receiver is to select the optimal measurement providing MD and the minimax strategy of a sender is to choose the prior probability providing the minimum of guessing probability, which is displayed in Figure 1.

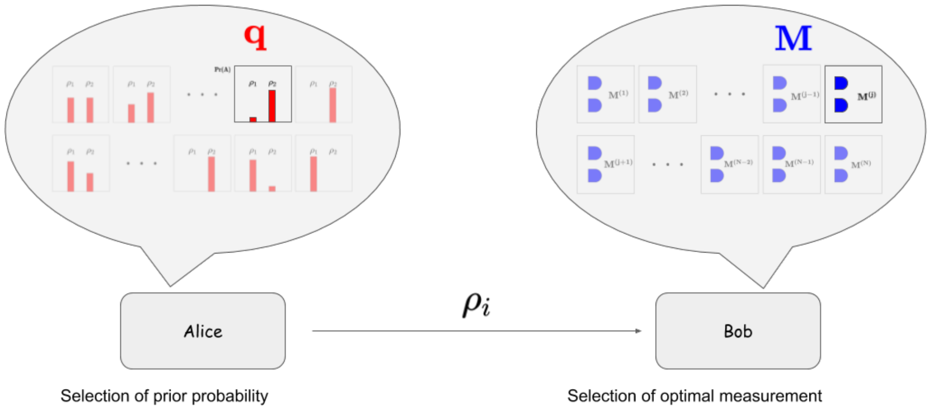

Figure 1. The strategy of the sender(Alice) and the receiver(Bob) in two-person zero-sum quantum game. The strategy of Alice is to choose the optimal prior probability **q**, which is the probability of quantum states prepared in the quantum system, to minimize the payoff. The strategy of Bob is to choose the optimal measurement to maximize payoff.

In this scenario, the prior probability and the measurement in MD are constructed as the strategy of a sender Alice and a receiver Bob [20,21]. First, Alice sends the quantum states, where classical information $(x = 1, 2)$ is encoded, to Bob. Because the quantum states are not orthogonal to each other, a single measurement of Bob cannot perfectly discriminate the quantum states. Therefore, a suitable strategy is needed. Here Bob should choose a measurement strategy that can perform MD.

Meanwhile, a suitable selection of prior probability can be obtained by Alice, as a sender's strategy. Alice's strategy is to interfere with the minimum error strategy of Bob to minimize the guessing probability. Because Bob should perform MD without noticing Alice's strategy, Bob tries to find an optimal strategy to obtain a payoff. Therefore, the minimum of guessing probability implies that a suitable selection of prior probability lets Bob obtain the minimum of guessing probability when Bob performs an optimal measurement. Furthermore, if Bob cannot perform an optimal measurement, he obtains a probability less than the guessing probability.

The quantum minimax theorem [20,21] can be used to prove that Alice and Bob can set up an optimal strategy on both sides. However, it is not known whether the minimax strategy is unique or not. The uniqueness of the optimal strategy of the game is important in performing the game. There is no alternative to a unique optimal strategy. Therefore, a strategy cannot be optimal if an error occurs when performing the strategy. However, a strategy can still be optimal if it is not unique, even though an error occurs in the strategy. In this light, it is crucial to know whether the minimax strategy is unique, when the strategy is optimal in the game. Here, we investigate the condition for uniqueness of the optimal strategy of a sender. The condition is described by the quantum states and the minimax strategy of a receiver. More explicitly, we study the necessary and sufficient condition for the uniqueness of a sender's strategy. Using the condition, we investigate the quantum states that exhibit the minimum of guessing probability when a sender's minimax strategy is unique.

Also, we show that a sender's minimax strategy and a receiver's minimum error strategy cannot be unique if two quantum states are simultaneously diagonalized with the optimal measurement of minimax strategy. Therefore, a sender can make the optimal strategy of only a single side unique by preparing specific quantum states. Our investigation can be applied to various fields. As the first example of our investigation, we explain how the BB84 protocol [23] with equal prior probability is optimal in terms of the minimax strategy. We also discuss how the results of this study can be applied to building a quantum random number generator(QRNG) [24–26].

This paper is organized as follows. In Section 2, we explain the necessary background of our investigation. In Section 3, for the minimax strategy of a sender, we provide the necessary and sufficient condition for uniqueness of the optimal strategy. We investigate the uniqueness of the strategy of the sender for some quantum states by using this condition. Furthermore, we obtain the condition under which both the sender's minimax strategy and the receiver's optimal minimum error strategy cannot be unique. Finally, we discuss the results and conclusions in Section 4.

2. Preliminaries

For two quantum states ρ_1 and ρ_2, the minimal subspace $\mathcal{H}$ for discriminating ρ_1 and ρ_2 should satisfy $\mathcal{H} = \text{Supp}(\rho_1 + \rho_2)$. In this study, we assume that the rank of quantum state is finite. Then, by the relation $\dim \mathcal{H} \leq \text{rank}(\rho_1) + \text{rank}(\rho_2)$, a quantum state or an optimal measurement can be represented as an operator on finite dimensional Hilbert space.

The MD of two quantum states ρ_1 and ρ_2 is a strategy to determine the maximum value of correct probability $\text{P}_{\text{corr}} = q\text{tr}(\rho_1 M_1) + (1-q)\text{tr}(\rho_2 M_2)$, which is called guessing probability, by performing an optimal measurement. The maximum value of the correct probability is known as Helstrom bound [27].

Assuming that the prior probabilities of two quantum states ρ_1 and ρ_2 are q and $1-q$, respectively, one can obtain the following lemma in the MD of the two quantum states. (The proof can be found in the Appendix A).

Lemma 1 (Optimal condition of MD for two quantum states [27,28])**.** *The necessary and sufficient condition for optimal measurement* $\{M_x\}_{x=1}^2$ *is given by*

$$(-1)^x \left((1-q)\rho_2 - q\rho_1\right) M_x \geq 0 \quad \forall x \in \{1,2\}. \tag{1}$$

In general, the optimal measurement in MD is not unique. If the nullity of operator $\Lambda \equiv (1-q)\rho_2 - q\rho_1$ is d, there exist at least 2^d number of optimal extreme POVMs. A convex combination of these POVM also provides an optimal measurement of MD. When Λ has full rank, the optimal measurement is unique. Quantum minimax theorem tells that among optimal MD strategies there is at least a POVM of minimax strategy in a prior probability providing the minimum of guessing probability [20,21].

Theorem 1 (Quantum minimax theorem [20,21])**.** *There exists an a priori probability* $\mathbf{q}^\star = (q^\star, 1-q^\star)$ *for the states* ρ_1 *and* ρ_2*, and a measurement* $\mathbf{M}^\star = (M_1^\star, M_2^\star)$ *such that*

$$\min_{\mathbf{q}}\max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\star,\mathbf{M}^\star) = \max_{\mathbf{M}}\min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) \tag{2}$$

where $q^\star \in (0,1)$*,* $P_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \sum_{x=1}^{2} q_x \mathrm{tr}(\rho_x M_x)$*.*

Note that when quantum states are prepared in a prior probability $\mathbf{q}$, $\max_{\mathbf{M}}\min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\star,\mathbf{M}^\star)$ implies that the measurement of $\mathbf{M}^\star$ is optimal and $\min_{\mathbf{q}}\max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\star,\mathbf{M}^\star)$ implies that the prior probability of $\mathbf{q}^\star$ provides the minimum of guessing probability. However, every optimal MD in the prior probability of $\mathbf{q}^\star$ is not a minimax strategy of Bob. Suppose that a measurement of $\mathbf{N} = (N_1, N_2)$ in the prior probability of $\mathbf{q}^\star$ is an optimal strategy of MD, satisfying $\mathrm{tr}(\rho_1 N_1) > \mathrm{tr}(\rho_2 N_2) > 0$. Then, the strategy of Alice in $\mathbf{q}^\star$ cannot be a prior probability for the minimax strategy, as $\tilde{\mathbf{q}} = (0,1)$ of Alice's strategy provides a lower guessing probability than that of $\mathbf{q}^\star$:

$$P_{\mathrm{corr}}(\mathbf{q}^\star,\mathbf{N}) = q^\star\mathrm{tr}(\rho_1 N_1) + (1-q^\star)\mathrm{tr}(\rho_2 N_2) > \mathrm{tr}(\rho_2 N_2) = P_{\mathrm{corr}}(\tilde{\mathbf{q}},\mathbf{N}). \tag{3}$$

Therefore, the first condition that the minimax strategy $\mathbf{M}^\star$ of Bob should satisfy is $\mathrm{tr}(\rho_1 M_1^\star) = \mathrm{tr}(\rho_2 M_2^\star)$. Because the measurement of $\mathbf{M}^\star$ is an optimal strategy for the prior probability of $\mathbf{q}^\star$, it satisfies the optimal condition of MD, which is the second condition. Inversely, the fulfillment of the two conditions is the sufficient condition for the minimax strategy.

