No-Signaling Principle Can Determine Optimal Quantum State Discrimination

Joonwoo Bae,[1,*] Won-Young Hwang,[2] and Yeong-Deok Han[3]

[1]*School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 130-012, Republic of Korea*
[2]*Department of Physics Education, Chonnam National University, Gwangju 500-757, Republic of Korea*
[3]*Department of Game Contents, Woosuk University, Wanju, Cheonbuk 565-701, Republic of Korea*

(Received 7 March 2011; published 20 October 2011)

We provide a general framework of utilizing the no-signaling principle in derivation of the guessing probability in the minimum-error quantum state discrimination. We show that, remarkably, the guessing probability can be determined by the no-signaling principle. This is shown by proving that, in the semidefinite programing for the discrimination, the optimality condition corresponds to the constraint that quantum theory cannot be used for a superluminal communication. Finally, a general bound to the guessing probability is presented in a closed form.

DOI: 10.1103/PhysRevLett.107.170403 PACS numbers: 03.65.Ud, 03.65.Ta, 03.65.Wj, 03.67.Hk

To find and characterize the capabilities of quantum systems in their applications to information processing often leads to optimization problems which are in general considered to be difficult. Nevertheless, any optimal performance to be obtained at the end should satisfy the fundamental principles that quantum theory fulfills, although it is neither known nor clear if they are tightly related one another, e.g., see Ref. [1]. Fundamental principles can be found to be a useful tool to derive limitations on optimal quantum performance in such a way that a performance that is too good would be contradictory.

It turns out that the no-signaling principle, one of the most conservative assumptions in physics, can be used to characterize correlations that are not allowed among parties sharing physical systems [1,2]. Assuming quantum systems are shared, consequently, it follows that local operations such as quantum cloning or quantum state discrimination (QSD) cannot work arbitrarily well, since the no-signaling constraint would be violated. This has been considered in specific cases to derive only bounds to optimal quantum performances, e.g., [3,4]. In particular, QSD is of both fundamental and practical importance in a wide range of quantum information applications [5]. It is not only related to fundamental results, such as no cloning, no signaling, and nonlocality in quantum mechanics [3,4,6], but it is also applied to quantum communication or signal processing, e.g., Ref. [5].

In this work, we provide a general framework of utilizing the no-signaling principle in the derivation of optimal QSD, in such a way that if QSD works better than some threshold (in terms of the guessing probability, or the minimum error), superluminal communication would follow. We show that, remarkably, the obtained threshold actually coincides to that of the optimal QSD. This is shown by proving that the optimality condition in a mathematical formulation for optimal QSD, which will be introduced in the semidefinite programing later, corresponds to those in QSD constrained by the no-signaling principle. Hence, the no-signaling constraint turns out to be the physical principle that dictates the optimal performance in discriminating among quantum states. A general and computable bound to optimal QSD is then provided in a closed form. The result also strengthens relations among fundamental no-go theorems in Refs. [3,4,6].

Let us begin by fixing notations. Throughout the Letter, $\{q_x, \rho_x\}_{x=1}^N$ denotes the situation that a quantum state ρ_x is generated with an *a priori* probability q_x, where $\sum_x q_x = 1$. Measuring quantum systems is described by positive-operator-valued-measure (POVM) $\{M_x\}_{x=1}^N$, where (i) $M_x \geq 0$ for all x, and (ii) $\sum_x M_x = I$. Then, the minimum-error QSD among $\{q_x, \rho_x\}_{x=1}^N$ defines an optimization problem over POVMs such that the error is minimized or equivalently the guessing probability, i.e., the probability of making a correct guess, is maximized. We write $P(x|y)$ the probability that measurement M_x is "clicked" when a quantum state ρ_y is actually given. The probability measure for quantum states is given by the Born rule, $P(x|y) = \mathrm{tr}[\rho_y M_x]$, known as Gleason's theorem [7].

The guessing probability denotes the maximum probability of correctly guessing,

$$P_{\mathrm{guess}} = \sum_{x=1}^{N} q_x P(x|x) = \max_{\{M_x\}_{x=1}^N} \sum_{x=1}^{N} q_x \mathrm{tr}[\rho_x M_x]. \quad (1)$$

For the simplest case of two-state discrimination $\{q_x, \rho_x\}_{x=1}^{N=2}$, the optimal one is known as the Helstrom bound denoted by $P_{\mathrm{guess}}^{(H)}$ as follows:

$$P_{\mathrm{guess}}^{(H)} = \tfrac{1}{2}(1 + \| q_1\rho_1 - q_2\rho_2 \|). \quad (2)$$

For more than two quantum states, the guessing probability is known only in restricted cases, for instance, geometrically uniform states [8].

