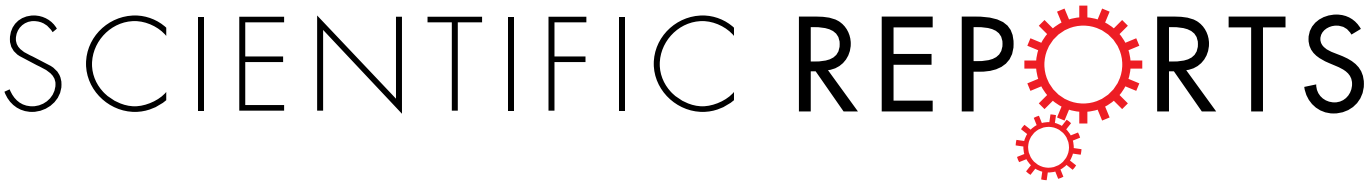

OPEN

Analysis of Optimal Sequential State Discrimination for Linearly Independent Pure Quantum States

Received: 11 December 2017
Accepted: 19 March 2018
Published online: 25 April 2018

Min Namkung & Younghun Kwon

Recently, J. A. Bergou *et al*. proposed sequential state discrimination as a new quantum state discrimination scheme. In the scheme, by the successful sequential discrimination of a qubit state, receivers Bob and Charlie can share the information of the qubit prepared by a sender Alice. A merit of the scheme is that a quantum channel is established between Bob and Charlie, but a classical communication is not allowed. In this report, we present a method for extending the original sequential state discrimination of two qubit states to a scheme of *N* linearly independent pure quantum states. Specifically, we obtain the conditions for the sequential state discrimination of $N=3$ pure quantum states. We can analytically provide conditions when there is a special symmetry among $N=3$ linearly independent pure quantum states. Additionally, we show that the scenario proposed in this study can be applied to quantum key distribution. Furthermore, we show that the sequential state discrimination of three qutrit states performs better than the strategy of probabilistic quantum cloning.

Quantum state discrimination is one of the main research topics in quantum information processing. The information used in quantum communication or quantum computing is encoded by quantum states. Naturally, this requires quantum state discrimination. In quantum state discrimination, a sender Alice prepares a quantum state with a prior probability and sends it to a receiver Bob. Bob, knowing the prior probability, performs a measurement to discriminate the quantum state of Alice. When Alice's quantum states are orthogonal to each other, Bob can always discriminate Alice's quantum states. However, Alice's quantum states are usually not orthogonal. Therefore, Bob cannot perfectly discriminate these quantum states[1]. The result of Bob's measurement can be divided into two cases:conclusive results and inconclusive results. When Bob obtains an inconclusive result, he cannot find any information about Alice's quantum state. When Bob's measurement result is conclusive, Bob can obtain information about Alice's quantum state. Minimum error discrimination(ME)[1–5] is the strategy for discriminating quantum states with measurements, which always provide conclusive results with a minimum error. When the probability of incorrect guessing becomes zero, a strategy called unambiguous discrimination(UD) is used. Therefore, in the unambiguous discrimination(UD)[6–9], measurements are designed to provide conclusive results which are always correct, and inconclusive result which is minimized. UD can be applied only when Alice's quantum states are either linearly independent pure states[10] or mixed quantum states whose support space does not completely overlap[11]. Other strategies for quantum state discrimination employ maximal confidence(MC)[12], error margin(EM) methods[13–16], and fixed rate of inconclusive result(FRIR) methods[17–20].

Recently, Bergou *et al*.[21] proposed *sequential state discrimination(SSD)*, a new strategy for quantum state discrimination, that contains multi-receivers. Suppose that the receivers are Bob and Charlie. The receivers knows the prior probability of quantum states, prepared by Alice. In this strategy, Bob discriminates Alice's quantum state using nonoptimal unambiguous discrimination. When Bob obtain a conclusive result, he sends his post-measurement state to Charlie. Charlie performs an optimal unambiguous discrimination on Bob's post-measurement state. In this strategy, there is no classical communication between Bob and Charlie. If Bob and Charlie can successfully discriminate Alice's quantum state, every party can share the information of Alice's quantum state. In fact, sequential state discrimination strategy originates from the question of "Can one obtain the information of original quantum sate by performing a measurement on the post-measurement state?"[22]. The optimal success probability of sequential state discrimination for two pure qubits with identical prior probabilities was analytically provided by Bergou *et al*.[21,23], which was shown in experiment[24]. A solution to sequential state

Department of Applied Physics, Hanyang University, Ansan, Kyounggi-Do, 425-791, South Korea. Correspondence and requests for materials should be addressed to M.N. (email: mslab.nk@gmail.com) or Y.K. (email: yyhkwon@hanyang.ac.kr)

discrimination for two pure qubits with arbitrary prior probabilities was suggested by Zhang *et al.*[25]. Hillery *et al.*[26] proposed sequential state discrimination for a symmetric $N-$qudit, which can be obtained by embedding qubits into an extra Hilbert space. In addition, the authors of present report provided the sequential state discrimination for mixed qubit states[27].

In this report, we investigate the structure of sequential state discrimination for N pure qudit states. When N pure states are linearly independent, a Gram matrix composed of pure states is positive-definite, which implies the existence of the inverse of the Gram matrix[28]. From the Gram matrix, the POVM of Bob and Charlie for unambiguous discrimination may be found[29,30]. In general, the POVM is composed of $N+1$ complex positive D-dimensional matrices. However, in this report, we will let the POVM correspond to a vector composed of N real numbers. The detailed procedure will be explained in the formulation of problem. The POVM set, used in unambiguous discrimination, is convex[30], and the set of real vectors corresponding to it is convex. When $N=2$, the convex set can be easily understood. However, when $N \geq 3$, the convex set has not been investigated.

In this report, we study the structure of the convex set of linearly independent N pure states for sequential state discrimination, mainly dealing with the convex set of $N=3$[31–33]. Because Bob performs an nonoptimal unambiguous discrimination, the real vector corresponding to Bob's POVM exists inside the convex set. However, Charlie performs the optimal unambiguous discrimination, and the real vector corresponding to Charlie's POVM exists on the surface of the convex set. Charlie's convex set depends on Bob's POVM. When Bob uses an optimal unambiguous discrimination, the Charlie's convex set element is only a zero vector. Meanwhile, when Bob performs a nonoptimal unambiguous discrimination, the Charlie's convex set contains other elements, except for the zero vector. This implies that Charlie can obtain some information from the post-measurement states of Bob.

Results

Now, let us propose a sequential state discrimination for N linearly independent pure quantum states. Up to now, the solution to sequential state discrimination for two linearly independent pure qubit states is known, which is the result of Bergou *et al.*[21,25]. Therefore, we need to formulate the sequential state discrimination for N linearly independent pure quantum states, which can be considered as a optimization problem based on the conditions of POVM of receivers Bob and Charlie. Then, we obtain a solution for the cases of $N=3$ linearly independent quantum states with arbitrary prior probabilities. In addition, we compare our strategy with probabilistic quantum cloning strategy. We find that sequential state discrimination for $N=3$ linearly independent quantum states performs better than the strategy of probabilistic quantum cloning. Finally, we show that our proposal can be used for quantum key distribution.

Scenario of Sequential State Discrimination. Let us explain a sequential state discrimination scenario of N linearly independent pure quantum states. A sender Alice prepares a quantum state $|\psi_i\rangle$ with a prior probability q_i, out of a set of N linearly independent pure quantum states $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}$. Then, she sends this quantum state to Bob. Bob discriminates Alice's quantum state, using POVM $\{M_0, M_1, \ldots, M_N\}$. Here, $M_i (i \neq 0)$ is an element corresponding to conclusive result $i \in \{1, \ldots, N\}$ and M_0 is an element corresponding to inconclusive result $i=0$. If Bob obtains $i \in \{1, \ldots, N\}$ as a measurement result, he sends his post-measurement state $|\psi'_i\rangle$ to Charlie. Then, Charlie performs POVM $\{M'_0, M'_1, \cdots, M'_N\}$ on Bob's post-measurement state, to determine the post-measurement state of Bob. Likewise, Charlie's $M'_i (i \neq 0)$ corresponds to conclusive result $i \in \{1, \ldots, N\}$ and M'_0 corresponds to inconclusive result $i=0$. Receivers Bob and Charlie should obey the following rules.

Rule 1. Bob discriminates Alice's quantum state using a nonoptimal unambiguous discrimination strategy. However, using an optimal unambiguous discrimination strategy, Charlie mesures Bob's post-measurement state.
Rule 2. Classical communication is not allowed between Bob and Charlie. Therefore, the only way for Charlie to obtain information about Alice's quantum state is to measure Bob's post-measurement state.

Therefore, the probability that Bob and Charlie successfully share Alice's quantum state is given by

$$P_s^{(B,C)} = \sum_{i=1}^{N} q_i \langle\psi_i|M_i|\psi_i\rangle \langle\psi'_i|M'_i|\psi'_i\rangle. \tag{1}$$

The important problem in sequential state discrimination is in finding the POVM condition of Bob and Charlie, for optimizing the success probability of Eq. (1). If the optimal value of (1) is not zero, Bob and Charlie have a chance of successfully sharing Alice's quantum state. When Alice prepares a qubit state out of two pure qubit states, the success probability is proven to be nonzero[21,23–25]. To date, researchers have considered the optimal success probability only for two qubit states. In this report, proposing the sequential state discrimination for N linearly independent pure quantum states, we provide a method for finding the optimized success probability condition.