Here, the conditions can be explained as follows. Suppose that a measurement $M^\circ = (M_1^\circ, M_2^\circ)$ satisfies $\mathrm{tr}(\rho_1 M_1^\circ) = \mathrm{tr}(\rho_2 M_2^\circ)$ and is optimal for the prior probability of $\mathbf{q}^\circ$. Then, we find the following relation:

$$\min_{\mathbf{q}}\max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) \le \max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}) = \mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}^\circ) = \min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}^\circ). \tag{4}$$

The last equality holds by $\mathrm{tr}(\rho_1 M_1^\circ) = \mathrm{tr}(\rho_2 M_2^\circ)$. Because of $\min_{\mathbf{q}}\max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) \ge \min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}^\circ)$, we find $\min_{\mathbf{q}}\max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}^\circ)$. And the following relation holds:

$$\max_{\mathbf{M}}\min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) \le \min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}^\circ) = \mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}^\circ) = \max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}) \tag{5}$$

The first equality is obtained by $\mathrm{tr}(\rho_1 M_1^\circ) = \mathrm{tr}(\rho_2 M_2^\circ)$. Because of $\max_{\mathbf{M}}\min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) \ge \max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M})$, we obtain $\max_{\mathbf{M}}\min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}^\circ)$ and $\min_{\mathbf{q}}\max_{\mathbf{M}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M}) = \mathrm{P}_{\mathrm{corr}}(\mathbf{q}^\circ,\mathbf{M}^\circ) = \max_{\mathbf{M}}\min_{\mathbf{q}}\mathrm{P}_{\mathrm{corr}}(\mathbf{q},\mathbf{M})$. It implies that $(\mathbf{q}^\circ,\mathbf{M}^\circ)$ is a minimax strategy. Then, one can obtain the following lemma.

Lemma 2. *When MD is performed for a given prior probability, the minimum of guessing probability is obtained iff an optimal measurement* $\{M_x\}_{x=1}^2$ *satisfies* $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2)$*.*

3. Results

This section presents the necessary and sufficient condition that ensures the uniqueness of the minimax strategy of a sender. Because there always exists a minimax strategy for the quantum minimax theorem, when one finds a minimax strategy, one can obtain the condition by which the strategy is unique. When MDs with different prior probabilities can provide the same guessing probability, the following lemma provides the condition by which the MDs with different prior probabilities can have the same optimal measurement (The proof of this lemma can be found in the Appendix A).

Lemma 3. *The quantum ensembles of S_1 and S_2 are given as $\{p_x, \rho_x\}_{x=1}^2$ and $\{q_x, \rho_x\}_{x=1}^2$, respectively, where $p_1 \neq q_1$. Suppose that in the MD of a quantum ensemble S_x, the guessing probability is $p_{\text{guess}}^{(x)}$ and the minimum value of guessing probability is $p_{\text{guess}}^{\star}$. Then, when $p_{\text{guess}}^{(1)} = p_{\text{guess}}^{(2)}$, if there exists an measurement that can simultaneously perform MD on two quantum ensembles S_1 and S_2, one can obtain $p_{\text{guess}}^{(1)} = p_{\text{guess}}^{\star}$.*

Note that the optimal measurement performing simultaneous MD on two quantum ensemble S_1 and S_2 satisfies the equal probabilities of correct detection. It is the minimax strategy of the receiver. Here, the set of prior probability providing the minimum of guessing probability is a convex set. It can be shown in the following way. Suppose that the prior probabilities of $\mathbf{q}$ and $\mathbf{p}$ provide the minimum of guessing probability $p_{\text{guess}}^{\star}$. Then, by Lemma 3 there exists a measurement $\mathbf{M}$ that can perform MD on both the quantum states, satisfying $\sum_{x=1}^2 q_x \text{tr}(\rho_x M_x) = p_{\text{guess}}^{\star} = \sum_{x=1}^2 p_x \text{tr}(\rho_x M_x)$. Now, one can see that the relation of $\sum_{x=1}^2 (\theta q_x + (1-\theta) p_x) \text{tr}(\rho_x M_x) = p_{\text{guess}}^{\star}$ holds for $\theta \in [0,1]$. If one assumes that the minimax strategy $(\mathbf{q}, \mathbf{M})$ is not unique and there is another strategy $\mathbf{p}$ for a sender, then the minimax strategy of the sender forms a convex set, and one can find the prior probability where $\mathbf{M}$ is optimal in the ϵ-neighborhood of $\mathbf{q}$ for an arbitrary positive number of ϵ. Therefore, one can check the uniqueness of the prior probability of $\mathbf{q}$ providing the minimum of guessing probability, by deciding whether there exists a prior probability exhibiting optimal $\mathbf{M}$ in the ϵ neighborhood of $\mathbf{q}$ after finding the optimal POVM $\mathbf{M}$ for minimax strategy in the prior probability of $\mathbf{q}$ providing the minimum of guessing probability. Proposition 1 shows the necessary and sufficient condition for the non-uniqueness of a prior probability $\mathbf{q}$ of which $\mathbf{M}$ is optimal in the ϵ neighborhood (The proof of this proposition can be found in the Appendix A).

Proposition 1. *The prior probability providing the minimum of guessing probability is not unique if and only if $\{M_x\}_{x=1}^2$ satisfies the following conditions.*

1. $[\rho_x, M_1] = 0 \quad \forall x \in \{1,2\}$,
2. *For some $x \in \{1,2\}$, every $|v\rangle \in \text{Supp}(M_x)$ satisfies $\langle v| \rho_1 |v\rangle : \langle v| \rho_2 |v\rangle \neq 1 - q : q$.*

where $[A, B] = AB - BA$.

Lemma 2 and Proposition 1 can be applied to check whether the strategy under a situation is unique. By applying Lemma 2, one can explain why the identical prior probability in the BB84 protocol is the best strategy of a sender. The quantum states used in the BB84 protocol are $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ [23]. Alice encodes (a_0, a_1) into quantum states and sends them to Bob. In general, a_0 is selected by Alice, but a_1 is randomly chosen. Suppose that Table 1 is used for encoding bit. Here, encoding means that a quantum state corresponding to $a_0 a_1$ is prepared for communication.

Table 1. Encoding table for Alice.

a_0a_1	Quantum States
00	$\|0\rangle$
01	$\|1\rangle$
10	$\|-\rangle$
11	$\|+\rangle$

When Alice chooses 0 as the value of a_0, the quantum state is determined by a_1. If the value of a_1 is 0, the quantum state becomes $|0\rangle$. However, when a_1 is 1, $|1\rangle$ is prepared for the quantum state. If the quantum state does not interact with the environment, Bob receives the quantum state prepared by Alice. Then, Bob performs the following measurements:

$$M_0 = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}, \quad M_1 = \{|+\rangle\langle +|, |-\rangle\langle -|\} \tag{6}$$

When for the quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ the prior probability of the quantum states is identical, the optimal measurement becomes

$$M = \{\frac{1}{2}|0\rangle\langle 0|, \frac{1}{2}|1\rangle\langle 1|, \frac{1}{2}|+\rangle\langle +|, \frac{1}{2}|-\rangle\langle -|\}. \tag{7}$$

The optimal measurement satisfies the following relation:

$$\mathrm{tr}(|0\rangle\langle 0|\frac{1}{2}|0\rangle\langle 0|) = \mathrm{tr}(|1\rangle\langle 1|\frac{1}{2}|1\rangle\langle 1|) = \mathrm{tr}(|+\rangle\langle +|\frac{1}{2}|+\rangle\langle +|) = \mathrm{tr}(|-\rangle\langle -|\frac{1}{2}|-\rangle\langle -|) = 0.5 \tag{8}$$

It implies that the identical prior probability provides the minimum of guessing probability. It is because if there exists an optimal measurement satisfying the above condition, the prior probability provides the minimum of guessing probability. It should be noted that Lemma 3 implies that the measurement of M is optimal for every prior probability providing the minimum of guessing probability. Meanwhile, if the prior probability is not identical, all the quantum states in the BB84 protocol does not have M as an optimal measurement. It can be shown in the following way. Let us assume that the probability of a_1 to become 0 or 1 is equal, and the probability of a_0 to become 0 or 1 is q. Then, the prior probability of each quantum state becomes $q/2, q/2, (1-q)/2, (1-q)/2$. We can show that if the measurement M is optimal at $q \neq 0.5$, the following inequalities should be satisfied [2,28]:

$$\frac{q}{4}|0\rangle\langle 0| + \frac{q}{4}|1\rangle\langle 1| + \frac{1-q}{4}|+\rangle\langle +| + \frac{1-q}{4}|-\rangle\langle -| - \frac{q}{2}|0\rangle\langle 0| \geq 0 \tag{9}$$

$$\frac{q}{4}|0\rangle\langle 0| + \frac{q}{4}|1\rangle\langle 1| + \frac{1-q}{4}|+\rangle\langle +| + \frac{1-q}{4}|-\rangle\langle -| - \frac{1-q}{2}|+\rangle\langle +| \geq 0 \tag{10}$$

However, when $q \neq 0.5$, one of these inequalities cannot be satisfied. Therefore, the prior probability providing the minimum of the guessing probability is only the case of $q = 1/2$.

