Optimal Detection of Symmetric Mixed Quantum States

Yonina C. Eldar[*], Alexandre Megretski[†], and George C. Verghese[‡]

July 8, 2018

Abstract

We develop a sufficient condition for the least-squares measurement (LSM), or the square-root measurement, to minimize the probability of a detection error when distinguishing between a collection of mixed quantum states. Using this condition we derive the optimal measurement for state sets with a broad class of symmetries.

We first consider geometrically uniform (GU) state sets with a possibly nonabelian generating group, and show that if the generator satisfies a certain constraint, then the LSM is optimal. In particular, for pure-state GU ensembles the LSM is shown to be optimal. For arbitrary GU state sets we show that the optimal measurement operators are GU with generator that can be computed very efficiently in polynomial time, within any desired accuracy.

We then consider compound GU (CGU) state sets which consist of subsets that are GU. When the generators satisfy a certain constraint, the LSM is again optimal. For arbitrary CGU state sets the optimal measurement operators are shown to be CGU with generators that can be computed efficiently in polynomial time.

[*]The author was with the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA and is now with the Technion, Israel Institute of Technology, Haifa 32000, Israel. E-mail: yonina@ee.technion.ac.il.

[†]Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139. E-mail: ameg@mit.edu.

[‡]Laboratory for Electromagnetic and Electronic Systems, Massachusetts Institute of Technology, Cambridge, MA 02139. E-mail: verghese@mit.edu.

1 Introduction

In a quantum detection problem a transmitter conveys classical information to a receiver using a quantum-mechanical channel. Each message corresponds to a preparation of the quantum channel in an associated quantum state represented by a density operator, drawn from a collection of known states. To detect the information, the receiver subjects the channel to a quantum measurement. Our problem is to construct a measurement that minimizes the probability of a detection error.

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 density operator ρ is a positive semidefinite (PSD) Hermitian operator with $\text{Tr}(\rho) = 1$; we write $\rho \geq 0$ to indicate ρ is PSD. A mixed state ensemble is one in which at least one of the density operators ρ_i has rank larger than one. 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.

For our *measurement* we consider general positive operator-valued measures [1, 2]. Necessary and sufficient conditions for an optimum measurement minimizing the probability of a detection error have been derived [3, 4, 5]. However, in general, obtaining a closed-form analytical expression for the optimal measurement directly from these conditions is a difficult and unsolved problem. Iterative algorithms minimizing the probability of a detection error have been proposed in [6, 5].

There are some particular cases in which the solution to the quantum detection problem is known explicitly [1, 7, 8, 9, 10]. Ban *et al.* [9] derive the solution for a pure-state ensemble consisting of density operators $\rho_i = |\phi_i\rangle\langle\phi_i|$ where the vectors $|\phi_i\rangle$ form a cyclic set, *i.e.,* the vectors are generated by a cyclic group of unitary matrices using a single generating vector. The optimal measurement coincides with the least-squares measurement (LSM) [10], also known as the square-root measurement [11, 12]. Eldar and Forney [10] derive the optimal measurement for a pure-state ensemble in which the vectors $|\phi_i\rangle$ have a strong symmetry property called geometric

uniformity. In this case the vectors $|\phi_i\rangle$ are defined over a finite abelian group of unitary matrices and generated by a single generating vector; the optimal measurement again coincides with the LSM. Note, that a cyclic state set is a special case of a geometrically uniform state set.

The LSM has many desirable properties [10, 11, 12, 13, 9, 14, 15] and has therefore been proposed as a detection measurement in many settings (see *e.g.,* [16, 17, 18]). In Section 3 we derive a sufficient condition on the density operators for the LSM to minimize the probability of a detection error. For rank-one ensembles we show that the LSM minimizes the probability of a detection error if the probability of correctly detecting each of the states using the LSM is the same, regardless of the state transmitted.

In Section 4 we consider geometrically uniform (GU) state sets defined over a finite group of unitary matrices. In contrast to [10], the GU state sets we consider are not constrained to be rank-one state sets but rather can be mixed state sets, and the unitary group is not constrained to be abelian. We obtain a convenient characterization of the LSM and show that the LSM operators have the same symmetries as the original state set. We then show that for such GU state sets the probability of correctly detecting each of the states using the LSM is the same, so that for rank-one ensembles, the LSM minimizes the probability of a detection error. For an arbitrary GU ensemble, the optimal measurement operators are shown to be GU with the same generating group, and can be computed very efficiently in polynomial time. Furthermore, under a certain constraint on the generators, the LSM again minimizes the probability of a detection error.

In Section 5 we consider the case in which the state set is generated by a group of unitary matrices using *multiple* generators. Such a collection of states is referred to as a *compound GU (CGU)* state set [19]. We obtain a convenient characterization of the LSM for CGU state sets, and show that the LSM vectors are themselves CGU. When the probability of correctly detecting each of the *generators* using the LSM is the same, we show that the probability of correctly detecting each of the states using the LSM is the same. Therefore, for rank-one CGU ensembles with this

3

property, the LSM minimizes the probability of a detection error. An interesting class of CGU state sets results when the set of generating vectors is itself GU, which we refer to as *CGU state sets with GU generators*. In the case in which the generating vectors are GU and generated by a group that commutes up to a phase factor with the CGU group, we show that the LSM vectors are also CGU with GU generators so that they are generated by a *single* generating vector. For such state sets, the probability of correctly detecting each of the states using the LSM is the same, so that for rank-one ensembles, the LSM minimizes the probability of a detection error. Finally we show that for arbitrary CGU state sets, the measurement operators minimizing the probability of a detection error are also CGU, and we propose an efficient algorithm for computing the optimal generators.

Before proceeding to the detailed development, in the next section we present our problem and summarize results from [5] pertaining to the conditions on the optimal measurement operators.

2 Optimal Detection of Quantum States

Assume that a quantum channel is prepared in a quantum state drawn from a collection of given states represented by density operators $\{\rho_i, 1 \leq i \leq m\}$ in 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[1] $\mathcal{H}$ so that $m \geq n$. Since ρ_i is Hermitian and PSD, we can express ρ_i as $\rho_i = \phi_i \phi_i^*$ for some matrix ϕ_i, *e.g.*, via the Cholesky or eigendecomposition of ρ_i [20]. We refer to ϕ_i as a *factor* of ρ_i. Note that the choice of ϕ_i is not unique; if ϕ_i is a factor of ρ_i, then any matrix of the form $\phi_i' = \phi_i Q_i$ where Q_i is an arbitrary matrix satisfying $Q_i Q_i^* = I$, is also a factor of ρ_i.

At the receiver, the constructed measurement comprises m PSD Hermitian measurement operators $\{\Pi_i, 1 \leq i \leq m\}$ on $\mathcal{H}$ that satisfy $\sum_{i=1}^{m} \Pi_i = I$, where I is the identity operator on $\mathcal{H}$. We

---

[1]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 $\{\rho_i, 1 \leq i \leq m\}$.

seek the measurement operators $\{\Pi_i, 1 \leq i \leq m\}$ satisfying

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

that minimize the probability of a detection error, or equivalently, maximize the probability of correct detection. Given that the transmitted state is ρ_j, the probability of correctly detecting the state using measurement operators $\{\Pi_i, 1 \leq i \leq m\}$ is $\text{Tr}(\rho_j \Pi_j)$. Therefore, the probability of correct detection is given by

$$P_d = \sum_{i=1}^{m} p_i \text{Tr}(\rho_i \Pi_i), \tag{2}$$

where $p_i > 0$ is the prior probability of ρ_i, with $\sum_i p_i = 1$.

