Unambiguous discrimination of sequences of quantum states

Tathagata Gupta[*]
Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India

Shayeef Murshid[†]
Electronics and Communication Sciences Unit, Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India

Somshubhro Bandyopadhyay[‡]
Department of Physical Sciences, Bose Institute, EN 80, Bidhannagar, Kolkata 700091, India

(Received 19 February 2024; revised 13 April 2024; accepted 6 May 2024; published 22 May 2024)

We consider the problem of determining the state of an unknown quantum sequence without error. The elements of the given sequence are drawn with equal probability from a known set of linearly independent pure quantum states with the property that their mutual inner products are all real and equal. This problem can be posed as an instance of unambiguous state discrimination where the states correspond to that of all possible sequences having the same length as the given one. We calculate the optimum probability by solving the optimality conditions of a semidefinite program. The optimum value is achievable by measuring individual members of the sequence, and no collective measurement is necessary.

DOI: 10.1103/PhysRevA.109.052222

I. INTRODUCTION

One of the remarkable features of quantum theory that shows a radical departure from classical physics is that distinct quantum states may not be reliably distinguished from one another. In particular, if a quantum system is prepared in one of two nonorthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, then no quantum measurement could determine the state of the system with certainty. In other words, quantum theory allows us to distinguish only between orthogonal states.

Even though nonorthogonal states cannot be reliably distinguished, one may still try to glean as much "which state" information as possible. Consider a quantum system prepared in one of several nonorthogonal states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$, but we do not know which one. The objective is to determine, as well as possible, the state of the system by performing a suitable measurement. This problem is known as quantum state discrimination (see [1–3] for excellent reviews).

Two approaches are usually considered to study a state discrimination problem. The first is known as minimum-error discrimination, which aims to design a measurement that minimizes the average error and applies to any set of nonorthogonal states. For two states $|\psi_1\rangle$ and $|\psi_2\rangle$ with prior probabilities p_1 and p_2, the maximum probability of success is given by $1 - p_e$, where

$$p_e = \tfrac{1}{2}(1 - \sqrt{1 - 4p_1p_2|\langle\psi_1|\psi_2\rangle|^2}) \tag{1}$$

is the minimum probability of error [4].

The second strategy is called unambiguous discrimination, which seeks definite knowledge of the state balanced against a probability of failure. Here a measurement outcome either correctly identifies the given state or is inconclusive, in which case, we do not learn anything about the state. Once again, for the two-state problem, the maximum probability of success is given by $1 - p_I$, where

$$p_I = 2\sqrt{p_1p_2}|\langle\psi_1|\psi_2\rangle| \tag{2}$$

is the minimum probability for an inconclusive result [5–8]. Unlike minimum-error discrimination, which applies to any set of states, unambiguous discrimination is possible if and only if the given states are linearly independent [9]. Finding optimal solutions, however, is considerably hard in general (for different approaches and solutions for specific cases see [10–20]).

In this paper we consider a variant of the state discrimination problem, namely, sequence discrimination, where, instead of learning about the state of a single quantum system as in state discrimination, we wish to do the same about the state of a sequence of quantum systems. We note that a closely related problem, viz., quantum state comparison, where the objective is to determine if the members of a given sequence are all identical or all different, has been studied before [17].

Sequence discrimination can be described as follows. Suppose that we are given a sequence of pure quantum states, where each member (of the given sequence) belongs to a known set of states (this set will sometimes be referred to as the parent). We do not know the identity of the individual members but have complete information about the parent set. The objective is to learn about the given sequence as well as allowed by quantum theory. As we will explain, for a given sequence of finite length, this amounts to discriminating

[*]tathagatagupta@gmail.com
[†]shayeef.murshid91@gmail.com
[‡]som@jcbose.ac.in

 ©2024 American Physical Society

between all sequences of the same length constructed from the parent set. Since every sequence, by construction, is in a product state, sequence discrimination is an instance of state discrimination where the concerned states are all product states.

As in a state discrimination problem, one could consider either the minimum-error or unambiguous discrimination strategy for sequence discrimination. Here we focus on the latter as we wish to identify the state of a given sequence without error. This would be possible, as we know from [9], if and only if the states corresponding to all sequences of the same length form a linearly independent set, a condition fulfilled if and only if the parent set is linearly independent [17]. Therefore, one could determine the state of any given sequence with a nonzero probability, provided the parent set is linearly independent, and assuming this is indeed the case, one would then like to know the optimum success probability and the corresponding measurement. The present paper is about answering these two questions.

To solve this problem with full generality, besides the requirement that the parent set must consist of linearly independent states, one would set the associated prior probabilities to be different and the mutual inner products to be unequal and complex. However, in this work we do not attempt to solve the most general scenario; instead, we assume that the elements of the parent set are all equally probable and the inner products are all real and equal and solve the sequence discrimination problem completely. The optimum success probability is computed by solving the optimality conditions of a semidefinite program. We find that the optimum value is achievable by measuring individual members of the sequence and no collective measurement is necessary, even though the states under consideration are all product states.