Using Proposition 1, we can investigate the quantum states of the unique prior probability, which provides the minimum of the guessing probability. Here we consider the MD of the following two quantum states:

$$\rho_1 = \frac{2}{3}|\phi^-\rangle\langle\phi^-| + \frac{I}{12}, \tag{11}$$

$$\rho_2 = \frac{1}{3}|\phi^-\rangle\langle\phi^-| + \frac{I}{6}. \tag{12}$$

From Figure 2, we can check whether the prior probability providing the minimum of guessing probability is unique. We can see that the prior probabilities providing the minimum of guessing probability are $q_1 = \frac{2}{5}$ and $q_2 = \frac{3}{5}$. The optimal measurement for the quantum ensemble is $\{M_1 = \frac{4}{5}|\phi^-\rangle\langle\phi^-|, M_2 = I - \frac{4}{5}|\phi^-\rangle\langle\phi^-|\}$, since the measurement satisfies Lemma 1 as follows:

$$(q\rho_1 - (1-q)\rho_2)M_1 = \left(\frac{2}{5}\rho_1 - \frac{3}{5}\rho_2\right)M_1 = \left(\frac{1}{15}|\phi^-\rangle\langle\phi^-| - \frac{1}{15}I\right)\frac{4}{5}|\phi^-\rangle\langle\phi^-| = 0 \tag{13}$$

$$\begin{aligned}((1-q)\rho_2 - q\rho_1)M_2 &= \left(\frac{3}{5}\rho_2 - \frac{2}{5}\rho_1\right)M_2 \\ &= \left(\frac{1}{15}I - \frac{1}{15}|\phi^-\rangle\langle\phi^-|\right)\left(I - \frac{4}{5}|\phi^-\rangle\langle\phi^-|\right) = \frac{1}{15}\left(I - |\phi^-\rangle\langle\phi^-|\right) \geq 0\end{aligned} \tag{14}$$

In addition, $\{M_x\}_{x=1}^2$ satisfies the relation of $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_1 - \frac{4}{5}|\phi^-\rangle\langle\phi^-|) = 0.6 = \mathrm{tr}(\rho_2\left(I - \frac{4}{5}|\phi^-\rangle\langle\phi^-|\right)) = \mathrm{tr}(\rho_2 M_2)$. From Lemma 2, the prior probability of $q_1 = \frac{2}{5}$ and $q_2 = \frac{3}{5}$ provides the minimum of guessing probability. Now, we verify the uniqueness of the prior probability which provides the minimum of the guessing probability for the given quantum states. The following relations show $[\rho_1+\rho_2, M_1] = [\rho_2, M_1] = 0$, which is the first condition of Proposition 1:

$$(\rho_1+\rho_2)M_1 = \left(|\phi^-\rangle\langle\phi^-| + \frac{I}{4}\right)|\phi^-\rangle\langle\phi^-| = |\phi^-\rangle\langle\phi^-|\left(|\phi^-\rangle\langle\phi^-| + \frac{I}{4}\right) = M_1(\rho_1+\rho_2) \tag{15}$$

$$\rho_2 M_1 = \left(\frac{1}{3}|\phi^-\rangle\langle\phi^-| + \frac{2}{3}\frac{I}{4}\right)|\phi^-\rangle\langle\phi^-| = |\phi^-\rangle\langle\phi^-|\left(\frac{1}{3}|\phi^-\rangle\langle\phi^-| + \frac{2}{3}\frac{I}{4}\right) = M_1\rho_2 \tag{16}$$

However, $|\phi^-\rangle$ which is the support of M_1 and M_2, satisfies the following relation:

$$\langle\phi^-|\rho_1|\phi^-\rangle : \langle\phi^-|\rho_2|\phi^-\rangle = \frac{9}{12} : \frac{6}{12} = \frac{3}{5} : \frac{2}{5} = 1-q : q \tag{17}$$

Because the second condition of Proposition 1 cannot be satisfied, the prior probability providing the minimum of the guessing probability is unique.

Now, to investigate the case of non-unique prior probability, which provides the minimum of the guessing probability, we consider the following quantum states:

$$\rho_1 = \begin{pmatrix} 0.3 & 0 \\ 0 & 0.7 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 0.7 & 0 \\ 0 & 0.3 \end{pmatrix}$$

From Figure 2, we can see non-uniqueness of the prior probability, which can provide the minimum of guessing probability.

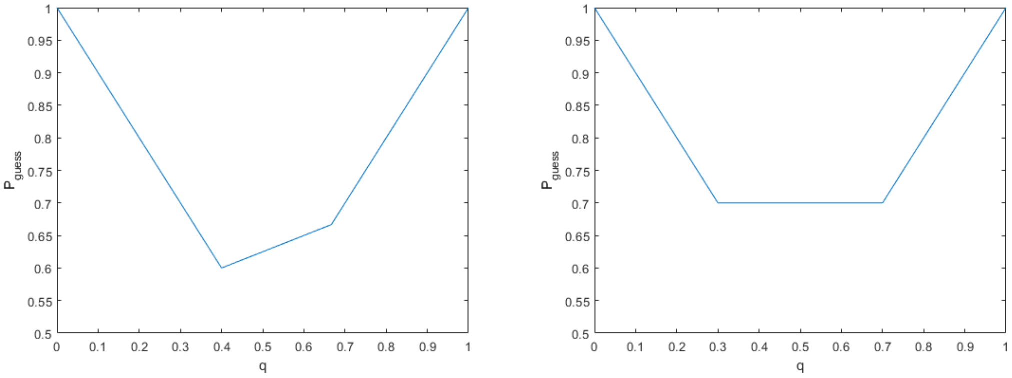

Figure 2. (**Left:**) Example of unique prior probability providing the minimum of guessing probability. The guessing probability of two quantum states $\rho_1 = \frac{2}{3}|\phi^-\rangle\langle\phi^-| + \frac{I}{12}$ and $\rho_2 = \frac{1}{3}|\phi^-\rangle\langle\phi^-| + \frac{I}{6}$ is shown in terms of prior probability $(q, 1-q)$. (**Right:**) Example of non-unique prior probability providing the minimum of guessing probability. The guessing probability of two quantum states $\rho_1 = \mathrm{diag}[0.3, 0.7]$ and $\rho_2 = \mathrm{diag}[0.7, 0.3]$ is shown in terms of prior probability $(q, 1-q)$.

For ρ_1 and ρ_2 with the prior probability of $q = 0.5$, we can obtain the minimum of the guessing probability, which is 0.7. Then, the optimal measurements are $M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Because of $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2) = 0.7$, the minimum of the guessing probability becomes 0.7 at $q = 0.5$. And because of $(\rho_1+\rho_2)M_1 = M_1$, the support of M_1 is $|e_2\rangle = (0,1)^T$, which is unique. Then, one has

$$\langle e_2| q\rho_1 - (1-q)\rho_2 |e_2\rangle = \langle e_2| \frac{1}{2}\begin{pmatrix} -0.4 & 0 \\ 0 & 0.4 \end{pmatrix}|e_2\rangle = 0.2 > 0.$$

Further, because of $(\rho_1+\rho_2)M_2 = M_2$, the support of M_2 is $|e_1\rangle = (1,0)^T$, which is unique. We have

$$\langle e_1|\, q\rho_1 - (1-q)\rho_2\, |e_1\rangle = \langle e_1|\, \frac{1}{2}\begin{pmatrix} -0.4 & 0 \\ 0 & 0.4 \end{pmatrix} |e_1\rangle = -0.2 < 0.$$

Then, the prior probability providing the minimum of the guessing probability is not unique.