It was shown in [4, 5] that a set of measurement operators $\{\widehat{\Pi}_i, 1 \leq i \leq m\}$ minimizes the probability of a detection error for a state set $\{\rho_i, 1 \leq i \leq m\}$ with prior probabilities $\{p_i, 1 \leq i \leq m\}$ if and only if there exists an Hermitian $\widehat{X}$ satisfying

$$\widehat{X} \geq p_i \rho_i, \quad 1 \leq i \leq m, \tag{3}$$

such that

$$(\widehat{X} - p_i \rho_i)\widehat{\Pi}_i = 0, \quad 1 \leq i \leq m. \tag{4}$$

The matrix $\widehat{X}$ can be determined as the solution to the problem

$$\min_{X \in \mathcal{B}} \text{Tr}(X) \tag{5}$$

5

where $\mathcal{B}$ is the set of Hermitian operators on $\mathcal{H}$, subject to

$$X \geq p_i \rho_i, \quad 1 \leq i \leq m. \tag{6}$$

Except in some particular cases [1, 7, 8, 9, 10], obtaining a closed-form analytical expression for the optimal measurement operators directly from these necessary and sufficient conditions for optimality is a difficult and unsolved problem. Since (5) is a (convex) semidefinite programming [21, 22, 23] problem, there are very efficient methods for solving (5). In particular, the optimal matrix $\widehat{X}$ minimizing $\mathrm{Tr}(X)$ subject to (6) can be computed in Matlab using the linear matrix inequality (LMI) Toolbox. A convenient interface for using the LMI toolbox is the Matlab package[2] IQCβ (see [5] for further details). Once we determine $\widehat{X}$, the optimal measurement operators $\widehat{\Pi}_i$ can be computed using (4) and (1) as described in [5].

A suboptimal measurement that has been employed as a detection measurement in many applications and has many desirable properties is the LSM [10, 15]. Using the necessary and sufficient conditions (1), (3) and (4), in Section 3 we derive a general condition under which the LSM is optimal, *i.e.,* minimizes the probability of a detection error when distinguishing between possibly mixed quantum states. In Sections 4 and 5 we consider some special cases of mixed and pure state sets for which the LSM is optimal, and derive explicit formulas for the optimal measurement operators.

---

[2]This software was created by A. Megretski, C-Y. Kao, U. Jönsson and A. Rantzer and is available at `http://www.mit.edu/cykao/home.html`.

3 The LSM and the Optimal Measurement

The LSM corresponding to a set of density operators $\{\rho_i = \phi_i \phi_i^*, 1 \leq i \leq m\}$ with eigenvectors that collectively span $\mathcal{H}$ and prior probabilities $\{p_i, 1 \leq i \leq m\}$ consists of the measurement operators $\{\Sigma_i = \mu_i \mu_i^*, 1 \leq i \leq m\}$ where [15, 10]

$$\mu_i = (\Psi\Psi^*)^{-1/2}\psi_i \overset{\triangle}{=} T\psi_i, \tag{7}$$

with

$$T = (\Psi\Psi^*)^{-1/2}. \tag{8}$$

Here Ψ is the matrix of (block) columns $\psi_i = \sqrt{p_i}\phi_i$ and $(\cdot)^{1/2}$ is the unique Hermitian square root of the corresponding matrix. Note that since the eigenvectors of the $\{\rho_i\}$ collectively span $\mathcal{H}$, the columns of the $\{\psi_i\}$ also together span $\mathcal{H}$, so $\Psi\Psi^*$ is invertible. From (7),

$$\sum_{i=1}^{m} \mu_i \mu_i^* = (\Psi\Psi^*)^{-1/2}\left(\sum_{i=1}^{m} \psi_i \psi_i^*\right)(\Psi\Psi^*)^{-1/2} = (\Psi\Psi^*)^{-1/2}\Psi\Psi^*(\Psi\Psi^*)^{-1/2} = I, \tag{9}$$

so that the LSM operators defined by (7) satisfy (1). In the case in which the prior probabilities are all equal,

$$\mu_i = (\Phi\Phi^*)^{-1/2}\phi_i, \tag{10}$$

where Φ is the matrix of (block) columns ϕ_i.

Since the factors ϕ_i are not unique, the LSM factors μ_i are also not unique. In particular, if μ_i are the LSM factors corresponding to ϕ_i, then the LSM factors corresponding to $\phi_i' = \phi_i Q_i$ with $Q_i Q_i^* = I$ are $\mu_i' = \mu_i Q_i$. Therefore, although the LSM factors are not unique, the LSM operators $\Sigma_i = \mu_i \mu_i^*$ are unique.

The LSM corresponding to a pure-state ensemble $|\phi_i\rangle$ consists of the measurement vectors $|\mu_i\rangle = T|\psi_i\rangle$, where $|\psi_i\rangle = \sqrt{p_i}|\phi_i\rangle$. It was shown in [10] that for rank-one ensembles the LSM

7

vectors $|\mu_i\rangle$ minimize the sum of the squared norms of the error vectors $|e_i\rangle = |\mu_i\rangle - |\psi_i\rangle$, so that they are the measurement vectors that satisfy (1), and are closest in a squared error sense to the weighted state vectors $|\psi_i\rangle = \sqrt{p_i}|\phi_i\rangle$. In the case in which the vectors $|\phi_i\rangle$ are linearly independent so that $n = m$, (1) implies that the vectors $|\mu_i\rangle$ must be orthonormal, so that the LSM vectors are the closest orthonormal vectors to the vectors $|\psi_i\rangle$ in a least-squares sense, as illustrated in Fig. 1. A similar result was obtained for the LSM factor μ_i corresponding to a mixed-state ensemble with factors ϕ_i [14].

Figure 1: Example of the least-squares measurement (LSM). Since the vectors $|\psi_i\rangle$ are linearly independent, the LSM vectors $|\mu_i\rangle$ are orthonormal and minimize $\sum_i \langle e_i|e_i\rangle$ where $|e_i\rangle = |\psi_i\rangle - |\mu_i\rangle$.

The LSM is equivalent to the square-root measurement [9, 11, 12, 16, 17, 18], and has many desirable properties. Its construction is relatively simple; it can be determined directly from the given collection of states; it minimizes the probability of a detection error for pure-state ensembles that exhibit certain symmetries [9, 10]; it is "pretty good" when the states to be distinguished are equally likely and almost orthogonal [11]; it achieves a probability of error within a factor of two of the optimal probability of error [13]; and it is asymptotically optimal [12, 15]. Because of these

properties, the LSM has been proposed as a detection measurement in many applications (see *e.g.*, [16, 17, 18]).

It turns out that in many cases of practical interest the LSM is optimal, *i.e.*, it minimizes the probability of a detection error. From the necessary and sufficient conditions for optimality discussed in Section 2 it follows that the LSM minimizes the probability of a detection error if and only if the measurement operators $\widehat{\Pi}_i = \mu_i \mu_i^*$ defined by (7) satisfy (4) for some Hermitian $\widehat{X}$ satisfying (6). A sufficient condition for optimality of the LSM is given in the following theorem, the proof of which is provided in the Appendix.

Theorem 1. *Let $\{\rho_i = \phi_i \phi_i^*, 1 \leq i \leq m\}$ denote a collection of quantum states with prior probabilities $\{p_i, 1 \leq i \leq m\}$. Let $\{\Sigma_i = \mu_i \mu_i^*, 1 \leq i \leq m\}$ with $\{\mu_i = T\psi_i, 1 \leq i \leq m\}$ denote the least-squares measurement (LSM) operators corresponding to $\{\psi_i = \sqrt{p_i}\phi_i, 1 \leq i \leq m\}$, where $T = (\Psi\Psi^*)^{-1/2}$ and Ψ is the matrix with block columns ψ_i. Then the LSM minimizes the probability of a detection error if for each i, $\mu_i^*\psi_i = \psi_i^*T\psi_i = \alpha I$, where α is a constant independent of i.*

A similar result for the special case in which the density operators ρ_i are rank-one operators of the form $\rho_i = |\phi_i\rangle\langle\phi_i|$ and the vectors $|\phi_i\rangle$ are linearly independent was derived in [16].