One may have noticed that our problem is motivated by the working of quantum key distribution protocols, especially B92 [21] and its generalizations. Recall that in the B92 protocol [21], Alice sends a sequence of quantum systems, where each system is prepared in one of two nonorthogonal pure states, to Bob, who performs an unambiguous discrimination measurement on each of them to determine its state. In order to generate the secret key, the conclusive outcomes are kept and the inconclusive outcomes are discarded. A generalization of this protocol involves Alice sending a sequence of quantum states, where each state is chosen from a linearly independent set, so unambiguous discrimination is possible. Note that the protocol requires Bob to measure the quantum systems individually as and when he receives them. However, one could ask whether Bob could do better by performing a joint measurement on the whole sequence (assuming Bob has access to quantum memory). Of course, this comes with the drawback that if the outcome is inconclusive, they will need to discard the entire sequence, but the possible upshot is that a joint measurement could increase the probability of identifying the sequence correctly. However, our result shows that Bob gains no advantage by choosing a collective measurement over measuring the systems individually.

The paper is organized as follows. Section II discusses the sequence discrimination problem in detail, presents the necessary lemmas related to the properties of a collection of pure states with mutual inner products all being real and equal, and states the main result as Theorem 1. In Sec. III we discuss the semidefinite programming (SDP) formulation of unambiguous state discrimination. Section IV proves the main result by solving the optimality conditions of the relevant SDP. This section is divided into four subsections for easy reading and understanding of the proof. We conclude the paper with a brief review of the results and a discussion of the open problems in Sec. V.

II. SEQUENCE DISCRIMINATION: FORMULATION AND MAIN RESULT

We begin by describing the general formulation. Consider an unknown sequence of $k \in \mathbb{N}$ quantum systems, each prepared in a state chosen from a known parent set $\{p_i, |\psi_i\rangle : 2 \leqslant i \leqslant N\}$, where p_i is the prior probability associated with $|\psi_i\rangle$. The objective is to determine the sequence (more precisely, the state of the sequence) as well as possible. This can be posed as a state discrimination problem.

Let $[n] = \{1, 2, \ldots, n : n \in \mathbb{N}\}$ denote the set of natural numbers from 1 to n and $\mathscr{F}(k, N)$ be the set of all functions from $[k]$ to $[N]$. Then the state of a sequence is a product state of the form

$$|\psi_\sigma\rangle = |\psi_{\sigma(1)}\rangle \otimes \cdots \otimes |\psi_{\sigma(k)}\rangle, \quad \sigma \in \mathscr{F}(k, N).$$

To learn about a given sequence of length k, we therefore need to distinguish between all such possible sequences. These sequences form the set

$$\{p_\sigma, |\psi_\sigma\rangle : \sigma \in \mathscr{F}(k, N)\}, \tag{3}$$

where $p_\sigma = p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(k)}$ is the prior probability associated with the sequence state $|\psi_\sigma\rangle$. The cardinality of the above set is N^k. The sequence discrimination problem is therefore a state discrimination problem involving states belonging to the set defined by (3).

Here we consider the problem of unambiguous sequence discrimination. This requires $\{|\psi_\sigma\rangle\}$ to be linearly independent, a condition that is satisfied (for any $k \geqslant 1$) if and only if $\{|\psi_i\rangle\}$ is linearly independent [17]. In other words, any given sequence of unknown pure states can be correctly determined with nonzero probability if and only if it is composed of states drawn from a linearly independent set.

Let us now assume that $\{|\psi_i\rangle\}$ is a set of linearly independent states and further assume that they are equally likely, i.e., $p_i = \frac{1}{N}$ for all $i = 1, \ldots, N$. This implies that the elements of $\{|\psi_\sigma\rangle\}$ are also linearly independent and equally likely with $p_\sigma = \frac{1}{N^k}$. Since the elements of $\{|\psi_\sigma\rangle\}$ are linearly independent, they can be unambiguously distinguished. A lower bound on the optimum success probability can be easily obtained.

Lemma 1. Let p and $p_{N,k}$ be the respective probabilities for unambiguous optimal discrimination among the elements of $\{|\psi_i\rangle\}$ and $\{|\psi_\sigma\rangle\}$. Then

$$p_{N,k} \geqslant p^k. \tag{4}$$

Proof. First note that every member of a given sequence is an element of $\{|\psi_i\rangle\}$. Let the optimal measurement that unambiguously distinguishes between the elements of $\{|\psi_i\rangle\}$ be $\mathbb{M}$. Then, by performing this measurement on individual members of the sequence, we can determine the state of each

of them with probability p. Thus the state of the sequence can be correctly determined with probability p^k (note that for the lower bound to hold the probability distribution need not be uniform). ■

The lower bound in (4) is obtained by the strategy that unambiguously determines the state of each member of the sequence separately. However, such a strategy could well be suboptimal. The reasoning goes as follows: Since $\{|\psi_\sigma\rangle\}$ is a collection of linearly independent product states, to optimally distinguish between them, a joint measurement on the whole system may be necessary and, if so, inequality (4) would be strict. Indeed, there are instances where joint measurements are required to optimally distinguish between product states (see, e.g., [22–24]).

The main contribution of this paper is to show that if the states $|\psi_i\rangle$, in addition to being linearly independent, have the property that their mutual inner products are all real and equal, then equality holds in (4). Therefore, the optimum probability to unambiguously determine the state of an unknown sequence, whose elements are drawn with equal probability from a set of linearly independent states with real and equal inner products, can be achieved by measuring the members of the sequence individually.

The following results are proved in [20]. The first gives us the condition under which a collection of pure states, with inner products real and equal, can be linearly independent.

Lemma 2 (from [20]). Let $S_N = \{|\psi_i\rangle : 2 \leqslant i \leqslant N\}$ be a set of pure states with the property $\langle\psi_i|\psi_j\rangle = s \in \mathbb{R}$ for $i \neq j$. The states are linearly independent if and only if $s \in (-\frac{1}{N-1}, 1)$.

