arXiv:quant-ph/0312061 v1 7 Dec 2003

Optimal quantum detectors for unambiguous detection of mixed states

Yonina C. Eldar

*Department of Electrical Engineering, Technion—Israel Institute of Technology, Haifa 32000, Israel**

Mihailo Stojnic and Babak Hassibi

Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125, USA†

(Dated: December 7, 2003)

We consider the problem of designing an optimal quantum detector that distinguishes unambiguously between a collection of mixed quantum states. Using arguments of duality in vector space optimization, we derive necessary and sufficient conditions for an optimal measurement that maximizes the probability of correct detection. We show that the previous optimal measurements that were derived for certain special cases satisfy these optimality conditions. We then consider state sets with strong symmetry properties, and show that the optimal measurement operators for distinguishing between these states share the same symmetries, and can be computed very efficiently by solving a reduced size semidefinite program.

PACS numbers: 03.67.Hk

I. INTRODUCTION

The problem of detecting information stored in the state of a quantum system is a fundamental problem in quantum information theory. Several approaches have emerged to distinguishing between a collection of non-orthogonal quantum states. In one approach, a measurement is designed to maximize the probability of correct detection [1, 2, 3, 4, 5, 6, 7, 7, 8, 9]. A more recent approach, referred to as unambiguous detection [10, 11, 12, 13, 14, 15, 16, 17, 18], is to design a measurement that with a certain probability returns an inconclusive result, but such that if the measurement returns an answer, then the answer is correct with probability 1. An interesting alternative approach for distinguishing between a collection of quantum states, which is a combination of the previous two approaches, is to allow for a certain probability of an inconclusive result, and then maximize the probability of correct detection [18, 19, 20].

We consider a quantum state ensemble consisting of m density operators $\{\rho_i, 1 \leq i \leq m\}$ on an n-dimensional complex Hilbert space $\mathcal{H}$, with prior probabilities $\{p_i > 0, 1 \leq i \leq m\}$. A pure-state ensemble is one in which each density operator ρ_i is a rank-one projector $|\phi_i\rangle\langle\phi_i|$, where the vectors $|\phi_i\rangle$, though evidently normalized to unit length, are not necessarily orthogonal. Our problem is to design a quantum detector to distinguish unambiguously between the states $\{\rho_i\}$.

Chefles [15] showed that a necessary and sufficient condition for the existence of unambiguous measurements for distinguishing between a collection of *pure* quantum states is that the states are linearly independent. Necessary and sufficient conditions on the optimal measurement minimizing the probability of an inconclusive result for pure states were derived in [17]. The optimal measurement when distinguishing between a broad class of symmetric pure-state sets was also considered in [17].

The problem of unambiguous detection between *mixed* state ensembles has received considerably less attention. Rudolph *et al.* [21] showed that unambiguous detection between mixed quantum states is possible as long as one of the density operators in the ensemble has a non-zero overlap with the intersection of the kernels of the other density operators. They then consider the problem of unambiguous detection between two mixed quantum states, and derive upper and lower bounds on the probability of an inconclusive result. They also develop a closed form solution for the optimal measurement in the case in which both states have kernels of dimension 1.

In this paper we develop a general framework for unambiguous state discrimination between a collection of mixed quantum states, which can be applied to any number of states with arbitrary prior probabilities. For our measurement we consider general positive operator-valued measures [2, 22], consisting of $m+1$ measurement operators. We derive a set of necessary and sufficient conditions for an optimal measurement that minimizes the probability of an inconclusive result, by exploiting principles of duality theory in vector space optimization. We then show that the previous optimal measurements that were derived for certain special cases satisfy these optimality conditions.

Next, we consider geometrically uniform (GU) and compound GU state sets [7, 8, 23], which are state sets with strong symmetry properties. We show that the optimal measurement operators for unambiguous discrimination between such state sets are also GU and CGU respectively, with generators that can be computed very efficiently by solving a reduced size semidefinite program.

The paper is organized as follows. In Section II, we provide a statement of our problem. In Section III we develop the necessary and sufficient conditions for optimality using Lagrange duality theory. Some special cases are

*Electronic address: yonina@ee.technion.ac.il

†Electronic address: mihailo,hassibi@systems.caltech.edu

considered in Section IV. In Section V we consider the problem of distinguishing between a collection of states with a broad class of symmetry properties.

II. PROBLEM FORMULATION

Assume that a quantum channel is prepared in a quantum state drawn from a collection of mixed states, represented by density operators $\{\rho_i, 1 \leq i \leq m\}$ on an n-dimensional complex Hilbert space $\mathcal{H}$. We assume without loss of generality that the eigenvectors of $\rho_i, 1 \leq i \leq m$, collectively span[31] $\mathcal{H}$.

To detect the state of the system a measurement is constructed comprising $m+1$ measurement operators $\{\Pi_i, 0 \leq i \leq m\}$ that satisfy

$$\begin{aligned} \Pi_i \geq 0, \quad 0 \leq i \leq m; \\ \sum_{i=0}^m \Pi_i = I. \end{aligned} \tag{1}$$

The measurement operators are constructed so that either the state is correctly detected, or the measurement returns an inconclusive result. Thus, each of the operators $\Pi_i, 1 \leq i \leq m$ correspond to detection of the corresponding states $\rho_i, 1 \leq i \leq m$, and Π_0 corresponds to an inconclusive result.

Given that the state of the system is ρ_j, the probability of obtaining outcome i is $\mathrm{Tr}(\rho_j \Pi_i)$. Therefore, to ensure that each state is either correctly detected or an inconclusive result is obtained, we must have

$$\mathrm{Tr}(\rho_j \Pi_i) = \eta_i \delta_{ij}, \quad 1 \leq i, j \leq m, \tag{2}$$

for some $0 \leq \eta_i \leq 1$. Since from (1), $\Pi_0 = I - \sum_{i=1}^m \Pi_i$, (2) implies that $\mathrm{Tr}(\rho_i \Pi_0) = 1 - \eta_i$, so that given that the state of the system is ρ_i, the state is correctly detected with probability η_i, and an inconclusive result is returned with probability $1 - \eta_i$.

It was shown in [15] that for pure-state ensembles consisting of rank-one density operators $\rho_i = |\phi_i\rangle\langle\phi_i|$, (2) can be satisfied if and only if the vectors $|\phi_i\rangle$ are linearly independent. For mixed states, it was shown in [21] that (2) can be satisfied if and only if one of the density operators ρ_i has a non-zero overlap with the intersection of the kernels of the other density operators. Specifically, denote by $\mathcal{K}_i$ the null space of ρ_i and let

$$\mathcal{S}_i = \cap_{j=1, j \neq i}^m \mathcal{K}_j \tag{3}$$

denote the intersection of $\mathcal{K}_j, 1 \leq j \leq m, j \neq i$. Then to satisfy (2) the eigenvectors of Π_i must be contained in $\mathcal{S}_i$ and must not be entirely contained in $\mathcal{K}_i$. This implies that $\mathcal{K}_i$ must not be entirely contained in $\mathcal{S}_i$. Some examples of mixed states for which unambiguous detection is possible are given in [21].