Note that the condition $\psi_i^*T\psi_i = \alpha I$ does not depend on the choice of factor ϕ_i. Indeed, if $\phi_i' = \phi_i Q_i$ is another factor of ρ_i with Q_i satisfying $Q_i Q_i^* = I$, and if Ψ' is the matrix of block columns $\psi_i' = \sqrt{p_i}\phi_i' = \sqrt{p_i}\phi_i Q_i$, then it is easy to see that $(\psi_i')^*(\Psi'\Psi'^*)^{-1/2}\psi_i' = \alpha I$ if and only if $\psi_i^*T\psi_i = \alpha I$.

If the state $\rho_i = \phi_i\phi_i^*$ is transmitted with prior probability p_i, then the probability of correctly detecting the state using measurement operators $\Sigma_i = \mu_i\mu_i^*$ is $p_i \text{Tr}(\mu_i^*\phi_i\phi_i^*\mu_i) = \text{Tr}(\mu_i^*\psi_i\psi_i^*\mu_i)$. It follows that if the condition for optimality of Theorem 1 is met, so that $\mu_i^*\psi_i = \alpha I$, then the probability of correctly detecting each of the states ρ_i using the LSM is α^2, independent of i.

For a pure-state ensemble consisting of states $|\phi_i\rangle$ with prior probabilities p_i, the probability of correct detection of the ith state is given by $|\langle\mu_i|\psi_i\rangle|^2$. Since $\langle\mu_i|\psi_i\rangle = \langle\psi_i|T|\psi_i\rangle > 0$ for any set

9

of weighted vectors $|\psi_i\rangle$, $\langle\mu_i|\psi_i\rangle$ is constant for all i if and only if $|\langle\mu_i|\psi_i\rangle|^2$ is constant for all i. Therefore, we may interpret the condition in Theorem 1 for pure-state ensembles as follows: The LSM is optimal for a set of states $|\phi_i\rangle$ with prior probabilities p_i if the probability of detecting each one of the states using the LSM vectors is the same, regardless of the specific state chosen.

In the remainder of the paper we use Theorem 1 to derive the optimal measurement for mixed and pure state sets with certain symmetry properties. The symmetry properties we consider are quite general, and include many cases of practical interest.

4 Geometrically Uniform State Sets

In this section we consider the case in which the density operators ρ_i are defined over a (not necessarily abelian) group of unitary matrices and are generated by a single generating matrix. Such a state set is called *geometrically uniform (GU)* [24]. We first obtain a convenient characterization of the LSM in this case and then show that under a certain constraint on the generator, the LSM minimizes the probability of a detection error. In particular, for pure-state ensembles the LSM minimizes the probability of a detection error.

Let $\mathcal{G} = \{U_i, 1 \leq i \leq m\}$ be a finite group of m unitary matrices U_i. That is, $\mathcal{G}$ contains the identity matrix I; if $\mathcal{G}$ contains U_i, then it also contains its inverse $U_i^{-1} = U_i^*$; and the product $U_i U_j$ of any two elements of $\mathcal{G}$ is in $\mathcal{G}$ [25].

A state set generated by $\mathcal{G}$ using a single generating operator ρ is a set $\mathcal{S} = \{\rho_i = U_i \rho U_i^*, U_i \in \mathcal{G}\}$. The group $\mathcal{G}$ will be called the *generating group* of $\mathcal{S}$. For concreteness we assume that $U_1 = I$ so that $\rho_1 = \rho$. Such a state set has strong symmetry properties and is called GU. For consistency with the symmetry of $\mathcal{S}$, we will assume equiprobable prior probabilities on $\mathcal{S}$.

If the state set $\{\rho_i, 1 \leq i \leq m\}$ is GU, then we can always choose factors ϕ_i of ρ_i such that $\{\phi_i = U_i \phi, U_i \in \mathcal{G}\}$ where ϕ is a factor of ρ, so that the factors ϕ_i are also GU with generator ϕ. In the remainder of this section we explicitly assume that the factors are chosen to be GU.

10

We note that in [10] a GU state set was defined for the case of rank-one ensembles. Furthermore, the generating group was assumed to be *abelian*.

In the next section we derive the LSM operators for GU state sets and show that the LSM operators are also GU with the same generating group. We will see that this implies that when using the LSM, the probability of correct detection of each of the states in a GU state set is the same regardless of the particular state chosen. From Theorem 1 it then follows that for pure-state ensembles, the LSM is optimal.

4.1 The LSM for GU States

To derive the LSM for a GU state set with generating group $\mathcal{G}$, we first show that $\Phi\Phi^*$ commutes with each of the matrices $U_i \in \mathcal{G}$. Indeed, expressing $\Phi\Phi^*$ as

$$\Phi\Phi^* = \sum_{i=1}^{m} \phi_i \phi_i^* = \sum_{i=1}^{m} U_i \phi\phi^* U_i^*, \tag{11}$$

we have that for all j,

$$
\begin{aligned}
\Phi\Phi^* U_j &= \sum_{i=1}^{m} U_i \phi\phi^* U_i^* U_j \\
&= U_j \sum_{i=1}^{m} U_j^* U_i \phi\phi^* U_i^* U_j \\
&= U_j \sum_{i=1}^{m} U_i \phi\phi^* U_i \\
&= U_j \Phi\Phi^*, \tag{12}
\end{aligned}
$$

since $\{U_j^* U_i, 1 \leq i \leq m\}$ is just a permutation of $\mathcal{G}$.

If $\Phi\Phi^*$ commutes with U_j, then

$$M = (\Phi\Phi^*)^{-1/2} \tag{13}$$

11

also commutes with U_j for all j. Thus, from (10) the LSM operators are $\Sigma_i = \mu_i \mu_i^*$ with

$$\mu_i = M\phi_i = MU_i\phi = U_iM\phi = U_i\mu, \tag{14}$$

where

$$\mu = M\phi = (\Phi\Phi^*)^{-1/2}\phi. \tag{15}$$

It follows that the LSM factors μ_i are also GU with generating group $\mathcal{G}$ and generator μ given by (15). Therefore, to compute the LSM factors for a GU state set all we need is to compute the generator μ. The remaining measurement factors are then obtained by applying the group $\mathcal{G}$ to μ.

A similar result was developed in [10] for rank-one ensembles in the case in which the group $\mathcal{G}$ is abelian using the Fourier transform defined over $\mathcal{G}$.

4.2   Optimality of the LSM

We have seen that for a GU state set $\{\rho_i = \phi_i\phi_i^*, 1 \leq i \leq m\}$ with equal prior probabilities $1/m$ and generating group $\mathcal{G} = \{U_i, 1 \leq i \leq m\}$, the LSM operators $\{\Sigma_i = \mu_i\mu_i^*, 1 \leq i \leq m\}$ are also GU with generating group $\mathcal{G}$. Therefore,

$$\mu_i^*\psi_i = \frac{1}{\sqrt{m}}\mu_i^*\phi_i = \frac{1}{\sqrt{m}}\mu^*U_i^*U_i\phi = \frac{1}{\sqrt{m}}\mu^*\phi, \tag{16}$$

where ϕ and μ are the generators of the the state factors and the LSM factors, respectively. It follows that the probability of correct detection of each one of the states ρ_i using the LSM is the same, regardless of the state transmitted. This then implies from Theorem 1 that for pure-state GU ensembles the LSM is optimal. For a mixed-state ensemble, if the generator ϕ satisfies

$$\mu^*\phi = \phi^*(\Phi\Phi^*)^{-1/2}\phi = \alpha I, \tag{17}$$

for some α, then from Theorem 1 the LSM minimizes the probability of a detection error.