The lemma tells us that once we require the inner products to all be real and equal to, say, s, then the states $|\psi_i\rangle$ cannot be linearly independent for all permissible values of s; they are linearly independent provided $s \in (-\frac{1}{N-1}, 1)$. The proof follows by requiring the Gram determinant to be greater than 0, which is an equivalent criterion for linear independence.

For a set of linearly independent, equally likely pure states with real and equal inner products, the following lemma tells us how well they can be distinguished unambiguously.

Lemma 3 (from [20]). Let $S_N = \{|\psi_i\rangle : 2 \leqslant i \leqslant N\}$ be a set of equally likely, linearly independent pure states with the property $\langle\psi_i|\psi_j\rangle = s$ for $i \neq j$, where $s \in (-\frac{1}{N-1}, 1)$. Then the optimum probability for unambiguous discrimination among the states $|\psi_i\rangle$ is

$$p = \begin{cases} 1 - s, & s \in [0, 1) \\ 1 + (N-1)s, & s \in \left(-\frac{1}{N-1}, 0\right]. \end{cases}$$

The proof can be found in [20] (the result in [20] was more general and was proved for states having equal inner products, real or complex). The basic idea is to attach an ancilla with the given system (in an unknown state), apply a joint unitary transformation on the whole system, and finally measure the ancilla in an orthogonal basis. By choosing an appropriate unitary transformation, the measurement on the ancilla maps the system of interest onto the unambiguous subspace with a nonzero probability.

We now state our main result.

Theorem 1. Let $S_{N,k} = \{|\psi_\sigma\rangle \equiv |\psi_{\sigma(1)}\rangle \otimes \cdots \otimes |\psi_{\sigma(k)}\rangle : \sigma \in \mathscr{F}(k, N)\}$ be the set of all sequences of k states, where each member of a sequence is drawn from S_N (defined in Lemma 3) with equal probability (hence, the sequences are all equiprobable). Then the optimum probability of unambiguous discrimination between the elements of $S_{N,k}$ is

$$p_{N,k} = \begin{cases} (1-s)^k, & s \in [0, 1) \\ [1 + (N-1)s]^k, & s \in \left(-\frac{1}{N-1}, 0\right]. \end{cases}$$

This probability is achievable by measuring the individual systems forming a sequence.

From Lemma 3 and Theorem 1 we see that $p_{N,k} = p^k$ for all $s \in (-\frac{1}{N-1}, 1)$. We will prove this theorem by solving the optimality conditions of a semidefinite program. So we proceed by formulating the unambiguous state discrimination problem as an SDP and deriving the dual problem.

III. SDP FORMULATION

Given a set of N linearly independent pure states $|\chi_i\rangle$ with prior probabilities η_i, the problem of unambiguous discrimination can be cast as an SDP [18,19]. The primal problem is

$$\begin{aligned} \underset{\boldsymbol{p}}{\text{maximize}} \quad & \boldsymbol{\eta} \cdot \boldsymbol{p} \\ \text{subject to} \quad & \Gamma - P \succeq 0, \\ & \boldsymbol{p} \succeq 0. \end{aligned} \tag{5}$$

Here $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_N)$ and $\boldsymbol{p} = (p_1, \ldots, p_N)$, where p_i is the SDP variable representing the probability of successfully detecting the input $|\chi_i\rangle$; Γ is the Gram matrix whose elements are $\Gamma_{ij} = \langle\chi_i|\chi_j\rangle$ and $P = \text{diag}(p_1, \ldots, p_N)$. The first constraint says that the matrix $\Gamma - P$ should be positive semidefinite and the second constraint is simply the positive semidefiniteness of the probabilities p_i.

To construct the dual SDP, we first construct the Lagrangian

$$L(\boldsymbol{p}, Z, \boldsymbol{z}) = \boldsymbol{\eta} \cdot \boldsymbol{p} + \text{tr}[(\Gamma - P)Z] + \boldsymbol{z} \cdot \boldsymbol{p},$$

where the dual variable Z is an $N \times N$ real symmetric matrix and $\boldsymbol{z}$ is a real N-tuple. If $Z, \boldsymbol{z} \succeq 0$, then $L(\boldsymbol{p}, Z, \boldsymbol{z}) \geqslant \boldsymbol{\eta} \cdot \tilde{\boldsymbol{p}}$ for any feasible solution $\tilde{\boldsymbol{p}}$ of the primal SDP. Therefore, the inequality must also hold for the optimum $\boldsymbol{p}$, say, $\boldsymbol{p}^*$, which implies that $L(\boldsymbol{p}^*, Z, \boldsymbol{z}) \geqslant \boldsymbol{\eta} \cdot \boldsymbol{p}^*$. With this in mind, we define the Lagrange dual function

$$g(Z, \boldsymbol{z}) = \sup_{\boldsymbol{p}} L(\boldsymbol{p}, Z, \boldsymbol{z})$$

and note that it satisfies $g(Z, \boldsymbol{z}) \geqslant \max_{\boldsymbol{p}} \boldsymbol{\eta} \cdot \boldsymbol{p}$. The dual SDP seeks to

$$\begin{aligned} \underset{Z, \boldsymbol{z}}{\text{minimize}} \quad & g(Z, \boldsymbol{z}) \\ \text{subject to} \quad & Z, \boldsymbol{z} \succeq 0. \end{aligned}$$