If the state ρ_i is prepared with prior probability p_i, then the total probability of correctly detecting the state is

$$P_D = \sum_{i=1}^m p_i \mathrm{Tr}(\rho_i \Pi_i). \tag{4}$$

Our problem therefore is to choose the measurement operators $\Pi_i, 0 \leq i \leq m$ to maximize P_D, subject to the constraints (1) and

$$\mathrm{Tr}(\rho_j \Pi_i) = 0, \quad 1 \leq i, j \leq m, i \neq j. \tag{5}$$

To satisfy (5), Π_i must lie in $\mathcal{S}_i$ defined by (3), so that

$$\Pi_i = P_i \Pi_i P_i, \quad 1 \leq i \leq m, \tag{6}$$

where P_i is the orthogonal projection onto $\mathcal{S}_i$. Denoting by Θ_i an $n \times r$ matrix whose columns form an arbitrary orthonormal basis for $\mathcal{S}_i$, where $r = \dim(\mathcal{S}_i)$, we can express P_i as $P_i = \Theta_i \Theta_i^*$. From (6) and (1) we then have that

$$\Pi_i = \Theta_i \Delta_i \Theta_i^*, \quad 1 \leq i \leq m, \tag{7}$$

where $\Delta_i = \Theta_i^* \Pi_i \Theta_i$ is an $r \times r$ matrix satisfying

$$\begin{aligned} \Delta_i \geq 0, \quad 1 \leq i \leq m; \\ \sum_{i=1}^m \Theta_i \Delta_i \Theta_i^* \leq I. \end{aligned} \tag{8}$$

Therefore, our problem reduces to maximizing

$$P_D = \sum_{i=1}^m p_i \mathrm{Tr}(\rho_i \Theta_i \Delta_i \Theta_i^*), \tag{9}$$

subject to (8).

To show that the problem of (9) and (8) does not depend on the choice of orthonormal basis Θ_i, we note that any orthonormal basis for $\mathcal{S}_i$ can be expressed as the columns of Ψ_i, where $\Psi_i = \Theta_i U_i$ for some $r \times r$ unitary matrix U_i. Substituting Ψ_i instead of Θ_i in (9) and (8), our problem becomes that of maximizing

$$P_D = \sum_{i=1}^m p_i \mathrm{Tr}(\rho_i \Psi_i \Delta_i \Psi_i^*) = \sum_{i=1}^m p_i \mathrm{Tr}(\rho_i \Theta_i \Delta_i' \Theta_i^*), \tag{10}$$

where $\Delta_i' = U_i \Delta_i U_i^*$, subject to

$$\begin{aligned} \Delta_i \geq 0, \quad 1 \leq i \leq m; \\ \sum_{i=1}^m \Psi_i \Delta_i \Psi_i^* = \sum_{i=1}^m \Theta_i \Delta_i' \Theta_i^* \leq I. \end{aligned} \tag{11}$$

Since $\Delta_i \geq 0$ if and only if $\Delta_i' \geq 0$, the problem of (10) and (11) is equivalent to that of (9) and (8).

Equipped with the standard operations of addition and multiplication by real numbers, the space $\mathcal{B}$ of all Hermitian $n \times n$ matrices is an n^2-dimensional *real* vector space. As noted in [21], by choosing an appropriate basis for $\mathcal{B}$, the problem of maximizing P_D subject to (8) can be put in the form of a standard semidefinite programming problem, which is a convex optimization problem; for a detailed treatment of semidefinite programming problems see, *e.g.,* [24, 25, 26, 27]. By exploiting the many well known algorithms for solving semidefinite programs [27], *e.g.,* interior point methods[32] [24, 26], the optimal measurement can be computed very efficiently in polynomial time within any desired accuracy.

Using elements of duality theory in vector space optimization, in the next section we derive necessary and sufficient conditions on the measurement operators $\Pi_i = \Theta_i \Delta_i \Theta_i^*$ to maximize P_D of (9) subject to (8).

III. CONDITIONS FOR OPTIMALITY

A. Dual Problem Formulation

To derive necessary and sufficient conditions for optimality on the matrices Δ_i we first derive a dual problem, using Lagrange duality theory [28].

Denote by Λ the set of all ordered sets $\Pi = \{\Pi_i = \Theta_i\Delta_i\Theta_i^*\}_{i=1}^m$ satisfying (8) and define $J(\Pi) = \sum_{i=1}^m p_i \mathrm{Tr}(\rho_i\Theta_i\Delta_i\Theta_i^*)$. Then our problem is

$$\max_{\Pi\in\Lambda} J(\Pi). \tag{12}$$

We refer to this problem as the primal problem, and to any $\Pi \in \Lambda$ as a primal feasible point. The optimal value of $J(\Pi)$ is denoted by $\widehat{J}$.

To develop the dual problem associated with (12) we first compute the Lagrange dual function, which is given by

$$\begin{aligned} g(Z) &= \\ &= \min_{\Delta_i\geq 0}\left\{-\sum_{i=1}^m p_i\mathrm{Tr}(\rho_i\Theta_i\Delta_i\Theta_i^*) + \right. \\ &\quad \left. + \mathrm{Tr}\left(Z\left(\sum_{i=0}^m \Theta_i\Delta_i\Theta_i^* - I\right)\right)\right\} \\ &= \min_{\Delta_i\geq 0}\left\{\sum_{i=1}^m \mathrm{Tr}\left(\Delta_i\Theta_i^*\left(Z-p_i\rho_i\right)\Theta_i\right) - \mathrm{Tr}(Z)\right\}, \end{aligned} \tag{13}$$

where $Z \geq 0$ is the Lagrange dual variable. Since $\Delta_i \geq 0, 1 \leq i \leq m$, we have that $\mathrm{Tr}(\Delta_i X) \geq 0$ for any $X \geq 0$. If X is not positive semidefinite, then we can always choose Δ_i such that $\mathrm{Tr}(\Delta_i X)$ is unbounded below. Therefore,

$$g(Z) = \begin{cases} -\mathrm{Tr}(Z), & A_i \geq 0, 1\leq i\leq m, Z\geq 0; \\ -\infty, & \text{otherwise,} \end{cases} \tag{14}$$

where

$$A_i = \Theta_i^*(Z - p_i\rho_i)\Theta_i, \quad 1 \leq i \leq m. \tag{15}$$

It follows that the dual problem associated with (12) is

$$\min_Z \mathrm{Tr}(Z) \tag{16}$$

subject to

$$\begin{aligned} \Theta_i^*(Z - p_i\rho_i)\Theta_i \geq 0, \quad 1\leq i\leq m; \\ Z \geq 0. \end{aligned} \tag{17}$$

Denoting by Γ the set of all Hermitian operators Z such that $\Theta_i^*(Z - p_i\rho_i)\Theta_i \geq 0, 1 \leq i \leq m$ and $Z \geq 0$, and defining $T(Z) = \mathrm{Tr}(Z)$, the dual problem can be written as

$$\min_{Z\in\Gamma} T(Z). \tag{18}$$

We refer to any $Z \in \Gamma$ as a dual feasible point. The optimal value of $T(Z)$ is denoted by $\widehat{T}$.