Note that the condition $\mu^* \phi = \alpha I$ does not depend on the choice of generator ϕ. Indeed, if $\phi' = \phi Q$ is another factor of ρ, then from (15) the generator of the LSM factors is $\mu' = \mu Q$ so that $\mu'^* \phi' = \alpha I$ if and only if $\mu^* \phi = \alpha I$.

4.3   Optimal Measurement for Arbitrary GU State Sets

If the generator ϕ does not satisfy (17), then the LSM is no longer guaranteed to be optimal. Nonetheless, as we now show, the optimal measurement operators that minimize the probability of a detection error are GU with generating group $\mathcal{G}$. The corresponding generator can be computed very efficiently in polynomial time.

Suppose that the optimal measurement operators that maximize

$$J(\{\Pi_i\}) = \sum_{i=1}^{m} \mathrm{Tr}(\rho_i \Pi_i), \tag{18}$$

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 $\widehat{\Pi}'_i = U_j \widehat{\Pi}_{r(j,i)} U_j^*$ for any $1 \le j \le m$ are also optimal. Indeed, since $\widehat{\Pi}_i \ge 0$ and $\sum_{i=1}^{m} \widehat{\Pi}_i = I$, $\widehat{\Pi}'_i \ge 0$ and

$$\sum_{i=1}^{m} \widehat{\Pi}'_i = U_j \left(\sum_{i=1}^{m} \widehat{\Pi}_i \right) U_j^* = U_j U_j^* = I. \tag{19}$$

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

$$J(\{\widehat{\Pi}'_i\}) = \sum_{i=1}^{m} \mathrm{Tr}(\rho U_i^* U_j \widehat{\Pi}_{r(j,i)} U_j^* U_i) = \sum_{k=1}^{m} \mathrm{Tr}(\rho U_k^* \widehat{\Pi}_k U_k) = \sum_{i=1}^{m} \mathrm{Tr}(\rho_i \widehat{\Pi}_i) = \widehat{J}. \tag{20}$$

Since the measurement operators $\{\widehat{\Pi}'_i = U_j \widehat{\Pi}_{r(j,i)} U_j^*, 1 \le i \le m\}$ are optimal for any j, it follows immediately that the measurement operators $\{\overline{\Pi}_i = (1/m) \sum_{j=1}^{m} U_j \widehat{\Pi}_{r(j,i)} U_j^*, 1 \le i \le m\}$ are also

13

optimal. Indeed, it is immediate that $\overline{\Pi}_i$ satisfy (1). In addition, $J(\{\overline{\Pi}_i\}) = J(\{\widehat{\Pi}'_i\}) = \widehat{J}$. Now,

$$
\begin{aligned}
\overline{\Pi}_i &= \frac{1}{m}\sum_{j=1}^{m} U_j \widehat{\Pi}_{r(j,i)} U_j^* \\
&= \frac{1}{m}\sum_{k=1}^{m} U_i U_k^* \widehat{\Pi}_k U_k U_i^* \\
&= U_i \left(\frac{1}{m}\sum_{k=1}^{m} U_k^* \widehat{\Pi}_k U_k\right) U_i^* \\
&= U_i \widehat{\Pi} U_i^*,
\end{aligned}
\tag{21}
$$

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 $\Pi_i = U_i \Pi U_i^*$ and $\rho_i = U_i \rho U_i^*$, $\mathrm{Tr}(\rho_i \Pi_i) = \mathrm{Tr}(\rho \Pi)$, so that the problem (2) reduces to the maximization problem

$$
\max_{\Pi \in \mathcal{B}} \mathrm{Tr}(\rho \Pi),
\tag{22}
$$

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

$$
\begin{aligned}
\Pi &\geq 0; \\
\sum_{i=1}^{m} U_i \Pi U_i^* &= I.
\end{aligned}
\tag{23}
$$

Since this problem is a (convex) semidefinite programming problem, the optimal Π can be computed very efficiently in polynomial time within any desired accuracy [21, 22, 23], for example using the LMI toolbox on Matlab. Note that the problem of (22) and (23) has n^2 real unknowns and 2

constraints, in contrast with the original maximization problem (2) and (1) which has mn^2 real unknowns and $m + 1$ constraints.

We summarize our results regarding GU state sets in the following theorem:

Theorem 2 (GU state sets). *Let $\mathcal{S} = \{\rho_i = U_i \rho U_i^*, U_i \in \mathcal{G}\}$ be a geometrically uniform (GU) state set generated by a finite group $\mathcal{G}$ of unitary matrices, where $\rho = \phi\phi^*$ is an arbitrary generator, and let Φ be the matrix of columns $\phi_i = U_i\phi$. Then the least-squares measurement (LSM) is given by the measurement operators $\Sigma_i = \mu_i \mu_i^*$ with*

$$\mu_i = U_i\mu$$

where

$$\mu = (\Phi\Phi^*)^{-1/2}\phi.$$

The LSM has the following properties:

1. *The measurement operators are GU with generating group $\mathcal{G}$;*

2. *The probability of correctly detecting each of the states ρ_i using the LSM is the same;*

3. *If $\mu^*\phi = \phi^*(\Phi\Phi^*)^{-1/2}\phi = \alpha I$ then the LSM minimizes the probability of a detection error; In particular, if $\phi = |\phi\rangle$ is a vector so that the state set is a rank-one ensemble, then the LSM minimizes the probability of a detection error.*

For an arbitrary generator ϕ the optimal measurement operators that minimize the probability of a detection error are also GU with generating group $\mathcal{G}$ and generator Π that maximizes $Tr(\rho\Pi)$ subject to $\Pi \geq 0$ and $\sum_{i=1}^{m} U_i\Pi U_i^* = I$.

15

5   Compound Geometrically Uniform State Sets

In this section, we consider state sets which consist of subsets that are GU, and are therefore referred to as *compound geometrically uniform (CGU)* [19]. As we show, the LSM operators are also CGU so that they can be computed using a *set* of generators. Under a certain condition on the generators, we also show that the optimal measurement associated with a CGU state set is equal to the LSM. For arbitrary CGU state sets, the optimal measurement is no longer equal to the LSM. Nonetheless, as we show, the optimal measurement operators are also CGU and we derive an efficient computational method for finding the optimal generators.

A CGU state set is defined as a set of density operators $\mathcal{S} = \{\rho_{ik} = \phi_{ik}\phi_{ik}^*, 1 \leq i \leq l, 1 \leq k \leq r\}$ such that $\rho_{ik} = U_i \rho_k U_i^*$, where the matrices $\{U_i, 1 \leq i \leq l\}$ are unitary and form a group $\mathcal{G}$, and the operators $\{\rho_k, 1 \leq k \leq r\}$ are the generators. For concreteness we assume that $U_1 = I$ so that $\rho_{1k} = \rho_k$. We also assume equiprobable prior probabilities on $\mathcal{S}$.

If the state set $\{\rho_{ik}, 1 \leq i \leq l, 1 \leq k \leq r\}$ is CGU, then we can always choose factors ϕ_{ik} of ρ_{ik} such that $\{\phi_{ik} = U_i \phi_k, 1 \leq i \leq l\}$ where ϕ_k is a factor of ρ_k, so that the factors ϕ_{ik} are also CGU with generators $\{\phi_k, 1 \leq k \leq r\}$. In the remainder of this section we explicitly assume that the factors are chosen to be CGU.

A CGU state set is in general not GU. However, for every k, the matrices $\{\phi_{ik}, 1 \leq i \leq l\}$ and the operators $\{\rho_{ik}, 1 \leq i \leq l\}$ are GU with generating group $\mathcal{G}$.

