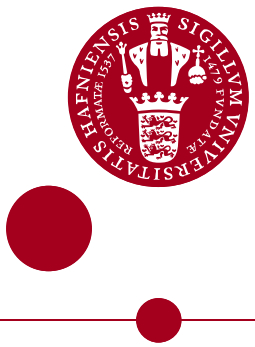
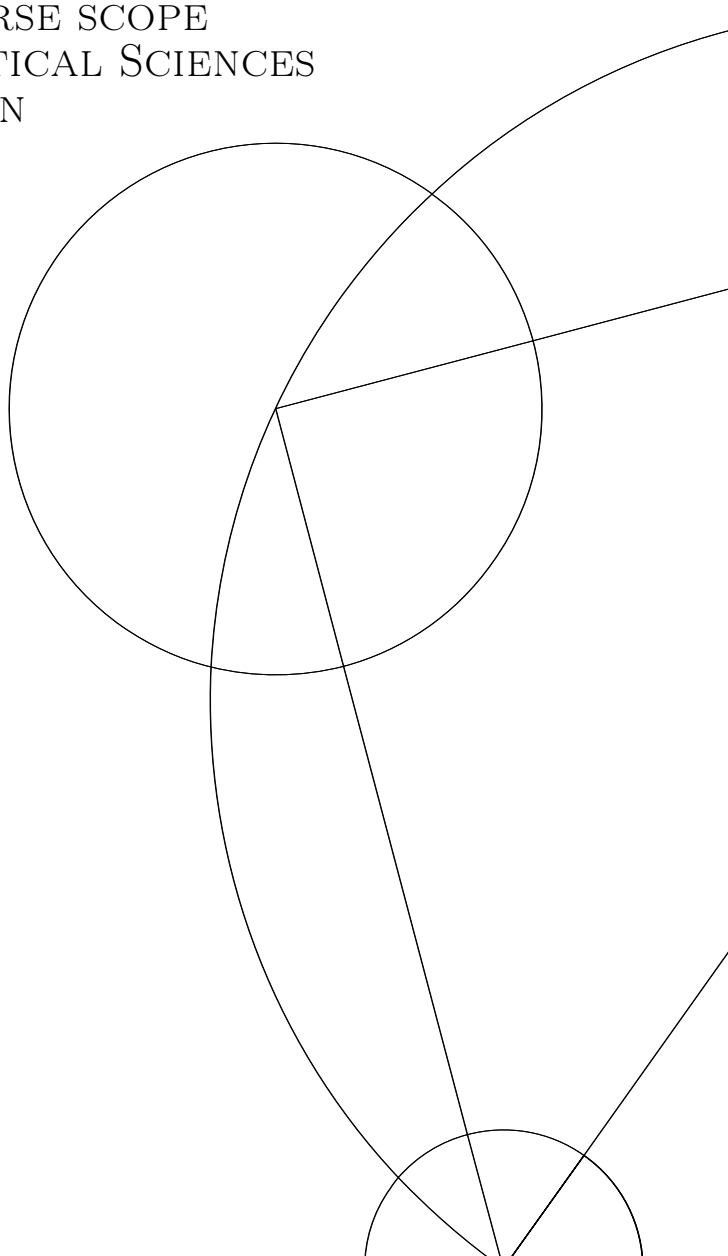
UNIVERSITY OF COPENHAGEN



Local quantum state discrimination

Project outside the course scope
Department of Mathematical Sciences
University of Copenhagen

Sigurd A. L. Storgaard
qmt293



Supervisor: Laura Mančinska

Date: January 27, 2022

Contents

Abstract

Quantum state discrimination is one of the most fundamental problems in quantum information theory and it has a very wide range of applications. Although widely studied, there are still many open problems within this field. In this thesis we will study a recently introduced discrimination problem termed *local simultaneous state discrimination* (LSSD) [12]. In this game the participants, Alice and Bob are to distinguish between a number of bipartite quantum states without communication. They win if and only if they both succeed in doing so. The entanglement and no-signalling assisted versions of the problem also introduced in [12] will be studied as well. We derive upper bounds on the winning probability in two different cases: Alice and Bob are to discriminate (1) two product states and (2) the states $\frac{1}{\sqrt{2}}(|i2\rangle + |2i\rangle)$ for $i = 0, 1$. In so doing, we find a gap with the upper bound in the no-signalling assisted problem in both of these cases. Moreover, we propose a numerical method of studying LSSD problems based on see-saw semi-definite programming.

1 Introduction

It is a consequence of the underlying axioms of quantum mechanics that non-orthogonal quantum states cannot be distinguished with certainty [2]. The task of optimally discriminating between quantum states is fundamental in quantum information science [18]. However, due to its close links to the foundation of quantum mechanics the interest arose long before the field of quantum information science was born.

In the late 1960's to mid 1970's, motivated by the development of optical communication [1], the problem was given a rigorous definition and solid mathematical foundation in the canonical works of Holevo and Helstrom [9, 10]. Optimal quantum state discrimination of two states was found. Unfortunately, apart from this simple case the problem is difficult. Much progress has been made within the last two decades [1]. For example, an analytical solution for optimal discrimination of qubits assigned at random has been obtained in [6].

Recently, in [12] the task of *local simultaneous state discrimination* (LSSD) was introduced as a type of quantum game. In this game the participants, Alice and Bob, receive one of N bipartite quantum states. By means of local operations they are to discriminate the states. They *win* if and only if they are both successful. As the authors of [12] note, this problem has only received little attention compared to the less restrictive more well-studied *local operations and classical communication* scenario (see e.g. [4]). The original motivation for introducing the LSSD problem in [12] comes from quantum cryptography. More specifically, when strengthening the encryption security notions from *indistinguishability* to *uncloneable indistinguishability* as in [3] the adversary is required to successfully perform LSSD.

In [12] the authors are mostly concerned with LSSD problems involving any number of classical states. They introduce versions of the LSSD problem where the players have access to shared entanglement and no-signaling correlations. The main contribution of [12] is the proof by example that the optimal success probabilities in 0) the non-assisted case, 1) the entanglement assisted case and 2) the no-signaling assisted case are in general different. However, they also prove that for exactly two classical states to be distinguished, the three optimal winning probabilities all coincide.

1.1 Our contribution

In this thesis we will study the LSSD problem as an interesting problem in its own right. We will mostly be concerned with the case where two quantum states are to be distinguished. But as a general potentially useful fact, we will show that the winning probability in any LSSD problem has the form of a product of two success probabilities of different, yet interdependent global

state discrimination problems.

Our most remarkable contribution are the derivations of optimal strategies in LSSD problems of the following two types. Alice and Bob are to simultaneously distinguish:

1. The states $|00\rangle$ and $|\varphi\varphi\rangle$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$ where $|\varphi\rangle = \cos(\omega)|0\rangle + \sin(\omega)|1\rangle$ for some $\omega \in [0, \frac{\pi}{2}]$[1], and

2. The states $\frac{1}{\sqrt{2}}\big(|02\rangle + |20\rangle\big)$ and $\frac{1}{\sqrt{2}}\big(|12\rangle + |21\rangle\big)$ in $\mathbb{C}^3 \otimes \mathbb{C}^3$

both with uniform prior. Equipped with these results we find counter examples to a generalization of Proposition 3.3 in [12] to quantum states. In both of the above cases we find strict separations with optimal no-signaling assisted strategies. This is done by numerically obtaining a lower bound on the optimal no-signaling assisted strategies.

The no-signaling assisted case has the advantage of being an SDP [7]. The two other cases are not. In order to study LSSD problems numerically we propose a see-saw SDP method (inspired by [11]) composed of two parts. First the measurement on Alice's side is kept fixed such that the problem on Bob's side is an SDP. Upon obtaining an optimal measurement for Bob we fix this and flip the problem to maximize on Alice's side. The process is iterated until the winning probability stabilizes. The method can be tested against the known upper bounds on the winning probabilities in 1. and 2. above. We successfully obtain these upper bounds using the see-saw method.

Also, the example of strict entanglement assisted separation the authors have found in [12] can successfully be obtained: By introducing a third part in the numerical procedure where the measurements for Alice and Bob are both fixed and we optimize over shared entangled states the upper bound on the entanglement assisted problem in theorem 3.1 in [12] is successfully obtained. However, with the level of complexity increasing in the problems the numerical procedure we propose has pitfalls. It sometimes finds local minima instead of global ones. Upon introducing the this third step we have not found entanglement assisted strategies that beat optimal non-assisted strategies when two quantum states are to be distinguished.

1.2 Organization of the thesis

We begin, in the second chapter, by introducing the necessary quantum mechanical notions such as quantum states and measurements. We will also review concepts about linear maps on square operators and lastly the Bloch

[1] This result is obtained in an unpublished note by Laura Mančinska and Eric Chitamber. The proof given in this thesis is obtained independently.

vector representation of quantum states along with the Fano form of an entangled state. The third chapter is a review of global quantum state discrimination and the Holevo-Helstrom bound. This has been reviewed extensively in the literature. However, we draw upon the central ideas of its proof later when studying LSSD problems.

In chapter 4 the LSSD problem is introduced and formalized in the three different variants as in [12]. We derive some general results about LSSD problems e. g. the winning probability having the product form mentioned earlier. Also, the proposed numerical method for studying LSSD problems is introduced.

In chapter 5 and 6 we consider the main examples of our work. We derive upper bounds on the winning probabilities and show that there is a strict separation with optimal no-signaling strategies. In the discussion section we consider possible directions for future research and open problems.

2 Preliminaries and notation

The reader is assumed to be familiar with general linear algebra theory in particular the trace map and tensor products of operators. In this thesis we consider only complex and finite dimensional Euclidean spaces. Equivalently, these are finite dimensional Hilbert spaces for which we use the notation $\mathcal{H}(\cong \mathbb{C}^n)$. The space of linear operators from one complex Euclidean space $\mathcal{H}_A$ to another $\mathcal{H}_B$ will be denoted $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$. When the spaces coincide we use the notation $\mathcal{L}(\mathcal{H})$. When endowed with matrix addition and scalar multiplication $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ has a vector space structure over $\mathbb{C}$. We can endow the vector space $\mathcal{L}(\mathcal{H})$ with the *Hilbert Schmidt inner product*,

$$(\cdot,\cdot)_{HS} : \mathcal{L}(\mathcal{H}) \times \mathcal{L}(\mathcal{H}) \longrightarrow \mathbb{C} \tag{1}$$

defined as $(X, Y)_{HS} \coloneqq \mathrm{Tr}[X^\dagger Y]$. One can show that this turns $\mathcal{L}(\mathcal{H})$ into a Hilbert space in its own right.

2.1 Quantum states

In this section we review the mathematical concepts of pure and mixed quantum states. This is followed by a discussion of quantum measurements. To this end we follow [15]. We start by giving some preliminary remarks about some frequently used quantum mechanical notation. We also make a number of claims that we will use without proof throughout this work.

According to the postulates of quantum mechanics we have that: The state space of an isolated physical system is a Hilbert space and the system is completely described by its state vector which is a unit vector in the system's state

space.

Elements of a complex Euclidean space of dimension n are represented by column vectors and denoted $|\varphi\rangle$. In this representation, the inner product of two elements, $|\varphi\rangle$ and $|\psi\rangle$, of an n dimensional complex Euclidean space is denoted $\langle\cdot|\cdot\rangle$ and given by

$$\langle\varphi|\psi\rangle := \sum_{i=1}^{n} \overline{\varphi}_i \psi_i. \tag{2}$$

A *pure state* of dimension n is an element, $|\varphi\rangle$, of an n-dimensional state space $\mathcal{H}$ which has unit norm, i. e. $\langle\varphi|\varphi\rangle = 1$. Equivalently, a pure state fulfills $\sum_{i=1}^{n} |\varphi_i|^2 = 1$.

The *dual* of $|\varphi\rangle$ is defined to be the Hermitian conjugate of $|\varphi\rangle$, which we denote by $|\varphi\rangle^\dagger$. We will also use the notation $\langle\varphi| := |\varphi\rangle^\dagger$.

The *outer product* of two elements $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ which we denote $|\varphi\rangle\langle\psi|$ is an element $\mathcal{L}(\mathcal{H})$ that has $\varphi_i\overline{\psi_j}$ in its (i,j)th entry.