B. Optimality Conditions

We can immediately verify that both the primal and the dual problem are strictly feasible. Therefore, their optimal values are attainable and the duality gap is zero [27], *i.e.,*

$$\widehat{J} = \widehat{T}. \tag{19}$$

In addition, for any $\Pi = \{\Pi_i = \Theta_i\Delta_i\Theta_i^*\}_{i=1}^m \in \Lambda$ and $Z \in \Gamma$,

$$\begin{aligned} T(Z) - J(\Pi) &= \\ &= \mathrm{Tr}\left(\sum_{i=1}^m \Theta_i\Delta_i\Theta_i^*(Z - p_i\rho_i) + \Pi_0 Z\right) \\ &\geq 0, \end{aligned} \tag{20}$$

where $\Pi_0 = I - \sum_{i=1}^m \Theta_i\Delta_i\Theta_i^* \geq 0$. Note, that (20) can be used to develop an upper bound on the optimal probability of correct detection $\widehat{J}$. Indeed, since for any $Z \in \Gamma$, $T(Z) \geq J(\Pi)$, we have that $\widehat{J} \leq T(Z)$ for any dual feasible Z.

Now, let $\widehat{\Pi}_i = \Theta_i\widehat{\Delta}_i\Theta_i^*, 1 \leq i \leq m$ and $\widehat{\Pi}_0 = I - \sum_{i=1}^m \widehat{\Pi}_i$ denote the optimal measurement operators that maximize (9) subject to (8), and let $\widehat{Z}$ denote the optimal Z that minimizes (16) subject to (17). From (19) and (20) we conclude that

$$\mathrm{Tr}\left(\sum_{i=1}^m \widehat{\Pi}_i\Theta_i^*(\widehat{Z} - p_i\rho_i)\Theta_i + \widehat{\Pi}_0\widehat{Z}\right) = 0. \tag{21}$$

Since $\widehat{\Delta}_i \geq 0$, $\widehat{Z} \geq 0$ and $\Theta_i^*(\widehat{Z} - p_i\rho_i)\Theta_i \geq 0, 1 \leq i \leq m$, (21) is satisfied if and only if

$$\widehat{Z}\widehat{\Pi}_0 = 0 \tag{22}$$

$$\Theta_i^*(\widehat{Z} - p_i\rho_i)\Theta_i\widehat{\Delta}_i = 0, \quad 1 \leq i \leq m. \tag{23}$$

Once we find the optimal $\widehat{Z}$ that minimizes the dual problem (16), the constraints (22) and (23) are necessary and sufficient conditions on the optimal measurement operators $\widehat{\Pi}_i$. We have already seen that these conditions are necessary. To show that they are sufficient, we note that if a set of feasible measurement operators $\widehat{\Pi}_i$ satisfies (22) and (23), then $\mathrm{Tr}\left(\sum_{i=1}^m \widehat{\Delta}_i\Theta_i^*(\widehat{Z} - p_i\rho_i)\Theta_i + \widehat{\Pi}_0\widehat{Z}\right) = 0$ so that from (20), $J(\widehat{\Pi}) = T(\widehat{Z}) = \widehat{J}$.

We summarize our results in the following theorem:

Theorem 1. *Let $\{\rho_i, 1 \leq i \leq m\}$ denote a set of density operators with prior probabilities $\{p_i > 0, 1 \leq i \leq m\}$, and let $\{\Theta_i, 1 \leq i \leq m\}$ denote a set of matrices such that the columns of Θ_i form an orthonormal basis for $\mathcal{S}_i = \cap_{j=1, j\neq i}^m \mathcal{K}_j$, where $\mathcal{K}_i$ the null space of ρ_i. Let Λ denote the set of all ordered sets of Hermitian measurement operators $\Pi = \{\Pi_i\}_{i=0}^m$ that satisfy $\Pi_i \geq 0$,*

$\sum_{i=0}^m \Pi_i = I$, *and* $Tr(\rho_j\Pi_i) = 0, 1 \leq i \leq m, i \neq j$ *and let* Γ *denote the set of Hermitian matrices* Z *such that* $Z \geq 0$, $\Theta_i^*(Z - p_i\rho_i)\Theta_i, 1 \leq i \leq m$. *Consider the problem* $\max_{\Pi\in\Lambda} J(\Pi)$ *and the dual problem* $\min_{Z\in\Gamma} T(Z)$, *where* $J(\Pi) = \sum_{i=1}^m p_i Tr(\rho_i\Pi_i)$ *and* $T(Z) = Tr(Z)$. *Then*

1. *For any* $Z \in \Gamma$ *and* $\Pi \in \Lambda$, $T(Z) \geq J(\Pi)$.

2. *There is an optimal* Π, *denoted* $\widehat{\Pi}$, *such that* $\widehat{J} = J(\widehat{\Pi}) \geq J(\Pi)$ *for any* $\Pi \in \Lambda$;

3. *There is an optimal* Z, *denoted* $\widehat{Z}$ *and such that* $\widehat{T} = T(\widehat{Z}) \leq T(Z)$ *for any* $Z \in \Gamma$;

4. $\widehat{T} = \widehat{J}$;

5. *Necessary and sufficient conditions on the optimal measurement operators* $\widehat{\Pi}_i$ *are that there exists a* $Z \in \Gamma$ *such that*

$$Z\widehat{\Pi}_0 = 0 \tag{24}$$

$$\Theta_i^*(Z - p_i\rho)\Theta_i\widehat{\Delta}_i = 0, \quad 1 \leq i \leq m, \tag{25}$$

where $\widehat{\Pi}_i = \Theta_i\widehat{\Delta}_i\Theta_i^*, 1 \leq i \leq m$, *and* $\widehat{\Delta}_i \geq 0$.