5.1 Example of a Compound Geometrically Uniform State Set

An example of a CGU state set is illustrated in Fig. 2. In this example the state set is $\{\rho_{ik} = |\phi_{ik}\rangle\langle\phi_{ik}|, 1 \leq i, k \leq 2\}$ where $\{|\phi_{ik}\rangle = U_i|\phi_k\rangle, U_i \in \mathcal{G}\}$, $\mathcal{G} = \{I_2, U\}$ with

$$U = \frac{1}{2}\begin{bmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}, \tag{24}$$

and the generating vectors are

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |\phi_2\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}. \tag{25}$$

The matrix U represents a reflection about the dashed line in Fig. 2. Thus, the vector $|\phi_{21}\rangle$ is obtained by reflecting the generator $|\phi_{11}\rangle$ about this line, and similarly the vector $|\phi_{22}\rangle$ is obtained by reflecting the generator $|\phi_{12}\rangle$ about this line.

As can be seen from the figure, the state set is not GU. In particular, there is no isometry that transforms $|\phi_{11}\rangle$ into $|\phi_{12}\rangle$ while leaving the set invariant. However, the sets $\mathcal{S}_1 = \{|\phi_{11}\rangle, |\phi_{21}\rangle\}$ and $\mathcal{S}_2 = \{|\phi_{12}\rangle, |\phi_{22}\rangle\}$ are both GU with generating group $\mathcal{G}$.

5.2 The LSM for CGU State Sets

We now derive the LSM for a CGU state set with equal prior probabilities. Let Φ denote the matrix of columns ϕ_{ik}. Then for a CGU state set with generating group $\mathcal{G}$, $\Phi\Phi^*$ commutes with each of the matrices $U_i \in \mathcal{G}$. Indeed, expressing $\Phi\Phi^*$ as

$$\Phi\Phi^* = \sum_{i=1}^{l}\sum_{k=1}^{r}\phi_{ik}\phi_{ik} = \sum_{i=1}^{l} U_i\left(\sum_{k=1}^{r}\phi_k\phi_k\right)U_i^*, \tag{26}$$

17

Figure 2: A compound geometrically uniform pure-state set. The state sets $\mathcal{S}_1 = \{|\phi_{11}\rangle, |\phi_{21}\rangle\}$ and $\mathcal{S}_2 = \{|\phi_{12}\rangle, |\phi_{22}\rangle\}$ are both geometrically uniform (GU) with the same generating group; Both sets are invariant under a reflection about the dashed line. However, the combined set $\mathcal{S} = \{|\phi_{11}\rangle, |\phi_{21}\rangle, |\phi_{12}\rangle, |\phi_{22}\rangle\}$ is no longer GU.

we have that for all j,

$$
\begin{aligned}
\Phi\Phi^* U_j &= \sum_{i=1}^{l} U_i \left(\sum_{k=1}^{r} \phi_k \phi_k \right) U_i^* U_j \\
&= U_j \sum_{i=1}^{l} U_j^* U_i \left(\sum_{k=1}^{r} \phi_k \phi_k \right) U_i^* U_j \\
&= U_j \sum_{i=1}^{l} U_i \left(\sum_{k=1}^{r} \phi_k \phi_k \right) U_i^* \\
&= U_j \Phi\Phi^*,
\end{aligned}
\tag{27}
$$

since $\{U_j^* U_i, 1 \leq i \leq l\}$ is just a permutation of $\mathcal{G}$.

If $\Phi\Phi^*$ commutes with U_j, then $M = (\Phi\Phi^*)^{-1/2}$ also commutes with U_j for all j. Thus, the LSM operators are $\Sigma_{ik} = \mu_{ik}\mu_{ik}^*$ with

$$
\mu_{ik} = M\phi_{ik} = MU_i\phi_k = U_iM\phi_k = U_i\mu_k,
\tag{28}
$$

18

where

$$\mu_k = M\phi_k = (\Phi\Phi^*)^{-1/2}\phi_k. \tag{29}$$

Therefore the LSM factors are also CGU with generating group $\mathcal{G}$ and generators μ_k given by (29). To compute the LSM factors all we need is to compute the generators μ_k. The remaining measurement factors are then obtained by applying the group $\mathcal{G}$ to each of the generators.

For the CGU state set of Fig. 2 we have that

$$\Phi\Phi^* = 2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{30}$$

Therefore, the LSM vectors are $\{|\mu_{ik}\rangle = U_i|\mu_k\rangle, U_i \in \mathcal{G}, 1 \leq i, k \leq 2\}$ where $\mathcal{G} = \{I_2, U\}$ with U given by (24), and from (29) the generating vectors are

$$|\mu_1\rangle = \frac{1}{\sqrt{2}}|\phi_1\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |\mu_2\rangle = \frac{1}{\sqrt{2}}|\phi_2\rangle = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix}. \tag{31}$$

The LSM vectors are depicted in Fig. 3. The vectors have the same symmetries as the state set of Fig. 2, with different generating vectors. Since in this example the generating vectors satisfy $|\mu_k\rangle = (1/\sqrt{2})|\phi_k\rangle$, we have that $|\mu_{ik}\rangle = (1/\sqrt{2})|\phi_{ik}\rangle$ for $1 \leq i, k \leq 2$.

5.3 CGU State Sets With GU Generators

A special class of CGU state sets is *CGU state sets with GU generators* in which the generators $\{\rho_k = \phi_k\phi_k^*, 1 \leq k \leq r\}$ and the factors ϕ_k are themselves GU. Specifically, $\{\phi_k = V_k\phi\}$ for some generator ϕ, where the matrices $\{V_k, 1 \leq k \leq r\}$ are unitary, and form a group $\mathcal{Q}$.

Suppose that U_p and V_t commute up to a phase factor for all t and p so that $U_pV_t = V_tU_pe^{j\theta(p,t)}$ where $\theta(p,t)$ is an arbitrary phase function that may depend on the indices p and t. In this case we say that $\mathcal{G}$ and $\mathcal{Q}$ commute up to a phase factor and that the corresponding state set is *CGU*

Figure 3: The least-squares measurement vectors associated with the compound geometrically uniform state set of Fig. 2. As can be seen from the figure, the measurement vectors have the same symmetries as the original state set.

with commuting GU generators. (In the special case in which $\theta = 0$ so that $U_i V_k = V_k U_i$ for all i, k, the resulting state set is GU [19]). Then for all p, t,

$$
\begin{aligned}
\Phi\Phi^* U_p V_t &= \sum_{i=1}^{l} U_i \left(\sum_{k=1}^{r} V_k \phi\phi^* V_k^* \right) U_i^* U_p V_t \\
&= U_p V_t \sum_{i=1}^{l} V_t^* U_p^* U_i \left(\sum_{k=1}^{r} V_k \phi\phi^* V_k^* \right) U_i^* U_p V_t \\
&= U_p V_t \sum_{i=1}^{l} V_t^* U_i \left(\sum_{k=1}^{r} V_k \phi\phi^* V_k^* \right) U_i^* V_t \\
&= U_p V_t \sum_{i=1}^{l} U_i \left(\sum_{k=1}^{r} V_t^* V_k \phi\phi^* V_k^* V_t \right) U_i^* \\
&= U_p V_t \sum_{i=1}^{l} U_i \left(\sum_{k=1}^{r} V_k \phi\phi^* V_k^* \right) U_i^* \\
&= U_p V_t \Phi\Phi^*.
\end{aligned}
\tag{32}
$$

The LSM factors μ_{ik} are then given by

$$
\mu_{ik} = M\phi_{ik} = MU_i V_k \phi = U_i V_k M\phi = U_i V_k \bar{\mu},
\tag{33}
$$

20

where $\bar{\mu} = M\phi$. Thus even though the state set is not in general GU, the LSM factors can be computed using a single generator.

Alternatively, we can express μ_{ik} as $\mu_{ik} = U_i\mu_k$ where the generators μ_k are given by

$$\mu_k = V_k\bar{\mu}. \tag{34}$$

From (34) it follows that the generators μ_k are GU with generating group $\mathcal{Q} = \{V_k, 1 \leq k \leq r\}$ and generator $\bar{\mu}$.