We now approach to the QSD problem with a fundamental constraint, the no-signaling principle, that should be fulfilled in any information processing by quantum systems. The main idea is to incorporate the QSD problem to a communication scenario between two parties, Alice and Bob who attempt to communicate by making only use of shared quantum states and measurement. Then, the optimal performance of local operations and local measurements can be limited by the no-signaling constraint.

Let us consider the following communication protocol, where two parties share copies of a quantum state $|\psi\rangle_{AB}$. Suppose that Alice encodes a message $x \in \{1, \ldots, N\}$ into the application of one of POVMs, $M^{(A,x)} = \{M_y^{(A,x)}, y = 1, \ldots\}$, in which $M^{(A,x)}$ is complete, i.e., $\sum_y M_y^{(A,x)} = I$ for each $x = 1, \ldots, N$. For instance, the message x is encoded in the application of the complete POVM $M^{(A,x)}$. The resulting state in the Bob's side is one of those states, $\rho_y^{(x)} = (p_y^{(x)})^{-1} \mathrm{tr}_A |\psi\rangle_{AB}\langle\psi|(M_y^{(A,x)} \otimes I)$ with probability $p_y^{(x)} = \langle\psi|(M_y^{(A,x)} \otimes I)|\psi\rangle$. Given that the measurement outcome is not announced, Bob only knows his system is in $\rho_y^{(x)}$ with probability $p_y^{(x)}$, that is, described by a mixed state, $\rho_B^{(x)} = \sum_y p_y^{(x)} \rho_y^{(x)}$. For another message x' corresponding to the application of $M^{(A,x')}$, Bob's system results in the state $\rho_B^{(x')}$, which is equal to $\rho_B^{(x)}$ while they are in different mixtures. In fact, using an appropriate POVM, Alice can prepare any quantum states on Bob's side, i.e., any state decomposition in the Bob's ensemble. This is known as the Gisin-Hughston-Jozsa-Wootters (GHJW) theorem [9]. Since they are identical quantum states, Bob can never learn about the POVM Alice has applied, and consequently, no message is allowed to be transferred in this way.

Now, let $P_D(x|x')$ denote the probability that Bob's detector gives an answer x when Alice has applied measurement $M^{(A,x')}$. Note the normalization condition that for each x', it holds that $\sum_x P_D(x|x') = 1$. We also note that Bob's device for the discrimination is not specified, but only its input-output relation. This can be thought of as a black box scenario.

It is clear that if the no-signaling constraint is to be fulfilled, the input-output relation cannot be given arbitrarily. Suppose that $\sum_x P_D(x|x) > 1$, meaning that $\sum_x [P_D(x|x) - P_D(x|x')] > 0$ for some $x' \neq x$, from which there would be at least a single x such that $P_D(x|x) > P_D(x|x')$. This immediately implies that P_D is not non-signaling [6] since superluminal communication can be constructed in the following way: if Alice applies two POVMs $M^{(A,x)}$ and $M^{(A,x')}$ to encode 0 and 1, respectively, Bob finds from his detector how frequently the outcome x appears and then concludes if Alice's encoding is 0 or 1. Therefore, from the no-signaling constraint, we have

$$\sum_x P_D(x|x) \leq 1, \tag{3}$$

on the Bob's detector for the discrimination.

We now relate QSD of $\{q_x, \rho_x\}_{x=1}^N$ to the communication in the above. The key idea is to consider the case that one of the POVM elements in the set $M^{(A,x)}$, say, the first element $M_1^{(A,x)}$, prepares state ρ_x on the Bob's side with probability p_x, and the rest $I - \sum_{y \neq 1} M_y^{(A,x)}$ does a state σ_x,

$$\rho_B^{(x)} = p_x \rho_x + (1 - p_x)\sigma_x, \quad \text{for } x = 1, \ldots, N. \tag{4}$$

The reader is reminded that this is always possible from the GHJW theorem [9]. If QSD among $\{\rho_x\}_{x=1}^N$ works too well, Eq. (3) would be violated, meaning that the no-signaling constraint is not fulfilled. In this way, the no-signaling principle can constrain the guessing probability for QSD among $\{\rho_x\}_{x=1}^N$.