Suppose $|\varphi\rangle$ is a pure quantum state. The outer product of $|\varphi\rangle$ with itself, i. e. $|\varphi\rangle\langle\varphi| \in \mathcal{L}(\mathcal{H})$ is a rank one projection operator. In particular, it is positive semi-definite and has unit trace. Conversely, the spectral decomposition theorem ensures that any rank 1 projection operators can be written in the form $|\varphi\rangle\langle\varphi|$. Hence an equivalent definition of a pure state is a rank 1 projection operator in $\mathcal{L}(\mathcal{H})$. When a pure state is given in this way we use the notation $\varrho := |\varphi\rangle\langle\varphi|$.

Mixed states are convex combinations of pure states in the following sense: Suppose we have a physical system about which we know that it is in one of N states $\{\varrho_i\}_{i=1}^N$ and that the probability that it is in state φ_i is given by p_i. Since the system must be in some state, we have $p_1 + \ldots + p_N = 1$. The pair of $\{\varrho_i\}_{i=1}^N$ and the probability distribution $\{p_i\}_{i=1}^N$ is called an *ensemble*. The operator that we use to describe the system corresponding to the given ensemble is

$$\varrho = \sum_{i=1}^{N} p_i \varphi_i, \tag{3}$$

We call such a probabilistic mixture a *density operator*. Notice that a pure state is nothing but a mixed state for which $p_j = 1$ for some $j \in \{1, \ldots, n\}$. Any operator acting on $\mathcal{H}$ that admits a decomposition into rank one projectors as in Eq. (3), is the density operator corresponding to some ensemble. The set of mixed states is clearly a convex subset of $\mathcal{L}(\mathcal{H})$ of which the pure states are the extreme points.

Using that the set of positive semi-definite operators is closed under addition and scalar multiplication we have that any mixed state is positive semi-definite

and has unit trace. Conversely, it follows again from the spectral decomposition theorem, that any positive semi-definite (in particular, Hermitian) operator, ϱ, admits a decomposition into projections onto its n different orthogonal eigenspaces. If additionally we know that ϱ has unit trace we know that it, in fact, corresponds to the density matrix describing some ensemble. We denote by $D(\mathcal{H})$ the set of density operators on $\mathcal{H}$, i. e.

$$D(\mathcal{H}) \coloneqq \{\varrho \in \mathcal{L}(\mathcal{H}) |\ (1) : \varrho \geq 0, \quad (2) : \mathrm{Tr}[\varrho] = 1\}. \tag{4}$$

A crucial notion about quantum states is that of entanglement. This can happen when one considers quantum states belonging to a composite quantum state space. For simplicity we consider a composite system consisting of two subsystems. The discussion easily generalizes. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ we two state spaces, possibly of different dimensions and

$$\mathcal{H} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B. \tag{5}$$

Consider some $\varrho \in D(\mathcal{H})$. We call ϱ *separable* if it admits a decomposition given by

$$\varrho = \sum_k p_k \varrho_k^A \otimes \varrho_k^B \tag{6}$$

where $\varrho_k^A \in D(\mathcal{H}_A)$ and $\varrho_k^B \in D(\mathcal{H}_B)$ for all k and $\sum_k p_k = 1$. An *entangled* state is defined to be a state which is *not* separable.

2.2 Quantum measurements

Quantum measurements are, according to the postulates of quantum mechanics, described by a set of measurement operators. Suppose $\mathcal{X}$ is a finite set of measurement outcomes. A *quantum measurement* is then a set of measurement operators $\{M_x\}_{x\in\mathcal{X}} \subseteq \mathcal{L}(\mathcal{H})$, where x refers to the outcome, fulfilling the following completeness relation

$$\sum_{x\in\mathcal{X}} M_x^\dagger M_x = \mathbb{I}. \tag{7}$$

This ensures that the probability of obtaining some measurement outcome is 1. The most natural way of labeling the measurement outcomes is by the first $|\mathcal{X}|$ natural numbers. Hence we let $\mathcal{X} = [N]$ for some $N \geq 1$. If, initially, the system is in state $\varrho \in D(\mathcal{H})$, then (according to the postulate) performing a measurement described by $\{M_x\}_{x\in[N]}$ yields a probability

$$\mathrm{Tr}\left[M_x^\dagger M_x \varrho\right] \tag{8}$$

of getting outcome m.

The postulate also contains a statement about the state of the system after the

measurement. Given outcome $m \in [N]$ was obtained, the post-measurement state is given by

$$\frac{M_m \varrho M_m^\dagger}{\mathrm{Tr}[M_m^\dagger M_m \varrho]}. \tag{9}$$

In this thesis we are mostly concerned with the measurement statistics so we omit considerations about the state of the system after measurement. When this is the case, the most common formalism is that of a *positive operator-valued measure* (POVM). We define this to be a partition of unity into N positive semi-definite operators for some number of possible measurement outcomes N. The motivation behind this definition is the following:

For some quantum measurement $\{M_x\}_{x\in[N]}$ let $Q_x := M_x M_x^\dagger$. Then $\{Q_x\}_{x\in[N]}$ is a partition of unity into N positive semi-definite operators. And if a quantum system is in state $\rho \in D(\mathcal{H})$ then the probability of getting outcome x upon measurement is $\mathrm{Tr}[Q_x\rho]$. Hence the set of operators given by $\{Q_x\}_{x\in[N]}$ is sufficient to determine the probabilities associated with the original quantum measurement.

Conversely, if $\{Q_x\}_{x\in[N]}$ is a partition of unity into positive semi-definite operators, then there is a quantum measurement, $\{M_x\}_{x\in[N]}$, associated with it: This follows from the fact that positive semidefinite matrices have unique positive semidefinite square roots such that if we let $M_x := \sqrt{Q_x}$ we see that the completeness requirement is fulfilled.

In this thesis we will often use the notation

$$\mathcal{Q}_N(\mathcal{H}) = \{Q_1, ..., Q_N\} \tag{10}$$

about an N-outcome POVM on the state space $\mathcal{H}$.

An important subset of the set of POVMs is the set of projective measurements. A *projective measurement* is a POVM with the additional property that all of its elements are idempotent. We often denote an N-outcome projective measurement on $\mathcal{H}$ by

$$\mathcal{P}_N(\mathcal{H}) = \{P_1, ..., P_N\} \tag{11}$$

where $P_i^2 = P_i$ for all $i \in [N]$.

2.3 Linear maps on square operators

Consider two complex Euclidean space $\mathcal{H}_A$ and $\mathcal{H}_B$ of dimensions d_A and d_B. In the following we denote by $\mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ the set of linear maps of the form

$$\Phi : \mathcal{L}(\mathcal{H}_A) \longrightarrow \mathcal{L}(\mathcal{H}_B). \tag{12}$$

This, when endowed with the addition,

$$(\Phi_1 + \Phi_2)(X) \coloneqq \Phi_1(X) + \Phi_2(X) \tag{13}$$

and scalar multiplication

$$(c\Phi_1)(X) \coloneqq c\Phi_1(X) \tag{14}$$

for all $\Phi_1, \Phi_2 \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ and $c \in \mathbb{C}$ becomes a complex vector space. We use the notation $\mathcal{T}(\mathcal{H}) \coloneqq \mathcal{T}(\mathcal{H}, \mathcal{H})$ for some complex Euclidean space $\mathcal{H}$.

Let $\Phi \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ and $\Psi \in \mathcal{T}(\mathcal{H}_{A'}, \mathcal{H}_{B'})$. The tensor product

$$\Phi \otimes \Psi \in \mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_{A'}, \mathcal{H}_B \otimes \mathcal{H}_{B'}) \tag{15}$$

is defined as the unique linear map that fulfills

$$\Phi \otimes \Psi(X \otimes X') = \Phi(X) \otimes \Psi(X') \tag{16}$$

for all $X \in \mathcal{L}(\mathcal{H}_A)$ and $X' \in \mathcal{L}(\mathcal{H}_{A'})$.

The *adjoint* of an element $\Phi \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ is the unique $\Phi^* \in \mathcal{T}(\mathcal{H}_B, \mathcal{H}_A)$ map that fulfills

$$(Y, \Phi(X))_{HS} = (\Phi^*(Y), X)_{HS} \tag{17}$$

for all $X \in \mathcal{L}(\mathcal{H}_A)$ and $Y \in \mathcal{L}(\mathcal{H}_B)$.

Notice that the trace function for operators on $\mathcal{H}$ is itself an element of $\mathcal{T}(\mathcal{H}, \mathbb{C})$ where $\mathcal{L}(\mathbb{C})$ and $\mathbb{C}$ are identified. Inspired by this we can define the *partial trace* of an operator on a composite system on a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$. This is denoted

$$\mathrm{Tr}_B \in \mathcal{T}(\mathcal{H}_A \otimes \mathcal{H}_B, \mathcal{H}_A) \tag{18}$$

and defined as

$$\mathrm{Tr}_B \coloneqq \mathbb{I}_{\mathcal{L}(\mathcal{H}_A)} \otimes \mathrm{Tr}. \tag{19}$$

We invoke the notation $X^A \coloneqq \mathrm{Tr}_B[X^{AB}]$. Of course we can define Tr_A similarly. Note that the full trace is just the composition of the partial traces i. e. $\mathrm{Tr} = \mathrm{Tr}_A \otimes \mathrm{Tr}_B$. Note that the partial trace is CPTP. Note also that if we let Q be an element of a POVM on $\mathcal{H}_A$, then the partial trace is consistent with the measurement statistics in the sense that

$$\mathrm{Tr}\left[Q\varrho^A\right] = \mathrm{Tr}\left[(Q \otimes \mathbb{I}^B)\varrho^{AB}\right]. \tag{20}$$

The *trace norm* of a linear and continuous operator, T, from $\mathcal{H}$ to $\mathcal{H}$ is given by

$$\|T\|_{\mathrm{Tr}} \coloneqq \mathrm{Tr}\left[\sqrt{T^\dagger T}\right] \tag{21}$$

where $|T| = \sqrt{T^*T}$. If T is a normal operator, it can be diagonalized by a unitary operator, U, i.e. $U^\dagger DU = T$ where $D = \mathrm{diag}(\lambda_1, ..., \lambda_n)$ and λ_i are the eigenvalues of T. In this case the trace norm can be calculated as

$$\|T\|_{\mathrm{Tr}} = \sum_{i=1}^{n} |\lambda_i| \,. \tag{22}$$

For any $\Phi \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ we make the following definitions: The map Φ is *trace preserving (TP)* if we have $\mathrm{Tr}[X] = \mathrm{Tr}[\Phi(X)]$ for all $X \in \mathcal{L}(\mathcal{H})$. The map Φ is *completely positive (CP)* if for any complex Euclidean space $\mathcal{H}$ the map $\Phi \otimes \mathbb{I}_{\mathcal{L}(\mathcal{H})}$ is positive in the sense that it sends positive semi-definite operators to positive semi-definite operators. Maps that have both of these properties are called *CPTP* maps.

A map $\Phi \in \mathcal{T}(\mathcal{H}_A, \mathcal{H}_B)$ is called a *quantum channel* from $\mathcal{H}_A$ to $\mathcal{H}_B$ if it is CPTP map. The collection of all such channels is denoted $\mathfrak{C}(\mathcal{H}_A, \mathcal{H}_B)$. The reason for this name is that for any $\Phi \in \mathfrak{C}(\mathcal{H}_A, \mathcal{H}_B)$ we have that if $\varrho \in D(\mathcal{H}_A)$ then $\Phi(\varrho) \in D(\mathcal{H}_B)$. In order for this to hold it would be enough to require that Φ be positive. We require a quantum channel to be completely positive since if we consider any ancillary space $\mathcal{H}$ and a state $\varrho' \in \mathcal{H}_A \otimes \mathcal{H}$ we want $\Phi \otimes \mathbb{I}_{\mathcal{L}(\mathcal{H})}(\varrho')$ to be a state on $\mathcal{H}_B \otimes \mathcal{H}$.

Let $\Phi \in \mathfrak{C}(\mathcal{H}_A, \mathcal{H}_B)$ and $\{|a_i\rangle\}_{i=1}^{d_A}$ be and orthonormal basis for $\mathcal{H}_A$ and $\mathcal{H}_B$. The channel ϕ can be representation by its *Choi matrix* which is defined as the $d_A d_B$ square matrix

$$J(\Phi) := \sum_{i,j=1}^{d_A} \Phi(|a_i\rangle \langle a_j|) \otimes |a_i\rangle \langle a_j| \,. \tag{23}$$

Choi proved in [5] that Φ is completely positve if and only if $J(\Phi)$ is positive semi-definite.