6. *Given* $\widehat{Z}$, *necessary and sufficient conditions on the optimal measurement operators* $\widehat{\Pi}_i$ *are*

$$\widehat{Z}\widehat{\Pi}_0 = 0 \tag{26}$$

$$\Theta_i^*(\widehat{Z} - p_i\rho_i)\Theta_i\widehat{\Delta}_i = 0, \quad 1 \leq i \leq m. \tag{27}$$

Although the necessary and sufficient conditions of Theorem 1 are hard to solve, they can be used to verify a solution and to gain some insight into the optimal measurement operators. In the next section we show that the previous optimal measurements that were derived in the literature for certain special cases satisfy these optimality conditions.

IV. SPECIAL CASES

We now consider two special cases that where addressed in [21], for which a closed form solution exists. In Section IV A we consider the case in which the spaces $\mathcal{S}_i$ defined by (3) are orthogonal, and in Section IV B we consider the problem of distinguishing unambiguously between two density operators with $\dim(\mathcal{S}_i) = 1, 1 \leq i \leq 2$.

A. Orthogonal Null Spaces $\mathcal{S}_i$

The first case we consider is the case in which the null spaces $\mathcal{S}_i$ are orthogonal, so that

$$P_iP_j = \delta_{ij}, \quad 1 \leq i, j, \leq m, \tag{28}$$

where P_i is an orthogonal projection onto $\mathcal{S}_i$. It was shown in [21] that in this case the optimal measurement operators are

$$\widehat{\Pi}_i = P_i = \Theta_i\Theta_i^*, \quad 1 \leq i \leq m. \tag{29}$$

In Appendix A we show that the optimal solution of the dual problem can be expressed as

$$\widehat{Z} = \sum_{i=1}^m p_iP_i\rho_iP_i. \tag{30}$$

It can easily be shown that $\widehat{Z}$ and $\widehat{\Pi}_i$ of (30) and (29) satisfy the optimality conditions of Theorem 1.

B. Null Spaces of Dimension 1

We now consider the case of distinguishing between two density operators ρ_1 and ρ_2, where $\mathcal{S}_1$ and $\mathcal{S}_2$ both have dimension equal to 1. In this case, as we show in Appendix B, the optimal dual solution is

$$\widehat{Z} = \begin{cases} d_1P_1, & d_2 - d_1|f|^2 \leq 0; \\ d_2P_2, & d_1 - d_2|f|^2 \leq 0; \\ d_2(\Theta_2 + s\Theta_2^\perp)(\Theta_2 + s\Theta_2^\perp)^*, & \text{otherwise}, \end{cases} \tag{31}$$

where P_i is an orthogonal projection onto $\mathcal{S}_i$, $\Theta_2^\perp$ is a unit norm vector in the span of Θ_1 and Θ_2 such that $\Theta_2^*\Theta_2^\perp = 0$, and

$$\begin{aligned} d_i &= p_i\Theta_i^*\rho_i\Theta_i, \quad 1 \leq i \leq 2; \\ s &= \tfrac{f^*}{e^*}\left(\sqrt{\tfrac{d_1}{d_2|f|^2}} - 1\right); \\ f &= \Theta_2^*\Theta_1; \\ e &= (\Theta_2^\perp)^*\Theta_1. \end{aligned} \tag{32}$$

The optimal measurement operators for this case were developed in [21], and can be written as

$$\{\widehat{\Pi}_i\}_{i=1}^2 = \begin{cases} \widehat{\Pi}_1 = P_1, \widehat{\Pi}_2 = 0, & d_2 - d_1|f|^2 \leq 0; \\ \widehat{\Pi}_1 = 0, \widehat{\Pi}_2 = P_2, & d_1 - d_2|f|^2 \leq 0; \\ \widehat{\Pi}_1 = \alpha_1P_1, \widehat{\Pi}_2 = \alpha_2P_2, & \text{otherwise}, \end{cases} \tag{33}$$

where

$$\begin{aligned} \alpha_1 &= \tfrac{1-\sqrt{\frac{d_2|f|^2}{d1}}}{1-|f|^2}; \\ \alpha_2 &= \tfrac{1-\sqrt{\frac{d_1|f|^2}{d2}}}{1-|f|^2}. \end{aligned} \tag{34}$$

We now show that $\widehat{Z}$ and $\widehat{\Pi}$ of (31) and (33) satisfy the optimality conditions of Theorem 1. To this end we note that from (33),

$$\{\widehat{\Delta}_i\}_{i=1}^2 = \begin{cases} \widehat{\Delta}_1 = 1, \widehat{\Delta}_2 = 0, & d_2 - d_1|f|^2 \leq 0; \\ \widehat{\Delta}_1 = 0, \widehat{\Delta}_2 = 1, & d_1 - d_2|f|^2 \leq 0; \\ \widehat{\Delta}_1 = \alpha_1, \widehat{\Delta}_2 = \alpha_2, & \text{otherwise}. \end{cases} \tag{35}$$

From (31)–(35) we have that if $d_2 - d_1|f|^2 \leq 0$, then

$$\Theta_1^*(\widehat{Z} - p_1\rho_1)\Theta_1\widehat{\Delta}_1 = d_1 - \Theta_1^* p_1\rho_1\Theta_1 = 0;$$
$$\Theta_2^*(\widehat{Z} - p_2\rho_2)\Theta_2\widehat{\Delta}_2 = 0;$$
$$\widehat{Z}\widehat{\Pi}_0 = \widehat{Z}(I - \widehat{\Pi}_1) = d_1\Theta_1\Theta_1^* - d_1\Theta_1\Theta_1^* = 0. \quad (36)$$

Similarly, if $d_1 - d_2|f|^2 \leq 0$, then

$$\Theta_1^*(\widehat{Z} - p_1\rho_1)\Theta_1\widehat{\Delta}_1 = 0;$$
$$\Theta_2^*(\widehat{Z} - p_2\rho_2)\Theta_2\widehat{\Delta}_2 = d_2 - \Theta_2^* p_2\rho_2\Theta_2 = 0;$$
$$\widehat{Z}\widehat{\Pi}_0 = \widehat{Z}(I - \widehat{\Pi}_2) = d_2\Theta_2\Theta_2^* - d_2\Theta_2\Theta_2^* = 0. \quad (37)$$