Consider a family of $N \times N$ matrices $\{F_i\}$ for $i = 1, \ldots, N$, where each F_i has exactly one nonzero element -1 at position (i, i). Now note that

$$\begin{aligned} g(Z, \boldsymbol{z}) &= \sup_{\boldsymbol{p}} L(\boldsymbol{p}, Z, \boldsymbol{z}) \\ &= \sup_{\boldsymbol{p}} \{\boldsymbol{\eta} \cdot \boldsymbol{p} + \text{tr}[(\Gamma - P)Z] + \boldsymbol{z} \cdot \boldsymbol{p}\} \end{aligned}$$

$$= \sup_{\boldsymbol{p}} \left(\sum_{i=1}^{N} p_i [z_i + \eta_i + \mathrm{tr}(F_i Z)] + \mathrm{tr}(\Gamma Z) \right)$$
$$= \begin{cases} \mathrm{tr}(\Gamma Z) & \text{if } z_i + \eta_i + \mathrm{tr}(F_i Z) = 0 \,\forall\, i \\ \infty & \text{otherwise.} \end{cases}$$

Therefore, the dual problem becomes

$$\begin{aligned} \underset{Z,z}{\text{minimize}} \quad & \mathrm{tr}(\Gamma Z) \\ \text{subject to} \quad & z_i + \eta_i + \mathrm{tr}(F_i Z) = 0, \\ & Z, z \succeq 0. \end{aligned}$$

In the next section we prove the main result.

IV. PROOF OF THEOREM 1

Proof outline. First note that the primal problem is convex and there exists a $\boldsymbol{p}$ (equivalently P) that is strictly feasible. Under these conditions, Slater's theorem guarantees that the strong duality holds, and the duality gap is zero. The way we will proceed is the following. We will present an ansatz P and obtain a solution for the primal problem, which is not necessarily optimal. Then we will present candidates for the dual variables Z and z and show that this makes the dual value equal to the primal one. Since strong duality holds, this implies that our ansatz must be the optimal solution for the primal problem.

A. Technical lemmas

First we will prove a couple of technical lemmas.

Lemma 4. If A is a block matrix with each block being a diagonal matrix of the same size, then A is similar to a block-diagonal matrix.

Proof. Let

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix},$$

where the A_{ij}'s are diagonal matrices of size $m \times m$. Let α_{ijk} denote the k-th diagonal entry of A_{ij}. Then

$$A = \sum_{i,j=1}^{n} \sum_{k=1}^{m} \alpha_{ijk} E_{ij}^{(n)} \otimes E_{kk}^{(m)}, \tag{6}$$

where $E_{\mu\nu}^{(t)}$ is a $t \times t$ matrix whose (μ, ν)th entry is 1 and all other entries are 0. Now, if U and V are square matrices, then $U \otimes V = P^{-1}(V \otimes U)P$ for some permutation matrix P that depends only on the dimensions of U and V [25]. It then follows that A is similar to $\sum_{i,j=1}^{n} \sum_{k=1}^{m} \alpha_{ijk} E_{kk}^{(m)} \otimes E_{ij}^{(n)}$, which has the block-diagonal form

$$\begin{pmatrix} D_1 & 0 & \cdots & 0 \\ 0 & D_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & D_m \end{pmatrix},$$

where the (i, j) entry of D_k is α_{ijk}. ■

Lemma 5. Let Λ be a real $n \times n$ matrix of the form

$$\Lambda = \begin{pmatrix} 1 & r & \cdots & r \\ r & 1 & \cdots & r \\ \vdots & \vdots & \ddots & \vdots \\ r & r & \cdots & 1 \end{pmatrix}, \quad r \in \mathbb{R}. \tag{7}$$

The distinct (except when $r = 0$) eigenvalues of Λ are $1 - r$ and $1 + (n-1)r$.

Proof. The characteristic polynomial is

$$\det(\Lambda - \lambda I) = \det \begin{pmatrix} 1-\lambda & r & \cdots & r \\ r & 1-\lambda & \cdots & r \\ \vdots & \vdots & \ddots & \vdots \\ r & r & \cdots & 1-\lambda \end{pmatrix} = \det \begin{pmatrix} h-\lambda & r & \cdots & r \\ h-\lambda & 1-\lambda & \cdots & r \\ \vdots & \vdots & \ddots & \vdots \\ h-\lambda & r & \cdots & 1-\lambda \end{pmatrix}, \quad \begin{cases} C_1 \to C_1 + \cdots + C_n \\ h = 1 + (n-1)r \end{cases}$$
$$= (h-\lambda) \det \begin{pmatrix} 1 & r & \cdots & r \\ 1 & 1-\lambda & \cdots & r \\ \vdots & \vdots & \ddots & \vdots \\ 1 & r & \cdots & 1-\lambda \end{pmatrix} = (h-\lambda) \det \begin{pmatrix} 1 & r & \cdots & r \\ 0 & 1-r-\lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1-r-\lambda \end{pmatrix}, \quad \begin{cases} R_i \to R_i - R_1 \\ i \neq 1 \end{cases}$$
$$= (h-\lambda)(1-r-\lambda)^{n-1}.$$

The distinct (except for $r = 0$) eigenvalues are therefore $1 - r$ and $h = 1 + (n-1)r$. ■

B. Eigenvalues of the Gram matrix

First we would like to calculate the eigenvalues of $\Gamma(N, k)$, the Gram matrix of the states of $S_{N,k}$. We begin by finding the eigenvalues of $\Gamma(N, 1)$, which is a real $N \times N$ matrix

$$\Gamma(N, 1) = \begin{pmatrix} 1 & s & \cdots & s \\ s & 1 & \cdots & s \\ \vdots & \vdots & \ddots & \vdots \\ s & s & \cdots & 1 \end{pmatrix}, \quad s \in \left(-\frac{1}{N-1}, 1 \right). \tag{8}$$

The eigenvalues of $\Gamma(N, 1)$ are immediately obtained by applying Lemma 5.