Formulation of Optimization Problem. Now, let us describe how to formulate an optimization problem for the sequential state discrimination of N linearly independent pure quantum states. The conditions for Bob to discriminate Alice's quantum state without error are (B1) $M_i \geq 0 (\forall i \in \{0, \ldots, N\})$, (B2) $M_0 + M_1 + \ldots + M_N = I$, (B3) $\langle\psi_j|M_i|\psi_j\rangle = 0 (\ \forall\ i \neq j)$. Let us assume that $G = \{\langle\psi_i|\psi_j\rangle\}_{i,j=1}^{N}$ is a Gram matrix made by Alice's pure states. When Alice's pure states are linearly independent, $G > 0 (\leftrightarrow \exists G^{-1})$[28] is satisfied. Therefore, the POVM that can discriminate every Alice's pure state without error can be described by[30],

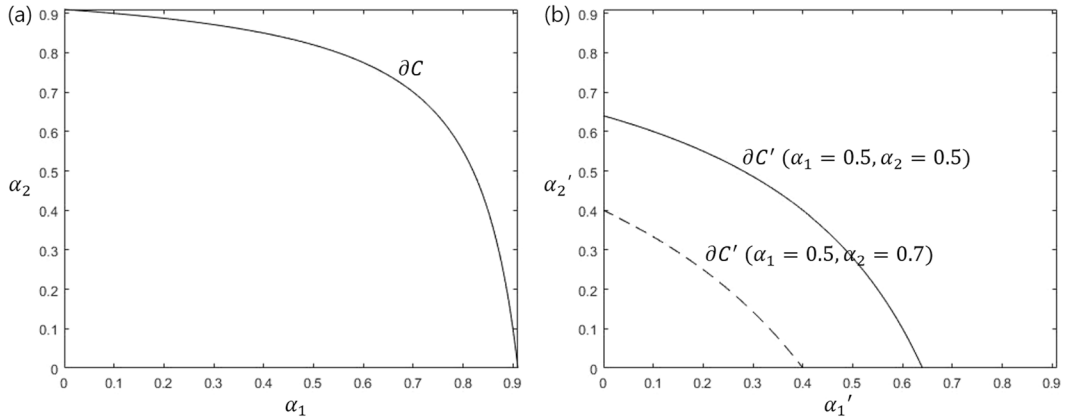

Figure 1. In sequential state discrimination of two pure qubits, the convex sets of Bob and Charlie, C and C'. (**a**) shows the Bob's convex set C when the overlap between two pure qubits is $s = 0.3$. In (**b**), solid(dashed) line displays the boundary $\partial C'$ of Charlie's convex set when $(\alpha_1, \alpha_2) = (0.5, 0.5)((\alpha_1, \alpha_2) = (0.5, 0.7))$.

$$M_i = \alpha_i |\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i|, \ |\widetilde{\psi}_i\rangle = \sum_{j=1}^{N} G_{ji}^{-1} |\psi_j\rangle. \tag{2}$$

where $0 \leq \alpha_i \leq 1$, $i \in \{1, \ldots, N\}$. If $M_0 = I - (M_1 + M_2 + \ldots + M_N)$ is non-negative, (B1) and (B2) also hold. Eq. (2) implies that Bob's POVM can correspond to a real vector $(\alpha_1, \alpha_2, \ldots, \alpha_N)$ in $N-$dimensional vector space. Additionally, Bob's POVM set is convex[30]. The convex set is denoted as $C \subset \mathbb{R}^N$. The conditions under which M_0 is positive-semidefinite are equivalent to $\langle\psi|M_0|\psi\rangle \geq 0$ for an N dimensional vector $|\psi\rangle$[28]. Because $|\psi\rangle$ can be obtained from a linear combination of $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$, C is an N dimensional real vector space where $\widetilde{G} = \{\langle\psi_i|M_0|\psi_j\rangle\}_{i,j=1}^N$ is non-negative. Every component of real vector α_i, which is an element of C, is non-negative. Then, we have the following conjecture about C:

Conjecture 1. *C, being the set of N dimensional real vectors, is a convex set composed of $N + 1$ vertices. The edges of convex set C contain N segments satisfying $\alpha_i = 0$.*

In Conjecture 1, convex set C contains a line segment $\alpha_i = 0$, since there exists a case where Bob discriminates unambiguously remaining quantum states except i-th pure state. For $N = 3$, the geometric argument can be found in refs[31–33]. Let us assume that Bob's set of post-measurement states, which corresponds to conclusive result of Bob, is $\{|\psi'_1\rangle, \cdots, |\psi'_N\rangle\}$. When Bob discriminates Alice's quantum state using a nonoptimal unambiguous discrimination, information remains in Bob's post measurement state, which can be obtained by Charlie. Additionally, Bob's post-measurement states are linearly independent, which implies that Charlie's POVM can discriminate Bob's post-measurement state without error. The conditions for Charlie's POVM, which can discriminates the Bob's post-measurement state without error, are (C1) $M'_i \geq 0 (\forall i \in \{0, \cdots, N\})$, (C2) $M'_1 + M'_2 + \cdots + M'_N = I$, (C3) $\langle\psi'_j|M'_i|\psi'_j\rangle = 0 (\forall i \neq j)$. When Bob's post-measurement states are linearly independent, if their Gram matrix is $G' = \{\langle\psi'_i|\psi'_j\rangle\}_{i,j=1}^N$, we have $G' > 0 (\leftrightarrow \exists G'^{-1})$. Then, Charlie's POVM becomes

$$M'_i = \alpha'_i |\widetilde{\psi}'_i\rangle\langle\widetilde{\psi}'_i|, \ |\widetilde{\psi}'_i\rangle = \sum_{j=1}^{N} G'^{-1}_{ji} |\psi'_j\rangle. \tag{3}$$

where $0 \leq \alpha_{i'} \leq 1$, $i \in \{1, \ldots, N\}$. If $M'_0 = I - (M'_1 + M'_2 + \cdots + M'_N)$ is non-negative, (C1) and (C2) also hold. Then, Charlie's POVM corresponds to the N dimensional real vector $(\alpha'_1, \alpha'_2, \cdots, \alpha'_N)$. Let the set of the real vectors be $C' \subset \mathbb{R}^N$. Like in the case of Bob, C' is the set of N dimensional real vectors, where $\widetilde{G}' = \{\langle\psi'_i|M'_0|\psi'_j\rangle\}_{i,j=1}^N$ is non-negative. The set is convex and depends on Bob's POVM. Then, we have the following Conjecture about C'.

Conjecture 2. *When Bob performs an nonoptimal unambiguous discrimination, C' has a non-zero element. C' depends on Bob's POVM and is composed of $N + 1$ vertices. The edges of C' contain N segments fulfilling $\alpha'_i = 0$.*

In Conjecture 2, the fact that convex set C' contains a line segment of $\alpha'_i = 0$ means that there exists a case where Charlie discriminates unambiguously remaining quantum states except i-th state. It can be shown from Figs 1 and 2 that Conjecture 2 is satisfied when $N = 2, 3$. In the following section, we will explain how Bob's POVM affects C'. In sequential state discrimination, Bob performs a nonoptimal unambiguous discrimination, and $(\alpha_1, \ldots, \alpha_N)$ belongs to the interior of C, int(C). Meanwhile, Charlie performs an optimal unambiguous discrimination, and a vector $(\alpha'_1, \cdots, \alpha'_N) (\forall \alpha'_i \neq 0)$ is located in the boundary of C', $\partial C'$. Therefore, the sequential state discrimination problem is equivalent to the following optimization problem.

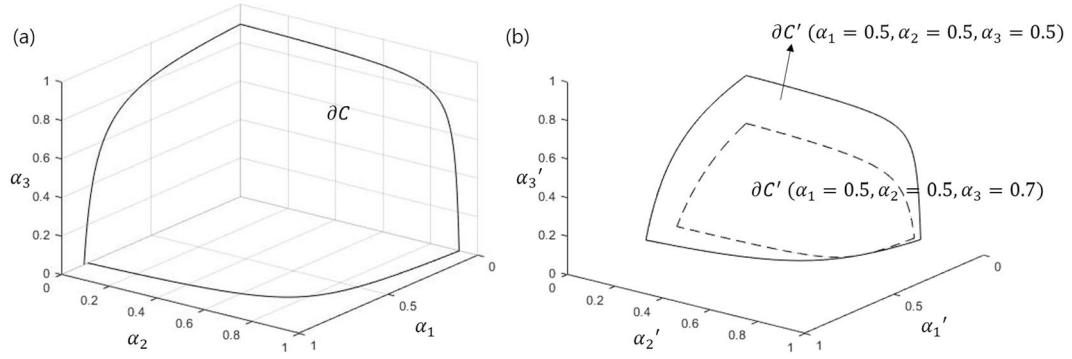

Figure 2. Two set C and $\partial C'$ that contain the real vectors $(\alpha_1, \alpha_2, \alpha_3)$ and $(\alpha'_1, \alpha'_2, \alpha'_3)$ corresponding to the POVM of Bob and Charlie. Here, $\partial C'$ is a surface of the convex set C'. Here, we assume that the overlap among three pure qutrits are $s_1 = 0.2$, $s_2 = 0.3$, and $s_3 = 0.25$. In (**a**), it displays the Bob's convex set C. In (**b**), solid line(dashed line) shows the boundary of Charlie's convex set C' when $\alpha_1 = \alpha_2 = \alpha_3 = 0.5$ ($\alpha_1 = \alpha_2 = 0.5$, $\alpha_3 = 0.7$)

$$\begin{aligned} &\text{maximize} \quad P_s^{(B,C)} \\ &\text{subjectto} \quad (\alpha_1, \alpha_2, \cdots, \alpha_N) \in \text{int}\,(C), \\ &\qquad\qquad (\alpha'_1, \alpha'_2, \cdots, \alpha'_N) \in \partial C'. \end{aligned} \tag{4}$$

$\partial C'$ relies on $(\alpha_1, \alpha_2, \ldots, \alpha_N)$. Now, we prove that Conjecture 1 and Conjecture 2 hold in cases of $N = 2$ and $N = 3$. And we investigate the optimization problems of Eq. (4) when $N = 2$ and $N = 3$. We expect that our approach can be extended to a case where $N > 3$.