We conclude that for a CGU state set with commuting GU generators and generating group $\mathcal{Q}$, the LSM vectors are also CGU with commuting GU generators and generating group $\mathcal{Q}$.

5.4 Example of a CGU State Set with Commuting GU Generators

We now consider an example of a CGU state set with commuting GU generators. Consider the group $\mathcal{G}$ of l unitary matrices on $\mathbb{C}^l$ where $U_i = Z^i, 1 \leq i \leq l$ and Z is the matrix defined by

$$Z \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{l-1} \\ x_l \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ \vdots \\ x_l \\ x_1 \end{bmatrix}. \tag{35}$$

Let $\mathcal{Q}$ be the group of $r = l$ unitary matrices $V_k = B^k, 1 \leq k \leq l$ where B is the diagonal matrix with diagonal elements $e^{j2\pi s/l}, 0 \leq s \leq l-1$. We can immediately verify that for this choice of $\mathcal{Q}$ and $\mathcal{G}$, $U_iV_k = V_kU_ie^{j2\pi/l}$. We therefore conclude that the LSM operators corresponding to the CGU state set $\mathcal{S} = \{\rho_{ik} = \phi_{ik}\phi_{ik}^*\}$ with $\{\phi_{ik} = U_i\phi_k, U_i \in \mathcal{G}\}$ and $\{\phi_k = V_k\phi, V_k \in \mathcal{Q}\}$ for some generator ϕ, are also CGU with commuting GU generators and can therefore be generated by a

single generator.

As a special case, suppose that $l = 2$ so that $\mathcal{G}$ consists of the matrices $U_1 = I_2$ and $U_2 = Z$ where

$$Z = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{36}$$

and $\mathcal{Q}$ consists of the matrices $V_1 = I_2$ and $V_2 = B$ where

$$B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{37}$$

Let the state set be $\mathcal{S} = \{|\phi_{ik}\rangle = U_i V_k |\phi\rangle, \ 1 \leq i, k \leq 2\}$, where $\phi = [\beta_1 \ \beta_2]^*$. Since $|\phi\rangle$ must be normalized, $\beta_1^2 + \beta_2^2 = 1$. Then,

$$|\phi_{11}\rangle = \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}, \ |\phi_{21}\rangle = \begin{bmatrix} \beta_2 \\ \beta_1 \end{bmatrix}, \ |\phi_{12}\rangle = \begin{bmatrix} \beta_1 \\ -\beta_2 \end{bmatrix}, \ |\phi_{22}\rangle = \begin{bmatrix} -\beta_2 \\ \beta_1 \end{bmatrix}. \tag{38}$$

The LSM vectors are given by $\{|\mu_{ik}\rangle = U_i V_k |\bar{\mu}\rangle, \ 1 \leq i, k \leq 2\}$, where $|\bar{\mu}\rangle = (\Phi\Phi^*)^{-1/2}|\phi\rangle$, and

$$\Phi = \begin{bmatrix} \beta_1 & \beta_2 & \beta_1 & -\beta_2 \\ \beta_2 & \beta_1 & -\beta_2 & \beta_1 \end{bmatrix}. \tag{39}$$

We can immediately verify that

$$\Phi\Phi^* = \begin{bmatrix} 2(\beta_1^2 + \beta_2^2) & 0 \\ 0 & 2(\beta_1^2 + \beta_2^2) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}. \tag{40}$$

Thus, the LSM vectors are

$$|\mu_{ik}\rangle = \frac{1}{\sqrt{2}}|\phi_{ik}\rangle. \tag{41}$$

22

In Fig. 4 we plot the state vectors given by (38) for the case in which $|\phi\rangle = (1/\sqrt{5})[2\ 1]^*$. As can be seen from the figure, the state set is not GU. In particular, there is no isometry that transforms $|\phi_{11}\rangle$ into $|\phi_{12}\rangle$ while leaving the set invariant. Nonetheless, we have seen that the LSM vectors can be generated by a single generating vector $|\mu\rangle = (1/\sqrt{2})|\phi\rangle$.

Figure 4: A compound geometrically uniform state set with commuting geometrically uniform (GU) generators. The state sets $\mathcal{S}_1 = \{|\phi_{11}\rangle, |\phi_{21}\rangle\}$ and $\mathcal{S}_2 = \{|\phi_{12}\rangle, |\phi_{22}\rangle\}$ are both GU with the same generating group; Both sets are invariant under a reflection about the dashed line. The set of generators $\{|\phi_{11}\rangle, |\phi_{12}\rangle\}$ is GU and is invariant under a reflection about the x-axis. The combined set $\mathcal{S} = \{|\phi_{11}\rangle, |\phi_{21}\rangle, |\phi_{12}\rangle, |\phi_{22}\rangle\}$ is no longer GU. Nonetheless, the LSM vectors are generated by a single generating vector and are given by $|\mu_{ik}\rangle = (1/\sqrt{2})|\phi_{ik}\rangle$.

Note, that in the example of Section 5.1 the CGU state set also has GU generators. Specifically, the set of generators $\{|\phi_1\rangle, |\phi_2\rangle\}$ with $|\phi_1\rangle = |\phi_{11}\rangle$ and $|\phi_2\rangle = |\phi_{12}\rangle$ is invariant under a reflection about the x-axis: $|\phi_2\rangle = B|\phi_1\rangle$ where B is given by (37). However, the group $\mathcal{Q} = \{I_2, B\}$ of generators does not commute up to a phase with the generating group $\mathcal{G} = \{I_2, U\}$, where U is given by (24) and represents a reflection about the dashed line in Fig. 2. This can be verified graphically from Fig. 2: Suppose we apply B to $|\phi_{11}\rangle$ and then apply U. Then the resulting vector is equal to $|\phi_{22}\rangle$. If on the other hand we first apply U to $|\phi_{11}\rangle$ and then apply B, then the resulting vector is the reflection of $|\phi_{21}\rangle$ about the x-axis, which is not related to $|\phi_{22}\rangle$ by a phase factor.

Now, consider the state set in Fig. 4. In this case $\mathcal{Q} = \{I_2, B\}$ and $\mathcal{G} = \{I_2, Z\}$ where B

represents a reflection about the x-axis and Z represents a reflection about the dashed line in Fig. 4. We can immediately verify from the figure that applying Z and then B to any vector in the set results in a vector that is equal up to a minus sign to the vector that results from first applying B and then Z. For example, applying B to $|\phi_{11}\rangle$ and then applying Z results in $|\phi_{22}\rangle$. If on the other hand we first apply Z to $|\phi_{11}\rangle$ and then apply B, then the resulting vector is the reflection of $|\phi_{21}\rangle$ about the x-axis, which is equal to $-|\phi_{22}\rangle$.

5.5   Optimality of the LSM

We have seen in the previous section that the LSM operators corresponding to a CGU state set with generating group $\mathcal{G} = \{U_i, 1 \leq i \leq l\}$ is also CGU with the same generating group. In particular for each k, the sets $\mathcal{S}'_k = \{\mu_{ik}, 1 \leq i \leq l\}$ and $\mathcal{S}_k = \{\phi_{ik}, 1 \leq i \leq l\}$ are both GU with generating group $\mathcal{G}$. Therefore,

$$\mu_{ik}^* \phi_{ik} = \mu_k^* U_i^* U_i \phi_k = \mu_k^* \phi_k, \tag{42}$$

which implies that the probability of correctly detecting each of the states in $\mathcal{S}_k$ using the LSM is the same. It follows from Theorem 1 that if

$$\mu_k^* \phi_k = \phi_k^* M \phi_k = \alpha I, \quad 1 \leq k \leq r, \tag{43}$$

then the LSM minimizes the probability of a detection error.