Finally, if neither of the conditions $d_1 - d_2|f|^2 \leq 0$, $d_2 - d_1|f|^2 \leq 0$ hold, then

$$\begin{aligned}
&\Theta_1^*(\widehat{Z} - p_1\rho_1)\Theta_1\widehat{\Delta}_1 = \\
&= (d_2(f^* + e^*s)(f^* + e^*s)^* - d_1)\frac{1 - \sqrt{\frac{d_2|f|^2}{d_1}}}{1 - |f|^2} \\
&= \left(d_2|f|^2\left(\sqrt{\frac{d_1}{d_2|f|^2}}\right)^2 - d_1\right)\frac{1 - \sqrt{\frac{d_2|f|^2}{d_1}}}{1 - |f|^2} \\
&= 0, \qquad (38)
\end{aligned}$$

$$\begin{aligned}
\Theta_2^*(\widehat{Z} - p_2\rho_2)\Theta_2\widehat{\Delta}_2 &= (\Theta_2^*\widehat{Z}\Theta_2 - d_2)\frac{1 - \sqrt{\frac{d_1|f|^2}{d_2}}}{1 - |f|^2} \\
&= 0, \qquad (39)
\end{aligned}$$

and

$$\begin{aligned}
\widehat{Z}\widehat{\Pi}_0 &= \widehat{Z} - \widehat{Z}\widehat{\Pi}_1 - \widehat{Z}\widehat{\Pi}_2 \\
&= \widehat{Z} - \widehat{\Delta}_1\widehat{Z}\Theta_1\Theta_1^* - \widehat{\Delta}_2\widehat{Z}\Theta_2\Theta_2^*. \qquad (40)
\end{aligned}$$

To show that $\widehat{Z}\widehat{\Pi}_0 = 0$, we note that

$$\begin{aligned}
\widehat{Z}\Theta_1\Theta_1^* &= d_2(|f|^2 + s^*ef^*)\Theta_2\Theta_2^* \\
&+ d_2(s|f|^2 + ss^*ef^*)\Theta_2^\perp\Theta_2^* \\
&+ d_2(e^*f + s^*|e|^2)\Theta_2\Theta_2^{\perp *} \\
&+ d_2(se^*f + ss^*|e|^2)\Theta_2^\perp\Theta_2^{\perp *}, \qquad (41)
\end{aligned}$$

and

$$\widehat{Z}\Theta_2\Theta_2^* = d_2\Theta_2\Theta_2^* + d_2 s\Theta_2^\perp\Theta_2^*. \quad (42)$$

Substituting (41) and (42) into (40), and after some algebraic manipulations, we have that

$$\widehat{Z}\widehat{\Pi}_0 = \widehat{Z} - \widehat{\Delta}_1\widehat{Z}\Theta_1\Theta_1^* - \widehat{\Delta}_2\widehat{Z}\Theta_2\Theta_2^* = 0. \quad (43)$$

Combining (36)–(43) we conclude that the optimal measurement operators of [21] satisfy the optimality conditions of Theorem 1.

V. OPTIMAL DETECTION OF SYMMETRIC STATES

We now consider the case in which the quantum state ensemble has symmetry properties referred to as geometric uniformity (GU) and compound geometric uniformity (CGU). These symmetry properties are quite general, and include many cases of practical interest.

Under a variety of different optimality criteria the optimal measurement for distinguishing between GU and CGU state sets was shown to be GU and CGU respectively [7, 8, 17, 18]. In particular it was shown in [17] that the optimal measurement for unambiguous detection between linearly independent GU and CGU pure-states is GU and CGU respectively. We now generalize this result to unambiguous detection of mixed GU and CGU state sets.

VI. GU STATE SETS

A GU state set is defined as a set of density operators $\{\rho_i, 1 \leq i \leq m\}$ such that $\rho_i = U_i\rho U_i^*$ where ρ is an arbitrary *generating operator* and the matrices $\{U_i, 1 \leq i \leq m\}$ are unitary and form an abelian group $\mathcal{G}$ [8, 29]. For concreteness, we assume that $U_1 = I$. The group $\mathcal{G}$ is the *generating group* of $\mathcal{S}$. For consistency with the symmetry of $\mathcal{S}$, we will assume equiprobable prior probabilities on $\mathcal{S}$.

As we now show, the optimal measurement operators that maximize the probability of correct detection when distinguishing unambiguously between the density operators of a GU state set are also GU with the same generating group. The corresponding generator can be computed very efficiently in polynomial time.

Suppose that the optimal measurement operators that maximize

$$J(\{\Pi_i\}) = \sum_{i=1}^{m} \mathrm{Tr}(\rho_i\Pi_i) \quad (44)$$

subject to (8) and (5) are $\widehat{\Pi}_i$, and let $\widehat{J} = J(\{\widehat{\Pi}_i\}) = \sum_{i=1}^m \mathrm{Tr}(\rho_i\widehat{\Pi}_i)$. Let $r(j,i)$ be the mapping from $\mathcal{I}\times\mathcal{I}$ to $\mathcal{I}$ with $\mathcal{I} = \{1,\ldots,m\}$, defined by $r(j,i) = k$ if $U_j^*U_i = U_k$. Then the measurement operators $\widehat{\Pi}_i^{(j)} = U_j\widehat{\Pi}_{r(j,i)}U_j^*$ and $\widehat{\Pi}_0^{(j)} = I - \sum_{i=1}^m \widehat{\Pi}_i^{(j)}$ for any $1 \leq j \leq m$ are also optimal. Indeed, since $\widehat{\Pi}_i \geq 0, 1 \leq i \leq m$ and $\sum_{i=1}^m \widehat{\Pi}_i \leq I$, $\widehat{\Pi}_i^{(j)} \geq 0, 1 \leq i \leq m$ and

$$\sum_{i=1}^{m} \widehat{\Pi}_i^{(j)} = U_j\left(\sum_{i=1}^{m}\widehat{\Pi}_i\right)U_j^* \leq U_jU_j^* = I. \quad (45)$$

Using the fact that $\rho_i = U_i \rho U_i^*$ for some generator ρ,

$$\begin{aligned} J(\{\widehat{\Pi}_i^{(j)}\}) &= \sum_{i=1}^m \mathrm{Tr}(\rho U_i^* U_j \widehat{\Pi}_{r(j,i)} U_j^* U_i) \\ &= \sum_{k=1}^m \mathrm{Tr}(\rho U_k^* \widehat{\Pi}_k U_k) \\ &= \sum_{i=1}^m \mathrm{Tr}(\rho_i \widehat{\Pi}_i) \\ &= \widehat{J}. \end{aligned} \tag{46}$$

Finally, for $l \neq i$,

$$\begin{aligned} \mathrm{Tr}\left(\rho_l \widehat{\Pi}_i^{(j)}\right) &= \mathrm{Tr}\left(U_l \rho U_l^* U_j \widehat{\Pi}_{r(j,i)} U_j^*\right) \\ &= \mathrm{Tr}\left(U_s \rho U_s^* \widehat{\Pi}_{r(j,i)}\right) \\ &= \mathrm{Tr}\left(\rho_s \widehat{\Pi}_k\right) \\ &= 0, \end{aligned} \tag{47}$$

where $U_s = U_j^* U_l$ and $U_k = U_j^* U_i$ and the last equality follows from the fact that since $l \neq i$, $s \neq k$.