From Proposition 1, the unique prior probability providing the minimum of the guessing probability has two cases. The interesting case of the two cases is one where the prior probability providing the minimum of the guessing probability is unique, with the condition that the second inequality of Proposition 1 does not hold. This is because, in this case, Bob's optimal MD strategy is not unique. When the second condition of Proposition 1 is satisfied, an element $|v_1\rangle$ in the support of M_1 satisfies the relation of $\langle v_1|\,\rho_1\,|v_1\rangle : \langle v_1|\,\rho_2\,|v_1\rangle = 1-q : q$. Then, from Lemma A1 in Appendix B, there exists $\epsilon > 0$ providing $M_1 - \epsilon\,|v_1\rangle\langle v_1| \geq 0$. Now, we define M_1' and M_2' as $M_1 - \epsilon\,|v_1\rangle\langle v_1|$ and $M_2 + \epsilon\,|v_1\rangle\langle v_1|$, respectively. Then, M_1' and M_2' are positive semidefinite operators. Because of $M_1' + M_2' = (M_1 - \epsilon\,|v_1\rangle\langle v_1|) + (M_2 + \epsilon\,|v_1\rangle\langle v_1|) = I$, $\mathbf{M}' = (M_1', M_2')$ is a POVM. We can verify whether $\mathbf{M}'$ is an optimal measurement at $\mathbf{q}$. First, from the relation of $\langle v_1|\,\rho_1\,|v_1\rangle : \langle v_1|\,\rho_2\,|v_1\rangle = 1-q : q$, we have $\langle v_1|\,(1-q)\rho_2 - q\rho_1\,|v_1\rangle = 0$. For $|v_1\rangle \in \mathrm{Supp}(M_1)$, by Lemma A2, we can obtain $((1-q)\rho_2 - q\rho_1)\,|v_1\rangle\langle v_1| = 0$. Then, we have the following relations that show that $\mathbf{M}'$ is an optimal measurement at $\mathbf{q}$:

$$\begin{aligned} ((1-q)\rho_2 - q\rho_1)\,M_1' &= ((1-q)\rho_2 - q\rho - 1)\,(M_1 - \epsilon\,|v_1\rangle\langle v_1|) = ((1-q)\rho_2 - q\rho_1)\,M_1 \geq 0 \\ (q\rho_1 - (1-q)\rho_2)\,M_2' &= (q\rho_1 - (1-q)\rho_2)\,(M_2 + \epsilon\,|v_1\rangle\langle v_1|) = (q\rho_1 - (1-q)\rho_2)\,M_2 \geq 0 \end{aligned}$$

According to Lemma A3 in the Appendix B, the necessary and sufficient condition that two conditions of $[\rho_1+\rho_2, M_1] = 0$ and $[\rho_2, M_1] = 0$ are satisfied is that the optimal measurement $\mathbf{M}$ of a receiver can be simultaneously diagonalized with two quantum states ρ_1 and ρ_2. Therefore, if the optimal measurement $\mathbf{M}$ of a receiver is simultaneously diagonalized with two quantum states ρ_1 and ρ_2, the uniqueness of the sender's minimax strategy cannot be compatible with the uniqueness of the receiver's MD strategy. The following Corollary summarizes this result.

Corollary 1. *If the optimal measurement* $\mathbf{M}$ *can be simultaneously diagonalized with two quantum states* ρ_1 *and* ρ_2*, the uniqueness of minimax strategy of a sender and the uniqueness of MD of a receiver cannot be compatible.*

The above result can be applied to cases of building quantum random number generator(QRNG). Suppose that only one side's strategy is unique. Therefore, either the minimax strategy of a sender or the minimum error strategy is unique. The randomness in QRNG is defined as the min-entropy to the classical bit in the quantum-classical state and depends on the prior probability [25,29]. If the prior probability providing minimum guessing probability is not unique, we can build QRNG that is not sensitive to the prior probability. When QRNG is built such that the receiver's strategy is unique, even a slight error in the measurement leads to the loss of the optimality of the receiver's strategy. The quantum states with a unique receiver's strategy in QRNG can be found by using Corollary 1.

4. Conclusions

We studied the two person zero sum game where the payoff is defined by the correct probability of the two quantum states. Because it is known that the optimal strategy of the game is a minimax strategy, and it is important to verify its uniqueness of the minimax strategy, we focused on the uniqueness condition of the minimax strategy of a sender and the minimax strategy of a receiver. In this study, we obtained the necessary and sufficient condition for the uniqueness of the sender's strategy. Using this condition, we investigated the quantum states providing the minimum guessing probability when a sender's minimax strategy is unique. Further, we found the condition where both the sender's minimax strategy and the receiver's optimal minimum error strategy cannot be unique.

Our result helps to understand the fundamental aspect of minimax strategy. We studied the minimax strategy in the quantum state discrimination of two quantum states. The uniqueness of the minimax strategy in the quantum state discrimination of more than two quantum states is not known yet. In our future work, we hope to investigate this problem.

Author Contributions: Conceptualization, J.K. and D.H.; Investigation, J.K.; Methodology, J.K.; Supervision and Critical advice Y.K.; Writing—first draft, J.K.; Revision, Y.K. All authors have read and approved the final manuscript.

Funding: 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 & NRF2018R1D1A1B07049420) and Institute for Information and Communication Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. R0190-15-2028, PSQKD).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MD	Minimum error Discrimination
QRNG	Quantum Random Number Generator

Appendix A. Proofs

Proof of Lemma 1. ($\Rightarrow$) Suppose that measurement $\{M_x\}_{x=1}^2$ satisfies the above condition. We define the operator K to be $q\rho_1 M_1 + (1-q)\rho_2 M_2$. Then, we obtain the following relations:

$$\begin{aligned} K - q\rho_1 &= q\rho_1 M_1 + (1-q)\rho_2 M_2 - q\rho_1 = \left((1-q)\rho_2 - q\rho_1\right) M_2 \geq 0 \\ K - (1-q)\rho_2 &= q\rho_1 M_1 + (1-q)\rho_2 M_2 - (1-q)\rho_2 = \left(q\rho_1 - (1-q)\rho_2\right) M_1 \geq 0. \end{aligned}$$

For an arbitrary measurement $\{N_x\}_{x=1}^2$, we obtain:

$$\mathrm{tr}(K) - \mathrm{tr}(q\rho_1 N_1 + (1-q)\rho_2 N_2) = \mathrm{tr}(\left(K - q\rho_1\right) N_1) + \mathrm{tr}(\left(K - (1-q)\rho_2\right) N_2) \geq 0.$$

This implies that the measurement $\{M_x\}_{x=1}^2$ is optimal.
($\Leftarrow$) Let us assume that measurement $\{M_x\}_{x=1}^2$ is optimal in the MD of two quantum state. This implies that the measurement provides the guessing probability:

$$\begin{aligned} p_{\text{guess}} &= q\mathrm{tr}(\rho_1 M_1) + (1-q)\mathrm{tr}(\rho_2 M_2) \\ &= \frac{1}{2}\left(1 + \mathrm{tr}(\left((1-q)\rho_2 - q\rho_1\right)\left(M_2 - M_1\right))\right) \\ &= \frac{1}{2}\left(1 + \mathrm{tr}(\mathit{\Lambda}(M_2 - M_1))\right), \end{aligned}$$

where Λ is $(1-q)\rho_2 - q\rho_1$. Because Λ is a Hermitian operator, from the spectrum theorem, we know that there is a projection operator onto the eigenspace:

$$\Lambda = \sum_{i\in\Omega} \lambda_i P_i = \sum_{i\in\Omega_>} \lambda_i P_i + \sum_{i\in\Omega_<} \lambda_i P_i$$

Here, λ_i are eigenvalues and $P_iP_j = P_i\delta_{ij}$ is satisfied for every $i, j \in \Omega$. Further, $\Omega_> = \{i \in \Omega : \lambda_i > 0\}$ and $\Omega_< = \{i \in \Omega : \lambda_i < 0\}$. Then, $I - \sum_{i\in\Omega_>\cup\Omega_<} P_i$ is a projection onto the kernel of Λ. Because measurement $\{M_x\}_{x=1}^2$ is optimal, the general form is given as:

$$M_1 = \sum_{i\in\Omega_<} P_i + N_1, \quad M_2 = \sum_{i\in\Omega_>} P_i + N_2$$