Note that the condition $\mu_k^* \phi_k = \alpha I$ does not depend on the choice of generator ϕ_k. Indeed, if $\phi'_k = \phi_k Q_k$ is another factor of ρ_k, then from (29) the generator of the LSM factors is $\mu'_k = \mu_k Q_k$ so that $\mu_k'^* \phi'_k = \alpha I$ if and only if $\mu_k^* \phi_k = \alpha I$.

In Section 5.3 we showed that the LSM operators corresponding to a CGU state set with GU generators $\{\phi_k = V_k \phi\}$ where $V_k \in \mathcal{Q}$ and $\mathcal{G}$ and $\mathcal{Q}$ commute up to a phase factor, are also CGU

with GU generators generated by the same group $\mathcal{Q}$ and some generator $\bar{\mu}$. Therefore for all k,

$$\mu_k^* \phi_k = \bar{\mu}^* V_k^* V_k \phi = \bar{\mu}^* \phi, \tag{44}$$

so that the probability of correctly detecting each of the states ϕ_{ik} is the same. If in addition,

$$\bar{\mu}^* \phi = \phi^* M \phi = \alpha I, \tag{45}$$

then combining (42), (44) and (45) with Theorem 1 we conclude that the LSM minimizes the probability of a detection error. In particular, for a rank-one ensemble, $\bar{\mu}^* \phi$ is a scalar so that (45) is always satisfied. Therefore, for a rank-one CGU state set with commuting GU generators, the LSM minimizes the probability of a detection error.

5.6 Optimal Measurement for Arbitrary CGU State Sets

If the generators ϕ_k do not satisfy (43), then the LSM is no longer guaranteed to be optimal. Nonetheless, as we now show, the optimal measurement operators that minimize the probability of a detection error are CGU with generating group $\mathcal{G}$. The corresponding generators can be computed very efficiently in polynomial time within any desired accuracy.

Suppose that the optimal measurement operators that maximize

$$J(\{\Pi_{ik}\}) = \sum_{i=1}^{l} \sum_{k=1}^{r} \text{Tr}(\rho_{ik} \Pi_{ik}), \tag{46}$$

are $\widehat{\Pi}_{ik}$, and let $\widehat{J} = J(\{\widehat{\Pi}_{ik}\}) = \sum_{i=1}^{l} \sum_{k=1}^{r} \text{Tr}(\rho_{ik} \widehat{\Pi}_{ik})$. Let $r(j,i)$ be the mapping from $\mathcal{I} \times \mathcal{I}$ to $\mathcal{I}$ with $\mathcal{I} = \{1, \ldots, l\}$, defined by $r(j,i) = s$ if $U_j^* U_i = U_s$. Then the measurement operators $\widehat{\Pi}'_{ik} = U_j \widehat{\Pi}_{r(j,i)k} U_j^*$ for any $1 \leq j \leq l$ are also optimal. Indeed, since $\widehat{\Pi}_{ik} \geq 0$ and $\sum_{i,k} \widehat{\Pi}_{ik} = I$,

$\widehat{\Pi}'_{ik} \geq 0$ and

$$\sum_{i=1}^{l} \sum_{k=1}^{r} \widehat{\Pi}'_{ik} = U_j \left(\sum_{i=1}^{l} \sum_{k=1}^{r} \widehat{\Pi}_{ik} \right) U_j^* = U_j U_j^* = I. \tag{47}$$

Finally, using the fact that $\rho_{ik} = U_i \rho_k U_i^*$ for some generators ρ_k,

$$J(\{\widehat{\Pi}'_{ik}\}) = \sum_{i=1}^{l} \sum_{k=1}^{r} \mathrm{Tr}(\rho_k U_i^* U_j \widehat{\Pi}_{r(j,i)k} U_j^* U_i) = \sum_{s=1}^{l} \sum_{k=1}^{r} \mathrm{Tr}(\rho_k U_s^* \widehat{\Pi}_{sk} U_s) = \sum_{i=1}^{l} \sum_{k=1}^{r} \mathrm{Tr}(\rho_{ik} \widehat{\Pi}_{ik}) = \widehat{J}. \tag{48}$$

Since the measurement operators $\{\widehat{\Pi}'_{ik} = U_j \widehat{\Pi}_{r(j,i)k} U_j^*, 1 \leq i \leq l, 1 \leq k \leq r\}$ are optimal for any j, it follows immediately that the measurement operators $\{\overline{\Pi}_{ik} = (1/l) \sum_{j=1}^{l} U_j \widehat{\Pi}_{r(j,i)k} U_j^*, 1 \leq i \leq l, 1 \leq k \leq r\}$ are also optimal. Indeed, it is immediate that $\overline{\Pi}_{ik}$ satisfy (1). In addition, $J(\{\overline{\Pi}_{ik}\}) = J(\{\widehat{\Pi}'_{ik}\}) = \widehat{J}$. Now,

$$\begin{aligned}
\overline{\Pi}_{ik} &= \frac{1}{l} \sum_{j=1}^{l} U_j \widehat{\Pi}_{r(j,i)k} U_j^* \\
&= \frac{1}{l} \sum_{s=1}^{l} U_i U_s^* \widehat{\Pi}_{sk} U_s U_i^* \\
&= U_i \left(\frac{1}{l} \sum_{s=1}^{l} U_s^* \widehat{\Pi}_{sk} U_s \right) U_i^* \\
&= U_i \widehat{\Pi}_k U_i^*, \tag{49}
\end{aligned}$$

where $\widehat{\Pi}_k = (1/l) \sum_{s=1}^{l} U_s^* \widehat{\Pi}_{sk} U_s$.

We therefore conclude that the optimal measurement operators can always be chosen to be CGU 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 $\{\widehat{\Pi}_k, 1 \leq k \leq r\}$. The remaining operators are obtained by applying the group $\mathcal{G}$ to each of the generators.

Since the optimal measurement operators satisfy $\Pi_{ik} = U_i \Pi_k U_i^*$ and $\rho_{ik} = U_i \rho_k U_i^*$, $\mathrm{Tr}(\rho_{ik} \Pi_{ik}) =$

$\text{Tr}(\rho_k \Pi_k)$, so that the problem (2) reduces to the maximization problem

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

subject to the constraints

$$\begin{aligned} \Pi_k &\geq 0, \quad 1 \leq k \leq r \\ \sum_{i=1}^{l} \sum_{k=1}^{r} U_i \Pi_k U_i^* &= I. \end{aligned} \qquad (51)$$

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 [21, 22, 23], for example using the LMI toolbox on Matlab. Note that the problem of (50) and (51) has rn^2 real unknowns and $r + 1$ constraints, in contrast with the original maximization problem (2) and (1) which has lrn^2 real unknowns and $lr + 1$ constraints.

We summarize our results regarding CGU state sets in the following theorem:

Theorem 3 (CGU state sets). *Let $\mathcal{S} = \{\rho_{ik} = U_i \rho_k U_i^*, U_i \in \mathcal{G}, 1 \leq k \leq r\}$ be a compound geometrically uniform (CGU) state set generated by a finite group $\mathcal{G}$ of unitary matrices and generators $\{\rho_k = \phi_k \phi_k^*, 1 \leq k \leq r\}$, and let Φ be the matrix of columns $\phi_{ik} = U_i \phi_k$. Then the least-squares measurement (LSM) is given by the measurement operators $\Sigma_i = \mu_i \mu_i^*$ with*

$$\mu_{ik} = U_i \mu_k$$

where

$$\mu_k = (\Phi\Phi^*)^{-1/2} \phi_k.$$

The LSM has the following properties:

1. The measurement operators are CGU with generating group $\mathcal{G}$;

2. The probability of correctly detecting each of the states ϕ_{ik} for fixed k using the LSM is the same;

3. If $\mu_k^* \phi_k = \phi_k^* (\Phi\Phi^*)^{-1/2} \phi_k = \alpha I$ for $1 \leq k \leq r$ then the LSM minimizes the probability of a detection error.