Examples: sequential state discrimination for two or three pure states. Suppose that Alice prepares a quantum state out of two(or three) pure quantum states[6–9,31–33].

Two pure states(Qubits). Assume that with a prior probability q_i, Alice prepares a qubit state out of two pure qubit states $|\psi_i\rangle \in \{|\psi_1\rangle, |\psi_2\rangle\}$ and sends it to Bob. The overlap between two qubit states is $\langle\psi_1|\psi_2\rangle = s\exp(i\phi)$, $s \geq 0$. When $s \in [0, 1)$, there exists the inverse of the Gram matrix G for Alice's quantum states. This implies the existence of Bob's POVM discriminating Alice's qubit state without error. Bob's POVM can be represented by a two-dimensional real vector (α_1, α_2). $(\alpha_1, \alpha_2) \in C$, satisfying the conditions of Bob's POVM (B1), (B2), (B3), fulfills the following inequality:

$$(1 - \alpha_1)(1 - \alpha_2) - s^2 \geq 0. \tag{5}$$

The inequality is obtained by the non-negativity condition of $\widetilde{G} = \{\langle\psi_i|M_0|\psi_j\rangle\}_{i,j=1}^2$. Eq. (5) indicates that C is a convex set. One can show that the set C of (α_1, α_2) fulfilling Eq. (5) is convex, in the following way. The strict equality $\alpha_2 = f(\alpha_1)(f(x) \equiv 1 + s^2(x-1)^{-1})$ of Eq. (5) is monotonic decreasing as α_1 varies from 0 to $1-s^2$. In addition, $f''(\alpha_1)$ of strict equality is negative-definite. Therefore, C surrounded by strict equality of Eq. (5) and $\alpha_1 = 0$, $\alpha_2 = 0$ is convex. Figure 1(a) displays the structure of C when the overlap s between two pure qubits, prepared by Alice is 0.3, which shows that C is convex. Because of the fact that in sequential state discrimination the post-measurement states of Bob should be considered, we need to find the Kraus operator K_i that corresponds to M_i. When $i = 1,2$, from singular value decomposition[34], we have $K_i = \sqrt{\alpha_i}|\psi'_i\rangle\langle\widetilde{\psi}_i|$, where $|\widetilde{\psi}_i\rangle = \sum_{j=1}^2 G_{ji}^{-1}|\psi_j\rangle$ and $|\psi'_i\rangle$ is one of Bob's post-measurement state. (It is not a general form of the Kraus operator[35]. However, because Charlie performs unambiguous discrimination, it is sufficient to consider a special type of Kraus operator.). Now, let us find the Kraus operator K_0 corresponding to M_0. K_0 can be thought of as a linear map that sends two of Alice's qubit states to linear independent states $|\psi'_1\rangle$ and $\psi'_2\rangle$,

$$K_0 = \sqrt{\gamma_1}|\psi'_1\rangle\langle\widetilde{\psi}_1| + \sqrt{\gamma_2}|\psi'_2\rangle\langle\widetilde{\psi}_2|. \tag{6}$$

where $\gamma_1, \gamma_2 \geq 0$. The condition of $M_0 = K_0^\dagger K_0$ can be understood in terms of $\langle\psi_i|M_0\rangle|\psi_j\rangle = \langle\psi_i|K_0^\dagger K_0|\psi_j\rangle(\forall i, j)$, which gives $s' = s/\sqrt{(1-\alpha_1)(1-\alpha_2)}$ $(s' = |\langle\psi'_1|\psi'_2\rangle|)$. When Bob performs an optimal unambiguous discrimination, s' becomes one($s' = 1$). This means that Charlie cannot discriminate Bob's post-measurement states. Therefore, Bob should use a nonoptimal unambiguous discrimination. Then, the Gram matrix G' of Bob's post-measurement states has its inverse. Charlie's POVM, which can discriminate Bob's post-measurement states without error, corresponds to a two-dimensional real vector (α'_1, α'_2). The condition for $(\alpha'_1, \alpha'_2) \in C'$ is given by

$$(1 - \alpha'_1)(1 - \alpha'_2) - s'^2 \geq 0. \tag{7}$$

This tells us that C' is a convex set and depends on C. In Eq. (7), s' is a function of (α_1, α_2), being not a function of (α'_1, α'_2). One can show that the set C' of (α'_1, α'_2) satisfying Eq. (7) is convex, in similar fashion of C. The fact that Bob

can obtain an information from Alice's quantum state implies that the success probability α_i is non-zero. From the relation between s' and s for non-zero α_i, we find a strict inequality $s' > s$. As s increases, $f(x)$ decreases and the size of C' is smaller than that of C. From Fig. 1(b), one can see that C' is convex and the size of C' is smaller than that of C. Here, solid line(dashed line) displays $\partial C'$ when $(\alpha_1, \alpha_2) = (0.5, 0.5)((\alpha_1, \alpha_2) = (0.5, 0.7))$. As (α_1, α_2) approaches to ∂C, the size of C' decreases, implying the trade-off phenomena which tells that more information Bob obtains from Alice's pure states, less information Charlie gets. Therefore, we show that Conjecture 1 and 2 hold. Eqs (5) and (7) are the constraints of optimization problem (4). Because Bob(Charlie) uses a nonoptimal(optimal) unambiguous discrimination, Eqs (5) and (7) becomes a strict inequality(strict equality). If Bob does not optimally discriminate Alice's pure qubit, (α_1, α_2) exists in the interior of C. Therefore, (α_1, α_2) satisfies the strict inequality of Eq. (5)[27]. In the similar way, if Charlie optimally discriminate the post-measurement state of Bob, (α'_1, α'_2) exists on $\partial C'$. Therefore, (α'_1, α'_2) satisfies the strict equality of Eq. (7)[27]. Then, Eq. (4) becomes the following optimization problem;

$$\begin{aligned} \text{maximize} \quad & P_s^{(B,C)} = q_1\alpha_1\alpha'_1 + q_2\alpha_2\alpha'_2 \\ \text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) - s^2 > 0, \\ & (1-\alpha'_1)(1-\alpha'_2) - s'^2 = 0. \end{aligned} \tag{8}$$

If (α'_1, α'_2) are $\alpha'_1, \alpha'_2 > 0$, the best strategy for Charlie is to discriminate two of Bob's post-measurement states. This implies that the best strategy for Bob and Charlie is to discriminate every of the two pure quantum state. In this case, the sequential discrimination scenario for Bob and Charlie is summarized as Theorem 1.

Theorem 1. *Suppose that with a prior probability q_i, Alice prepares a pure state $|\psi_i\rangle$ out of $\{|\psi_1\rangle, |\psi_2\rangle\}$ satisfying $\langle\psi_1|\psi_2\rangle = s\exp(i\phi)$, $s \geq 0$. The sequential state discrimination problem in which Bob and Charlie discriminate two pure states is equivalent to the following optimization problem*:

$$\begin{aligned} \text{maximize} \quad & P_s^{(B,C)} = q_1\alpha_1 + q_2\alpha_2 - 2s\sqrt{\frac{q_1q_2\alpha_1\alpha_2}{(1-\alpha_1)(1-\alpha_2)}} \\ \text{subject to} \quad & \alpha_2 < \frac{\alpha_1(1-\alpha_1)}{x+\alpha_1(1-\alpha_1)}, \quad \alpha_1 < \frac{\alpha_2(1-\alpha_2)}{y+\alpha_2(1-\alpha_2)}, \quad x = s^2\frac{q_2}{q_1}, \quad y = s^2\frac{q_1}{q_2}. \end{aligned} \tag{9}$$

The proof of Theorem. 1 is shown in the Methods.