Here, we have $N_1 \geq 0$, $N_2 \geq 0$ and $N_1 + N_2 = I - \sum_{i\in\Omega_>\cup\Omega_<} P_i$. First, M_1 is optimal and Λ contains the projector $\sum_{i\in\Omega_<} P_i$ onto the eigenspace of negative eigenvalues. And M_2 is optimal and Λ includes projector $\sum_{i\in\Omega_>} P_i$ onto eigenspace of positive eigenvalues. However, for $\Omega \neq \Omega_> \cup \Omega_<$, $\sum_{i\in\Omega_>} P_i + \sum_{i\in\Omega_<} P_i = I$ is not generally satisfied. Meanwhile, $I - \sum_{i\in\Omega_>\cup\Omega_<} P_i$ is a projector onto the null space of Λ, which does not affect optimization. Therefore, for $N_1 \geq 0$ and $N_2 \geq 0$, one can find $N_1 + N_2 = I - \sum_{i\in\Omega_>\cup\Omega_<} P_i$. Because $\Lambda N_x = 0 (x = 1, 2)$, for $x \in \{1, 2\}$, we have

$$(-1)^x \Lambda M_x = (-1)^x \Lambda(M_x - N_x) = (-1)^x (M_x - N_x)\Lambda(M_x - N_x) \geq 0.$$

Therefore, when measurement $\{M_x\}_{x=1}^2$ is optimal in the MD of two quantum states, the relation of $(-1)^x ((1-q)\rho_2 - q\rho_1) M_x \geq 0$ $(x = 1, 2)$ is satisfied. □

Proof of Lemma 3. ($\Rightarrow$) Suppose that a measurement $\{M_x\}_{x=1}^2$ can simultaneously perform MD on $\{p_x, \rho_x\}_{x=1}^2$ and $\{q_x, \rho_x\}_{x=1}^2$. This implies that $\sum_{x=1}^2 p_x \mathrm{tr}(\rho_x M_x) = \sum_{x=1}^2 q_x \mathrm{tr}(\rho_x M_x)$ and one has $\sum_{x=1}^2 (p_x - q_x)\mathrm{tr}(\rho_x M_x) = 0$. Therefore, $(p_1 - q_1)(\mathrm{tr}(\rho_1 M_1) - \mathrm{tr}(\rho_2 M_2)) = 0$. Because of $p_1 \neq q_1$, we obtain $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2)$. Note that only in the prior probability providing the minimum guessing probability, there exists an optimal measurement that satisfies $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2)$. Therefore, when an optimal measurement of the simultaneous MD on $\{p_x, \rho_x\}_{x=1}^2$ and $\{q_x, \rho_x\}_{x=1}^2$ exists, we have $p_{\mathrm{guess}}^{(1)} = p_{\mathrm{guess}}^{\star}$.
($\Leftarrow$) When a prior probability can provide the minimum guessing probability, there exists at least one optimal measurement $\{M_x\}_{x=1}^2$ satisfying $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2)$. Because of $p_{\mathrm{guess}}^{(1)} = p_{\mathrm{guess}}^{\star}$, an optimal measurement $\{M_x\}_{x=1}^2$ satisfies $\mathrm{tr}(\rho_1 M_1) = \mathrm{tr}(\rho_2 M_2)$ and we have $\sum_{x=1}^2 q_x \mathrm{tr}(\rho_x M_x) = \sum_{x=1}^2 p_x \mathrm{tr}(\rho_x M_x) = p_{\mathrm{guess}}^{(1)} = p_{\mathrm{guess}}^{(2)}$. This implies that the optimal measurement $\{M_x\}_{x=1}^2$ which performs the minimum error discrimination on $\{p_x, \rho_x\}_{x=1}^2$ can discriminate $\{q_x, \rho_x\}_{x=1}^2$ with minimum error. Therefore, when $p_{\mathrm{guess}}^{(1)} = p_{\mathrm{guess}}^{\star}$, there exists an optimal measurement that can simultaneously perform MD on $\{p_x, \rho_x\}_{x=1}^2$ and $\{q_x, \rho_x\}_{x=1}^2$. □

Proof of Proposition 1. ($\Rightarrow$) Suppose that the prior probability providing the minimum of guessing probability is not unique. For example, prior prbability $(p, 1-p)$ or $(q, 1-q)$ exhibits the minimum of the guessing probability. In this case, we will show $[\rho_1 + \rho_2, M_1] = 0$ and $[\rho_2, M_1] = 0$. By Lemmas 2 and 3, measurement $\{M_x\}_{x=1}^2$ is optimal in both prior probabilities p and q to ρ_1. Therefore, one can have the following relations:

$$(q\rho_1 - (1-q)\rho_2)M_1 \geq 0 \tag{A1}$$

$$(p\rho_1 - (1-p)\rho_2)M_1 \geq 0. \tag{A2}$$

Note that the two operators are Hermitian and their difference is $(p-q)(\rho_1 + \rho_2)M_1$, which is also Hermitian. Because of $p \neq q$, $(\rho_1 + \rho_2)M_1$ is a Hermitian operator and the relation of $[\rho_1 + \rho_2, M_1] = 0$ holds. This is because $(\rho_1 + \rho_2)M_1 = ((\rho_1 + \rho_2)M_1)^\dagger = M_1^\dagger(\rho_1 + \rho_2)^\dagger = M_1(\rho_1 + \rho_2)$ when $(\rho_1 + \rho_2)M_1$ is Hermitian. Further, $(p-q)\rho_2 M_1$ is also Hermitian, and because of $p \neq q$ and $\rho_2 M_1$ is Hermitian. Because of $\rho_2 M_1 = (\rho_2 M_1)^\dagger = M_1^\dagger \rho_2^\dagger = M_1 \rho_2$, we have $[\rho_2, M_1] = 0$. This implies that both $(\rho_1 + \rho_2)M_1$ and $\rho_2 M_1$ are positive semidefinite operator. $\rho_1 + \rho_2$ and M_1 (ρ_2 and M_1) commute each other and are simultaneously diagonalizable. Furthermore, the positive semidefinite operator $\sqrt{M_1}$

can be diagonalized by any basis that can diagonalize M_1. Therefore, we can find $[\rho_1+\rho_2, \sqrt{M_1}] = 0$ and $[\rho_2, \sqrt{M_1}] = 0$. Then, we can obtain the following relations for a vector $|v\rangle$:

$$\langle v| (\rho_1+\rho_2)M_1 |v\rangle = \langle v| \sqrt{M_1}(\rho_1+\rho_2)\sqrt{M_1} |v\rangle \geq 0 \tag{A3}$$

$$\langle v| \rho_2 M_1 |v\rangle = \langle v| \sqrt{M_1}\rho_2\sqrt{M_1} |v\rangle \geq 0 \tag{A4}$$

Hence, $(\rho_1+\rho_2)M_1 \geq 0$ and $\rho_2 M_1 \geq 0$. In the prior probability $(p, 1-p)$ because $\{M_x\}_{x=1}^2$ is optimal, $(p\rho_1 - (1-p)\rho_2)M_1$ and $((1-p)\rho_2 - p\rho_1)M_2$ are positive semidefinite. Therefore we obtain the following relations:

$$(q\rho_1 - (1-q)\rho_2)M_1 \geq (q-p)(\rho_1+\rho_2)M_1 \tag{A5}$$

$$((1-q)\rho_2 - q\rho_1)M_2 \geq (p-q)(\rho_1+\rho_2)M_2 \tag{A6}$$

We will show that for $x \in \{1,2\}$ an element $|v\rangle$ of support of M_x does not satisfy $\langle v| \rho_1 |v\rangle : \langle v| \rho_2 |v\rangle = 1-q : q$. First, we consider the case of $p < q$. Then, $q\rho_1 - (1-q)\rho_2$ and M_1 commute each other and a vector $|v\rangle$ satisfies the following relation:

$$\begin{aligned}\langle v| \sqrt{M_1}(q\rho_1 - (1-q)\rho_2)\sqrt{M_1} |v\rangle &= \langle v| (q\rho_1 - (1-q)\rho_2)M_1 |v\rangle \\ &\geq (q-p) \langle v| (\rho_1+\rho_2)M_1 |v\rangle \\ &= (p-q) \langle v| \sqrt{M_1}(\rho_1+\rho_2)\sqrt{M_1} |v\rangle \geq 0\end{aligned} \tag{A7}$$

Here, the first and the last equalities are satisfied by Corollary A1. $\sqrt{M_1}$ and M_1 have the same support and $\sqrt{M_1}\,|v\rangle$ is a element of M_1's support. Every element of the support of M_1 can be expressed by $\sqrt{M_1}\,|v\rangle$ for a vector $|v\rangle$. Moreover, $\rho_1+\rho_2$ is full rank and we obtain $\langle v| \rho_1+\rho_2 |v\rangle > 0$ for a non-zero vector $|v\rangle$. Therefore, the condition for equality in the last inequality becomes $\sqrt{M_1}\,|v\rangle = 0$, which implies that $|v\rangle$ is a kernel of M_1. Therefore, a non-zero element $|v_1\rangle$ in the support of M_1 satisfies the inequality $\langle v_1| (q\rho_1 - (1-q)\rho_2) |v_1\rangle > 0$.