In what follows, we derive a threshold of the guessing probability in QSD among $\{\rho_x\}_{x=1}^N$ in such a way that the no-signaling principle is not violated. From Eq. (4), it follows that $p_x P(x|x) \leq P_D(x|x)$ since, for Alice's measurement $M^{(A,x)}$, the probability that Bob's detector answers x consists of contributions both by the state ρ_x with probability p_x and the rest from state σ_x. Then, the no-signaling constraint in Eq. (3) leads to the following bound:

$$\sum_x p_x P(x|x) \leq 1. \tag{5}$$

Recall that Bob's measurement device for the discrimination is not specified, but only its input-output relation—like a black box scenario. Note also that the probability measure, Born rule, is not applied yet. The bound in Eq. (5) is only the condition that the guessing probabilities $P(x|x)$ do not lead to superluminal communication. The following are assumed, so far: (a) bipartite quantum states, (b) the Born rule to the Alice's system, and (c) the no-signaling principle between the two parties.

In fact, in the above scenario, the bound obtained in Eq. (5) corresponds to QSD among $\{q_x, \rho_x\}_{x=1}^N$ where

$$q_x = \frac{p_x}{\sum_{x'=1}^N p_{x'}}. \tag{6}$$

This is because Bob's device aims at discriminating among $\{\rho_x\}_{x=1}^N$, and the *a priori* probability that state ρ_x appears from $\{\rho_x\}_{x=1}^N$ can be found as q_x in the above. Having collected all these, it is straightforward to derive the main result.

Proposition.—From the no-signaling principle, the guessing probability in QSD among $\{q_x, \rho_x\}_{x=1}^N$ must be bounded as follows:

$$P_{\text{guess}} = \sum_x q_x P(x|x) \leq \frac{1}{\sum_x p_x}, \tag{7}$$

where $\{p_x\}_{x=1}^N$ are from the identical ensembles in Eq. (4) with the relation in Eq. (6). The equality holds when the equality in Eq. (5) holds for all $x = 1, \ldots, N$.

The equality in Eq. (5) means that Bob's measurement device works in a way that for each ensemble $\rho_B^{(x)}$

[see Eq. (4)], the measurement device responds only to $\{\rho_x\}_{x=1}^N$ but not $\{\sigma_x\}_{x=1}^N$. Therefore, the condition that the equality in Eq. (7) holds is the existence of identical ensembles in Eq. (4) such that the measurement device only responds to those states $\{\rho_x\}_{x=1}^N$ but not $\{\sigma_x\}_{x=1}^N$. Taking the measurement postulate in quantum theory into account [see Eq. (1)], the condition of the equality in Eq. (7) means the existence of POVM $\{M_x\}_{x=1}^N$ and $\{\sigma_x\}_{x=1}^N$ such that, for all $x = 1, \ldots, N$,

$$\sum_x p_x \mathrm{tr}[\rho_x M_x] = 1, \quad \text{or equivalently, } \mathrm{tr}[\sigma_x M_x] = 0. \tag{8}$$

When each state σ_x satisfies the condition in the above with respect to POVM $\{M_x\}_{x=1}^N$, we call it complementary to ρ_x. This defines the relation between ρ_x and σ_x in the ensemble in Eq. (4) for the inequality in Eq. (7) to be saturated.

To summarize what we have shown so far, a general framework for utilizing the no-signaling principle in QSD among $\{q_x, \rho_x\}_{x=1}^N$ is presented, and a general bound is also obtained in Eq. (7). The equality also holds if complementary states $\{\sigma_x\}_{x=1}^N$ exist for given states $\{\rho_x\}_{x=1}^N$ to be discriminated among, i.e., (i) the measurement device does not respond to these states [see Eq. (8) under the assumption of the Born rule], (ii) the identical ensembles in Eq. (4) can be found fulfilling the relation between p_x and q_x in Eq. (6). Once the equality holds, it is also crucial to know if (iii) the bound coincides to the guessing probability of optimal QSD.

In the rest of the Letter, we answer to three questions addressed in the above. Namely, we show that for any optimal QSD, one can find identical ensembles in Eq. (4) fulfilling (i), (ii), and (iii). This leads to the following conclusion.

The guessing probability of optimal QSD can be determined by the no-signaling principle.

To proceed the proof, we consider the optimality condition of the semidefinite programing (SDP) for the guessing probability of optimal QSD. In an SDP, an optimization problem can be written in two forms, called primal and dual, and each one is called feasible when variables satisfying given constraints are not of an empty set [10]. When both problems are feasible, it follows that optimal solutions exist and can be obtained by solving either form of the problem.