Let $\mathcal{H}_X$ and $\mathcal{H}_Y$ be two additional complex Euclidean spaces of dimensions d_X and d_Y. A quantum channel

$$\Phi \in \mathfrak{C}(\mathcal{H}_X \otimes \mathcal{H}_Y, \mathcal{H}_A \otimes \mathcal{H}_B) \tag{24}$$

is called a *quantum correlation* over (X, Y, A, B) as in [16]. A quantum correlation (24) is called *no-signalling* if for all $\varrho_1, \varrho_2 \in D(\mathcal{H}_X)$ and $\sigma_1, \sigma_2 \in D(\mathcal{H}_Y)$ we have that

$$\mathrm{Tr}_A[\Phi(\varrho_1 \otimes \sigma_1)] = \mathrm{Tr}_A[\Phi(\varrho_2 \otimes \sigma_1)] \tag{25}$$

and likewise

$$\mathrm{Tr}_B[\Phi(\varrho_1 \otimes \sigma_1)] = \mathrm{Tr}_A[\Phi(\varrho_1 \otimes \sigma_2)] \tag{26}$$

The following is shown in [7] (see also [16]): A quantum channel Φ (as in (24)) is no-signalling if and only if whenever $\sigma, \sigma' \in \mathcal{L}(\mathcal{H}_X \otimes \mathcal{H}_Y)$ fulfill $\mathrm{Tr}_X[\sigma] = 0$

and $\mathrm{Tr}_Y[\sigma'] = 0$ we have

$$\mathrm{Tr}_A\Phi(\sigma) = 0 \quad \text{and} \quad \mathrm{Tr}_B\Phi(\sigma') = 0. \tag{27}$$

They use this to derive the conditions for the Choi matrix of Φ to be a no-signalling correlation. These are

$$1) \quad J(\Phi) \geq 0 \tag{28}$$
$$2) \quad \mathrm{Tr}_{AB}[J(\Phi)] = \mathbb{I}_{XY} \tag{29}$$
$$3) \quad \mathrm{Tr}_{XA}[J(\Phi)(\phi_X \otimes \mathbb{I}_Y \otimes \mathbb{I}_{AB})] = 0 \ \forall \phi_X \text{ Hermitian s.t. } \mathrm{Tr}[\phi_X] = 0 \tag{30}$$
$$4) \quad \mathrm{Tr}_{YB}[J(\Phi)(\mathbb{I}_X \otimes \phi_Y \otimes \mathbb{I}_{AB})] = 0 \ \forall \phi_Y \text{ Hermitian s.t. } \mathrm{Tr}[\phi_Y] = 0 \tag{31}$$

where 1) acounts for Φ being CP. 2) for its being TP and 3) and 4) the no-signalling conditions. This fact will be useful later, when we will study the no-signalling assisted version of the local quantum state discrimination problem.

In the last section of this preliminary chapter we review the Bloch vector representation of quantum states and the Fano form of quantum states on composite systems. These concepts are often useful in the study of quantum discrimination problems since they can guide intuition, especially in the qubit case.

2.4 Bloch vectors and the Fano form

In this section we briefly review the Bloch vector representation of quantum states as well as the so called Fano form of an operator on a composite space. For a more in-depth treatment see [14]. Let $\Sigma := \{\boldsymbol{\sigma}_i\}_{i\in[d^2-1]}$ be a subset of $\mathcal{L}(\mathcal{H})$ where $\mathcal{H}$ is of dimension d, fulfilling

$$(i)\ \boldsymbol{\sigma}_i = \boldsymbol{\sigma}_i^\dagger,\ (ii)\ \mathrm{Tr}[\boldsymbol{\sigma}_i] = 0,\ (iii)\ (\boldsymbol{\sigma}_i, \boldsymbol{\sigma}_j)_{HS} = 2\delta_{ij}. \tag{32}$$

for all $i, j \in [d^2 - 1]$. In other words, Σ is a set of Hermitian, traceless operators that, along with the identity, spans $\mathcal{L}(\mathcal{H})$. Such a set is called a *set of generators*. It follows, that if $X \in \mathcal{L}(\mathcal{H})$, then there exist unique $\alpha_0 \in \mathbb{C}$ and $\alpha \in \mathbb{C}^{d^2-1}$ such that

$$X = \alpha_0\mathbb{I}_d + \tfrac{1}{2}\sum_{i=1}^{d^2-1} \alpha_i\boldsymbol{\sigma}_i, \tag{33}$$

Note that $\alpha_0 = \frac{1}{n}\mathrm{Tr}[X]$ and $\alpha_i = \frac{1}{2}\mathrm{Tr}[T\boldsymbol{\sigma}_i]$ and that the operator, X, is Hermitian if and only if α_0 and α are real. Thus, for any density operator, $\varrho \in D(\mathcal{H})$ the component α_0 must be fixed and equal to $\frac{1}{d}$ such that it is uniquely given by a real vector in $\mathbb{R}^{d^2-1}$. This we define as the *Bloch vector* of ϱ. We see that there is a bijective correspondence between $\mathbb{R}^{d^2-1}$ and Hermitian , unit trace operators on $\mathcal{H}$. The subset of $\mathbb{R}^{n^2-1}$ that corresponds to density operators we define as the *Bloch space*. We denote the Bloch space, $\mathcal{B}_d$ and the

Bloch vector of a state β_ϱ. It can be shown that $\mathcal{B}_d$ is a compact and convex subset of $\mathbb{R}^{d^2-1}$ and that the following inclusions hold

$$B_{r_d} \subseteq \mathcal{B}_d \subseteq B_{R_d}. \tag{34}$$

where B_{r_d} and B_{R_d} are balls with center at the origin and radii $r_d \coloneqq \sqrt{\frac{2}{d(d-1)}}$ and $R_d \coloneqq \sqrt{\frac{2(d-1)}{d}}$. We call r_d and R_d the radius of *inball* and outball, respectively. Note that for qubits we have $r_2 = R_2 = 1$. The above inclusions coincide in this case and Bloch space becomes the well-known unit ball.

Suppose $\varrho, \varrho' \in D(\mathcal{H})$ with corresponding Bloch vectors β_ϱ and $\beta_{\varrho'}$. The overlap of ϱ and ϱ' can, in terms of their Bloch vectors be calculated as

$$\mathrm{Tr}[\varrho\varrho'] = \tfrac{1}{d} + \tfrac{1}{2}\langle \beta_\varrho, \beta_{\varrho'} \rangle . \tag{35}$$

Now consider a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ where $\mathcal{H}_A$ has dimension d_A and $\mathcal{H}_B$ has dimension d_B. Let $\Sigma^A = \{\boldsymbol{\sigma}_i^A\}_{i=1}^{d_A^2-1}$ and $\Sigma^B = \{\boldsymbol{\sigma}_i^B\}_{i=1}^{d_B^2-1}$ be sets of generators for the subsystems A and B, respectively. Consider also the following operators,

$$\tfrac{1}{\sqrt{d_B}}\boldsymbol{\sigma}_i^A \otimes \mathbb{I}_B, \quad \tfrac{1}{\sqrt{d_A}}\mathbb{I}_A \otimes \boldsymbol{\sigma}_j^B \text{ and } \tfrac{1}{\sqrt{2}}\boldsymbol{\sigma}_i^A \otimes \boldsymbol{\sigma}_j^B. \tag{36}$$

It is straightforward to check that the set containing all the operators in (36) forms a set of generators for $\mathcal{H}_A \otimes \mathcal{H}_B$.

Suppose ϱ^{AB} is a state on $\mathcal{H}_A \otimes \mathcal{H}_B$. Due to the above discussion, it is uniquely given by some $\beta^A \in \mathbb{R}^{d_A^2-1}$, $\beta^B \in \mathbb{R}^{d_B^2-1}$ and $\mathcal{C} \in \mathbb{R}^{(d_A^2-1)\times(d_B^2-1)}$ as

$$\varrho^{AB} = \tfrac{1}{d_A d_B}\mathbb{I}_{AB} + \tfrac{1}{2d_B}\sum_{i=1}^{d_A^2-1}\beta_i^A\boldsymbol{\sigma}_i^A \otimes \mathbb{I}_B + \tfrac{1}{2d_A}\sum_{j=1}^{d_B^2-1}\beta_j^B\mathbb{I}_A \otimes \boldsymbol{\sigma}_j^B + \tfrac{1}{4}\sum_{i=1}^{d_A^2-1}\sum_{j=1}^{d_B^2-1}\mathcal{C}_{ij}\boldsymbol{\sigma}_i^A \otimes \boldsymbol{\sigma}_j^B. \tag{37}$$

This is called the *Fano form* of ϱ_{AB}. The components are explicitly given by

$$\beta_i^A = \mathrm{Tr}[\boldsymbol{\sigma}_i^A \otimes \mathbb{I}_B\varrho^{AB}], \quad \beta_j^B = \mathrm{Tr}[\mathbb{I}_A \otimes \boldsymbol{\sigma}_j^B\varrho^{AB}], \quad \mathcal{C}_{ij} = \mathrm{Tr}[\boldsymbol{\sigma}_i^A \otimes \boldsymbol{\sigma}_j^B\varrho^{AB}]. \tag{38}$$

Note that

$$\varrho^A = \mathrm{Tr}_B[\varrho^{AB}] = \tfrac{1}{d_A}\mathbb{I}_{d_A} + \tfrac{1}{2}\sum_{i=1}^{d_A^2-1}\beta_i^A\boldsymbol{\sigma}_i^A, \tag{39}$$

and similarly for $\mathrm{Tr}_A[\varrho^{AB}]$. So β^A and β^B are indeed valid Bloch vectors corresponding states in their respective subsystems. The vectors β^A and β^B account for the properties of the individual particles whereas the matrix $\mathcal{C}^{AB}$ accounts for correlations. Motivated by this we will henceforth call β^A and β^B the *Bloch vectors of* ϱ^{AB} whereas $\mathcal{C}$ will be called the *correlation matrix of* ϱ^{AB}.

Notice that the overlap of ϱ^{AB} with some other density operator ϱ'^{AB} defined by β'^{A}, β'^{B} and $\mathcal{C}'$ can in a straightforward way similar to Eq. (35) be calculated as

$$\mathrm{Tr}[\varrho_{AB}\varrho'_{AB}] = \tfrac{1}{d_A d_B} + \tfrac{1}{2d_B}\langle \beta^A, \beta'^A \rangle + \tfrac{1}{2d_A}\langle \beta^B, \beta'^B \rangle + \tfrac{1}{2}(\mathcal{C}, \mathcal{C}')_{HS}. \tag{40}$$

3 Review of global quantum state discrimination (QSD)

3.1 Definition of the problem

Imagine we have a physical system about which we know the possible states. Suppose that we also know the probabilities with which the system is in any of these known possible states. How likely can we determine the state of that system? This is essentially the problem of quantum state discrimination (QSD).

Equipped with the formalism of the previous sections we can formalize the problem of global QSD as follows:

Problem 1. (N-QSD-problem). Given a set of N states on a complex Euclidean space $\mathcal{H}$ of dimension d, denoted $\{\varrho_x\}_{x\in[N]} \subseteq D(\mathcal{H})$, prepared according to the prior $(p_1, ..., p_N)$, determine a POVM, $\mathcal{Q}_N(\mathcal{H})$ that optimizes the probability of correctly identifying the state of the system.

A global N-QSD-problem is thus characterized by the pair of $\{\varrho_x\}_{x\in[N]}$ and $(p_1, ..., p_N)$. In this general formulation the problem is open (ref). However, special cases have been solved. Before we investigate these further, let us quantify the problem a bit more.

When we talk about a probability of *correctly identifying a state* ϱ_x we really mean the conditional probability of getting outcome $x \in [N]$ given that the state of the system indeed is ϱ_x. We denote this $P_x^{\mathcal{Q}_N}$ and it is given by $\mathrm{Tr}[Q_x\varrho_x]$. The total probability of correctly determining the state of the system is denoted $P^{\mathcal{Q}_N}$ and is given by

$$P^{\mathcal{Q}_N} := \sum_{x=1}^{N} p_x P_x^{\mathcal{Q}_N}. \tag{41}$$

and is termed *the success probability*. A solution to a QSD-problem is thus given by a measurement $\mathcal{Q}_N^{\max}$ such that

$$\mathcal{Q}_N^{\max} = \sup_{\mathcal{Q}_N} P^{\mathcal{Q}_N}. \tag{42}$$

Note that a solution is not unique in general i. e. there might be another measurement $\mathcal{Q}'_N \neq \mathcal{Q}_N^{\max}$ such that $P^{\mathcal{Q}'_N} = P^{\mathcal{Q}_N^{\max}}$. This will become evident after we have studied the example of the 2-QSD-problem. This has famously been solved completely by Holevo and Helstrom already in 1969 [9].