Now, we consider the case of $p > q$. By the completeness condition of POVM, $q\rho_1 - (1-q)\rho_2$ and M_2 commute each other and for a vector $|v\rangle$ we have the following relation:

$$\begin{aligned}\langle v| \sqrt{M_2}((1-q)\rho_2 - q\rho_1)\sqrt{M_2} |v\rangle &= \langle v| ((1-q)\rho_2 - q\rho_1)M_2 |v\rangle \\ &\geq (p-q) \langle v| (\rho_1+\rho_2)M_2 |v\rangle \\ &= (p-q) \langle v| \sqrt{M_2}(\rho_1+\rho_2)\sqrt{M_2} |v\rangle \geq 0\end{aligned} \tag{A8}$$

The first and the last equalities are obtained by Corollary A1. $\sqrt{M_2}$ and M_2 have the same support and $\sqrt{M_2}\,|v\rangle$ is an element of M_2's support. Every element of the support of M_2 can be expressed by $\sqrt{M_2}\,|v\rangle$ for an element of $|v\rangle$. The condition for the equality in the last inequality is $\sqrt{M_2}\,|v\rangle$, which implies that $|v\rangle$ is a kernel of M_2. Then, a non-zero element $|v_2\rangle$ in the support of M_2 satisfies $\langle v_2| (1-q)\rho_2 - q\rho_1 |v_2\rangle > 0$. Therefore, when $p < q$, any vector $|v_1\rangle$ in the support of M_1 does not satisfy $\langle v_1| \rho_1 |v_1\rangle : \langle v_1| \rho_2 |v_1\rangle = 1-q : q$. When $p > q$, any vector $|v_2\rangle$ in the support of M_2 does not satisfy $\langle v_2| \rho_1 |v_2\rangle : \langle v_2| \rho_2 |v_2\rangle = 1-q : q$.

In summary, if the prior probability providing the minimum of guessing probability is not unique, the relations of $[\rho_1+\rho_2, M_1] = 0$ and $[\rho_2, M_1] = 0$ hold and for $x \in \{1,2\}$, any vector $|v_x\rangle$ in the support of M_x does not satisfy $\langle v_x| \rho_1 |v_x\rangle : \langle v_x| \rho_2 |v_x\rangle = 1-q : q$. This contradicts the assumption that condition 1 and 2 hold. Therefore, when condition 1 and 2 are satisfied, the prior probability providing the minimum of guessing probability is unique.

($\Leftarrow$) Assume that the measurement $\{M_x\}_{x=1}^2$ satisfies $[\rho_1+\rho_2, M_1] = 0$, $[\rho_2, M_1] = 0$ and for some $x' \in \{1,2\}$ there is no $|v_{x'}\rangle$ of the support of $M_{x'}$ that satisfies the relation $\langle v_{x'}| \rho_1 |v_{x'}\rangle : \langle v_{x'}| \rho_2 |v_{x'}\rangle =$

$1-q:q$. For every $x \in \{1,2\}$ the support of M_x is a subspace of the direct sum of the non-negative eigenspace of $(-1)^x((1-q)\rho_2 - q\rho_1)$. Therefore, for an element $|v_x\rangle$ in the support of M_x the relation of $(-1)^x((1-q)\rho_2 - q\rho_1)$ holds. However, when $x = x'$, because of $\langle v_{x'}| (1-q)\rho_2 - q\rho_1 |v_{x'}\rangle \neq 0$, we can have $(-1)^{x'} \langle v_{x'}| (1-q)\rho_2 - q\rho_1 |v_{x'}\rangle > 0$.

Now, let us find the other prior probability which can share the optimal measurement. We define p as $q + \frac{(-1)^{x'}}{2} \min_{|v\rangle \in \mathrm{Supp}(\mathrm{M}_{x'})} (-1)^{x'} \langle v| (1-q)\rho_2 - q\rho_1 |v\rangle$. When $x' = 1$, we have $p < q$. By $\min_{|v\rangle \in \mathrm{Supp}(\mathrm{M}_1)} \langle v| q\rho_1 - (1-q)\rho_2 |v\rangle \leq q$ we have $p \geq 0$. When $x' = 2$, one has $p > q$ and by $\min_{|v\rangle \in \mathrm{Supp}(\mathrm{M}_2)} \langle v| (1-q)\rho_2 - q\rho_1 |v\rangle \leq 1-q$ we obtain $p \leq 1$.

Then, we will show that $\{M_x\}_{x=1}^2$ is optimal in $(q, 1-q)$. Note that the following two relations hold:

$$\langle v_1| q\rho_1 - (1-q)\rho_2 |v_1\rangle \geq -(p-q) \langle v_1| \rho_1 + \rho_2 |v_1\rangle \quad \text{for all } |v_1\rangle \in \mathrm{Supp}(\mathrm{M}_1) \tag{A9}$$

$$\langle v_2| (1-q)\rho_2 - q\rho_1 |v_2\rangle \geq (p-q) \langle v_2| \rho_1 + \rho_2 |v_2\rangle \quad \text{for all } |v_2\rangle \in \mathrm{Supp}(\mathrm{M}_2). \tag{A10}$$

Here, $\rho_1 + \rho_2$ is full rank and for every vector $|v\rangle$ one has $\langle v| \rho_1 + \rho_2 |v\rangle > 0$. When $x' = 1$, $p < q$ and because of $\langle v_2| (1-q)\rho_2 - q\rho_1 |v_2\rangle \geq 0$ the second condition holds. By the following relation the first inequality (A13) holds:

$$\begin{aligned} \langle v_1| q\rho_1 - (1-q)\rho_2 |v_1\rangle &\geq \min_{|v\rangle \in \mathrm{Supp}(\mathrm{M}_1)} \langle v| q\rho_1 - (1-q)\rho_2 |v\rangle \\ &= -2(p-q) \geq -(p-q) \langle v_1| \rho_1 + \rho_2 |v_1\rangle \end{aligned} \tag{A11}$$

Let us consider the case of $x' = 2$. Because $p > q$ and $\langle v_1| q\rho_1 - (1-q)\rho_2 |v_1\rangle \geq 0$, the first condition holds. By the following relation, the second inequality holds:

$$\begin{aligned} \langle v_2| (1-q)\rho_2 - q\rho_1 |v_2\rangle &\geq \min_{|v\rangle \in \mathrm{Supp}(\mathrm{M}_2)} \langle v| (1-q)\rho_2 - q\rho_1 |v\rangle \\ &= 2(p-q) \geq (p-q) \langle v_2| \rho_1 + \rho_2 |v_2\rangle \end{aligned} \tag{A12}$$

Because $[\rho_1 + \rho_2, M_1] = 0$ and $[\rho_2, M_1] = 0$, have the relation $[p\rho_1 - (1-p)\rho_2, M_1] = [p(\rho_1 + \rho_2) - \rho_2, M_1] = 0$. This implies that $p\rho_1 - (1-p)\rho_2$ and M_1 are simultaneously diagonalizable. Then, $p\rho_1 - (1-p)\rho_2$ and the positive semidefinite operator satisfying $N_1^2 = M_1$ are simultaneously diagonalizable, which has the same support as to that of M_1. Therefore, for every vector $|v\rangle$ the following relation holds:

$$\langle v| (p\rho_1 - (1-p)\rho_2) M_1 |v\rangle = \langle v| N_1 (p\rho_1 - (1-p)\rho_2) N_1 |v\rangle \geq 0 \tag{A13}$$

Note that $N_1 |v\rangle$ is an element of M_1. Therefore, we have $(p\rho_1 - (1-p)\rho_2) M_1 \geq 0$. In the same manner, by the completeness relation of POVM, $p\rho_1 - (1-p)\rho_2$ and M_2 are simultaneously diagonalizable. $p\rho_1 - (1-p)\rho_2$ and positive semidefinite operator N_2 satisfying $N_2^2 = M_2$ are simultaneously diagonalizable, which has the same support as that of M_2 by Corollary A1. Therefore, for every vector $|v\rangle$, the following relation holds:

$$\langle v| ((1-p)\rho_2 - p\rho_1) M_2 |v\rangle = \langle v| N_2 ((1-p)\rho_2 - p\rho_1) N_2 |v\rangle \geq 0 \tag{A14}$$

Note that $N_2 |v\rangle$ is support of M_2 and one has $((1-p)\rho_2 - p\rho_1) M_2 \geq 0$.