Lemma 6. The distinct (except when $s = 0$) eigenvalues of $\Gamma(N, 1)$ are $1 - s$ and $1 + (N-1)s$, where $s \in (-\frac{1}{N-1}, 1)$.

The proof follows from Lemma 5.

We will use Lemmas 4 and 5 to calculate the eigenvalues of $\Gamma(N, k)$.

Theorem 2. The eigenvalues of $\Gamma(N, k)$ are of the form $(1-s)^a[1 + (N-1)s]^b$ for non-negative integers a and b satisfying $a + b = k$.

Proof. We will prove the theorem by induction on k. For the proof, we will need the following result that shows the connection between $\Gamma(N, l+1)$ and $\Gamma(N, l)$, where $l \in \mathbb{N}$.

Lemma 7. The Gram matrix of the states of $S_{N,l+1}$ is given by

$$\Gamma(N, l+1) = \begin{bmatrix} \Gamma(N,l) & s\Gamma(N,l) & \cdots & s\Gamma(N,l) \\ s\Gamma(N,l) & \Gamma(N,l) & \cdots & s\Gamma(N,l) \\ \vdots & \vdots & \ddots & \vdots \\ s\Gamma(N,l) & s\Gamma(N,l) & \cdots & \Gamma(N,l) \end{bmatrix}. \tag{9}$$

Proof. For ease of understanding, denote the elements of $S_{N,l}$ by $|\phi_i\rangle$, where $i = 1, \ldots, N^l$. Then the elements of $S_{N,l+1}$ are of the form $|\phi_i\rangle \otimes |\psi_j\rangle$ for $i = 1, \ldots, N^l$ and $j = 1, \ldots, N$. Then it holds that $\Gamma(N, l+1)$ must be of the form given by (9), where the (x, y)-th entry of the (i, j)-th block is the inner product between $|\phi_x\rangle \otimes |\psi_i\rangle$ and $|\phi_y\rangle \otimes |\psi_j\rangle$. ■

From Lemma 6 we know the result holds for $k = 1$. Now assume the result is true for $k = l$.

Let G be a matrix such that $G\Gamma(N, l)G^{-1}$ is diagonal of the form

$$\alpha = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_m \end{pmatrix},$$

where $m = N^l$ and let

$$R = \begin{pmatrix} G & & \\ & \ddots & \\ & & G \end{pmatrix},$$

where the number of G matrices along its diagonal is N. Then

$$R\Gamma(N, l+1)R^{-1} = \begin{bmatrix} G\Gamma(N,l)G^{-1} & sG\Gamma(N,l)G^{-1} & \cdots & sG\Gamma(N,l)G^{-1} \\ sG\Gamma(N,l)G^{-1} & G\Gamma(N,l)G^{-1} & \cdots & sG\Gamma(N,l)G^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ sG\Gamma(N,l)G^{-1} & sG\Gamma(N,l)G^{-1} & \cdots & G\Gamma(N,l)G^{-1} \end{bmatrix}$$
$$= \begin{pmatrix} \alpha & s\alpha & \cdots & s\alpha \\ s\alpha & \alpha & \cdots & s\alpha \\ \vdots & \vdots & \ddots & \vdots \\ s\alpha & s\alpha & \cdots & \alpha \end{pmatrix},$$

where we have used $\alpha = G\Gamma(N, l)G^{-1}$.

By Lemma 4, $\Gamma(n, l+1)$ is therefore similar to a block-diagonal matrix

$$\begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_m \end{pmatrix},$$

where

$$D_i = \begin{pmatrix} \alpha_i & s\alpha_i & \cdots & s\alpha_i \\ s\alpha_i & \alpha_i & \cdots & s\alpha_i \\ \vdots & \vdots & \ddots & \vdots \\ s\alpha_i & s\alpha_i & \cdots & \alpha_i \end{pmatrix} = \alpha_i \Gamma(N, 1).$$

Now, by the induction hypothesis,

$$\alpha_i = (1-s)^a [1 + (N-1)s]^b$$

for non-negative integers a and b satisfying $a + b = l$. Thus the eigenvalues of D_i are $(1-s)^{a+1}[1 + (N-1)s]^b$ or $(1-s)^a[1 + (N-1)s]^{b+1}$. Therefore, the result holds for $k = l + 1$, proving the theorem. ■

C. Feasible solution for the primal problem

Having found the eigenvalues of $\Gamma(N, k)$, we will now guess an ansatz for $\boldsymbol{p}$ (equivalently P) and then show that $\Gamma(N, k) - P(N, k)$ is positive semidefinite.

Theorem 3. $\Gamma(N, k) - P(N, k)$ is positive semidefinite, where

$$P(N, k) = \begin{cases} (1-s)^k I, & s \in [0, 1) \\ [1 + (N-1)s]^k I, & s \in (-\frac{1}{N-1}, 0] \end{cases}$$

and I is the $N^k \times N^k$ identity matrix.