3.2 Holevo-Helstrom Bound

Although the solution of the 2-QSD-problem has been reviewed extensively in the literature we include a proof here for completion and for the benefit of the reader. The main ideas of the proof will also prove useful in the discussion later on. In the following $\mathcal{H}$ is a complex Euclidean space of dimension d. First observe the following Lemma:

Lemma 2. *Let Q belong to some POVM $\mathcal{Q}_N$ for some N. Suppose $X \in \mathcal{L}(\mathcal{H})$ is Hermitian. Then*

$$\mathrm{Tr}[QX] \leq \tfrac{1}{2}(\mathrm{Tr}[X] + \|X\|_{\mathrm{Tr}}), \tag{43}$$

with equality if Q is the projection onto the strictly positive eigenspace of X.

Proof. The quantity $\mathrm{Tr}[QX]$ is maximized if Q is a projection onto the positive eigenspace of X in which case it becomes the sum of the positive eigenvalues. By the fact that the trace of X is the sum of its eigenvalues and the definition of the trace norm for normal operators we have that the negative eigenvalues cancel in the expression on the right hand side of (43). This yields the desired. □

Equipped with this Lemma we can quite readily prove the Holevo-Helstrom bound.

Theorem 3. *(The Holevo-Helstrom bound) Consider the 2-QSD-problem involving the states $\varrho_0, \varrho_1 \in D(\mathcal{H})$ with prior (p_0, p_1). The success probability is upper bounded by*

$$P^{\mathcal{Q}} \leq \tfrac{1}{2} + \tfrac{1}{2}\|p_0\varrho_0 - p_1\varrho_1\|_{\mathrm{Tr}} \tag{44}$$

with equality if one uses a measurement $\{Q_0, Q_1\}$ where Q_0 is a projection onto the strictly positive eigenspace of $p_0\varrho_0 - p_1\varrho_1$.

Proof. For some choice of POVM $\mathcal{Q} = \{Q_0, Q_1\}$ the success probability is given by

$$P^{\mathcal{Q}} = p_0\mathrm{Tr}[Q_0\varrho_0] + p_1\mathrm{Tr}[Q_1\varrho_1] \tag{45}$$

$$= p_1 + \mathrm{Tr}\big[Q_0\big(p_0\varrho_0 - p_1\varrho_1\big)\big]. \tag{46}$$

Note, that ϱ_0 and ϱ_1, in particular, are Hermitian. The set of Hermitian operators is closed under multiplication by real numbers and addition. Hence, we can use Lemma 2 to get an upper bound of

$$P^{\mathcal{Q}} \leq p_1 + \tfrac{1}{2}\mathrm{Tr}\big[\big(p_0\varrho_0 - p_1\varrho_1\big)\big] + \tfrac{1}{2}\Big\|\big(p_0\varrho_0 - p_1\rho_1\big)\Big\|_{\mathrm{Tr}} \tag{47}$$

$$= \tfrac{1}{2} + \tfrac{1}{2}\|p_0\varrho_0 - p_1\varrho_1\|_{\mathrm{Tr}} \tag{48}$$

using linearity of the trace map and the fact that $p_0 + p_1 = 1$. The right hand side of 47 is reached if Q is the projection onto the strictly positive eigenspace of $p_0\varrho_0 - p_1\varrho_1$. □

The proof of the Helstrom bound immediately solves the problem of globally discriminating between to quantum states completely. It gives an upper bound and identifies the projective measurement with which one reaches it.

It is important to remark the subtlety that it is in general picking Q to be a projection onto the strictly positive eigenspace is only sufficient to reach the Holevo-Helstrom bound. It is not a necessary condition. If the operator $p_0\varrho_0 - p_1\varrho_1$ has vanishing eigenvalues it leaves us with the choice of including the subspace spanned by the eigenvectors of these in the range of Q. The following definition will become convenient in later sections.

Definition 4. (Holevo-Helstrom class). For a 2-QSD-problem involving ϱ_0 and ϱ_1 with prior (p_0, p_1) let Π be the projection onto the strictly positive eigenspace of $p_0\varrho_0 - p_1\varrho_1$. The *Holevo-Helstrom class* (or, $\mathfrak{H}$ class, in short) for the problem is the following subset of 2-outcome POVMs on $\mathcal{H}$:

$$\mathfrak{H} \coloneqq \left\{ \{Q_0, Q_1\} \in \mathcal{Q}_2(\mathcal{H}) \mid \mathbb{I}_{|\mathrm{Im}(\Pi)} \preceq Q_0 \preceq \mathbb{I}_{|\mathrm{Im}(\Pi)\cup\ker(\Pi)} \right\} \tag{49}$$

With this definition, we may include the necessary condition in the particular formulation of the Holevo-Helstrom theorem we chose above: The bound is reached if and only if $\mathcal{Q}$ belongs to the $\mathfrak{H}$ class of the particular problem. As long as $\ker(\Gamma)$ is non-empty, an optimal solution to the 2-QSD problem is not unique.

In the rest of this section we illustrate how the problem is much less obvious when three or more states are to be discriminated.

3.3 Review of some result on QSD of three or more states

Although many results regarding quantum state discrimination have been obtained over the last half century, solving the N-QSD-problem for $N > 3$ is open, as mentioned earlier. We begin this section by a naive attempt at generalizing the method used in the proof of the Holevo-Helstrom bound to illustrate how the problem is more involved for $N > 3$.

Consider form some $N > 2$ the N-QSD-problem involving the states $\{\varrho_x\}_{x=1}^N \subseteq D(\mathcal{H})$ and the prior $\{p_x\}_{x=1}^N$. The success probability for some POVM $\mathcal{Q}_N$ is given by

$$P^{\mathcal{Q}} = p_{N'}\mathrm{Tr}[Q_{N'}\varrho_{N'}] + \sum_{i\in[N]\setminus\{N'\}} p_x \mathrm{Tr}[Q_x\varrho_x], \tag{50}$$

for some $N' \in [N]$. Using the completeness relation of the POVM we get

$$p_{N'} + \sum_{x\in[N]\setminus\{N'\}} \mathrm{Tr}[Q_x(p_x\varrho_x - p_{N'}\varrho_{N'})]. \tag{51}$$

By Lemma 2 this is upper bounded by

$$p_{N'} + \tfrac{1}{2} \sum_{x \in [N]\setminus\{N'\}} \left[\mathrm{Tr}[p_x \varrho_x - p_{N'} \varrho_{N'}] + \| p_x \varrho_x - p_{N'} \varrho_{N'} \|_{\mathrm{Tr}} \right] \tag{52}$$

$$= \tfrac{1}{2} - \tfrac{n-2}{2} p_{N'} + \tfrac{1}{2} \sum_{x \in [N]\setminus\{N'\}} \| p_x \varrho_x - p_{N'} \varrho_{N'} \|_{\mathrm{Tr}} \tag{53}$$

This upper bound can only be reached if it is possible to choose every Q_x to be the projection onto the positive eigenspace of $p_x \varrho_x - p_{N'} \varrho_{N'}$. This would require that the positive eigenspaces of all $p_x \varrho_x - p_{N'} \varrho_{N'}$ happen to be mutually orthogonal. Notice that the quantity in (53) depends on N'. So the strongest upper bound we can get in this way is the minimum over all $N' \in [N]$. However, as stated, unless there exists $N' \in [N]$ such that all $p_x \varrho_x - p_{N'} \varrho_{N'}$ have mutually orthogonal positive eigenspaces, one cannot in fact reach this upper bound.

The natural question now is how well we can in fact do? In other words, how strong a lower bound can we find on the quantity given in Eq. (42)? A famous way to produce a good but not optimal guessing probability for a given state discrimination problem is that of the so-called "pretty good" measurement [8]. These are defined as follows: If $\{\varrho_x\}_{i=1}^N$ are the $N > 2$ states to be discriminated with prior $(p_1, ..., p_N)$, let $\boldsymbol{\varrho}$ denote the ensemble

$$\boldsymbol{\varrho} = \sum_{x=1}^{N} p_x \varrho_x \tag{54}$$

The "pretty good" (or square root) measurement is then defined as $\{Q_x^{pg}\}_{x=1}^N$ where

$$Q_x^{pg} := p_x \boldsymbol{\varrho}^{-\frac{1}{2}} \varrho_x \boldsymbol{\varrho}^{-\frac{1}{2}}. \tag{55}$$

One can also take another approach in terms of Bloch space. Owing to the discussion in section 2.4 we can for some set of generators Σ write the elements, Q_x of a POVM, $\mathcal{Q}_N$ as

$$Q_x = q_x^0 I_d + \sum_{j=1}^{d} (q_x)_j \boldsymbol{\sigma}_j \tag{56}$$

for some $q_x^0 \in (0,1)$ and $q_x \in \mathbb{R}^{d^2-1}$. Since the Q_x's must sum to identity we have the following requirements

$$\sum_{x=1}^{N} q_x^0 = 1 \text{ and } \sum_{x=1}^{N} q_x = 0. \tag{57}$$

We can rewrite Eq. (56) as

$$Q_x = d q_x^0 \left(\tfrac{1}{d} I_d + \tfrac{1}{2} \sum_{j=1}^{d} (\beta_{Q_x})_j \boldsymbol{\sigma}_j \right) \tag{58}$$

where $\beta_{Q_x} := \frac{2}{q_x^0 d} q_x$ is the Bloch vector associated with Q_x. The state discrimination problem can now be recast in terms of Bloch vectors. Consider the

N-QSD-problem involving the states, $\{\beta_x\}_{x=1}^N$ with prior $(p_1, ..., p_N)$. Using Eqs. (35) and (58) we easily rewrite the success probability as

$$P^{\beta_\varrho} = \sum_{x=1}^{N} p_x q_x^0 \left(1 + \tfrac{d}{2} \langle \beta_x, \beta_{Q_x} \rangle\right). \tag{59}$$

Hence the problem becomes an optimization over (59) with the constraints that $\beta_{Q_x} \in \mathcal{B}_d$, $\sum q_x^0 = 1$ and $\sum_x q_0^x \beta_{Q_x} = 0$.

Such approach in terms of Bloch space has in fact already been taken in [6]. The simple geometry of Bloch space in the qubit case i. e. made it possible to analytically find optimal success probabilities for the discrimination problem involving any number of qubits.

3.4 Strategies based on solutions of semi-definite programs

An efficient method for solving QSD problems numerically is via the notion of semi-definite programming which we introduce in this section. We take a "pedestrians approach" since the full arsenal of theoretic background is not within the main interest of this thesis. We are merely interested in way in which QSD problems can be understood as SDPs and thereby solved numerically. To this end we follow chapter 1 in [17].

Let $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}$ be complex Euclidean spaces of dimension d_A, d_B and d, respectively. Let $\Phi : \mathcal{H}_A \to \mathcal{H}_B$ a Hermiticity-preserving map and A and B be Hermitian operators on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. A *semi-definite program (SDP)* is then a triple (Φ, A, B) with which two optimization problems are associated, the *primal* and the *dual*:

$$\begin{array}{ll} \textit{Primal}: & \textit{Dual}: \\ \text{Maximize}: \quad (A, X)_{HS} & \text{Minimize}: \quad (B, Y)_{HS} \\ \text{Such that}: \begin{cases} \Phi(X) = B \\ X \geq 0 \end{cases} & \text{Such that}: \begin{cases} \Phi^*(Y) \geq A \\ Y \in \mathrm{Herm}(\mathcal{H}_B) \end{cases} \end{array}.$$

The N-QSD-problem can be shown to be a primal SDP in the following way: Let $\{\varrho_x\}_{x=1}^N \subseteq \mathcal{H}$ and a prior $(p_1, ..., p_N)$ be given. Let X and A be given by the block diagonal operators,

$$A = \begin{pmatrix} p_1\varrho_1 & & 0 \\ & \ddots & \\ 0 & & p_N\varrho_N \end{pmatrix}, \quad X = \begin{pmatrix} Q_1 & & 0 \\ & \ddots & \\ 0 & & Q_N \end{pmatrix} \tag{60}$$

on a dN dimensional complex Euclidean space, $\mathcal{H}'$. Then $(A, X)_{HS}$ is equal to $P^{\mathcal{Q}}$ which we want to maximize. We also have that X is positive semi-definite if and only all the Q_xs are positive semi-definite so we only have to

implement the requirement that $\sum_{x=1}^{N} Q_x = \mathbb{I}_d$. This is done by considering the map $\Phi' : \mathcal{L}(\mathcal{H}') \to \mathcal{L}(\mathcal{H})$ that takes any dN-by-dN operator $Z \in \mathcal{L}(\mathcal{H}')$ and maps it to the sum of the N-by-N operators on its diagonal. This map is trivially Hermiticity preserving. By letting $B = \mathbb{I}_d$ we conclude that the N-QSD-problem is a semi-definite-program.