It was shown in [8, 18] that if the measurement operators $\widehat{\Pi}_i^{(j)}$ are optimal for any j, then $\{\overline{\Pi}_i = (1/m)\sum_{j=1}^m \widehat{\Pi}_i^{(j)}, 1 \leq i \leq m\}$ and $\overline{\Pi}_0 = I - \sum_{i=1}^m \overline{\Pi}_i$ are also optimal. Furthermore, $\overline{\Pi}_i = U_i \widehat{\Pi} U_i^*$ where $\widehat{\Pi} = (1/m)\sum_{k=1}^m U_k^* \widehat{\Pi}_k U_k$.

We therefore conclude that the optimal measurement operators can always be chosen to be GU with the same generating group $\mathcal{G}$ as the original state set. Thus, to find the optimal measurement operators all we need is to find the optimal generator $\widehat{\Pi}$. The remaining operators are obtained by applying the group $\mathcal{G}$ to $\widehat{\Pi}$.

Since the optimal measurement operators satisfy $\Pi_i = U_i \Pi U_i^*, 1 \leq i \leq m$ and $\rho_i = U_i \rho U_i^*$, $\mathrm{Tr}(\rho_i \Pi_i) = \mathrm{Tr}(\rho \Pi)$, so that the problem (9) reduces to the maximization problem

$$\max_{\Pi \in \mathcal{B}} \mathrm{Tr}(\rho \Pi), \tag{48}$$

where $\mathcal{B}$ is the set of $n \times n$ Hermitian operators, subject to the constraints

$$\begin{gathered} \Pi \geq 0; \\ \textstyle\sum_{i=1}^m U_i \Pi U_i^* \leq I; \\ \mathrm{Tr}(\Pi \rho_i) = 0, \quad 2 \leq i \leq m. \end{gathered} \tag{49}$$

The problem of (48) and (49) is a (convex) semidefinite programming problem, and therefore the optimal Π can be computed very efficiently in polynomial time within any desired accuracy [24, 26, 27], for example using the LMI toolbox on Matlab. Note that the problem of (48) and (49) has n^2 real unknowns and $m+1$ constraints, in contrast with the original maximization problem (9) subject to (8) and (5) which has mn^2 real unknowns and m^2+1 constraints.

VII. CGU STATE SETS

A CGU state set is defined as a set density operators $\{\rho_{ik}, 1 \leq i \leq l, 1 \leq k \leq r\}$ such that $\rho_{ik} = U_i \phi_k U_i^*$ for some generating density operators $\{\rho_k, 1 \leq k \leq r\}$, where the matrices $\{U_i, 1 \leq i \leq l\}$ are unitary and form an abelian group $\mathcal{G}$ [8, 23]. A CGU state set is in general not GU. However, for every k, the operators $\{\rho_{ik}, 1 \leq i \leq l\}$ are GU with generating group $\mathcal{G}$.

Using arguments similar to hose of Section VI and [18] we can show that the optimal measurement operators corresponding to a CGU state set can always be chosen to be GU with the same generating group $\mathcal{G}$ as the original state set. Thus, to find the optimal measurement operators all we need is to find the optimal generators $\widehat{\Pi}_k$. The remaining operators are obtained by applying the group $\mathcal{G}$ to each of the generators $\widehat{\Pi}_k$.

Since the optimal measurement operators satisfy $\Pi_{ik} = U_i \Pi_k U_i^*, 1 \leq i \leq l, 1 \leq k \leq r$ and $\rho_{ik} = U_i \rho_k U_i^*$, $\mathrm{Tr}(\rho_{ik}\Pi_{ik}) = \mathrm{Tr}(\rho_k \Pi_k)$, so that the problem (9) reduces to the maximization problem

$$\max_{\Pi_k \in \mathcal{B}} \sum_{k=1}^r \mathrm{Tr}(\rho_k \Pi_k), \tag{50}$$

subject to the constraints

$$\begin{gathered} \Pi_k \geq 0, \quad 1 \leq k \leq r; \\ \textstyle\sum_{i=1}^l \sum_{k=1}^r U_{ik} \Pi_k U_{ik}^* \leq I; \\ \mathrm{Tr}(\Pi_k \rho_{ik}) = 0, \quad 1 \leq k \leq r, 2 \leq i \leq l. \end{gathered} \tag{51}$$

Since this problem is a (convex) semidefinite programming problem, the optimal generators Π_k can be computed very efficiently in polynomial time within any desired accuracy [24, 26, 27]. Note that the problem of (50) and (51) has rn^2 real unknowns and $lr+1$ constraints, in contrast with the original maximization which has lrn^2 real unknowns and $(lr)^2+1$ constraints.

VIII. CONCLUSION

We considered the problem of distinguishing unambiguously between a collection of *mixed* quantum states. Using elements of duality theory in vector space optimization, we derived a set of necessary and sufficient conditions on the optimal measurement operators. We then considered some special cases for which closed form solutions are known, and showed that they satisfy our optimality conditions. We also showed that in the case in which the states to be distinguished have strong symmetry properties, the optimal measurement operators have the same symmetries, and can be determined efficiently by solving a semidefinite programming problem.

An interesting future direction to pursue is to use the optimality conditions we developed in this paper to derive closed form solutions for other special cases.

APPENDIX A: PROOF OF (30)

To develop the optimal dual solution in the case of orthogonal null spaces, let $\Theta = \begin{bmatrix}\Theta_1 & \Theta_2 & \dots & \Theta_m\end{bmatrix}$, and define a matrix $\Theta^\perp$ such that $\begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix}$ is a square, unitary matrix, *i.e.,* $\begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix}^* \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix} = I$. Denoting $Z = \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix} Y \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix}^*$, the dual problem can be expressed as

$$\min_Y \operatorname{Tr}\left(\begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix} Y \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix}^*\right) \tag{A1}$$

subject to

$$\begin{aligned} \Theta_i^*\begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix} Y \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix}^*\Theta_i \geq \Theta_i^* p_i\rho_i\Theta_i, \quad 1 \leq i \leq m;\\ Y \geq 0. \end{aligned} \tag{A2}$$

Using the orthogonality properties of Θ_i and $\Theta^\perp$, the problem of (A1) and (A2) is equivalent to

$$\min_Y \operatorname{Tr}(Y) \tag{A3}$$

subject to

$$\begin{aligned} Y_i \geq \Theta_i^* p_i\rho_i\Theta_i, \quad 1 \leq i \leq m;\\ Y \geq 0, \end{aligned} \tag{A4}$$

where

$$Y = \begin{bmatrix} Y_1 & & & & \\ & Y_2 & & & \\ & & \ddots & & \\ & & & Y_m & \\ & & & & 0 \end{bmatrix}. \tag{A5}$$