Proof. First note that $\Gamma(N, k)$ and $P(N, k)$ are diagonalizable in the same basis as $P(N, k)$ is a scalar multiple of the identity. To show that $[\Gamma(N, k) - P(N, k)]$ is positive semidefinite, we use the fact that when two positive-semidefinite matrices M_1 and M_2 are diagonalizable in the same basis, $M_1 - M_2$ is positive semidefinite if the smallest eigenvalue of M_1 is greater than or equal to the largest eigenvalue of M_2.

First consider the case $s \in [0, 1)$. We see that

$$(1-s)^a[1 + (N-1)s]^b \geqslant (1-s)^a(1-s)^b = (1-s)^k$$

since $[1 + (N-1)s]^b \geqslant (1-s)^b$ as $N \geqslant 2$ and $a + b = k$. Now consider $s \in (-\frac{1}{N-1}, 0]$. Here we have

$$(1-s)^a[1 + (N-1)s]^b \geqslant [1 + (N-1)s]^a[1 + (N-1)s]^b$$
$$= [1 + (N-1)s]^k$$

since $[1 + (N-1)s]^b \leqslant 1$ and $(1-s)^a \geqslant 1$ for $s \in (-\frac{1}{N-1}, 0]$. Therefore, $\Gamma(N, k) - P(N, k)$ is positive semidefinite for $s \in (-\frac{1}{N-1}, 1)$. ■

Theorem 3 shows that the ansatz

$$P(N, k) = \begin{cases} (1-s)^k I, & s \in [0, 1) \\ [1 + (N-1)s]^k I, & s \in \left(-\frac{1}{N-1}, 0\right] \end{cases} \tag{10}$$

will work if there exist positive-semidefinite Z and a vector $z \succeq \mathbf{0}$ such that

$$\mathrm{tr}[\Gamma(N,k)Z] = \begin{cases} (1-s)^k, & s \in [0,1) \\ [1+(N-1)s]^k, & s \in \left(-\frac{1}{N-1}, 0\right] \end{cases} \tag{11}$$

and $z_i + \eta_i + \mathrm{tr}(F_i Z) = 0$ for all $i = 1, \ldots, N^k$.

D. Optimal solution

First we show that one can indeed find a suitable Z satisfying (11).

Theorem 4. For any choice of $N, k \in \mathbb{N}$ there exists an $N^k \times N^k$ positive-semidefinite matrix $Z(N,k)$ with diagonal entries $1/N^k$ such that

$$\mathrm{tr}[\Gamma(N,k)Z(N,k)] = \begin{cases} (1-s)^k, & s \in [0,1) \\ [1+(N-1)s]^k, & s \in \left(-\frac{1}{N-1}, 0\right]. \end{cases} \tag{12}$$

Proof. To prove the theorem we proceed by induction on k. First consider the case $s \in [0,1)$. For $k = 1$ let

$$Z(N,1) = \frac{1}{N}\begin{pmatrix} 1 & -\frac{1}{(N-1)} & \cdots & -\frac{1}{(N-1)} \\ -\frac{1}{(N-1)} & 1 & \cdots & -\frac{1}{(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{1}{(N-1)} & -\frac{1}{(N-1)} & \cdots & 1 \end{pmatrix}.$$

Then by Lemma 5 the eigenvalues of $Z(N,1)$ are $\frac{1}{N-1}$ and 0. Hence it is positive semidefinite. With the above choice of $Z(N,1)$ we have

$$\mathrm{tr}[\Gamma(N,1)Z(N,1)] = \frac{1}{N}\mathrm{tr}\left[\begin{pmatrix} 1 & s & \cdots & s \\ s & 1 & \cdots & s \\ \vdots & \vdots & \cdots & \vdots \\ s & s & \cdots & 1 \end{pmatrix}\begin{pmatrix} 1 & -\frac{1}{(N-1)} & \cdots & -\frac{1}{(N-1)} \\ -\frac{1}{(N-1)} & 1 & \cdots & -\frac{1}{(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{1}{(N-1)} & -\frac{1}{(N-1)} & \cdots & 1 \end{pmatrix}\right]$$
$$= 1 - s.$$

Now assume the result holds for $k = l$, i.e., $\mathrm{tr}[\Gamma(N,l)Z(N,l)] = (1-s)^l$ and $Z(N,l)$ is positive semidefinite. First we will show that the trace equality holds for $k = l+1$ for $l \geqslant 1$. Define

$$Z(N,l+1) = \frac{1}{N}\begin{pmatrix} Z(N,l) & -\frac{Z(N,l)}{(N-1)} & \cdots & -\frac{Z(N,l)}{(N-1)} \\ -\frac{Z(N,l)}{(N-1)} & Z(N,l) & \cdots & -\frac{Z(N,l)}{(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{Z(N,l)}{(N-1)} & -\frac{Z(N,l)}{(N-1)} & \cdots & Z(N,l) \end{pmatrix},$$
$$l \geqslant 1.$$

Then

$$\begin{aligned} \mathrm{tr}[\Gamma(N,l+1)Z(N,l+1)] &= \mathrm{tr}[\Gamma(N,l)Z(N,l)] \\ &\quad - s\,\mathrm{tr}[\Gamma(N,l)Z(N,l)] \\ &= (1-s)\mathrm{tr}[\Gamma(N,l)Z(N,l)] \\ &= (1-s)^{l+1}, \end{aligned}$$

which proves the equality holds for $k = l+1$.