4 Local simultaneous state discrimination (LSSD)

4.1 Definition of the problem

In this section we will study the main problem of this thesis i. e. the problem of locally discriminating states with the requirement that the individual parties simultaneously be correct. Before we go on to define the problem formally we make a few preliminary remarks:

Suppose we have a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ and we know that the system is one of two possible states, ϱ_0^{AB} and ϱ_1^{AB} with prior (p_0, p_1). Two parties - Alice and Bob - attempt at discriminating the states by using 2-outcome measurements on their respective subsystems. Suppose we first ask Alice to define a measurement that gives her a good chance of correctly identifying the state of the system. Her task is to find a POVM, $\{A_0, A_1\}$, on the subsystem $\mathcal{H}_A$. As we have seen, the measurement statistics are the same when using $\{A_0 \otimes \mathbb{I}^B, A_1 \otimes \mathbb{I}^B\}$ to discriminate ϱ_0^{AB} and ϱ_1^{AB} as using $\{A_0, A_1\}$ to discriminate ϱ_0^A and ϱ_1^A. Her probability of correctly determining the state is hence given by

$$p_1 + \mathrm{Tr}[A_0(p_0\varrho_0^A - p_1\varrho_1^A)] \tag{61}$$

Not surprisingly, we see that Alice optimizes her chances if she chooses A_0 to be some element of the $\mathfrak{H}$ class for her local QSD problem. We call this $\mathfrak{H}^A$.

Of course one could establish the analogous scenario in which Bob must attempt at determining the state of the system based on a measurement on the subsystem $\mathcal{H}_B$. Bob would also perform optimally by choosing a $\mathfrak{H}$-class operator for his local QSD-problem. We call this $\mathfrak{H}^B$.

But imagine now that we ask both of them to attempt at determining the state - without the possibility of communicating. If they manage to simultaneously, correctly identify the state we say that Alice and Bob *win*. The question is then, how do they optimize their winning probability? Which local measurements should they use in order to have the best possible chance of winning? We now go on to formalize the problem in a more general setting.

Problem 5. (N-LSSD problem). Consider a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ that is prepared in one of N possible states $\{\varrho_x^{AB}\}_{x=1}^N$ according to the prior $(p_1, ...p_N)$. Determine local POVMs for Alice and Bob, for which we use the notation $\mathcal{A}$

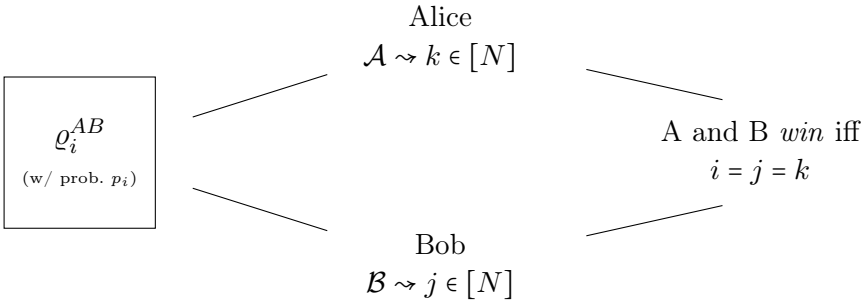


Figure 1: Schematic representation of the LSSD problem.

and $\mathcal{B}$, i. e.

$$\mathcal{A} \coloneqq \{A_1, ..., A_N\}, \quad \mathcal{B} \coloneqq \{B_1, ..., B_N\}. \tag{62}$$

such that their simultaneous success probability (SSP) given by

$$P^{\mathcal{AB}} \coloneqq \sum_{x=1}^{N} p_x \mathrm{Tr}\left[A_x \otimes B_x \varrho_{AB}^x\right], \tag{63}$$

is maximized.

When we refer to a *strategy* for Alice (or Bob) in some N-LSSD-problem this will be synonymous with the N-outcome POVM $\mathcal{A}$ (or $\mathcal{B}$). When we refer to a *joint strategy* it will be synonymous with the pair $(\mathcal{A}, \mathcal{B})$. The situation is illustrated in Figure 1.

We invoke the following notation: Given an N-LSSD problem involving the states $\{\varrho_x^{AB}\}_{x=1}^N$ with prior $(p_1, ..., p_N)$ and given some strategy $\{\mathcal{A}, \mathcal{B}\}$ we denote by $P_x^{\mathcal{A}}$, Alice's probability of correctly identifying the state ϱ_x^{AB}. This is given by

$$P_x^{\mathcal{A}} \coloneqq \mathrm{Tr}[A_x \varrho_x^A]. \tag{64}$$

Her total probability of correctly identifying the state of the system is then

$$P^{\mathcal{A}} \coloneqq \sum_{x=1}^{N} p_x P_x^{\mathcal{A}}. \tag{65}$$

Analogously, we define $P_x^{\mathcal{B}}$ and $P^{\mathcal{B}}$ for Bob. Remark that for any choice of joint strategy the winning probability is upper bounded by the minimum of Alice's and Bob's individual success probabilities, i. e. by the quantity $\min\{P^{\mathcal{A}}, P^{\mathcal{B}}\}$. They only reach this bound if their answers are coordinated in the sense that they always get the same measurement outcome.

It is instructive to consider the case of $N = 2$ and a simple example. Naively, one might think that they would have to perform local Helstrom measurements to optimize their chances. That is, Alice and Bob individually choose an element of the $\mathfrak{H}^A$ class and the $\mathfrak{H}^B$ class. However, that does not give them

an optimal chance of winning in general. We illustrate this by the following example:

Example 6. (The trivial example) Suppose Alice and. Bob were to discriminate two states ϱ_0^{AB} and ϱ_1^{AB} with uniform prior. Suppose also that these states are indistinguishable to Alice but to Bob they can be distinguished with non-trivial success probability. In the notation of section 2.4 this corresponds to fixing $\beta_0^A = \beta_1^A$ and requiring $\beta_0^B \neq \beta_1^B$. The simultaneous success probability is upper bounded by minimum of the local Helstrom bounds given by the local QSD problems i. e. the quantity

$$\tfrac{1}{2} + \tfrac{1}{4} \min \left\{ \left\| \varrho_0^A - \varrho_1^A \right\|_1, \left\| \varrho_0^B - \varrho_1^B \right\|_1 \right\} = \tfrac{1}{2}. \tag{66}$$

Now, Alice and Bob can reach this upper bound only if they can make sure that they get the same measurement outcome. Since $\varrho_0^A - \varrho_1^A = 0$, the $\mathfrak{H}^A$ class consists of all 2-outcome POVMs on $\mathcal{H}_A$. So let us, for example, fix Alice's measurement as $\{\mathbb{I}^A, 0\}$ which corresponds to Alice simply outputting 0 no matter what. Then suppose Bob uses some measurement given by $\{B_0, \mathbb{I}_B - B_0\}$. It is clear that they can reach the upper bound of $\frac{1}{2}$ if and only if $B_0 = \mathbb{I}^B$ which certainly is not in the $\mathfrak{H}^B$ class.•

More generally, there are two cases in which this bound $\min\{P^{\mathcal{A}}, P^{\mathcal{B}}\}$ can be reached: (1) Alice and Bob have probability 1 of outputting the same answer or (2) either Alice or Bob has a local success probability of 1. In the following we exclude the case where

In the following we will show how $P^{\mathcal{AB}}$ is in fact given by the product of success probabilities of two different but interdependent QSD problems. For this it is convenient to define the operators,

$$\kappa_x^B := \tfrac{1}{P_x^{\mathcal{A}}} \mathrm{Tr}_A \left[A_x \otimes \mathbb{I}^B \varrho_x^{AB} \right], \tag{67}$$

where $\mathcal{A}$ is some fixed POVM on $\mathcal{H}_A$. These are states since they have unit trace and the partial trace is completely positive and invariant under cyclic permutations. So,

$$\mathrm{Tr}_A \left[A_x \otimes \mathbb{I}^B \varrho_x^{AB} \right] = \mathrm{Tr}_A \left[\sqrt{\varrho_x^{AB}}^\dagger A_x \otimes \mathbb{I}^B \sqrt{\varrho_x^{AB}} \right] \tag{68}$$

is positive semi-definite since the argument on the right hand side is positive semi-definite.

Lemma 7. *Consider the N-LSSD-problem involving the states $\{\varrho_x^{AB}\}_{x=1}^N$ with prior $(p_1, ..., p_N)$. Suppose Alice and Bob have a joint strategy given by $\{\mathcal{A}, \mathcal{B}\}$. Their winning probability can be expressed as the following product of local success probabilities:*

$$P^{\mathcal{AB}} = P^{\mathcal{A}} P'^{\mathcal{B}}, \tag{69}$$

where $P'^{\mathcal{B}}$ is Bob's success probability of discriminating the states $\{\kappa_x^B\}_{x=1}^N \subseteq D(\mathcal{H}_B)$ defined in Eq. (67) with prior

$$(p'_1, ..., p'_N) \coloneqq (p_1 \tfrac{P_1^{\mathcal{A}}}{P^{\mathcal{A}}}, ..., p_N \tfrac{P_N^{\mathcal{A}}}{P^{\mathcal{A}}}). \tag{70}$$

Proof. Given some joint strategy $(\mathcal{A}, \mathcal{B})$ we can rewrite the winning probability as follows

$$P^{\mathcal{AB}} = \sum_{x=1}^N p_x \mathrm{Tr}\left[A_x \otimes B_x \varrho_{AB}^x\right] \tag{71}$$

$$= \sum_{x=1}^N p_x \mathrm{Tr}\left[\mathrm{Tr}_A\left[A_x \otimes \mathbb{I}^B \varrho_{AB}^x\right] B_x\right] \tag{72}$$

$$= \sum_{x=1}^N p_x P_x^{\mathcal{A}} \mathrm{Tr}\left[\kappa_x^B B_x\right] \tag{73}$$

Now, in order to transform this into a success probability corresponding to the QSD problem involving the κ_x^B's we multiply by $1 = \frac{P^{\mathcal{A}}}{P^{\mathcal{A}}}$ to get

$$P^{\mathcal{AB}} = P^{\mathcal{A}} \sum_{x=1}^N \tfrac{p_x P_x^{\mathcal{A}}}{P^{\mathcal{A}}} \mathrm{Tr}\left[B_x \kappa_x^B\right]. \tag{74}$$

The summation in the above expression exactly corresponds with the success probability in a QSD-problem involving the κ_x^B's with a prior given by $(p'_1, ..., p'_N)$ as desired. □

In the remainder of this thesis we will exclusively be concerned with 2-LSSD-problems. Consider two states ϱ_0^{AB} and ϱ_1^{AB} with prior (p_0, p_1). Bob can, according to the above Lemma, for any fixed measurement $\mathcal{A}$ on $\mathcal{H}_A$, optimize the winning probability by choosing a Holevo-Helstrom class measurement for his corresponding QSD problem involving the states κ_x^B. We call this class $\mathfrak{H}'^B$. In this case the winning probability becomes

$$P^{\mathcal{AB}} = \tfrac{1}{2} P^{\mathcal{A}} \left(1 + \left\| p'_0 \kappa_0^B - p'_1 \kappa_1^B \right\|_{\mathrm{Tr}}\right). \tag{75}$$

Example 8. (The trivial example revisited). We build upon example 6 using this notation. No matter which measurement Alice chooses she stays within the $\mathfrak{H}^A$ class of her local problem. Suppose she chooses $\mathcal{A} = \{a_0 \mathbb{I}^A, a_1 \mathbb{I}^A\}$ for some parameters $a_0, a_1 \in [0, 1]$ where $a_0 + a_1 = 1$. Then, $P_x^{\mathcal{A}} = a_x$ and $x = 0, 1$. Bob is left with the states $\kappa_x^B = \varrho_x^B$ with prior (a_0, a_1) and the winning probability is bounded by

$$P^{\mathcal{AB}} = \tfrac{1}{4} \left(1 + \left\| a_0 \varrho_0^B - a_1 \varrho_1^B \right\|_{\mathrm{Tr}}\right). \tag{76}$$

Note that Alice should in fact choose either $a_0 = 1$ and $a_1 = 0$ or $a_0 = 0$ and $a_1 = 1$ as in Example 6 to optimize the winning probability •

More generally it is worth noticing that the determination of the optimal winning strategy requires an optimization over POVMs on $\mathcal{H}_A$ only. We see in particular that Alice can help Bob in the sense that she can skew his prior. In this example she could even do so without sacrifizing her own success probability. She was able to make sure that Bob, with certainty, can get the same outcome as her.