If in addition the generators $\{\phi_k = V_k \phi, 1 \leq k \leq r\}$ are geometrically uniform with $U_i V_k = V_k U_i e^{j\theta(i,k)}$ for all i, k, then

1. $\mu_{ik} = U_i V_k \bar{\mu}$ where $\bar{\mu} = (\Phi\Phi^*)^{-1/2}\phi$ so that the LSM operators are CGU with geometrically uniform generators;

2. The probability of correctly detecting each of the states ϕ_{ik} using the LSM is the same;

3. If $\bar{\mu}^* \phi = \phi^* (\Phi\Phi^*)^{-1/2} \phi = \alpha I$ then the LSM minimizes the probability of a detection error. In particular, if $\phi = |\phi\rangle$ is a vector so that the state set is a rank-one ensemble, then the LSM minimizes the probability of a detection error.

For arbitrary CGU state sets the optimal measurement operators that minimize the probability of a detection error are CGU with generating group $\mathcal{G}$ and generators Π_k that maximize $\sum_{k=1}^{r} Tr(\rho_k \Pi_k)$ subject to $\Pi_k \geq 0, 1 \leq k \leq r$ and $\sum_{i,k} U_i \Pi_k U_i^* = I$.

6 Conclusion

In this paper we considered the optimal measurement operators that minimize the probability of a detection error when distinguishing between a collection of *mixed* quantum states. We first derived a general condition under which the LSM minimizes the probability of a detection error. We then considered state sets with a broad class of symmetry properties for which the LSM is optimal. Specifically, we showed that for GU state sets and for CGU state sets with generators

that satisfy certain constraints, the LSM is optimal. We also showed that for arbitrary GU and CGU state sets, the optimal measurement operators have the same symmetries as the original state sets. Therefore, to compute the optimal measurement operators, we need only to compute the corresponding generators. As we showed, the generators can be computed very efficiently in polynomial time within any desired accuracy by solving a semidefinite programming problem.

Appendix

Proof of Theorem 1

In this appendix we prove Theorem 1. Specifically, we show that for a set of states $\rho_i = \phi_i \phi_i^*$ with prior probabilities p_i, if $\mu_i^* \psi_i = \alpha I$, where $\mu_i = (\Psi \Psi^*)^{-1/2} \psi_i$ are the LSM factors and $\psi_i = \sqrt{p_i} \phi_i$, then there exists an Hermitian X such that

$$
\begin{aligned}
X &\geq \psi_i \psi_i^*, \quad 1 \leq i \leq m; \\
(X - \psi_i \psi_i^*) \mu_i \mu_i^* &= 0, \quad 1 \leq i \leq m.
\end{aligned}
\tag{52}
$$

Let X be the symmetric matrix defined by $X = \alpha W^{1/2}$ where $W = \Psi \Psi^*$. Since $\alpha I = \psi_j^* W^{-1/2} \psi_j = \psi_j^* W^{-1/4} W^{-1/4} \psi_j$, it follows that

$$
\alpha I \geq W^{-1/4} \psi_j \psi_j^* W^{-1/4}.
\tag{53}
$$

Multiplying both sides of (53) by $W^{1/4}$ we have

$$
\alpha W^{1/2} \geq \psi_j \psi_j^*,
\tag{54}
$$

which verifies that the conditions (52) are satisfied.

Next,

$$(X - \psi_i\psi_i^*)\mu_i = \alpha(\Psi\Psi^*)^{1/2}(\Psi\Psi^*)^{-1/2}\psi_i - \alpha\psi_i = 0, \tag{55}$$

so that (52) is also satisfied.

References

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

[2] A. Peres, "Neumark's theorem and quantum inseparability," *Found. Phys.*, vol. 20, no. 12, pp. 1441–1453, 1990.

[3] A. S. Holevo, "Statistical decisions in quantum theory," *J. Multivar. Anal.*, vol. 3, pp. 337–394, Dec. 1973.

[4] H. P. Yuen, R. S. Kennedy, and M. Lax, "Optimum testing of multiple hypotheses in quantum detection theory," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 125–134, Mar. 1975.

[5] Y. C. Eldar, A. Megretski, and G. C. Verghese, "Designing optimal quantum detectors via semidefinite programming," *IEEE Trans. Inform. Theory*, to appear; also available at http://www.arXiv.org/abs/quant-ph/0205178.

[6] C. W. Helstrom, "Bayes-cost reduction algorithm in quantum hypothesis testing," *IEEE Trans. Inform. Theory*, vol. 28, pp. 359–366, Mar. 1982.

[7] M. Charbit, C. Bendjaballah, and C. W. Helstrom, "Cutoff rate for the m-ary PSK modulation channel with optimal quantum detection," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1131–1133, Sep. 1989.

[8] M. Osaki, M. Ban, and O. Hirota, "Derivation and physical interpretation of the optimum detection operators for coherent-state signals," *Phys. Rev. A*, vol. 54, pp. 1691–1701, Aug. 1996.

[9] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, "Optimum measurements for discrimination among symmetric quantum states and parameter estimation," *Int. J. Theor. Phys.*, vol. 36, pp. 1269–1288, 1997.

[10] Y. C. Eldar and G. D. Forney, Jr., "On quantum detection and the square-root measurement," *IEEE Trans. Inform. Theory*, vol. 47, pp. 858–872, Mar. 2001.

[11] P. Hausladen and W. K. Wootters, "A 'pretty good' measurement for distinguishing quantum states," *J. Mod. Opt.*, vol. 41, pp. 2385–2390, 1994.

[12] P. Hausladen, R. Josza, B. Schumacher, M. Westmoreland, and W. K. Wootters, "Classical information capacity of a quantum channel," *Phys. Rev. A*, vol. 54, pp. 1869–1876, Sep. 1996.

[13] H. Barnum and E. Knill, "Reversing quantum dynamics with near-optimal quantum and classical fidelity," http://xxx.lanl.gov/abs/quant-ph/0004088.

[14] J. I. Concha and H. V. Poor, "An optimality property of the square-root measurement for mixed states," *Proc. Sixth Int. Conf. Quantum Communication, Measurement, and Computing (Cambridge, MA)*, July 2002.

[15] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inform. Theory*, vol. 44, pp. 269–273, 1998.

[16] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," *Phys. Rev. A*, vol. 58, pp. 146–158, July 1998.

[17] M. Sasaki, T. Sasaki-Usuda, M. Izutsu, and O. Hirota, "Realization of a collective decoding of code-word states," *Phys. Rev. A*, vol. 58, pp. 159–164, July 1998.

[18] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, "Quantum detection and mutual information for QAM and PSK signals," *IEEE Trans. Commun*, vol. 47, pp. 248–254, Feb. 1999.

[19] Y. C. Eldar and H. Bölcskei, "Geometrically uniform frames," *IEEE Trans. Inform. Theory*, to appear; also available at `http://arXiv.org/abs/math.FA/0108096`.

[20] G. H. Golub and C. F. Van Loan, *Matrix Computations*, Baltimore MD: Johns Hopkins Univ. Press, third edition, 1996.

[21] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Rev.*, vol. 38, no. 1, pp. 40–95, Mar. 1996.

[22] F. Alizadeh, *Combinatorial Optimization With Interior Point Methods and Semi-Definite Matrices*, Ph.D. thesis, University of Minnesota, Minneapolis, MN, Oct. 1991.

[23] Y. Nesterov and A. Nemirovski, *Interior-Point Polynomial Algorithms in Convex Programming*, Philadelphia, PE: SIAM, 1994.

[24] G. D. Forney, Jr., "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, Sep. 1991.

[25] M. A. Armstrong, *Groups and Symmetry*, New York: Springer-Verlag, 1988.