There are so-called Karush-Kuhn-Tucker (KKT) conditions which can also decide if an optimal solution exists in an SDP problem. In fact, variables satisfying the KKT conditions give an optimal solution of both primal and dual problems. In summary, optimal solutions can be obtained in either way: (i) solving KKT conditions or (ii) solving either a primal or dual problem when both are feasible. KKT conditions contain more parameters than primal or dual problems, and are therefore considered not to be easier to solve than to do a primal or dual problem.

We now show that the lists (i), (ii), and (iii) correspond to the optimality condition, i.e., the KKT, of the SDP for the guessing probability in optimal QSD.

Proof of the result.—Let us start by formulating the SDP for the guessing probability of optimal QSD among $\{q_x, \rho_x\}_{x=1}^N$ as follows, what we call the primal problem,

$$\max f(\{M_x\}_{x=1}^N) = \sum_x q_x \mathrm{tr}[\rho_x M_x]$$
$$\text{subject to } M_x \geq 0, \qquad \sum_x M_x = I, \tag{9}$$

where POVM $\{M_x\}_{x=1}^N$ are called primal variables. The Lagrangian can be constructed as

$$L(\{M_x\}_{x=1}^N, \{\sigma_x\}_{x=1}^N, K) = f(\{M_x\}_{x=1}^N) - \sum_x \mathrm{tr}[\sigma_x M_x] + \mathrm{tr}\left[K\left(\sum_x M_x - I\right)\right], \tag{10}$$

with non-negative operators $\{\sigma_x\}_{x=1}^N$ and K called dual variables. It is also straightforward to derive the dual problem [10],

$$\min \mathrm{tr}[K]$$
$$\text{subject to } K \geq q_x \rho_x, \quad \forall\ x = 1, \ldots, N. \tag{11}$$

It is clear that primal and dual problems are feasible, and therefore optimal solutions exist and can be found by solving either form of the problem.

The optimal solutions can also be obtained by solving the KKT conditions, which are obtained from the Lagrangian in Eq. (10):

$$\mathrm{tr}[\sigma_x M_x] = 0, \tag{12}$$

and

$$K = q_x \rho_x + \sigma_x, \quad \forall\ x = 1, \ldots, N, \tag{13}$$

and the constraints in Eqs. (9) and (11). Note that the existence of optimal solutions is already guaranteed by the fact that both the primal and the dual problems are feasible.

We are now ready to show that, when the equality in Eq. (7) is saturated, the guessing probability corresponds to that of optimal QSD. First, the condition in Eq. (12) called complementary slackness means that each optimal M_x is orthogonal to dual variable σ_x. The existence of states $\{\sigma_x\}_{x=1}^N$ that satisfy the condition in Eq. (8) is therefore shown. Second, the condition in Eq. (13) assures the existence of an identical ensemble that can be decomposed N different ways such that each decomposition consists of one of states $\{\rho_x\}_{x=1}^N$ and its corresponding complementary state σ_x, as it is shown in Eq. (4). After the normalization $\tilde{K} = K/\mathrm{tr}[K]$, the identical ensembles $\tilde{K}$ can be explicitly seen,

$$\tilde{K} = \frac{q_x}{\mathrm{tr}[K]}\rho_x + \frac{1}{\mathrm{tr}[K]}\sigma_x, \quad \forall\ x = 1, \ldots, N. \tag{14}$$

Hence, the existence of an identical ensemble in Eq. (4) together with complementary states $\{\sigma_x\}_{x=1}^N$ is shown. Finally, the reader is reminded that the solution of the dual problem in Eq. (11) is given by $\mathrm{tr}[K]$. The ensemble in Eq. (14) has the state ρ_x with probability $q_x/\mathrm{tr}[K]$, which corresponds to p_x in Eq. (4). From the normalization $\sum_x q_x = 1$, it follows that $\mathrm{tr}[K] = 1/\sum_x p_x$, which coincides to the upper bound in Eq. (7) obtained by the no-signaling constraint. Therefore, the bound in Eq. (7) is shown to be indeed the guessing probability in optimal QSD. ■

A general bound to the guessing probability can be derived using the condition of the identical ensemble in Eq. (4): for all x, y,

$$\| p_x\rho_x - p_y\rho_y \| = \| (1-p_x)\sigma_x - (1-p_y)\sigma_y \|. \tag{15}$$