Equation (9) is a nonlinear optimization problem and is a difficult to solve analytically. In special cases, the optimization problem can be solved analytically. Because the object function is continuous, when (α_1, α_2) is an optimization point, the gradient of the object function becomes zero. Therefore, the following equations hold at the optimization point:

$$\begin{aligned} \alpha_2 &= \frac{\alpha_1(1-\alpha_1)^3}{x+\alpha_1(1-\alpha_1)^3}, \quad x = s^2\frac{q_2}{q_1}, \\ \alpha_1 &= \frac{\alpha_2(1-\alpha_2)^3}{y+\alpha_2(1-\alpha_2)^3}, \quad y = s^2\frac{q_1}{q_2}. \end{aligned} \tag{10}$$

The inverse does not generally hold. However, when two prior probabilities are equal, two equations have an inverse function relationship. Then, the optimization condition becomes $\alpha_1 = \alpha_2 = 1 - \sqrt{s}$, and the optimized success probability is $\max P_s^{(B,C)} = (1-\sqrt{s})^2$, which agrees with the result of ref.[21]. The solution of Eq. (9), $(\alpha_1, \alpha_2) = (1-\sqrt{s}, 1-\sqrt{s})$ is located in the interior of C. And the condition of Charlie for providing optimal success probability, $(\alpha'_1, \alpha'_2) = (1-\sqrt{s}, 1-\sqrt{s})$ exists on $\partial C'$. The fact that optimal condition for sequential state discrimination is $\alpha_i = \alpha'_i = 1 - \sqrt{s}$ implies that with the same probability, Bob and Charlie, without error, discriminate i-th pure qubit, with supports the result of ref.[21].

If two prior probabilities are not equal, it is difficult to analytically prove the argument of ref.[21]. However, it can be shown numerically[36,37]. For example, in the case of $q_1 = 0.55$, $q_2 = 0.45$, and $s = 0.12$, one can numerically find $(\alpha_1, \alpha_2) = (0.721987, 0.568364)$, which is the solution of Eq. (10). Then, by Eq. (26) of Method, one can obtain (α'_1, α'_2), which is the same as (α_1, α_2). It should be noted that $(\alpha'_1, \alpha'_2) = (0.721987, 0.568364)$ is located on $\partial C'$. In fact, the reason that the success probability of Bob and Charlie is the same is that even though Bob performs a nonoptimal unambigous discrimimination, Charlie should optimally discriminate Bob's post measurement state.

Let us assume that $\alpha'_2 = 0$. Then, Charlie discriminates only $|\psi'_1\rangle|$ without error. In this case, $\alpha'_1 = 1 - s'^2$ is obtained. Likewise, Bob also discriminates only ψ_1, which is the best strategy $(\alpha_2 = 0)$ for Bob and Charlie. Therefore, the problem of sequential state discrimination is equivalent to the following optimization problem:

$$\text{maximize} \quad P_s^{(B,C)} = q_1\alpha_1\left\{1 - \frac{s^2}{1-\alpha_1}\right\} \tag{11}$$

The optimized condition is $\alpha_1 = 1 - s$. Then, one has $\max P_s^{(B,C)} = q_1(1-s)^2$. When Bob and Charlie discriminate only $|\psi_2\rangle$(i.e., $\alpha_1 = \alpha'_1 = 0$), the optimized condition becomes $\alpha_2 = 1 - s$. Additionally, one has $\max P_s^{(B,C)} = q_2(1-s)^2$. Therefore, the optimized success probability that in sequential state discrimination Bob and Charlie discriminate only one of Alice's two pure qubit states, becomes $\max\{q_1(1-s^2), q_2(1-s^2)\}$. The case of $q_1 = q_2$ contains the result of Pang *et al.*[23].

If general prior probabilities $q_1 \neq q_2$ are considered, one must numerically find (α_1, α_2) satisfying Eq. (10). In this report, a random search method[36] based on Monte Carlo methods is used. By these methods, one can search almost entire (α_1, α_2), fulfilling the constraint of Eq. (9).

When Bob can obtain a partial information on Alice's qubit, since the overlap between Bob's post measurement states should be increased, s' is always greater than s. Therefore, the size of convex set C' is smaller than that of C. When Bob performs an optimal unambiguous discrimination, because of $s' = 1$, the element of C' is only a zero vector. This implies that Charlie cannot obtain any information from Bob's post-measurement state.

Three pure states(Qutrits). Now let us consider the case of three pure qutrit states. With a prior probability q_i, Alice prepares an element $|\psi_i\rangle$ out of a set of qutrits $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ and sends it to Bob. The overlap between those qutrit states is given by $\langle\psi_i|\psi_j\rangle = s_k \exp(i\varepsilon_{ijk}\phi_k)$, $s_k \geq 0$, where ε_{ijk} is the Levi-Civita symbol. Let the sub-matrices of $\widetilde{G} = \{\langle\psi_i|M_0|\psi_j\rangle\}_{i,j=1}^3$ be $\widetilde{G}_1$, $\widetilde{G}_2$, $\widetilde{G}_3$. When $\det \widetilde{G} \geq 0$, $\widetilde{G}_k \geq 0$, $\langle\psi_k|M_0|\psi_k\rangle \geq 0$, $\widetilde{G}$ is positive-semidefinite[32,33]. This condition indicates that three dimensional real vector $(\alpha_1, \alpha_2, \alpha_3) \in C$ corresponding to Bob's POVM satisfies the following relationship:

$$\begin{aligned} &\overline{\alpha}_1\overline{\alpha}_2\overline{\alpha}_3 - s_1^2\overline{\alpha}_1 - s_2^2\overline{\alpha}_2 - s_3^2\overline{\alpha}_3 + 2s_1s_2s_3\cos\Phi \geq 0, \\ &\overline{\alpha}_i\overline{\alpha}_j - s_k^2 \geq 0. \quad \forall\, i \neq j \neq k. \end{aligned} \tag{12}$$

Here, $\overline{\alpha}_i = 1 - \alpha_i$ and $\Phi = \phi_1 + \phi_2 + \phi_3$ are refered to as a geometric phase[32]. The set of $(\alpha_1, \alpha_2, \alpha_3)$ satisfying Eq. (12) is convex. Let us obtain Kraus operator K_i, corresponding to Bob's POVM. If $i = 1, 2, 3$, the necessary and sufficient condition for $M_i = K_i^\dagger K_i$ is $K_i = \alpha_i|\psi'_i\rangle\langle\widetilde{\psi}_i|$, where $|\widetilde{\psi}_i\rangle = \sum_{j=1}^3 G_{ji}^{-1}|\psi_j\rangle$ and $|\psi'_i\rangle$ is a Bob's post-measurement state. For $i = 0$, let us assume the Kraus operator as follows:

$$K_0 = \sqrt{\gamma_1}|\psi'_1\rangle\langle\widetilde{\psi}_1| + \sqrt{\gamma_2}|\psi'_2\rangle\langle\widetilde{\psi}_2| + \sqrt{\gamma_3}|\psi'_3\rangle\langle\widetilde{\psi}_3|. \tag{13}$$

Because K_0 is a linear map sending $|\psi_i\rangle$ to $|\psi_{i'}\rangle$, from the condition of $M_0 = K_0^\dagger K_0$ and $\langle\psi_i|M_0|\psi_j\rangle = \langle\psi_i|K_0^\dagger K_0|\psi_j\rangle (\forall i, j)$, $\langle\psi'_i|\psi'_j\rangle = \langle\psi_i|\psi_j\rangle/\sqrt{(1-\alpha_i)(1-\alpha_j)}$ is obtained. Assuming that $\langle\psi'_i|\psi'_j\rangle = s'_k \exp(i\varepsilon_{ijk}\phi'_k)$, one has the relations of $s'_k = s_k/\sqrt{(1-\alpha_i)(1-\alpha_j)}$, $\phi'_k = \phi_k (\forall i \neq j \neq k)$. When $(\alpha_1, \alpha_2, \alpha_3)$ exists in the interior of C, the Gram matrix G', composed of the post-measurement states of Bob, has an inverse matrix. Therefore, there exists Charlie's POVM, discriminating the post-measurement states of Bob without error. Like Bob's POVM, the conditions of Charlie's POVM are given by

$$\begin{aligned} &\overline{\alpha}'_1\overline{\alpha}'_2\overline{\alpha}'_3 - s'^2_1\overline{\alpha}'_1 - s'^2_2\overline{\alpha}'_2 - s'^2_3\overline{\alpha}'_3 + 2s'_1s'_2s'_3\cos\Phi \geq 0, \\ &\overline{\alpha}'_i\overline{\alpha}'_j - s'^2_k \geq 0. \quad \forall i \neq j \neq k. \end{aligned} \tag{14}$$

where $\overline{\alpha}'_i = 1 - \alpha'_i$. The set C' of three-dimensional real vectors satisfying Eq. (14) is convex and depends on Bob's POVM. Therefore, Conjecture 1 and 2 hold in the sequential state discrimination of the three qutrit states. Because Charlie performs an optimal unambiguous discrimination, $(\alpha'_1, \alpha'_2, \alpha'_3)$ exists on the surface of Eq. (14). The sequential state discrimination problem for three qutrit states by Bob and Charlie becomes the following optimization problem:

$$\begin{aligned} \text{maximize} \quad & P_s^{(B,C)} = q_1\alpha_1\alpha'_1 + q_2\alpha_2\alpha'_2 + q_3\alpha_3\alpha'_3 \\ \text{subjectto} \quad & (\alpha_1, \alpha_2, \alpha_3) \in \text{int}\,(C), \\ & (\alpha'_1, \alpha'_2, \alpha'_3) \in \partial C'. \end{aligned} \tag{15}$$

Here, int (C) is a set of $(\alpha_1, \alpha_2, \alpha_3)$ strictly satisfying Eq. (12). $\partial C'$ is a set of $(\alpha_1, \alpha_2, \alpha_3)$ fulfilling $\det \widetilde{G} = 0$ in Eq. (14). The sequential state discrimination of three qutrit states for Bob and Charlie can be categorized by the number of discriminations of qutrit states by Bob and Charlie. (The theorems are proven in the Methods).