The following corollary will be very useful in our further investigations. The consequence of this Lemma is that it suffices to consider projective measurements when upper bounding the winning probability of a given 2-LSSD-problem.

Corollary 9. *Consider the 2-LSSD-problem involving the states ϱ_0^{AB} and ϱ_1^{AB} with prior (p_0, p_1). For any POVMs $\mathcal{A}$ and $\mathcal{B}$, there exist projective measurements $\mathcal{A}'$ and $\mathcal{B}'$ such that $P^{\mathcal{AB}} \leq P^{\mathcal{A}'\mathcal{B}'}$.*

Proof. This is a direct consequence of Lemma 7: For any fixed measurement on Alice, Bob optimizes the winning probability by choosing a $\mathfrak{H}'^B$-class measurement - which, in particular, can be chosen to be projective. Denote this $\mathcal{B}'$. Then we have $P^{\mathcal{AB}} \leq P^{\mathcal{AB}'}$. Afterwards, we can fix Bob's measurement $\mathcal{B}'$ and make a similar argument to conclude that there exists a projective measurement $\mathcal{A}'$ such that $P^{\mathcal{AB}'} \leq P^{\mathcal{A}'\mathcal{B}'}$. □

We round off this section by calculating the states κ_x^B explicitly in terms of their Bloch vectors. If we write ϱ_x^{AB} in its Fano form with Bloch vectors α^x and β^x and correlation matrix $\mathcal{C}^x$ one finds by standard calculations,

$$\kappa_x^B = \tfrac{1}{d_B}\mathbb{I}^B + \tfrac{1}{2}\sum_{j=1}^{d_B^2-1} \tfrac{1}{P_x^{\mathcal{A}}} \mathrm{Tr}\left[A_x \left(\tfrac{\beta_j^x}{d_A}\mathbb{I}^A + \tfrac{1}{2}\sum_{i=1}^{d_A^2-1} \mathcal{C}_{ij}^x \boldsymbol{\sigma}_i^A \right) \right] \boldsymbol{\sigma}_j^B \tag{77}$$

The expression in the parentheses is, for every $j = 0, ..., d_B^2 - 1$, an operator on $\mathcal{H}_A$ we call $(\tau_x)_j$ whose trace is equal to β_j^x. Thus, the Bloch vector of κ_x^B has $\frac{\mathrm{Tr}[A_x(\tau_x)_j]}{P_x^{\mathcal{A}}}$ in its jth entry. It becomes evident that from Bob's perspective both the prior and the states he aims at discriminating in order to optimize the winning chance depend on Alice's measurement.

4.2 Entanglement assisted discrimination

Assume now that Alice and Bob are allowed to share some entangled state, $\sigma_{A'B'}$ which acts on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$. Let

$$\mathcal{H}_{\bar{A}} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_{A'} \text{ and } \mathcal{H}_{\bar{B}} \coloneqq \mathcal{H}_B \otimes \mathcal{H}_{B'}. \tag{78}$$

For any complex Euclidean space $\mathcal{H}_1$ (of dimension n) with orthonormal basis $\{|i\rangle\}_{i\in[n]}$ and $\mathcal{H}_2$ (of dimension m) with orthonormal basis $\{|j\rangle\}_{i\in[m]}$, we define a *swap operator*, on the composite space with orthonormal basis $\{|i,j\rangle\}$

$$S_{1,2} : \mathcal{H}_1 \otimes \mathcal{H}_2 \longrightarrow \mathcal{H}_2 \otimes \mathcal{H}_1 \tag{79}$$

by $S_{1,2}\left(|ij\rangle\right) := |ji\rangle$.

Now, for N states $\{\varrho_x^{AB}\}_{x=1}^N$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ we can consider the N-LSSD-problem involving the states

$$\varrho_x^{\bar{A}\bar{B}} := S_{B,A'} \varrho_x^{AB} \otimes \sigma^{A'B'} S_{B,A'}^\dagger \tag{80}$$

Similarly as in the previous section, we equip Alice and Bob with measurements

$$\mathcal{A}_\sigma = \{\bar{A}_1, ..., \bar{A}_N\} \quad \text{and} \quad \mathcal{B}_\sigma = \{\bar{B}_1, ..., \bar{B}_N\}, \tag{81}$$

and we can define

$$P_x^{\mathcal{A}_\sigma} := \mathrm{Tr}[\bar{A}_x \varrho_x^{\bar{A}}] = \mathrm{Tr}[\bar{A}_x \varrho_x^A \otimes \sigma^{A'}], \tag{82}$$

and

$$P^{\mathcal{A}_\sigma} := \sum_{x=0,1} p_x P_x^{\mathcal{A}_\sigma}. \tag{83}$$

with similar definitions for Bob. The winning probability in this case is denoted

$$P^{\mathcal{A}_\sigma \mathcal{B}_\sigma} := \sum_{x=1}^N p_x \mathrm{Tr}\left[\bar{A}_x \otimes \bar{B}_x \varrho_x^{\bar{A}\bar{B}}\right]. \tag{84}$$

We now go on to define the N-entanglement assisted local simultaneous state discrimination problem (N-EALSSD problem).

Problem 10. (N-EALSSD problem) Consider a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ and N states $\{\varrho_x^{AB}\}_{x=1}^N$ prepared according to the prior $(p_1, ..., p_N)$. Does there exist an entangled state $\sigma^{A'B'}$ on another bipartite space $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, where $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ are allowed to have any finite dimension, such that for some choice of $\mathcal{A}_\sigma$ and $\mathcal{B}_\sigma$ we have

$$P^{\mathcal{A}_\sigma \mathcal{B}_\sigma} > \sup_{\mathcal{A},\mathcal{B}} P^{\mathcal{A}\mathcal{B}} \ ? \tag{85}$$

In the affirmative case, determine the value of

$$\sup_\sigma \sup_{\mathcal{A}_\sigma, \mathcal{B}_\sigma} P^{\mathcal{A}_\sigma \mathcal{B}_\sigma} \tag{86}$$

where $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ are allowed to have any finite dimension.

From Lemma 7 we know that for any $\mathcal{A}_\sigma$ and $\mathcal{B}_\sigma$

$$P^{\mathcal{A}_\sigma \mathcal{B}_\sigma} \leq P^{\mathcal{A}_\sigma} P'^{\mathcal{B}_\sigma} \tag{87}$$

where $P'^{\mathcal{B}_\sigma}$ is Bob's probability of correctly discriminating the states

$$\kappa_x^{\bar{B}} := \tfrac{1}{P_x^{\mathcal{A}}} \mathrm{Tr}_{\bar{A}}\left[\bar{A}_x \otimes \mathbb{I}^{\bar{B}} \varrho_x^{\bar{A}\bar{B}}\right] \tag{88}$$

with prior

$$(p'_1, ..., p'_N) := \left(p_1 \tfrac{P_1^{\mathcal{A}_\sigma}}{P^{\mathcal{A}_\sigma}}, ..., p_N \tfrac{P_N^{\mathcal{A}_\sigma}}{P^{\mathcal{A}_\sigma}}\right) \tag{89}$$

As earlier, we restrict our attention to $N = 2$. When this is the case we can make use of the Holevo-Helstrom theorem to make the following observation:

Lemma 11. *Let $\{\mathcal{A},\mathcal{B}\}$ be optimal for the 2-LSSD problem of ϱ_0^{AB} and ϱ_1^{AB} with prior (p_0,p_1). Suppose $\mathcal{A}$ belongs to the $\mathfrak{H}^A$ class. For any $\sigma^{A'B'}$, if there exists $\{\mathcal{A}_\sigma,\mathcal{B}_\sigma\}$ such that $P^{\mathcal{A}_\sigma\mathcal{B}_\sigma} > P^{\mathcal{A}\mathcal{B}}$ then $\mathcal{P}^{\mathcal{A}_\sigma} < P^{\mathcal{A}}$.*

Proof. Assume $P^{\mathcal{A}_\sigma} = P^{\mathcal{A}}$. This is the case if and only if $\mathcal{A}_\sigma$ is $\mathfrak{H}^{\bar{A}}$ class. Since $\sigma^{A'B'}$ is a state it does not have strictly negative eigenvalues. We choose $\{|\lambda_i^A\lambda_j^{A'}\rangle\}$ as a basis for $\mathcal{H}_{\bar{A}}$, where $\{|\lambda_i^A\rangle\}$ are the normalized eigenvectors of $p_0\varrho_0^A - p_1\varrho_1^A$ and $\{|\lambda_j^{A'}\rangle\}$ the normalized eigenvectors of $\sigma^{A'}$. Then any $\mathfrak{H}^{\bar{A}}$ class POVM can be written as

$$\bar{A}_x = x\mathbb{I}^{\bar{A}} + (-1)^x A_0 \otimes P \tag{90}$$

for $x = 0,1$, where A_0 belongs to some $\mathfrak{H}^A$ class POVM and P fulfills

$$\mathbb{I}^{A'}_{|\mathrm{Im}(\sigma^{A'})} \leq P \leq \mathbb{I}^{A'}. \tag{91}$$

Then we have

$$\begin{aligned} P_x^{\mathcal{A}_\sigma} =& \mathrm{Tr}\left[\left(x\mathbb{I}^{\bar{A}} + (-1)^x A_0 \otimes P\right) \otimes \mathbb{I}^{\bar{B}} S_{A'B}\varrho_x^{AB} \otimes \sigma^{A'B'} S_{A'B}^\dagger\right] && (92)\\ =& x + (-1)^x \mathrm{Tr}\left[(A_0 \otimes \mathbb{I}^B \varrho_x^{AB}) \otimes (P \otimes \mathbb{I}^{B'}\sigma^{A'B'})\right] && (93)\\ =& x + (-1)^x \mathrm{Tr}\left[(A_0 \otimes \mathbb{I}^B \varrho_x^{AB})\right] && (94)\\ =& P_x^{\mathcal{A}}. && (95) \end{aligned}$$

so we clearly have $P_0^{\mathcal{A}_\sigma} = P_0^{\mathcal{A}}$ and

$$P_1^{\mathcal{A}_\sigma} = 1 - \mathrm{Tr}\left[\left(\mathbb{I}^A - A_1\right) \otimes \mathbb{I}^B \varrho_1^{AB}\right] = P_1^{\mathcal{A}} \tag{96}$$

where $P_x^{\mathcal{A}}$ is the success probability using $\mathcal{A} = \{A_0, A_1\}$. So the prior in the entanglement assisted case stays fixed. The states left for Bob are:

$$\begin{aligned} \kappa_x^{\bar{B}} =& \tfrac{1}{P_x^{\mathcal{A}_\sigma}} \mathrm{Tr}_{\bar{A}}\left[\left(x\mathbb{I}^{\bar{A}} + (-1)^x A_0 \otimes P\right) \otimes \mathbb{I}^{BB'} S_{A'B}\varrho_x^{AB} \otimes \sigma^{A'B'} S_{A'B}^\dagger\right] && (97)\\ =& \tfrac{1}{P_x^{\mathcal{A}}}\left(x\varrho_x^B \otimes \sigma^{B'} + (-1)^x \mathrm{Tr}_{\bar{A}}\left[S_{A'B}^\dagger A_0 \otimes P \otimes \mathbb{I}^{BB'} S_{A'B}\varrho_x^{AB} \otimes \sigma^{A'B'}\right]\right) && (98)\\ =& \tfrac{1}{P_x^{\mathcal{A}}}\left(x\varrho_x^B \otimes \sigma^{B'} + (-1)^x \mathrm{Tr}_A\left[A_0 \otimes \mathbb{I}^{A'}\varrho_x^{AB}\right] \otimes \mathrm{Tr}_{A'}\left[P \otimes \mathbb{I}^{B'} \otimes \sigma^{A'B'}\right]\right) && (99)\\ =& \tfrac{1}{P_x^{\mathcal{A}}}\left(x\varrho_x^B + (-1)^x \mathrm{Tr}_A\left[A_0 \otimes \mathbb{I}^{A'}\varrho_x^{AB}\right]\right) \otimes \sigma^{B'} && (100) \end{aligned}$$

We clearly have $\kappa_0^{\bar{B}} = \kappa_0^B \otimes \sigma^{B'}$ and

$$\kappa_1^{\bar{B}} = \tfrac{1}{P_1^{\mathcal{A}}}\left(\varrho_1^B - \mathrm{Tr}_A\left[\left(\mathbb{I}^A - A_1\right) \otimes \mathbb{I}^{A'}\varrho_1^{AB}\right]\right) \otimes \sigma^{B'} = \kappa_1^B \otimes \sigma^{B'} \tag{101}$$

Hence $P^{\mathcal{A}_\sigma\mathcal{B}_\sigma}$ is upper bounded by

$$\begin{aligned} & \tfrac{1}{2}P^{\mathcal{A}_\sigma}\left(1 + \left\|p_0'\kappa_0^B \otimes \sigma^{B'} - p_1'\kappa_1^B \otimes \sigma^{B'}\right\|_{\mathrm{Tr}}\right) && (102)\\ =& \tfrac{1}{2}P^{\mathcal{A}}\left(1 + \left\|p_0'\kappa_0^B - p_1'\kappa_1^B\right\|_{\mathrm{Tr}}\right) && (103)\\ =& P^{\mathcal{A}\mathcal{B}}. && (104) \end{aligned}$$

From this we can conclude the desired. □

4.3 No-signaling assisted discrimination

In this section we will study the LSSD problem where Alice and Bob have access to a no-signaling correlation. This corresponds to a more general setting where Alice and Bob can access any quantum resource that cannot be used for direct communication. This, of course, includes shared entanglement which we studied earlier.