What remains to be shown is that $Z(N,l+1)$ is positive semidefinite. The eigenvalues of $Z(N,l+1)$ are obtained by applying Theorem 2 with $s = -\frac{1}{N-1}$. The eigenvalues are either 0 or $\frac{1}{N}(\frac{N}{N-1})^{l+1}$, where the nonzero eigenvalue is obtained for $a = l+1$ and $b = 0$. Therefore, $Z(N,k)$ is positive semidefinite for $k = l+1$. Since we have already shown that $Z(N,1)$ is positive semidefinite, $Z(N,k)$ is positive semidefinite, for all $k \geqslant 1$.

Now consider $s \in (-\frac{1}{N-1}, 0]$. For $k = 1$ let

$$Z(N,1) = \frac{1}{N}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Once again, by applying Lemma 6 we find that the eigenvalues of $Z(N,1)$ are 1 and 0. Hence it is positive semidefinite.

Now with the above choice of $Z(N,1)$,

$$\begin{aligned} &\mathrm{tr}[\Gamma(N,1)Z(N,1)] \\ &= \frac{1}{N}\mathrm{tr}\left[\begin{pmatrix} 1 & s & \cdots & s \\ s & 1 & \cdots & s \\ \vdots & \vdots & \cdots & \vdots \\ s & s & \cdots & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}\right] \\ &= 1 + (N-1)s. \end{aligned}$$

As before, we assume the result holds for $k = l$, i.e., $\mathrm{tr}[\Gamma(N,l)Z(N,l)] = [1+(N-1)s]^l$ and $Z(N,l)$ is positive semidefinite. We first show that the trace equality holds for $k = l+1$ for $l \geqslant 1$. Define

$$Z(N,l+1) = \frac{1}{N}\begin{pmatrix} Z(N,l) & Z(N,l) & \cdots & Z(N,l) \\ Z(N,l) & Z(N,l) & \cdots & Z(N,l) \\ \vdots & \vdots & \ddots & \vdots \\ Z(N,l) & Z(N,l) & \cdots & Z(N,l) \end{pmatrix},$$
$$l \geqslant 1.$$

Then

$$\begin{aligned}&\mathrm{tr}[\Gamma(N,l+1)Z(N,l+1)]\\&\quad=\mathrm{tr}[\Gamma(N,l)Z(N,l)]+(N-1)s\,\mathrm{tr}[\Gamma(N,l)Z(N,l)]\\&\quad=[1+(N-1)s]\mathrm{tr}[\Gamma(N,l)Z(N,l)]\\&\quad=[1+(N-1)s]^{l+1}.\end{aligned}$$

Therefore, the trace equality holds for $k=l+1$. What remains to be shown is that $Z(N,l+1)$ is positive semidefinite. Now note that $Z(N,l+1)$ is an $N^{l+1}\times N^{l+1}$ matrix whose all elements are $\frac{1}{N^{l+1}}$. Therefore, its eigenvalues are 0 and 1; hence, $Z(N,l+1)$ is positive semidefinite. Since we have already shown $Z(N,1)$ is positive semidefinite, this completes the proof.

Thus we have proved the existence of positive-semidefinite $Z(N,k)$ that satisfies the trace equality (12) for all $s\in(-\frac{1}{N-1},1)$. ■

Since $\eta_i=1/N^k$ for all i, by choosing $\boldsymbol{z}=\boldsymbol{0}$ (null vector), one has $z_i+\eta_i+\mathrm{tr}(F_iZ)=0$ for all i. This completes the proof of our main result, Theorem 1.

Let us briefly go through the key elements of the proof once again. The proof was based on guessing an appropriate primal variable $\boldsymbol{p}$ (equivalently P) and showing its optimality. Since the primal problem is convex with a nonempty feasible set, strong duality holds. We showed that there exist feasible dual variables Z and $\boldsymbol{z}$ such that $\mathrm{tr}(\Gamma Z)=\boldsymbol{\eta}\cdot\boldsymbol{p}$, which is the dual objective function; hence, our guessed $\boldsymbol{p}$ is the optimal solution.

V. CONCLUSION

We considered the problem of unambiguously determining the state $|\psi_\sigma\rangle$ of an unknown quantum sequence of length $k\geqslant 1$, where the elements of the given sequence are drawn with equal probability from a set of linearly independent pure states $S_N=\{|\psi_i\rangle:2\leqslant i\leqslant N\}$ with real and equal inner products. This (and even the most general one without any assumption about inner product and/or prior probabilities) can be posed as an unambiguous state discrimination problem, where the objective is to discriminate between the states of all such possible sequences.

Let $S_{N,k}=\{|\psi_\sigma\rangle\}$ be the set of all possible sequences of length k. Let p and $p_{N,k}$ be the optimum probabilities for unambiguously discriminating between the elements of S_N and $S_{N,k}$, respectively. A simple argument shows that $p_{N,k}\geqslant p^k$, where the lower bound is achievable by measuring individual members of the sequence. Since any sequence of length k is a composite quantum system comprising k subsystems, one might expect the inequality, in general, to be strict, i.e., $p_{N,k}>p^k$, and to achieve the optimum value, a joint measurement is required.

Following earlier works on unambiguous state discrimination [18,19], we formulated the sequence discrimination problem as an SDP and calculated the optimum probability by solving the optimality conditions. In particular, we showed that $p_{N,k}=p^k$; thus, the optimum value is achieved by performing measurements on the individual members of the sequence.

Several problems in this context are still left open. First is where the inner products of the states $|\psi_i\rangle$ belonging to the parent set S_N are equal but complex. For $k=1$, this reduces to the standard unambiguous state discrimination problem which has been solved completely [20]. However, we could not solve the sequence discrimination problem in this scenario using the same approach.