Since $\operatorname{Tr}(Y) = \sum_{i=1}^m \operatorname{Tr}(Y_i)$, a solution to (A3) subject to (A4) is

$$\widehat{Y} = \begin{bmatrix} \widehat{Y}_1 & & & & \\ & \widehat{Y}_2 & & & \\ & & \ddots & & \\ & & & \widehat{Y}_m & \\ & & & & 0 \end{bmatrix}, \tag{A6}$$

where

$$\widehat{Y}_i = \Theta_i^* p_i\rho_i\Theta_i, \quad 1 \leq i \leq m. \tag{A7}$$

Then,

$$\widehat{Z} = \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix} \widehat{Y} \begin{bmatrix}\Theta & \Theta^\perp\end{bmatrix}^* = \sum_{i=1}^m p_i P_i \rho_i P_i, \tag{A8}$$

as in (30).

APPENDIX B: PROOF OF (31)

To develop the optimal dual solution $\widehat{Z}$ for one-dimensional null spaces, we note that $\widehat{Z}$ lies in the space spanned by Θ_1 and Θ_2. Denoting by Θ a matrix whose columns represent an orthonormal basis for this space, $\widehat{Z}$ can be written as $\widehat{Z} = \Theta\widehat{Y}\Theta^*$, where the 2×2 matrix $\widehat{Y}$ is the solution to

$$\min_Y \operatorname{Tr}(Y) \tag{B1}$$

subject to

$$\Phi_1^* Y \Phi_1 \geq d_1; \tag{B2}$$
$$\Phi_2^* Y \Phi_2 \geq d_2; \tag{B3}$$
$$Y \geq 0. \tag{B4}$$

Here $\Phi_i = \Theta^*\Theta_i$ and $d_i = p_i\Theta_i^*\rho_i\Theta_i$ for $1 \leq i \leq 2$.

To develop a solution to (B1) subject to (B2)–(B4), we form the Lagrangian

$$\mathcal{L} = \operatorname{Tr}(Y) - \sum_{i=1}^2 \gamma_i(\Phi_i^* Y \Phi_i - d_i) - \operatorname{Tr}(XY), \tag{B5}$$

where from the Karush-Kuhn-Tucker (KKT) conditions [30] we must have that $\gamma_i \geq 0, X \geq 0$, and

$$\gamma_i(\Phi_i^* Y \Phi_i - d_i) = 0, \quad i = 1, 2; \tag{B6}$$
$$\operatorname{Tr}(XY) = 0. \tag{B7}$$

Differentiating $\mathcal{L}$ with respect to Y and equating to zero,

$$I - \sum_{i=1}^2 \gamma_i \Phi_i \Phi_i^* - X = 0. \tag{B8}$$

If $X = 0$, then we must have that $I = \sum_{i=1}^2 \gamma_i \Phi_i \Phi_i^*$, which is possible only if Φ_1 and Φ_2 are orthogonal. Therefore, $X \neq 0$, which implies from (B7) that (B4) is active. Now, suppose that only (B4) is active. In this case our problem reduces to minimizing $\operatorname{Tr}(y^* y)$ whose optimal solution is $y = 0$, which does not satisfy (B2) and (B3).

We conclude that at the optimal solution (B4) and at least one of the constraints (B2) and (B3) are active. Thus, to determine the optimal solution we need to determine the solutions under each of the 3 possibilities: only (B2) is active, only (B3) is active, both (B2) and (B3) are active, and then choose the solution with the smallest objective.

Consider first the case in which (B2) and (B4) are active. In this case, $\widehat{Y} = \hat{y}\hat{y}^*$ for some vector $\hat{y}$, and without loss of generality we can assume that

$$\Phi_1^* \hat{y} = d_1. \tag{B9}$$

To satisfy (B9), $\hat{y}$ must have the form

$$\hat{y} = \sqrt{d_1}\Phi_1 + \hat{s}\Phi_1^\perp, \tag{B10}$$

where $\Phi_1^\perp$ is a unit norm vector orthogonal to Φ_1, so that $\Phi_1^*\Phi_1^\perp = 0$, and $\hat{s}$ is chosen to minimize $\mathrm{Tr}(\widehat{Y})$. Since,

$$\mathrm{Tr}(\widehat{Y}) = \hat{y}^*\hat{y} = d_1 + |\hat{s}|^2, \tag{B11}$$

$\hat{s} = 0$. Thus, $\widehat{Y} = d_1\Phi_1\Phi_1^*$, and $\mathrm{Tr}(\widehat{Y}) = d_1$. This solution is valid only if (B3) is satisfied, *i.e.,* only if

$$\Phi_2^*\widehat{Y}\Phi_2 = d_1|f|^2 \geq d_2. \tag{B12}$$

Here we used the fact that

$$\Phi_2^*\Phi_1 = \Theta_2^*\Theta\Theta^*\Theta_1 = \Theta_2^*\Theta_1 = f, \tag{B13}$$

since $\Theta\Theta^*$ is an orthogonal projection onto the space spanned by Θ_1 and Θ_2.

Next, suppose that (B3) and (B4) are active. In this case, $\widehat{Y} = \hat{y}\hat{y}^*$ where without loss of generality we can choose $\hat{y}$ such that

$$\Phi_2^*\hat{y} = d_2, \tag{B14}$$

and

$$\hat{y} = \sqrt{d_2}\Phi_2 + \hat{s}\Phi_2^\perp, \tag{B15}$$

where $\Phi_2^\perp$ is a unit norm vector orthogonal to Φ_2, and $\hat{s}$ is chosen to minimize $\mathrm{Tr}(\widehat{Y})$. Since $\mathrm{Tr}(\widehat{Y}) = d_2 + |\hat{s}|^2$, $\hat{s} = 0$, and $\mathrm{Tr}(\widehat{Y}) = d_2$. This solution is valid only if (B2) is satisfied, *i.e.,*

$$\Phi_1^* Y \Phi_1 = d_2|f|^2 \geq d_1. \tag{B16}$$

Finally, consider the case in which (B2)–(B4) are active. In this case, we can assume without loss of generality that $\Phi_2^*\hat{y} = \sqrt{d_2}$. Then,

$$\hat{y} = \sqrt{d_2}\Phi_2 + \hat{s}\Phi_2^\perp, \tag{B17}$$

where $\hat{s}$ is chosen such that

$$\Phi_1^*\widehat{Y}\Phi_1 = d_1, \tag{B18}$$

and $\mathrm{Tr}(\widehat{Y}) = \hat{y}^*\hat{y}$ is minimized. Now, for $\hat{y}$ given by (B17),