The setup is the following: Let X and Y be N-level classical systems and consider the correlation

$$\Phi \in \mathfrak{C}(\mathcal{H}_A \otimes \mathcal{H}_B, X \otimes Y) \tag{105}$$

with Choi matrix $\Omega := J(\Phi)$.

Problem 12. (N-NSLSSD problem). Consider a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ that is prepared in one of N possible states $\{\varrho_x^{AB}\}_{x=1}^N$ according to the prior $(p_1, ...p_N)$. Determine the no-signaling correlation $\Omega := J(\Phi)$ such that the winning probability given by

$$P^\Omega := \sum_{i=1}^N p_i \mathrm{Tr}\left[\Omega\left(\varrho_i^{AB} \otimes |ii\rangle\langle ii|^{XY}\right)\right] \tag{106}$$

is maximized.

In other words, we aim at determining the quantity

$$\sup_\Omega P^\Omega \tag{107}$$

where Ω is the Choi matrix of a no-signaling correlation. We now from earlier the conditions on a matrix, Ω, for being a no-signaling correlation. If we let Σ^A and Σ^B be sets of generators of $\mathcal{L}(\mathcal{H}_A)$ and $\mathcal{L}(\mathcal{H}_B)$ respectively, then these can be expressed as

$$\begin{aligned}
&1) \quad \Omega \geq 0 && (108)\\
&2) \quad \mathrm{Tr}_{AB}[\Omega] = \mathbb{I}^{AB} && (109)\\
&3) \quad \mathrm{Tr}_{AX}[\Omega(\phi^A \otimes \mathbb{I}_Y \otimes \mathbb{I}_{AB})] = 0, \ \forall \phi^A \in \Sigma^A && (110)\\
&4) \quad \mathrm{Tr}_{BY}[\Omega(\mathbb{I}_X \otimes \phi^B \otimes \mathbb{I}_{AB})] = 0, \ \forall \phi^B \in \Sigma^B. && (111)
\end{aligned}$$

One important advantage of this problem is that it is an SDP and can therefore be studied numerically using a standard SDP solver.

4.4 See-saw numerical method for LSSD problems

In this section we describe a numerical method for studying LSSD-problems that has proved very useful. The problem in itself is not an SDP. This is due to the tensor products of the POVM elements in the objective function

$P^{\mathcal{AB}}$. Hence we cannot immediately apply the method described in section 3.4.

However, inspired by the discussion in section 4.1 (and largely by the numerical method described in [11]) we can break the problem down in multiple pieces. As we have seen, by fixing Alice's measurement we get global QSD-problem for Bob which is an SDP. If we consider a fixed an N-outcome POVM $\mathcal{A}$ on $\mathcal{H}_A$ we saw earlier that from Bob's perspective must distinguish the states $\{\kappa_x^B\}_{x=1}^N$ with prior $\frac{p_x P_x}{P^{\mathcal{A}}}$. This is, locally for Bob, an SDP. So we could use the method described in section 3.4 to optimize the winning probability with fixed $\mathcal{A}$.

Upon finding this optimal measurement, $\mathcal{B}$, for Bob we fix this and make the analogous procedure for Alice i.e. we numerically solve the SDP involving the states

$$\kappa_x^A := \tfrac{1}{P_x^{\mathcal{B}}} \mathrm{Tr}_B[\mathbb{I}^A \otimes B_x \varrho_x^{AB}] \tag{112}$$

with prior

$$(q_1', ..., q_N') := (p_1 \tfrac{P_1^{\mathcal{B}}}{P^{\mathcal{B}}}, ..., p_N \tfrac{P_N^{\mathcal{B}}}{P^{\mathcal{B}}}). \tag{113}$$

as in Lemma 7.

Let us make this more precise: Consider an N LSSD problem involving the states $\{\varrho_i^{AB}\}_{i=1}^N$ with prior $(p_1, ..., p_N)$. Then we obtain two SDP's † and ‡ given by

$$(\dagger) \begin{cases} \text{Maximize}: & P^{\mathcal{A}} \sum_{x=1}^N p_x' \mathrm{Tr}\left[B_x \kappa_x^B\right] \\ \text{such that}: & \sum_{x=1}^n B_x = \mathbb{I}^B \\ & B_x \succeq 0, \ \forall x \in \{1, ..., N\} \end{cases},$$

$$(\ddagger) \begin{cases} \text{Maximize}: & P^{\mathcal{B}} \sum_{x=1}^N q_x' \mathrm{Tr}\left[A_x \kappa_x^A\right] \\ \text{such that}: & \sum_{x=1}^n A_x = \mathbb{I}^B \\ & A_x \succeq 0, \ \forall x \in \{1, ..., N\} \end{cases}$$

By going back and forth between (†) and (‡) until several iterations in a row show no increase in the winning probability we obtain well-performing strategies. In fact, we will later analytically calculate upper bounds on the winning probability for two types of LSSD problems. One involving a pair of product states, the other involving a pair of entangled states. The numerical method described in this section turns out to be efficient at finding optimal solutions in these cases.

5 LSSD of product states

In this section we will study one of the main examples of this thesis. Alice and Bob are locally to distinguish the states

$$\varrho_0^{AB} = \varrho_0^A \otimes \varrho_0^B, \quad \text{and} \quad \varrho_1^{AB} = \varrho_1^A \otimes \varrho_1^B \tag{114}$$

with a uniform prior, where $\varrho_x^A \in D(\mathcal{H}_A)$ and $\varrho_x^B \in D(\mathcal{H}_B)$ are pure states for some complex Euclidean spaces, $\mathcal{H}_A$ and $\mathcal{H}_B$ of finite dimension d_A and d_B respectively. We first make a few observations.

For some fixed measurement, $\mathcal{A}$, Bob is left with the states

$$\kappa_x^B = \tfrac{1}{P_x^{\mathcal{A}}} \mathrm{Tr}_A \left[A_x \otimes \mathbb{I}^B \varrho_x^A \otimes \varrho_x^B \right] = \varrho_x^B. \tag{115}$$

independently of $\mathcal{A}$. The prior Bob is left with is

$$p'_x = \tfrac{1}{2} \tfrac{P_x^{\mathcal{A}}}{P^{\mathcal{A}}} = \tfrac{P_x^{\mathcal{A}}}{P_0^{\mathcal{A}} + P_1^{\mathcal{A}}}. \tag{116}$$

and the optimal winning probability is

$$\tfrac{1}{2} P^{\mathcal{A}} + \tfrac{1}{4} \left\| P_0^{\mathcal{A}} \varrho_0^B - P_1^{\mathcal{A}} \varrho_1^B \right\|_{\mathrm{Tr}}. \tag{117}$$

It is evident that Alice has control over Bob's prior. She can skew Bob's prior by sacrificing her own success probability. To optimize, she has to strike a balance between helping Bob and not sacrificing too much of her own success probability. In the two following observations we will narrow down the set of feasible POVMs within which we have to search for optima.

Observation 13. *It suffices to consider the local dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ to be 2.*

Proof. Since ϱ_x^A and ϱ_x^B are pure, they are given by unit vectors $|\nu_x^A\rangle$ and $|\mu_x^B\rangle$. Due to Corollary 9 we only have to consider projective measurements. That is, there is some basis for $\mathcal{H}_A$ given by $\{|\psi_i^A\rangle\}_{i=1}^{d_A}$ such that we can write

$$A_x = \sum_{i \in I_x} |\psi_i^A\rangle \langle \psi_i^A| \tag{118}$$

where $I_0, I_1 \subseteq [d_A]$ fulfill $I_0 \cup I_1 = [d_A]$. One can define B_x similarly. Since the only terms that contribute to the winning probability are the ones that have a non-vanishing component in the plane spanned by $|\nu_0^A\rangle$ and $|\nu_1^A\rangle$ we do not lose generality by supposing that the local dimensions are 2, i. e. $d_A = d_B = 2$. So we consider the case $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$ □

The winning probability is given by

$$P^{\mathcal{AB}} = \tfrac{1}{2} \left| \langle \psi_0^A | \nu_0^A \rangle \right|^2 \left| \langle \psi_0^B | \mu_0^B \rangle \right|^2 + \tfrac{1}{2} \left| \langle \psi_1^A | \nu_1^A \rangle \right|^2 \left| \langle \psi_1^B | \mu_1^B \rangle \right|^2 \tag{119}$$

Observation 14. *Suppose Alice and Bob's measurements are given by projections onto* $\{|\psi_0^A\rangle, |\psi_1^A\rangle\}$ *and* $\{|\psi_0^B\rangle, |\psi_1^B\rangle\}$*. Then it suffices to consider* $|\psi_x^A\rangle$ *and* $|\psi_x^B\rangle$ *to be of the form*

$$|\psi_0^A\rangle = \begin{pmatrix} \sin(\alpha) \\ -e^{i\theta_\alpha}\cos(\alpha) \end{pmatrix} \text{ and } |\psi_1^A\rangle = \begin{pmatrix} \cos(\alpha) \\ e^{i\theta_\alpha}\sin(\alpha) \end{pmatrix} \tag{120}$$

and

$$|\psi_0^B\rangle = \begin{pmatrix} \sin(\beta) \\ -e^{i\theta_\beta}\cos(\beta) \end{pmatrix} \text{ and } |\psi_1^B\rangle = \begin{pmatrix} \cos(\beta) \\ e^{i\theta_\beta}\sin(\beta) \end{pmatrix} \tag{121}$$

where $\alpha, \beta \in [0, \pi/2]$ *and* $\theta_\alpha, \theta_\beta \in [0, 2\pi)$*.*

Proof. We can write the measurement basis vectors as

$$|\psi_x^A\rangle = \begin{pmatrix} \cos(\alpha_x) \\ \mathrm{e}^{i\gamma_x}\sin(\alpha_x) \end{pmatrix} \text{ and } |\psi_x^B\rangle = \begin{pmatrix} \cos(\beta_x) \\ \mathrm{e}^{i\delta_x}\sin(\beta_x) \end{pmatrix} \tag{122}$$

for some $\alpha_x, \beta_x \in [0, \pi/2]$ and $\gamma_x, \delta_x \in [0, 2\pi)$. Due to orthogonality we have

$$\langle\psi_0^A|\psi_1^A\rangle = \cos(\alpha_0)\cos(\alpha_1) + \mathrm{e}^{i(\gamma_1-\gamma_0)}\sin(\alpha_0)\sin(\alpha_1) = 0 \tag{123}$$

so we need $\gamma_1 - \gamma_0 \in \{0, \pi\}$ in which case

$$\cos(\alpha_0)\cos(\alpha_1) \pm \sin(\alpha_0)\sin(\alpha_1) = \cos(\alpha_0 \mp \alpha_1) = 0 \tag{124}$$

which is the case if and only if $\alpha_0 \mp \alpha_1 \in \{-\frac{\pi}{2}, \frac{\pi}{2}\}$ i. e. we have the following cases

1. $\underline{\gamma_0 = \gamma_1}$: Then $\alpha_0 - \alpha_1 \in \{-\frac{\pi}{2}, \frac{\pi}{2}\}$ so either $(\alpha_0, \alpha_1) = (0, \frac{\pi}{2})$ or $(\alpha_0, \alpha_1) = (\frac{\pi}{2}, 0)$.
2. $\underline{\gamma_0 = \gamma_1 - \pi}$: Then $\alpha_0 + \alpha_1 \in \{-\frac{\pi}{2}, \frac{\pi}{2}\}$ so $\alpha_0 = \frac{\pi}{2} - \alpha_1$.