Second is a more general scenario where S_N is simply a set of linearly independent pure states without any restrictions on the inner products. In this case, we carried out thousands of numerical SDP experiments with a limited number of parent states and very short sequences, namely, $N=3$ and $k=2,3$, and the results (assuming uniform prior probabilities) seemed to suggest that the optimum value, once again, is achievable by measuring the individual members without requiring any joint measurement.

In our scenario, as well as in more general ones (which we could not solve), repetitions of states are allowed in a sequence. The third problem considers the situation where it is not. Restrict $k<N$ and by $S'_{N,k}$ denote the set of sequences of length k, where no element is repeated. If we let $\mathscr{G}(k,N)$ be the set of injective functions from $[k]$ to $[N]$, then

$$S'_{N,k}=\{|\psi_{\tau(1)}\rangle\otimes\cdots\otimes|\psi_{\tau(k)}\rangle:\tau\in\mathscr{G}(k,N)\}.$$

The cardinality of this set is ${}^NP_k=\dfrac{N!}{(N-k)!}$ (note that the injective functions from $[k]$ to $[N]$ for $k\leqslant N$ correspond to the permutation of k objects chosen from N objects). Now assume that the inner products of the states $|\psi_i\rangle$ are equal and positive, say, $s>0$. Then $S'_{N,k}\subset S_{N,k}$, where $S_{N,k}$ is the set of sequences considered in this paper. Under these restricted conditions, numerical experiments ($N=3$, $k=3$) still suggest that the optimal probability for distinguishing between the elements of $S'_{N,k}$ unambiguously once again obeys $(1-s)^k$. However, for arbitrary values of both N and k, whether one could benefit from collective measurements in this scenario is an interesting problem to consider in the future.

To summarize, sequence discrimination considers the problem of distinguishing between sequences of some fixed length whose members are drawn from a set of pure states, the parent set. In an unambiguous sequence discrimination problem, the parent set must consist of linearly independent states; otherwise unambiguous discrimination will not be possible. We showed that if the elements of the parent set have the property that the inner products are all real and equal, then optimal unambiguous sequence discrimination does not require collective measurements and measuring the individual members will suffice. However, whether collective measurements would be necessary for general scenarios, without assumptions about inner products or prior probabilities, remains open, and so far our numerical attempts have failed to yield a counterexample.

[1] A. Chefles, Quantum state discrimination, Contemp. Phys. **41**, 401 (2000).
[2] S. M. Barnett and S. Croke, Quantum state discrimination, Adv. Opt. Photon. **1**, 238 (2009).
[3] J. Bae and L.-C. Kwek, Quantum state discrimination and its applications, J. Phys. A: Math. Theor. **48**, 083001 (2015).
[4] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[5] I. D. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987).
[6] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A **126**, 303 (1988).
[7] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988).
[8] G. Jaeger and A. Shimony, Optimal distinction between two non-orthogonal quantum states, Phys. Lett. A **197**, 83 (1995).
[9] A. Chefles, Unambiguous discrimination between linearly independent quantum states, Phys. Lett. A **239**, 339 (1998).
[10] A. Peres and D. Terno, Optimal distinction between non-orthogonal quantum states, J. Phys. A: Math. Gen. **31**, 7105 (1998).
[11] A. Chefles and S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states, Phys. Lett. A **250**, 223 (1998).
[12] M. A. Jafarizadeh, M. Rezaei, N. Karimi, and A. R. Amiri, Optimal unambiguous discrimination of quantum states, Phys. Rev. A **77**, 042314 (2008).
[13] S. Pang and S. Wu, Optimum unambiguous discrimination of linearly independent pure states, Phys. Rev. A **80**, 052320 (2009).
[14] J. A. Bergou, U. Futschik, and E. Feldman, Optimal unambiguous discrimination of pure quantum states, Phys. Rev. Lett. **108**, 250502 (2012).
[15] S. Bandyopadhyay, Unambiguous discrimination of linearly independent pure quantum states: Optimal average probability of success, Phys. Rev. A **90**, 030301(R) (2014).
[16] Y. Sun, M. Hillery, and J. A. Bergou, Optimum unambiguous discrimination between linearly independent nonorthogonal quantum states and its optical realization, Phys. Rev. A **64**, 022311 (2001).
[17] A. Chefles, E. Andersson, and I. Jex, Unambiguous comparison of the states of multiple quantum systems, J. Phys. A: Math. Gen. **37**, 7315 (2004).
[18] H. Sugimoto, T. Hashimoto, M. Horibe, and A. Hayashi, Complete solution for unambiguous discrimination of three pure states with real inner products, Phys. Rev. A **82**, 032338 (2010).
[19] Y. Eldar, A semidefinite programming approach to optimal unambiguous discrimination of quantum states, IEEE Trans. Inf. Theory **49**, 446 (2003).
[20] L. Roa, C. Hermann-Avigliano, R. Salazar, and A. B. Klimov, Conclusive discrimination among N equidistant pure states, Phys. Rev. A **84**, 014302 (2011).
[21] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).
[22] A. Peres and W. K. Wootters, Optimal detection of quantum information, Phys. Rev. Lett. **66**, 1119 (1991).
[23] S. Massar and S. Popescu, Optimal extraction of information from finite quantum ensembles, Phys. Rev. Lett. **74**, 1259 (1995).
[24] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Phys. Rev. A **59**, 1070 (1999).
[25] H. V. Henderson and S. R. Searle, The vec-permutation matrix, the vec operator and Kronecker products: A review, Linear Multilinear Algebra **9**, 271 (1981).