From this, one can compute the quantity, $\sum_x p_x$, in Eq. (7). Here, we derive a very general bound from the fact that in Eq. (15) the right-hand side is not larger than $2 - (p_x + p_y)$, and the left-hand side is equal to $(\sum_z p_z) \| q_x\rho_x - q_y\rho_y \|$. As a result, we have

$$P_{\mathrm{guess}} \geq \frac{1}{N}\left(1 + \frac{1}{2}\sum_{x=1}^{N} \| q_x\rho_x - q_{x+1}\rho_{x+1} \|\right),$$

where $p_{N+1} = p_1$ and $\rho_{N+1} = \rho_1$. Although this bound is in general not tight, in particular, when N exceeds to the dimension of the Hilbert space supporting quantum states $\{\rho_x\}_{x=1}^N$, the usefulness of this bound is especially worthy of notice as no assumption is made on both the structure among given quantum states and the *a priori* probabilities. For two-state discrimination, this bound actually coincides to the optimal one, Helstrom bound in Eq. (2).

To summarize, we have provided a general framework of utilizing the no-signaling principle in QSD problems. It is shown that the guessing probability in optimal QSD can be determined by the no-signaling principle; i.e., the no-signaling constraint is the physical principle that dictates the optimal performance in QSD. We also highlight the methodology employed, that the no-signaling principle is related to the optimality condition (i.e., KKT) of the SDP problem for QSD. This may envisage a usefulness of the SDP in quantum optimization problems as a method of characterizing physical principles that dictate optimal quantum performances. In this way, the guessing probability is obtained without resort to the measurement postulate via the Born rule, as follows.

Recall the list, (a), (b), and (c), assumed when deriving the guessing probability (with the equality) in Eq. (7). Note that the measurement postulate on Bob's quantum states is not assumed. Probabilities saturating the equality in Eq. (7) are actually obtained by imposing the no-signaling constraint to Bob's probabilities. Then, from SDP it is shown that there always exist POVMs that attain Bob's probabilities from his states via the Born rule. This shows that Gleason's theorem for any set of quantum states $\{q_x, \rho_x\}_{x=1}^N$ is derived from the three assumptions. This is in fact the converse of the recent result on the bipartite Gleason correlations [11,12]: any nonsignaling correlations between two systems for which local quantum measurements are possible can also be obtained by measurement on some bipartite quantum states. It would be interesting to derive a general proof of the converse: by assuming bipartite quantum states, local quantum measurement on Alice, and the no-signaling constraint between two parties, can Gleason's theorem for Bob's local quantum mechanics be derived?

The guessing probability is connected to the min-entropy, through which the max-entropy quantifying the so-called decoupling approach is also related [13]. Recently, the connection of the guessing probability to quantum nonlocality is shown via the no-signaling principle [14]. It would be interesting to investigate further operational relations between these entropic quantities and fundamental principles in physics.

This work is supported by the National Research Foundation of Korea (2010-0007208 and KRF-2008-313-C00185) and Woosuk University. J. B. also thanks the Institut Mittag-Leffler (Djursholm, Sweden) for the support during his visit.

*bae.joonwoo@gmail.com

[1] For instance, some of the nonsignaling correlations that are not allowed in quantum mechanics can be excluded by the information causality [2], e.g., J. Allcock *et al.*, Phys. Rev. A **80**, 040103(R) (2009).

[2] M. Pawlowski *et al.*, Nature (London) **461**, 1101 (2009).

[3] N. Gisin, Phys. Lett. A **242**, 1 (1998).

[4] W.-Y. Hwang, Phys. Rev. A **71**, 062315 (2005); W.-Y. Hwang and J. Bae, J. Math. Phys. (N.Y.) **51**, 022202 (2010).

[5] C. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[6] Ll. Masanes, A. Acín, and N. Gisin, Phys. Rev. A **73**, 012112 (2006); J. Barrett, Phys. Rev. A **75**, 032304 (2007).

[7] A. Gleason, J. Math. Mech. **6**, 885 (1957).

[8] Y. C. Eldar and G. D. Forney, IEEE Trans. Inf. Theory **47**, 858 (2001).

[9] N. Gisin, Helv. Phys. Acta **62**, 363 (1989); L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).

[10] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, U.K., 2004).

[11] H. Barnum *et al.*, Phys. Rev. Lett. **104**, 140401 (2010).

[12] A. Acín *et al.*, Phys. Rev. Lett. **104**, 140404 (2010).

[13] R. Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 9 (2009).

[14] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).