Theorem 2. *Alice prepares a element $|\psi_i\rangle$, with a prior probability q_i, from three pure qutrit states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ satisfying $\langle\psi_i|\psi_j\rangle = s_k \exp(i\varepsilon_{ijk}\phi_k)$, $s_k \geq 0$ and sends it to Bob. If in sequential state discrimination, Bob and Charlie discriminate only a single qutrit state (for example, $\alpha_2 = \alpha_3 = 0$, $\alpha'_2 = \alpha'_3 = 0$) out of three qutrit states, the optimal conditions for the sequential state discrimination are $\alpha_i = 1 - \sqrt{\chi_i(\Phi)}$ and $\alpha'_i = 1 - \chi_i(\Phi)$, where $\chi_i(\Phi) = (s_j^2 + s_k^2 - 2\, s_i s_j s_k \cos\Phi)/(1 - s_i^2)$. Then, the optimized success probability becomes $\max P_s^{(B,C)} = \max_i\{q_i (1 - \chi_i(\Phi))\}$.*

Theorem 3. *Suppose that Alice prepares a element $|\psi_i\rangle$, with a prior probability q_i, from three pure qutrit states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ satisfying $\langle\psi_i|\psi_j\rangle = s_k \exp(i\varepsilon_{ijk}\phi_k)$, $s_k \geq 0$ and sends it to Bob. If in sequential state discrimination, Bob and Charlie discriminate only two qutrit states (for example, $\alpha_3 = 0$, $\alpha'_3 = 0$) out of three qutrit states, the solution for the sequential state discrimination is equivalent to that of the following optimization problem:*

$$\begin{aligned}\text{maximize}\quad & P_s^{(B,C)} = q_i\alpha_i\left(1-\frac{s_j^2}{1-\alpha_i}\right)+q_j\alpha_j\left(1-\frac{s_i^2}{1-\alpha_j}\right)\\ & \qquad -2\sqrt{\frac{q_iq_j\alpha_i\alpha_j}{(1-\alpha_i)(1-\alpha_j)}}\,\xi_{ij}(\Phi)\\ \text{subject to}\quad & \alpha_j < \frac{\alpha_i(1-\alpha_i-s_j^2)^2}{\alpha_i(1-\alpha_i-s_j^2)^2+(q_j/q_i)\xi_{ij}^2(\Phi)(1-\alpha_i)},\\ & \alpha_i < \frac{\alpha_j(1-\alpha_j-s_i^2)^2}{\alpha_j(1-\alpha_j-s_i^2)^2+(q_i/q_j)\xi_{ij}^2(\Phi)(1-\alpha_j)}.\end{aligned} \tag{16}$$

where $\xi_{ij}(\Phi)=\sqrt{s_i^2s_j^2+s_k^2-2s_is_js_k\cos\Phi}$ and *every index satisfies* $i\neq j\neq k$,

When (α_1, α_2) is an optimal pint of Eq. (16), the gradient of the object function at the point is zero. Therefore, the optimal condition is given by

$$\begin{aligned}\alpha_j &= \frac{\alpha_i\{s_j^2-(1-\alpha_i)^2\}^2}{\alpha_i\{s_j^2-(1-\alpha_i)^2\}^2+(q_j/q_i)\xi_{ij}^2(\Phi)(1-\alpha_i)},\\ \alpha_i &= \frac{\alpha_j\{s_i^2-(1-\alpha_j)^2\}^2}{\alpha_j\{s_i^2-(1-\alpha_j)^2\}^2+(q_i/q_j)\xi_{ij}^2(\Phi)(1-\alpha_j)},\quad \forall i\neq j\neq k.\end{aligned} \tag{17}$$

However, the inverse does not hold. When $q_i=q_j$ and $s_1=s_2=s_3=s$, the equations have an inverse function relationship. Then, the optimal condition is obtained by $\alpha_i=\alpha_j=1-\sqrt{s^2+\xi(\Phi)}$ $(\forall\xi(\Phi)=\xi_{ij}(\Phi))$. If (α_i, α_j) does not fulfill Eq. (16), the best strategy for Bob and Charlie is to discriminate only a single qutrit state out of three pure qutrit states.

Theorem 4. *Suppose that Alice prepares an element* $|\psi_i\rangle$, *with a prior probability* q_i, *from three pure qutrit states* $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ *satisfying* $\langle\psi_i|\psi_j\rangle=s_k\exp(i\varepsilon_{ijk}\phi_k)$, $s_k\geq 0$ *and sends it to Bob. When* $\Phi=\phi_1+\phi_2+\phi_3=0$ *is fulfilled, if Bob and Charlie discriminate every three qutrit state in sequential state discrimination, the solution for the sequential state discrimination is equivalent to that of the following optimization problem*:

$$\begin{aligned}\text{maximize}\quad & P_s^{(B,C)} = q_1\alpha_1+q_2\alpha_2+q_3\alpha_3-2s_1\sqrt{\frac{q_2q_3\alpha_2\alpha_3}{(1-\alpha_2)(1-\alpha_3)}}\\ & \qquad -2s_2\sqrt{\frac{q_1q_3\alpha_1\alpha_3}{(1-\alpha_1)(1-\alpha_3)}}+2s_3\sqrt{\frac{q_1q_2\alpha_1\alpha_2}{(1-\alpha_1)(1-\alpha_2)}}\\ \text{subject to}\quad & (\alpha_1,\alpha_2,\alpha_3)\in \text{int}(C),\ (\alpha'_1,\alpha'_2,\alpha'_3)\in\partial C'.\end{aligned} \tag{18}$$

In addition, from the solution discussed in ref.[32], we can find the optimal condition for Charlie, which is $\alpha'_i=1-(s_js_k/s_i)(1-\alpha_i)^{-1}(i\neq j\neq k)$. The sequential state discrimination of the case becomes the following optimization problem.

$$\text{maximize}\quad P_s^{(B,C)} = q_1\alpha_1\left\{1-\frac{s_2s_3}{s_1}\frac{1}{1-\alpha_1}\right\}+q_2\alpha_2\left\{1-\frac{s_1s_3}{s_2}\frac{1}{1-\alpha_2}\right\}+q_3\alpha_3\left\{1-\frac{s_1s_2}{s_3}\frac{1}{1-\alpha_3}\right\} \tag{19}$$

The optimal solution of Eq. (19) is $\alpha_i=1-\sqrt{s_js_k/s_i}(i\neq j\neq k)$. The solution satisfies every equality of Eq. (14)[32]. When the overlap between every pure state is the same, the result in this report contains those of M. Hillery and J. Mimih[26].

Also, the success probability of Charlie is $\alpha'_i=\alpha_i=1-\sqrt{s_js_k/s_i}$, which is the same as Bob's. Here, $(\alpha_1, \alpha_2, \alpha_3)=(1-\sqrt{s_2s_3/s_1}, 1-\sqrt{s_1s_3/s_2}, 1-\sqrt{s_1s_2/s_3})$ is located in the interior of C and $(\alpha'_1, \alpha'_2, \alpha'_3)=(1-\sqrt{s_2s_3/s_1}, 1-\sqrt{s_1s_3/s_2}, 1-\sqrt{s_1s_2/s_3})$ exists on $\partial C'$.

However, for a arbitrary geometric phase Φ, the optimization problem cannot be analytically presented, as in the case of Theorem 4. A detailed explanation is given in the Methods.

Now, let us investigate the structure of C and C'. It can be shown that C and C' are convex. The vertices of C and C' are given by

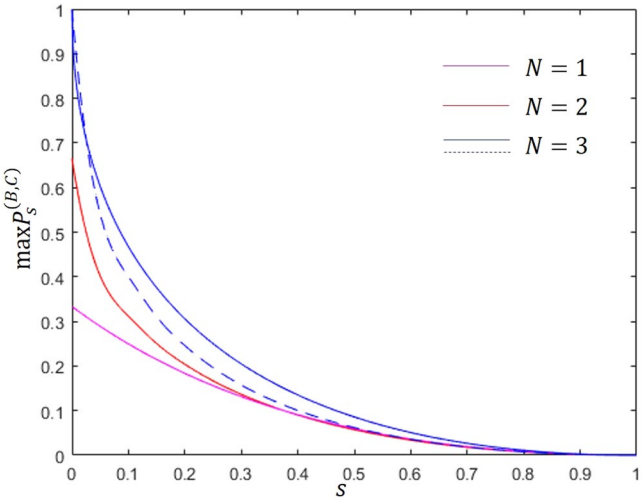

Figure 3. Optimal success probability of the sequential state discrimination of three linearly independent symmetric qutrits in terms of overlap s. Here, the prior probability of the three qutrits is assumed to be equal, and N denotes the number of pure qutrit states which Bob and Charlie discriminate. The blue solid line(blue dashed line) displays the optimal success probability of Eqs (18 and 19).