$$\begin{aligned}\widehat{Y} = d_2\Phi_2\Phi_2^* + |\hat{s}|^2\Phi_2^\perp\Phi_2^{\perp *} + \\ + \hat{s}\sqrt{d_2}\Phi_2^\perp\Phi_2^* + \hat{s}^*\sqrt{d_2}\Phi_2\Phi_2^{\perp *},\end{aligned} \tag{B19}$$

so that

$$\begin{aligned}\Phi_1^*\widehat{Y}\Phi_1 &= d_2|f|^2 + |\hat{s}|^2|e|^2 + \sqrt{d_2}\hat{s}e^*f + \sqrt{d_2}\hat{s}^*f^*e \\ &= |\sqrt{d_2}f + \hat{s}^*e|^2,\end{aligned} \tag{B20}$$

where we defined $\Theta_2^\perp = \Theta\Psi_2^\perp$, and e and f are given by (32). Therefore, to satisfy (B18), $\hat{s}$ must be of the form

$$\hat{s} = \frac{1}{e^*}\left(e^{j\varphi}\sqrt{d_1} - f^*\sqrt{d_2}\right), \tag{B21}$$

for some φ. The problem of (B1) then becomes

$$\min_{\varphi} \frac{1}{|e|^2}\left|e^{j\varphi}\sqrt{d_1} - f^*\sqrt{d_2}\right|^2, \tag{B22}$$

which is equivalent to

$$\max_{\varphi} \Re\left\{e^{j\varphi}f\right\}. \tag{B23}$$

Since

$$\Re\left\{e^{j\varphi}f\right\} \leq \left|e^{j\varphi}f\right| = |f|, \tag{B24}$$

the optimal choice of φ is $e^{j\varphi} = f^*/|f|$, and

$$\hat{s} = \frac{f^*\sqrt{d_2}}{e^*}\left(\frac{\sqrt{d_1}}{\sqrt{d_2}|f|} - 1\right). \tag{B25}$$

For this choice of $\hat{s}$,

$$\begin{aligned}\mathrm{Tr}(\widehat{Y}) &= d_2 + |\hat{s}|^2 \\ &= d_2\left(1 + \frac{|f|^2}{|e|^2}\left(\frac{\sqrt{d_1}}{\sqrt{d_2}|f|} - 1\right)^2\right) \\ &\triangleq \alpha.\end{aligned} \tag{B26}$$

Clearly, $\alpha \geq d_2$. Therefore, to complete the proof of (31) we need to show that $\alpha \geq d_1$. Now,

$$\begin{aligned}&|e|^2(\alpha - d_1) = \\ &= |e|^2(d_2 - d_1) + |f|^2\left(\frac{\sqrt{d_1}}{|f|} - \sqrt{d_2}\right)^2 \\ &= (1 - |e|^2)d_1 + (|e|^2 + |f|^2)d_2 - 2\sqrt{d_1}\sqrt{d_2}|f| \\ &= (|f|\sqrt{d_1} - \sqrt{d_2})^2 \\ &\geq 0,\end{aligned} \tag{B27}$$

where we used the fact that

$$\begin{aligned}|e|^2 + |f|^2 &= \Theta_1^*\Theta_2\Theta_2^*\Theta_1 + \Theta_1^*\Theta_2^\perp(\Theta_2^\perp)^*\Theta_1 \\ &= \Theta_1^*\Theta_1 = 1,\end{aligned} \tag{B28}$$

since $\Theta_2\Theta_2^* + \Theta_2^\perp(\Theta_2^\perp)^*$ is an orthogonal projection onto the space spanned by Θ_1 and Θ_2.

[1] A. S. Holevo, J. Multivar. Anal. **3**, 337 (1973).

[2] C. W. Helstrom, *Quantum Detection and Estimation Theory* (New York: Academic Press, 1976).

[3] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE

Trans. Inform. Theory **49**, 1012 (2003).
[4] M. Charbit, C. Bendjaballah, and C. W. Helstrom, IEEE Trans. Inform. Theory **35**, 1131 (1989).
[5] M. Osaki, M. Ban, and O. Hirota, Phys. Rev. A **54**, 1691 (1996).
[6] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[7] Y. C. Eldar and G. D. Forney, Jr., IEEE Trans. Inform. Theory **47**, 858 (2001).
[8] Y. C. Eldar, A. Megretski, and G. C. Verghese, quant-ph/0211111 (2002).
[9] Y. C. Eldar, Phys. Rev. A **68**, 052303 (2003).
[10] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[11] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[12] A. Peres, Phys. Lett. A **128**, 19 (1988).
[13] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[14] A. Peres and D. R. Terno, J. Phys. A **31**, 7105 (1998).
[15] A. Chefles, Phys. Lett. A **239**, 339 (1998).
[16] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
[17] Y. C. Eldar, IEEE Trans. Inform Theory **49**, 446 (2003).
[18] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).
[19] C. W. Zhang, C. F. Li, and G. C. Guo, Phys. Lett. A **261**, 25 (1999).
[20] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).
[21] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301 (2003).
[22] A. Peres, Found. Phys. **20**, 1441 (1990).
[23] Y. C. Eldar and H. Bölcskei, IEEE Trans. Inform. Theory **49**, 993 (2003).
[24] F. Alizadeh, Ph.D. thesis, University of Minnesota, Minneapolis, MN (1991).
[25] F. Alizadeh, in *Advances in Optimization and Parallel Computing*, edited by P. Pardalos (North-Holland, the Netherlands, 1992).
[26] Y. Nesterov and A. Nemirovski, *Interior-Point Polynomial Algorithms in Convex Programming* (Philadelphia, PE: SIAM, 1994).
[27] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 40 (1996).
[28] D. P. Bertsekas, *Nonlinear Programming* (Belmont MA: Athena Scientific, 1999), 2nd ed.
[29] G. D. Forney, Jr., IEEE Trans. Inform. Theory **37**, 1241 (1991).
[30] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization* (MPS-SIAM Series on Optimization, 2001).
[31] Otherwise we can transform the problem to a problem equivalent to the one considered in this paper by reformulating the problem on the subspace spanned by the eigenvectors of $\{\rho_i, 1 \leq i \leq m\}$.
[32] Interior point methods are iterative algorithms that terminate once a pre-specified accuracy has been reached. A worst-case analysis of interior point methods shows that the effort required to solve a semidefinite program to a given accuracy grows no faster than a polynomial of the problem size. In practice, the algorithms behave much better than predicted by the worst case analysis, and in fact in many cases the number of iterations is almost constant in the size of the problem.