By Lemma 1, for every $x \in \{1,2\}$, one finds $(-1)^x((1-p)\rho_2 - p\rho_1) M_x \geq 0$ and $\{M_x\}_{x=1}^2$ is optimal at the prior probability $(p, 1-p)$. This contradicts the assumption that the identical measurement cannot be shared in the different prior probabilities. Therefore, when the prior probability providing the minimum guessing probability is unique, the condition 1(or 2) holds. □

Appendix B. Lemmas

Let $\mathcal{H}$ be a finite dimensional Hilbert space.

Lemma A1. *Let A be a positive semidefinite operator. Let $|v\rangle$ be an element of support of A. Then there exists $\epsilon > 0$ such that $A - \epsilon |v\rangle \langle v| \geq 0$.*

Proof of Lemma A1. Let us assume that there exists no $\epsilon > 0$ satisfying $A - \epsilon |v\rangle \langle v| \geq 0$. This implies that for any $\epsilon > 0$, there exists $|w\rangle \in \mathcal{H}$ such that $\langle w| (A - \epsilon |v\rangle \langle v|) |w\rangle < 0$. Thus $\langle w| A |w\rangle < \epsilon |\langle w|v\rangle|^2$. Because $A \geq 0$, it follows that $0 \leq \langle w| A |w\rangle < \epsilon |\langle w|v\rangle|^2$.

Note that $\langle w| A |w\rangle$ cannot be zero. Because when we assume $\langle w| A |w\rangle = 0$, $|w\rangle$ is an element of $\ker(A)$. Since $|v\rangle$ is orthogonal to $\ker(A)$; this directly implies $\langle w|v\rangle = 0$. Hence, $0 < 0$, which is a contradiction. Therefore $\langle w| A |w\rangle > 0$.

Any vector in $\mathcal{H}$ can be decomposed as a linear combination of elements of $\mathrm{Supp}(A)$ and $\ker(A)$. Furthermore $|w\rangle$ cannot be an element of kernel. Thus there exists $|s\rangle \in \mathrm{Supp}(A)$ and $|k\rangle \in \ker(A)$ such that $|w\rangle = c_1 |s\rangle + c_2 |k\rangle$ and where $c_1 \neq 0$.

Because A is an operator on the finite dimensional Hilbert space, there exists $\gamma > 0$ such that $\gamma \equiv \inf_{|s\rangle \in \mathrm{Supp}(A)} \langle s| A |s\rangle$. When $\epsilon = \gamma$,

$$\langle w| A |w\rangle = |c_1|^2 \langle s| A |s\rangle \geq |c_1|^2 \epsilon \geq |c_1|^2 \epsilon |\langle s|v\rangle|^2 \geq \epsilon |\langle w|v\rangle|^2.$$

This contradicts the initial assumption. Therefore there exists $\epsilon > 0$ such that $A - \epsilon |v\rangle \langle v| \geq 0$. □

Lemma A2. *Let A be a Hermitian operator on $\mathcal{H}$. Let B be a positive semidefinite operator on $\mathcal{H}$. Suppose that A and B are commutable. If $|v\rangle \in \mathrm{Supp}(B)$ satisfies $\langle v| A |v\rangle = 0$, then $|v\rangle \in \ker(A)$.*

Proof of Lemma A2. Because A and B are commutable, there exists an orthonormal basis $\{|\phi_i\rangle\}_i$ such that $A = \sum_{i \in \chi_A} a_i |\phi_i\rangle \langle \phi_i|$, $B = \sum_{i \in \chi_B} b_i |\phi_i\rangle \langle \phi_i|$, where $a_i \neq 0$ for all $i \in \chi_A$ and $b_i > 0$ for all $i \in \chi_B$. Then $AB = \sum_{i \in \chi_A \cap \chi_B} a_i b_i |\phi_i\rangle \langle \phi_i|$. Because $AB \geq 0$, $a_i > 0$ for all $i \in \chi_A \cap \chi_B$. As $|v\rangle \in \mathrm{Supp}(B)$, we can express $|v\rangle$ as $\sum_{i \in \chi_B} c_i |\phi_i\rangle$. Then

$$\begin{aligned} \sum_{i \in \chi_A \cap \chi_B} |c_i|^2 a_i &= \sum_{i,j \in \chi_B} c_i^* \langle \phi_i| \sum_{k \in \chi_A} a_k |\phi_k\rangle \langle \phi_k| |\phi_j\rangle c_j \\ &= \langle v| A |v\rangle = 0. \end{aligned}$$

Because $a_i > 0$, it follows that $|c_i|^2 = 0$ for all $i \in \chi_A \cap \chi_B$. This implies that $c_i = 0$. Thus

$$A |v\rangle = \sum_{k \in \chi_A} a_k |\phi_k\rangle \langle \phi_k| \sum_{i \in \chi_B} c_i |\phi_i\rangle = \sum_{i \in \chi_A \cap \chi_B} a_i c_i |\phi_i\rangle = 0$$

Therefore if $|v\rangle \in \mathrm{Supp}(B)$ satisfies $\langle v| A |v\rangle = 0$, then $|v\rangle \in \ker(A)$ □

Let $\mathcal{H}$ be a Hilbert space with dimension d. Let A, B be Hermitian operators on $\mathcal{H}$.

Lemma A3. *If $[A, B] = 0$, then A, B can be simultaneously diagonalizable.*

Proof of lemma A3. Because A and B are Hermitian operators and $[A, B] = 0$, it follows that $(AB)^\dagger = B^\dagger A^\dagger = BA = AB$. This implies that AB is a Hermitian operator. Let $\sum_{i=1}^{d} a_i |a_i\rangle \langle a_i|$ be a spectral decomposition of A. Then

$$AB = \sum_{i,j=1}^{d} a_i |a_i\rangle \langle a_i| B |a_j\rangle \langle a_j| = \sum_{i,j=1}^{d} a_i \langle a_i| B |a_i\rangle |a_i\rangle \langle a_i| .$$

Because AB is a Hermitian operator, it follows that

$$a_l \langle a_k| B |a_l\rangle = (AB)^*_{lk} = (AB)_{kl} = a_k \langle a_k| B |a_l\rangle \quad \text{for all } k, l \in \{1, 2, \cdots, d\}$$

This implies that $(a_l - a_k) \langle a_k| B |a_l\rangle = 0$. Thus $a_l = a_k$ or $\langle a_k| B |a_l\rangle = 0$.

Let us define a set of indices $I \subset \{1, 2, \cdots, d\}$ such that for every $i \in I$, if $j \in \{1, 2, \cdots, d\} \backslash \{i\}$ satisfies $\langle a_i | B | a_j \rangle \neq 0$, then $j \in I$ and there is no non-empty subset $J \subset I$ such that for every $i \in I \backslash J$ and for every $j \in J$, $\langle a_i | B | a_j \rangle = 0$. Using the result above, $a_i = a_j$ for all $i, j \in I$. This implies that $\sum_{i,j \in I} \langle a_i | B | a_j \rangle |a_i\rangle \langle a_j|$ can be represented with a block matrix with a basis of $\{|a_i\rangle\}_{i \in I}$ by rearranging the indices. Define a' as the positive number satisfying $a_i = a'$ for all $i \in I$. Then $\sum_{i \in I} |a_i\rangle \langle a_i|$ is a projection operator on the eigenspace of A providing eigenvalue a'. Note that the eigenspace has a degree of freedom in choosing the orthonormal basis.