$$\begin{aligned}
\alpha_{i,\,\max} &= 1 - \frac{s_j^2 + s_k^2 - 2s_i s_j s_k \cos\Phi}{1 - s_i^2}, \\
\alpha'_{i,\,\max} &= 1 - \frac{s'^2_j + s'^2_k - 2s'_i s'_j s'_k \cos\Phi}{1 - s_i'^2} \\
&= 1 - \frac{s_j^2(1-\alpha_j) + s_k^2(1-\alpha_k) - 2s_i s_j s_k \cos\Phi}{(1-\alpha_i)\{(1-\alpha_j)(1-\alpha_k) - s_i^2\}}, \quad \forall i \neq j \neq k.
\end{aligned} \tag{20}$$

Three vertices of C' depend on Bob's POVM. According to Eq. (19), $0 \leq \alpha_{i,\max} \leq 1$. $\alpha_{i,\max} \leq 1$ can be easily proven. $\alpha_{i,\max} \geq 0$ is equivalent to a positive-semidefiniteness condition of the Gram matrix. Similarly, $\alpha'_{i,\,\max} \leq 1$ can be shown. $\alpha'_{i,\,\max}$ is a decreasing function to $(\alpha_1, \alpha_2, \alpha_3)$. When $\alpha_1 = \alpha_2 = \alpha_3 = 0$, $\alpha_{i,\,\max} = \alpha'_{i,\,\max}$ holds. Therefore, if $(\alpha_1, \alpha_2, \alpha_3)$ satisfies the condition of Bob's POVM, one can find $((\alpha_1, \alpha_2, \alpha_3) \in C \rightarrow \forall \alpha_i < 1)$ $\alpha'_{1,\,\max} < \alpha_{1,\,\max}$. This implies that the size of the convex set C' for Charlie is smaller than that of C. When Bob performs an optimal unambiguous discrimination, one has $\alpha'_{i,\,\max} = 0$, which means that Charlie cannot obtain any information from Bob's post-measurement state. In Fig. 2, Fig. 2(a) displays the Bob's convex set C when $s_1 = 0.2$, $s_2 = 0.3$, $s_3 = 0.25$. In Fig. 2(b), solid line(dashed line) indicates the boundary of Charlie's convex set C' when $\alpha_1 = \alpha_2 = \alpha_3 = 0.5 (\alpha_1 = \alpha_2 = 0.5, \alpha_3 = 0.7)$. Figure 2 clearly shows that C and C' are convex. Furthermore, Fig. 2(b) shows that as $(\alpha_1, \alpha_2, \alpha_3)$ approaches to its boundary ∂C, the size of Charlie's convex set becomes smaller.

It is difficult to analytically solve the optimization problem described by Theorem 4. Unlike the case for two qubits, it is difficult to find an analytic solution for the sequential state discrimination of three qutrit states even in a symmetric case. Therefore, we use a random search method[36] to obtain a numerical solution. Figure 3 displays the optimal success probability when $q_1 = q_2 = q_3$ and $s_1 = s_2 = s_3 = s$. Figure 3 shows that it is better for Bob and Charlie to discriminate every three pure qutrit state than it is for them to discriminate one(or two) pure qutrit state(s). This is different from the case involving two pure qubit states. In the case of two pure qubit states prepared with equal prior probability, when the overlap between the two qubit states is greater than $3 - 2\sqrt{2}$, discriminating only single qubit state is the best method[21,23]. However, for quantum key distribution, receivers should discriminate all quantum states prepared by a sender[21,38]. Therefore, our results for three pure qutrit states demonstrates the advantages of sequential state discrimination in quantum key distribution.

In addition, Hillery and Mimih[26] studied the specific cases of sequential state discrimination. Even though we do not explain in detail, some examples of M. Hillery and J. Mimih[26] can be understood by application of results of this report.

Comparison with an other scenario. Here, we compare the sequential state discrimination of three pure qutrit states with quantum probabilistic cloning strategy[39]. Unlike sequential state discrimination, the method allows a classical communication.

- (*Quantum probabilistic cloning)* Suppose that Alice prepares a quantum state $|\psi_i\rangle (i \in \{1, \ldots, N\})$ with a prior probability q_i and sends it to Bob. Bob clones this quantum state probabilistically[39]. When Bob successfully copies the state, the quantum state after Bob's copying becomes $|\psi_i\rangle \otimes |\psi_i\rangle$. Bob shares $|\psi_i\rangle \otimes |\psi_i\rangle$ with Charlie. Bob and Charlie perform an optimal unambiguous discrimination on his own state, respectively. If Bob fails to copy the quantum state of Alice, he tells Charlie that he fails to copy the quantum state of Alice.

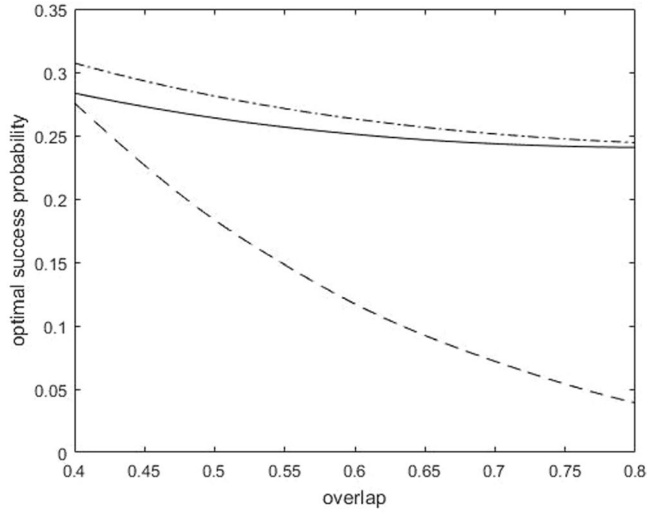

Figure 4. The optimal success probabilities of probabilistic quantum cloning and sequential state discrimination for three pure qutrit states. Here, the solid line(dash-dot line) shows the optimal success probability of sequential state discrimination based on Eqs (18 and 19), and the dashed line shows that of probabilistic quantum cloning.

Even though there is no unitary operation for copying non-orthogonal quantum states[40], one can clone a quantum state imperfectly[41]. There are many methods for copying a quantum state[39,42,43]. L. M. Duan *et al*[39]. showed that non-orthogonal pure quantum state can be cloned through Quantum probabilistic cloning.

Theorem 5. (L. M. Duan *et al*[39].) *Suppose that for a element* $|\psi_i\rangle$ *of a set composed of non-orthogonal pure states* $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$, *one can clone a quantum state* $|\psi_i\rangle \otimes |R\rangle \rightarrow |\psi_i\rangle \otimes |\psi_i\rangle$ *with a probability* γ_i. *The necessary and sufficient condition for such quantum operation is that* $X - \sqrt{\Gamma}\, Y \sqrt{\Gamma}$ *becomes positive-semidefinite, where* $X = \{\langle\psi_i|\psi\rangle_j\}_{i,j=1}^N, Y = \{\langle\psi_i|\psi_j\rangle^2\}_{i,j=1}^N$, and $\sqrt{\Gamma} = diag\{\sqrt{\gamma}_1, \cdots, \sqrt{\gamma}_N\}$[39,44].

Let us assume equal probability for successfully copying a quantum state ($\gamma_i = \gamma\ \forall i$). Then, the probability for successful quantum probabilistic cloning of Bob and Charlie is given by

$$P_{s,clone}^{(B,C)} = \sum_{i=1}^{N} \Pr[|\psi_i\rangle] \times \Pr[\text{clone}|\psi_i\rangle] \times \Pr[i|\text{clone}] \tag{21}$$

Here, $Pr[|\psi_i\rangle]$ is a prior probability with which Alice prepares $|\psi_i\rangle$. $\Pr[\text{clone}|\psi_i\rangle]$ is the probability that Bob successfully copies the quantum state $|\psi_i\rangle$ of Alice. $\Pr[i|\text{clone}]$ is the probability that Bob and Charlie obtain measurement result *i*. The necessary and sufficient condition for Theorem 5 is that the pure states are linearly independent[39,44]. Therefore, there exists a POVM of Bob and Charlie that can discriminate Alice's quantum states without error.

Suppose that Alice prepares a quantum state out of three linearly independent pure qutrits $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$. When Bob successfully copies the quantum state of Alice, Bob and Charlie independently discriminate Alice's quantum state. Therefore, the best way to perform a strategy of probabilistic quantum cloning is for Bob and Charlie to perform an optimal unambiguous discrimination. Therefore, the real vector corresponding to an optimal POVM of Bob and Charlie is $(\alpha_1, \alpha_2, \alpha_3)$. Then, the optimal success probability of Bob and Charlie, when probabilistic quantum cloning is imposed, becomes

$$P_{s,clone}^{(B,C)} = \gamma_{\text{opt}}(q_1\alpha_1^{\,2} + q_2\alpha_2^{\,2} + q_3\alpha_3^{\,2}) \tag{22}$$

Here, γ_{opt} is a maximal γ satisfying Theorem 5. The optimal value of γ depends on the overlap between pure states prepared by Alice. The success probability of probabilistic quantum cloning is a convex function of $(\alpha_1, \alpha_2, \alpha_3)$. Therefore, $(\alpha_1, \alpha_2, \alpha_3)$ exists on the boundary ∂C of C.

Example. Suppose that the overlap between three pure qutrits $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ can be given by

$$\langle\psi_1|\psi_2\rangle = -0.1, \quad \langle\psi_2|\psi_3\rangle = 0.1, \quad \langle\psi_3|\psi_1\rangle = -s \tag{23}$$

Suppose that the prior probabilities for the three pure qutrits are $q_1 = q_3 = 0.35$, and $q_2 = 0.3$. Let us assume that the geometric phase of the three pure qutrits is $\phi_1 + \phi_2 + \phi_3 = 0 + \pi + \pi = 2\pi$. Figure 4 displays the optimal success probabilities of probabilistic quantum cloning and sequential state discrimination, where the overlap *s* is $s \in [0.4, 0.8]$. According to Fig. 4, sequential state discrimination, unlike probabilistic quantum cloning, has a non-zero optimal success probability even when *s* becomes large. This is different from the case of two pure qubits

with equal prior probabilities[21]. This implies that sequential state discrimination performs better than a probabilistic quantum cloning strategy.

Revisiting The Security of Protocol Based on Sequential State Discrimination Scenario. Based on B92 protocol[38], the security of B92 protocol can be obtained when Bob performs an unambiguous discrimination on nonorthogonal quantum states encoded by a sender Alice[21]. However, if an eavesdropper Eve exists between Alice and Bob, then the conclusive result of Bob will contain an error. When a discrepancy occurs from the comparison between Alice's quantum state and Bob's conclusive result, Alice and Bob can notice the existence of eavesdropper Eve.

Note that Alice and Bob are separated in space. Alice should inform Bob of the prior probability, in order for Bob to perform a unambiguous discrimination. In this process, if Alice uses a classical communication, Eve can obtain the prior probability without being noticed. When Eve optimally discriminates two quantum states of Alice, the post-measurement states of Eve are entirely overlapped, which implies that Bob cannot obtain any information from the post-measurement state of Eve. Therefore, Bob's result is always inconclusive. Meanwhile, unless Bob notices Eve, Eve's measurement should be identity. This implies that Eve cannot obtain any information from Alice's quantum state. When Eve obtains a partial information from Alice's quantum state, the overlap between Eve's post-measurement states is larger than the overlap between Alice's quantum states. Therefore, Bob's conclusive result may contain an error with a probability.

In fact, this argument can be applied to the case of sequential state discrimination of three pure qutrit states. Now, we can have the following Conjecture.

Conjecture 3. *In sequential discrimination strategy, when a receiver can obtain a partial information about a sender's quantum state through a POVM, the size of convex set C′ of a second receiver is smaller than that of C of a first receiver*.

In fact, SSD strategy provides a protocol for distribution of secure key to multi-parties[21], based on B92 protocol[38]. When an eavesdropper Eve tries to obtain a partial information between Alice and Bob, the conclusive result of Bob inevitably contains an error. In the similar way, if Eve gains an information between Bob and Charlie, the conclusive result of Charlie should have an error. It implies that whenever Eve obtains an information, Bob and Charlie can notice the existence of eavesdropper Eve. Therefore, Alice, Bob, and Charlie can share a secure key.

In addition, the example of our report shows that the proposed SSD strategy can provide a higher success probability than probabilistic quantum cloning strategy. We should note that in two qubit case, SSD strategy is not better than probabilistic quantum cloning strategy[21]. Therefore, when Alice encodes an information using non-orthogonal pure qutrits, SSD strategy can be more efficient one for QKD than probabilistic quantum cloning. It implies that SSD strategy can be a good candidate for multi-party QKD[27].

Furthermore, if one uses larger number of linearly independent pure qudits, Alice can share more secure message with multi-parties[26]. Ref.[26] considers only symmetric pure qudits. The result of our report may provide a strategy using general(nonsymmetric) pure qudits, for QKD of multi-parties.

Discussion

In this report, we studied the sequential state discrimination of N pure states. One of advantages of the sequential state discrimination is that a sequential receiver Charlie can determine the pure state of a sender Alice, handling the post-measurement of a previous receiver Bob rather than the pure state of Alice. First, we provided a general formulation of sequential state discrimination for N pure states when Alice prepares a quantum state out of N pure states. Second, we obtained the condition for sequential state discrimination of two qubits with arbitrary prior probabilities. Third, we showed that when Alice prepares three qutrits with the identical prior probabilities, the best way for Bob and Charlie to perform sequential state discrimination of three qutrits is to unambiguously discriminate every three qutrit. This differs from the two qubits case, where the best sequential state discrimination method is not to discriminate every two qubit. In addition, we showed that the sequential state discrimination of three pure qutrit states performs better than probabilistic quantum cloning strategy.

If the three conjectures of our report can hold in the case of N qudits, we have a formulation of sequential state discrimination to N linearly independent qudits. In addition, we may generalize our sequential state discrimination approach to N parties. It is interesting to compare our strategy of N qudits for N parties with other strategies.

Methods

In this section, we prove Theorem 1–4.

Proof of Theorem 1. When Alice prepares one of two pure qubits, the optimization problem of Eq. (4) is formulated by

$$\begin{aligned} \text{maximize} \quad & P_s^{(B,C)} = q_1\alpha_1\alpha'_1 + q_2\alpha_2\alpha'_2 \\ \text{subject to} \quad & (1-\alpha_1)(1-\alpha_2) - s^2 > 0, \\ & (1-\alpha'_1)(1-\alpha'_2) - s'^2 = 0. \end{aligned} \tag{24}$$

First, let us consider (α'_1, α'_2). The objective function of Eq. (24) is a line with a slope of $-q_1\alpha_1/q_2\alpha_2$. (α'_1, α'_2), satisfying the objective function constraint. This is the tangential point between the equality condition and the

line of objective function. At this point, the condition under which the objective function and the gradient become parallel is given by

$$\frac{\partial P_s^{(B,C)}/\partial \alpha'_1}{\partial P_s^{(B,C)}/\partial \alpha'_2} = \frac{q_1\alpha_1}{q_2\alpha_2} = \frac{1-\alpha'_2}{1-\alpha'_1} \tag{25}$$

Substituting Eq. (25) into the equality condition of Eq. (24), one can find (α'_1, α'_2) as follows:

$$\begin{aligned} \alpha'_1 &= 1 - s'\sqrt{\frac{q_2\alpha_2}{q_1\alpha_1}}, \\ \alpha'_2 &= 1 - s'\sqrt{\frac{q_1\alpha_1}{q_2\alpha_2}}. \end{aligned} \tag{26}$$

For (α'_1, α'_2) of Eq. (26), if $\alpha'_1, \alpha'_2 > 0$, the best strategy of Charlie is to discriminate two post-measurement states of Bob, which is the proof of Theorem 1.

Meanwhile, for (α'_1, α'_2), if one of $\alpha'_1, \alpha'_2 > 0$ is zero, the objective function of Eq. (24) becomes Eq. (11).

Proof of Theorem 2. Suppose that Bob and Charlie discriminate only one of three pure qutrit states of Alice. Eq. (4) is equivalent to the following optimization problem

$$\begin{aligned} \text{maximize} \quad & P_s^{(B,C)} = q_i\alpha_i\alpha'_i \\ \text{subject to} \quad & \overline{\alpha}_i - s_i^2\overline{\alpha}_i - s_j^2 - s_k^2 + 2s_is_js_k\cos\Phi > 0, \\ & \overline{\alpha}'_i - s'^2_i\overline{\alpha}'_i - s'^2_j - s'^2_k + 2s'_is'_js'_k\cos\Phi = 0. \end{aligned} \tag{27}$$

where $\overline{\alpha}_i = 1 - \alpha_i, \overline{\alpha}'_i = 1 - \alpha'_i$. $(\alpha_1, \alpha_2, \alpha_3)$, satisfying Eq. (27), is a vertex of $\partial C'$. Substituting one of the vertices into Eq. (27), we can see that $\alpha_i = 1 - \sqrt{\chi_i(\Phi)}$ is the optimal condition, where $\chi_i(\Phi) = (s_j^2 + s_k^2 - 2s_is_js_k\cos\Phi)/(1 - s_i^2)$. Therefore, the optimized success probability becomes $\max P_s^{(B,C)} = \max_i\{q_i(1 - \chi_i(\Phi))\}$.

Proof of Theorem 3. Suppose that Bob and Charlie discriminate only two states out of three pure qutrit states of Alice. Eq. (4) can be written as the following optimization problem

$$\begin{aligned} \text{maximize} \quad & s^{(B,C)} = q_i\alpha_i\alpha_{i'} + q_j\alpha_j\alpha_{j'} \\ \text{subjectto} \quad & \overline{\alpha}_i\overline{\alpha}_j - s_i^2\overline{\alpha}_i - s_j^2\overline{\alpha}_j - s_k^2 + 2s_is_js_k\cos\Phi > 0, \\ & \overline{\alpha}_i'\overline{\alpha}_j' - s_i^{2\prime}\overline{\alpha}_i' - s_j^{2\prime}\overline{\alpha}_j' - s_k^{2\prime} + 2s_i's_j's_k'\cos\Phi = 0. \end{aligned} \tag{28}$$

(α'_1, α'_2), fulfilling the equality condition of Eq. (28), exists on the tangential point between a line $(q_i\alpha_i)\alpha'_i + (q_j\alpha_j)\alpha'_j$ and the equality condition. The condition for the tangential point to be located on $\partial C'$ becomes

$$\begin{aligned} \alpha_j &< \frac{\alpha_i(1-\alpha_i-s_j^2)^2}{\alpha_i(1-\alpha_i-s_j^2)^2 + (q_j/q_i)\xi_{ij}(\Phi)^2(1-\alpha_i)}, \\ \alpha_i &< \frac{\alpha_j(1-\alpha_j-s_i^2)^2}{\alpha_j(1-\alpha_j-s_i^2)^2 + (q_i/q_j)\xi_{ij}(\Phi)^2(1-\alpha_j)}. \end{aligned} \tag{29}$$

where $\xi_{ij}(\Phi) = \sqrt{s_i^2s_j^2 + s_k^2 - 2s_is_js_k\cos\Phi}$. When (α_i, α_j) satisfies Eq. (29), the optimization problem is equivalent to Theorem 3.