Now let us explain how to choose a basis that can diagonalize A and B simultaneously. Because $\sum_{i,j \in I} \langle a_i | B | a_i \rangle |a_i\rangle \langle a_i|$ is a Hermitian operator, it can be diagonalized with some orthonormal basis. Suppose that $\{|c_i\rangle\}_{i \in I}$ is the basis. Then $\sum_{i,j \in I} \langle a_i | B | a_j \rangle |a_i\rangle \langle a_j| = \sum_{i \in I} c_i |c_i\rangle \langle c_i|$ holds, where c_i is a eigenvalue of B. Furthermore, because $\texttt{span}\{|a_i\rangle\}_{i \in I}$ is an eigenspace of A, $\sum_{i \in I} a' |a_i\rangle \langle a_i|$ can be rewritten as $\sum_{i \in I} a' |c_i\rangle \langle c_i|$. Similarly, we can find a basis that diagonalizes each block matrix of B. A can be diagonalized using this basis. Therefore if $[A, B] = 0$, then A and B can be simultaneously diagonalizable. □

Let $\sum_{i=1}^{r} \lambda_i P_i$ be a spectral decomposition of B. Then $C = \sum_{i=1}^{r} \sqrt{\lambda_i} P_i$ satisfies $C^2 = B$. We show that the positive semidefinite operator satisfying $C^2 = B$ is unique.

Suppose that C is not unique. Then there exists another positive semidefinite operator C' such that $C'^2 = B$. Because $[B, C'] = 0$, from Lemma A3, B, C' are simultaneously diagonalizable. That is, there exists an orthornormal basis $\{|\nu_i^{(j)}\rangle\}_{i,j=1}^{r,d_i}$ such that

$$B = \sum_{i=1}^{r} \lambda_i \left(\sum_{j=1}^{d_i} |\nu_j^{(i)}\rangle \langle \nu_j^{(i)}| \right), \quad C' = \sum_{i=1}^{r} \left(\sum_{j=1}^{d_i} \nu_{ij} |\nu_i^{(j)}\rangle \langle \nu_i^{(j)}| \right)$$

for some non-negative $\lambda_i, \nu_{i,j} \in \mathbb{R}$. Because $C'^2 = B$, it follows that

$$B - C'^2 = \sum_{i=1}^{r} \sum_{j=1}^{d_i} (\lambda_i - \nu_{ij}^2) |\nu_i^{(j)}\rangle \langle \nu_i^{(j)}| = 0.$$

Thus $\nu_{ij} = \sqrt{\lambda_i}$ for all $i, j \in \{1, 2, \cdots, d\}$. Further, because $\sum_{j=1}^{d} |\nu_i^{(j)}\rangle \langle \nu_i^{(j)}| = P_i$, it follows that $C' = \sum_{i=1}^{r} \sqrt{\lambda_i} \left(\sum_{j=1}^{d_i} |\nu_i^{(j)}\rangle \langle \nu_i^{(j)}| \right) = \sum_{i=1}^{r} \sqrt{\lambda_i} P_i = C$. This contradicts the initial assumption. Therefore, the positive semidefinite operator satisfying $C^2 = B$ is unique.

Let A, B be positive semidefinite operators on $\mathcal{H}$. Let C be a positive semidefinite operator on $\mathcal{H}$ satisfying $C^2 = B$.

Corollary A1. *If* $[A, B] = 0$, *then* $[A, C] = 0$.

Proof of Corollary A1. According to Lemma A3, $[A, B] = 0$ implies that A and B are simultaneously diagonalizable. That is there exists an orthonormal basis $\{|\lambda_i\rangle\}_{i=1}^{d}$ such that

$$A = \sum_{i=1}^{d} a_i |\lambda_i\rangle \langle \lambda_i|, \quad B = \sum_{i=1}^{d} b_i |\lambda_i\rangle \langle \lambda_i|,$$

for some $a_i \geq 0$ and $b_i \geq 0$. Then C is uniquely defined as $C = \sum_{i=1}^{d} \sqrt{b_i} |\lambda_i\rangle \langle \lambda_i|$ by the statement above. Note that there exists an orthornormal basis $\{|\lambda_i\rangle\}_{i=1}^{d}$ diagonalizing A, C simultaneously. Therefore if $[A, B] = 0$, then $[A, C] = 0$. □

References

1. Chefles, A. Quantum state discrimination. *Contemp. Phys.* **2000**, *41*, 401–424. [CrossRef]
2. Barnett, S.M.; Croke, S. Quantum state discrimination. *Adv. Opt. Photon.* **2009**, *1*, 238–278. [CrossRef]
3. Bergou, J.A. Discrimination of quantum states. *J. Mod. Opt.* **2010**, *57*, 160–180. [CrossRef]

4. Bae, J.; Kwek, L. Quantum state discrimination and its applications. *J. Phys. A Math Theor.* **2015**, *48*, 083001. [CrossRef]
5. Ha, D.; Kwon, Y. Complete analysis for three-qubit mixed-state discrimination. *Phys. Rev. A* **2013**, *87*, 062302. [CrossRef]
6. Ha, D.; Kwon, Y. Discriminating *N*-qudit states using geometric structure. *Phys. Rev. A* **2014**, *90*, 022330. [CrossRef]
7. Herzog, U. Minimum-error discrimination between a pure and a mixed two-qubit state. *J. Opt. B Quantum Semiclass. Opt.* **2004**, *6*, S24–S28. [CrossRef]
8. Ivanovic, I. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1987**, *123*, 257–259. [CrossRef]
9. Dieks, D. Overlap and distinguishability of quantum states. *Phys. Lett. A* **1988**, *126*, 303–306. [CrossRef]
10. Peres, A. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1988**, *128*, 19. [CrossRef]
11. Jaeger, G.; Shimony, A. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A* **1995**, *197*, 83–87. [CrossRef]
12. Chefles, A. Unambiguous discrimination between linearly independent quantum states. *Phys. Lett. A* **1998**, *239*, 339–347. [CrossRef]
13. Croke, S.; Andersson, E.; Barnett, S.M.; Gilson, C.R.; Jeffers, J. Maximum Confidence Quantum Measurements. *Phys. Rev. Lett.* **2006**, *96*, 070401. [CrossRef] [PubMed]
14. Chefles, A.; Barnett, S.M. Strategies for discriminating between non-orthogonal quantum states. *J. Mod. Opt* **1998**, *45*, 1295–1302. [CrossRef]
15. Zhang, C.W.; Li, C.F.; Guo, G.C. General strategies for discrimination of quantum states. *Phys. Lett. A* **1999**, *261*, 25–29. [CrossRef]
16. Fiurášek, J.; Ježek, M. Optimal discrimination of mixed quantum states involving inconclusive results. *Phys. Rev. A* **2003**, *67*, 012321. [CrossRef]
17. Eldar, Y.C. Mixed-quantum-state detection with inconclusive results. *Phys. Rev. A* **2003**, *67*, 042309. [CrossRef]
18. Ha, D.; Kwon, Y. An optimal discrimination of two mixed qubit states with a fixed rate of inconclusive results. *Quantum Inf. Process.* **2017**, *16*, 273. [CrossRef]
19. Wald, A. Generalization of a Theorem By v. Neumann Concerning Zero Sum Two Person Games. *Ann. Math.* **1945**, *46*, 281–286. [CrossRef]
20. Hirota, O.; Ikehara, S. Minimax Strategy in the Quantum Detection Theory and Its Application to Optical Communications. *Trans. IECE Jpn.* **1982**, *E65*, 627–633.
21. D'Ariano, G.M.; Sacchi, M.F.; Kahn, J. Minimax quantum-state discrimination. *Phys. Rev. A* **2005**, *72*, 032310. [CrossRef]
22. Nakahira, K.; Kato, K.; Usuda, T.S. Minimax strategy in quantum signal detection with inconclusive results. *Phys. Rev. A* **2013**, *88*, 032314. [CrossRef]
23. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
24. Cao, Z.; Zhou, H.; Ma, X. Loss-tolerant measurement-device-independent quantum random number generation. *New J. Phys.* **2015**, *17*, 125011. [CrossRef]
25. Bischof, F.; Kampermann, H.; Bruß, D. Measurement-device-independent randomness generation with arbitrary quantum states. *Phys. Rev. A* **2017**, *95*, 062305. [CrossRef]
26. Ma, X.; Yuan, X.; Cao, Z.; Qi, B.; Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **2016**, *2*, 16021. [CrossRef]
27. Helstrom, C.W. *Quantum Detection and Estimation Thoery*; Academic Press: New York, NY, USA, 1976.
28. Eldar, Y.C.; Megretski, A.; Verghese, G.C. Designing optimal quantum detectors via semidefinite programming. *IEEE Trans. Inf. Theory* **2003**, *49*, 1007–1012. [CrossRef]
29. Konig, R.; Renner, R.; Schaffner, C. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. Inf. Theory* **2009**, *55*, 4337–4347. [CrossRef]