Proof of Theorem 4. Suppose that Bob and Charlie discriminate every three pure qutrit state of Alice. The measurement conditions of Charlie for the best sequential state discrimination correspond to the tangential points between the plane $(q_1\alpha_1)\alpha'_1 + (q_2\alpha_2)\alpha'_2 + (q_3\alpha_3)\alpha'_3$ and $\partial C'$. The tangential point can be analytically found when the geometric phase is $\Phi = 0, \pi$[45]. However, for a general geometric phase, the condition for the plane to be tangent to $\partial C'$ is given by a 6-th order of algebraic equation[32,33]. For similarity, we assume that $\Phi = 0$. Then, the tangential points become as follows:[32,33].

$$\begin{aligned} \alpha'_1 &= 1 - \frac{s'_2\sqrt{q_3\alpha_3} - s'_3\sqrt{q_2\alpha_2}}{\sqrt{q_1\alpha_1}}, \quad \alpha_{2'} = 1 - \frac{s'_1\sqrt{q_3\alpha_3} - s'_3\sqrt{q_1\alpha_1}}{\sqrt{q_2\alpha_2}}, \\ \alpha'_3 &= 1 - \frac{s'_2\sqrt{q_1\alpha_1} + s'_1\sqrt{q_2\alpha_2}}{\sqrt{q_3\alpha_3}}. \end{aligned} \tag{30}$$

References

1. Helstrom, C. W. *Quantum Detection and Estimation*. (Academic Press, New York, 1976).
2. Holevo, A. S. *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland 1979).
3. Yuen, H. P., Kennedy, R. S. & Lax, M. Optimum testing of multiple hypotheses in quantum detection theoty. *IEEE Trans. Inf. Theory* **21**, 125 (1975).
4. Ha, D. & Kwon, Y. Complete analysis for three-qubit mixed-state discrimination. *Phys. Rev. A* **87**, 062302 (2013).
5. Ha, D. & Kwon, Y. Discriminating N-qudit states using geometric structure. *Phys. Rev. A* **90**, 022330 (2014).
6. Ivanovic, I. D. How to differentiate between non-orthogonal states. *Phys. Lett. A* **123**, 257 (1987).
7. Dieks, D. Overlap and distinguishability of quantum states. *Phys. Lett. A* **126**, 303 (1988).
8. Peres, A. How to differentiate between non-orthogonal states. *Phys. Lett. A* **128**, 19 (1988).
9. Jaeger, G. & Shimony, A. Optimal distinction between two non-orthogonal quantum states. *Phys. Lett. A* **197**, 83 (1995).
10. Chefles, A. Unambiguous discrimination between linearly-independent quantum states. *Phys. Lett. A* **239**, 339 (1998).
11. Rudolph, T., Spekkens, R. W. & Turner, P. S. Unambiguous discrimination of mixed states. *Phys. Rev. A* **68**, 010301(R) (2003).
12. Croke, S., Andersson, E., Barnett, S. M., Gilson, C. R. & Jeffers, J. Maximum confidence quantum measurements. *Phys. Rev. Lett.* **96**, 070401 (2006).
13. Touzel, M. A. P., Adamson, R. B. A. & Steinberg, A. M. Optimal bounded-error stretegies for projective measurements in non-orthogonal state discrimination. *Phys. Rev. A* **76**, 062314 (2007).
14. Hayashi, A., Hashimoto, T. & Horibe, M. State discrimination with error margin and its locality. *Phys. Rev. A* **78**, 012333 (2008).
15. Sugimoto, H., Hashimoto, T., Horibe, M. & Hayashi, A. Discrimination with error margin between two states - case of general occurrence probabilities. *Phys. Rev. A* **80**, 052322 (2009).
16. Sugimoto, H., Taninaka, Y. & Hayashi, A. Discrimination with an error margin among three symmetric states of a qubit. *Phys. Rev. A* **86**, 042311 (2012).
17. Chefles, A. & Barnett, S. M. Quantum state separation, unambiguous discrimination and exact cloning. *J. Mod. Opt.* **45**, 1295 (1998).
18. Zhang, C.-W., Li, C.-F. & Guo, G.-C. General strategies for discrimination of quantum states. *Phys. Lett. A* **261**, 25 (1999).
19. Fiurasek, J. & Jezek, M. Optimal discrimination of mixed quantum states involving inconclusive result. *Phys. Rev. A* **67**, 012321 (2003).
20. Ha, D. & Kwon, Y. An optimal discrimination of two mixed qubit states with a fixed rate of inconclusive results. *Quantum Inf Process* **16**, 273 (2017).
21. Bergou, J. A., Feldman, E. & Hillery, M. Extracting information from a qubit by multiple observers: toward a theory of sequential state discrimination. *Phys. Rev. Lett.* **111**, 100501 (2013).
22. Rapcan, P., Calsamiglia, J., Munoz-Tapia, R., Bagan, E. & Buzek, V. Scavenging quantum information: multiple observations of quantum systems. *Phys. Rev. A* **84**, 032326 (2011).
23. Pang, C.-Q., Zhang, F.-L., Xu, L.-F., Liang, M.-L. & Chen, J.-L. Sequential state discrimination and requirement of quantum dissonance. *Phys. Rev. A* **88**, 052331 (2013).
24. Solis-Prosser, M. A. *et al*. Experimental multiparty sequential state discrimination. *Phys. Rev. A* **94**, 042309 (2016).
25. Zhang, J.-H., Zhang, F.-L. & Liang, M.-L. Sequential state discrimination with quantum correlation, arXiv:1701.02106(quant-ph) (2017).
26. Hillery, M. & Mimih, J. Sequential discrimination of qudits by multiple observers. *J. Phys. A: Math. and Theor.* **50**, 435301 (2017).
27. Namkung, M. & Kwon, Y. Optimal sequential state discrimination between two mixed quantum states. *Phys. Rev. A.* **96**, 022318 (2017).
28. Bhatia, R. *Positive Definite Matrices* (Princeton University Press 2007).
29. Chefles, A., Kitagawa, A., Takeoka, M., Sasaki, M. & Twamley, J. Unambiguous discrimination among oracle operators. *J. Phys. A: Math. Theor.* **40**, 10183 (2007).
30. Eldar, Y. C. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Trans. Inf. Theor.* **49**, 446 (2003).
31. Pang, S. & Wu, S. Optimal unambiguous discrimination of linearly independent pure states. *Phys. Rev. A* **80**, 052320 (2009).
32. Bergou, J. A., Futschik, U. & Feldman, E. Optimal unambiguous discrimination of pure quantum states. *Phys. Rev. Lett.* **108**, 250502 (2012).
33. Ha, D. & Kwon, Y. Analysis of optimal unambiguous discrimination of three pure quantum states. *Phys. Rev. A* **91**, 062312 (2015).
34. Nielson, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information*. (Cambridge University Press, New York, 2010).
35. Kraus, K. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. (Wiley, New York, 1991).
36. Pierre, D. A. *Optimization Theory with Application* (Dover 1969).
37. Kiusalaas, J. *Numerical Methods in Engineering with MATLAB* (Cambridge 2005).
38. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
39. Duan, L.-M. & Guo, G.-C. Probabilistic cloning and identification of linearly independent quantum states. *Phys. Rev. Lett.* **80**, 4999 (1998).
40. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802 (1982).
41. Buzek, V. & Hillery, M. Optimal copying: beyond the no-cloning theorem. *Phys. Rev. A* **54**, 1844 (1996).
42. Bruss, D. *et al*. Optimal universal and state-dependent quantum cloning. *Phys. Rev. A* **57**, 2368 (1998).
43. Chefles, A. & Barnett, S. M. Quantum state separation, unambiguous discrimination and exact cloning. *J. Phy. A: Math. Gen.* **31**, 10097 (1998).
44. Li, L., Qiu, D., Li, L., Wi, L. & Zou, X. Probabilistic broadcasting of mixed states. *J. Phys. A: Math. Theor.* **42**, 175302 (2009).
45. Sugimoto, H., Hashimoto, T. & Hayashi, A. Complete solution of unambiguous discrimination of three pure states with real inner product. *Phys. Rev. A* **82**, 032338 (2010).

Acknowledgements

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 and communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. R0190- 15-2028, PSQKD).

Author Contributions

M.N. and Y.K. analyzed the result and wrote the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.