If one considers the first case it is not hard to see that the expression in Eq. (119) is upper bounded by $\frac{1}{2}$. We therefore consider only the second case. Notice that one can make an entirely similar reasoning regarding Bob's measurement. We define $\alpha := \alpha_1$ and $\theta_\alpha := \gamma_1$, $\beta := \beta_1$ and $\theta_\beta = \delta_1$. Then $\mathcal{A}$ and $\mathcal{B}$ are given by only two parameters, α, θ_α and β, θ_β as

$$|\psi_0^A\rangle = \begin{pmatrix} \sin(\alpha) \\ -\mathrm{e}^{i\theta_\alpha}\cos(\alpha) \end{pmatrix} \text{ and } |\psi_1^A\rangle = \begin{pmatrix} \cos(\alpha) \\ \mathrm{e}^{i\theta_\alpha}\sin(\alpha) \end{pmatrix} \tag{125}$$

and similarly for Bob. □

We will now study the main example of this section.

5.1 Example: LSSD of $|00\rangle$ and $|\varphi\varphi\rangle$

To simplify expressions we consider in this section the case where

$$|\nu_0^A\rangle = |\mu_0^B\rangle = |0\rangle \text{ and } |\nu_1^A\rangle = |\mu_1^B\rangle = |\varphi\rangle \tag{126}$$

where

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |\varphi\rangle := \begin{pmatrix} \cos(\omega) \\ e^{i\theta}\sin(\omega) \end{pmatrix} \tag{127}$$

for some $\theta \in [0, 2\pi)$ and $\omega \in [0, \frac{\pi}{2}]$. Then by standard calculations using trigonometric simplifications we get

$$\begin{aligned} \left|\langle\psi_1^A|\varphi\rangle\right|^2 = \cos^2(\alpha)\cos^2(\omega) + \sin^2(\alpha)\sin^2(\omega) \\ + \tfrac{1}{2}\sin(2\alpha)\sin(2\omega)\cos(\theta - \theta_\alpha). \end{aligned} \tag{128}$$

Since $\sin(2\alpha)\sin(2\omega) \geq 0$ we choose $\theta = \theta_\alpha$. After additional trigonometric simplifications we get

$$\left|\langle\psi_1^A|\varphi\rangle\right|^2 = \cos^2(\alpha - \omega) \tag{129}$$

such that the winning probability becomes

$$P^{\mathcal{AB}} = \tfrac{1}{2}\sin^2(\alpha)\sin^2(\beta) + \tfrac{1}{2}\cos^2(\alpha - \omega)\cos^2(\beta - \omega) \tag{130}$$

Observation 15. *It suffices to consider the case where Alice and Bob use the same local measurement.*

Proof. For any $x, y \in \mathbb{R}$ we have $(x - y)^2 \geq 0$ with equality if and only if $a = b$. This can be restated as

$$xy \leq \tfrac{1}{2}(x^2 + y^2) \tag{131}$$

with equality if and only if $x = y$. Hence,

$$P^{\mathcal{AB}} \leq \tfrac{1}{4}\left(\sin^4(\alpha) + \sin^4(\beta)\right) + \tfrac{1}{4}\left(\cos^4(\alpha - \omega) + \cos^4(\beta - \omega)\right) \tag{132}$$

with saturation if $\alpha = \beta$. Equality holds if and only if both

$$\sin^2(\alpha) = \sin^2(\beta) \text{ and } \cos^2(\alpha - \omega) = \cos^2(\beta - \omega). \tag{133}$$

Since $\alpha, \beta \in [0, \frac{\pi}{2}]$, $\alpha \neq \beta$ implies in particular that $\sin^2(\alpha) \neq \sin^2(\beta)$ so the bound is reached only if $\alpha = \beta$. □

Due to this observation the upper bound on the winning has a single parameter we call x. It is given by

$$P^{\mathcal{AB}} \leq \sup\left\{\tfrac{1}{2}\sin^4(x) + \tfrac{1}{2}\cos^4(x - \omega) \mid x \in \left[0, \tfrac{\pi}{2}\right]\right\} \tag{134}$$

Observation 16. *Suppose Alice and Bob choose $\mathfrak{H}$ class measurements. Then they have a winning probability of*

$$P^{\mathcal{AB}} = \left(\tfrac{1}{2} + \tfrac{1}{2}\sin(\omega)\right)^2 \tag{135}$$

Proof. Since the dimension is 2 we do not have any freedom when choosing $\mathfrak{H}$ class measurements for non-trivial problems. We suppose that both A_0 and B_0 are projections onto the strictly positive eigenspace of

$$|0\rangle\langle 0| - |\varphi\rangle\langle\varphi| = \begin{pmatrix} \sin^2(\omega) & -\frac{1}{2}e^{i\theta}\sin(2\omega) \\ -\frac{1}{2}e^{-i\theta}\sin(2\omega) & -\sin^2(\omega) \end{pmatrix}. \tag{136}$$

By standard calculations we find the eigenvalues to be $\pm\sin(\omega)$ and

$$A_0 = B_0 = \tfrac{1}{2}\begin{pmatrix} 1+\sin(\omega) & -e^{i\theta}\cos(\omega) \\ -e^{-i\theta}\cos(\omega) & 1-\sin(\omega) \end{pmatrix}. \tag{137}$$

Hence

$$P_0^{\mathcal{A}} = P_1^{\mathcal{A}} = \tfrac{1}{2} + \tfrac{1}{2}\sin(\omega), \tag{138}$$

so Alice does not skew Bob's prior and the winning probability becomes

$$P^{\mathcal{AB}} = \left(\tfrac{1}{2} + \tfrac{1}{2}\sin(\omega)\right)^2 \tag{139}$$

as desired. □

The reason why (135) goes to $\frac{1}{4}$ for $\omega \to 0$ is that Alice and Bob do not cooperate in the sense that they only try to optimize their own local success probability. In contrast, (134) is lower bounded by $\frac{1}{2}$ obtained by choosing $x = \omega$. However, as the following proposition shows, for $\omega \geq \frac{\pi}{6}$ it is actually advantageous for Alice and Bob to use local Helstrom measurements.

Proposition 17. *The winning probability of the 2-LSSD problem involving the states* $|00\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ *and* $|\varphi\varphi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ *(with uniform prior) where*

$$|\varphi\rangle = \begin{pmatrix} \cos(\omega) \\ e^{i\theta}\sin(\omega), \end{pmatrix} \tag{140}$$

fulfills

$$P^{\mathcal{AB}} \leq \begin{cases} \frac{1}{2}\cos^4(\omega)\sec(2\omega) & \text{if } \omega \leq \frac{\pi}{6} \\ \left(\frac{1}{2} + \frac{1}{2}\sin(\omega)\right)^2 & \text{if } \omega > \frac{\pi}{6}. \end{cases} \tag{141}$$

We make the following change of variables

$$y := x - \tfrac{1}{2}\omega \quad \text{and} \quad \hat{\omega} := \tfrac{1}{2}\omega \tag{142}$$

where $y \in \left(-\frac{\pi}{4}, \frac{\pi}{2}\right)$ and $\hat{\omega} \in \left(0, \frac{\pi}{4}\right)$. Then we can rewrite Eq. (134) as

$$\tfrac{1}{2}\sin^4(y+\hat{\omega}) + \tfrac{1}{2}\cos^4(y-\hat{\omega}) =: P_{\hat{\omega}}(y) \tag{143}$$

Taking the derivative with respect to y yields

$$\tfrac{d}{dy}P_{\hat{\omega}}(y) = \cos(2y)\left(\sin(2\hat{\omega}) - \cos(4\hat{\omega})\sin(2y)\right) \tag{144}$$

after using trigonometric identities. Setting this equal to 0 has three solutions in the feasible domain. These are

$$y_1 = \tfrac{1}{2}\arcsin\left[\sin(2\hat{\omega})\sec(4\hat{\omega})\right], \tag{145}$$

$$y_2 = \tfrac{\pi}{2} - \tfrac{1}{2}\arcsin\left[\sin(2\hat{\omega})\sec(4\hat{\omega})\right] \tag{146}$$

$$y_3 = \tfrac{\pi}{4}. \tag{147}$$

Since $P_{\hat{\omega}}(y_1) = P_{\hat{\omega}}(y_2)$ we only have to consider y_1. One can check that

- when $\hat{\omega} \in (0, \frac{\pi}{12})$ we have $\frac{d^2}{dy^2}P_{\hat{\omega}}(y_1) < 0$ and $\frac{d^2}{dy^2}P_{\hat{\omega}}(y_3) > 0$ and
- when $\hat{\omega} \in (\frac{\pi}{12}, \frac{\pi}{4})$ we have $\frac{d^2}{dy^2}P_{\hat{\omega}}(y_3) < 0$ and $\frac{d^2}{dy^2}P_{\hat{\omega}}(y_1) > 0$.

Hence, in the regime $\hat{\omega} \in (0, \frac{\pi}{12}]$ we have that $P_{\hat{\omega}}(y_1)$ is a maximum and in the regime $\hat{\omega} \in (0, \frac{\pi}{12}]$ we have that $P_{\hat{\omega}}(y_3)$ is a maximum. One can easily check that these maxima are global. And after some algebraic simplification using trigonometric identities one finds

$$P_{\hat{\omega}}(y_1) = \tfrac{1}{2}\cos^4(\hat{\omega})\sec(4\hat{\omega}) \tag{148}$$

and

$$P_{\hat{\omega}}(y_3) = \tfrac{1}{4}\left(\sin(\hat{\omega}) + \cos(\hat{\omega})\right)^4 \tag{149}$$

which upon reinsertion of $\hat{\omega} := \frac{1}{2}\omega$ and additional simplifications yields the desired.

5.2 Entanglement assisted strategies for product states

In this section we first show that if Alice and Bob are allowed to share an entangled state when attempting to locally discriminate product states, it becomes possible for Alice to alter not only the prior but also the states left for Bob. Afterwards we consider an example where Alice and Bob are allowed to share a maximally entangled state.

Suppose now we let Alice and Bob share the entangled state $\sigma^{A'B'}$. Due to the discussion in Section 4.2 we are interested in the states $\kappa_x^{\bar{B}}$. Using the Fano form of $\sigma^{A'B'}$ in terms of $\beta^{A'}$, $\beta^{B'}$ and $\mathcal{C}_{ij}$ we can rewrite $\varrho_x^{\bar{A}\bar{B}}$ as

$$\varrho_x^{\bar{A}\bar{B}} = \tfrac{1}{d_{A'}d_{B'}}\varrho_x^A \otimes \mathbb{I}^{A'} \otimes \varrho_x^B \otimes \mathbb{I}^{B'} + \tfrac{1}{2d_{B'}}\sum_{i=1}^{d_{A'}^2-1}\beta_i^{A'}\varrho_x^A \otimes \boldsymbol{\sigma}_i^{A'} \otimes \varrho_x^B \otimes \mathbb{I}^{B'} \tag{150}$$

$$+ \tfrac{1}{2d_{A'}}\sum_{j=1}^{d_{B'}^2-1}\beta_j^{B'}\varrho_x^A \otimes \mathbb{I}^{A'} \otimes \varrho_x^B \otimes \boldsymbol{\sigma}_j^{B'} + \tfrac{1}{4}\sum_{i=1}^{d_{A'}^2-1}\sum_{j=1}^{d_{B'}^2-1}\mathcal{C}_{ij}\varrho_x^A \otimes \boldsymbol{\sigma}_i^{A'} \otimes \varrho_x^B \otimes \boldsymbol{\sigma}_j^{B'} \tag{151}$$

With this in mind, one can by standard calculations find $\frac{1}{P_x^{A\sigma}}\mathrm{Tr}_{\bar{A}}\left[\bar{A}_x \otimes \mathbb{I}^{\bar{B}}\varrho_x^{\bar{A}\bar{B}}\right]$ to be

$$\tfrac{1}{d'_B}\varrho_x^B \otimes \mathbb{I}_{B'} + \tfrac{1}{2P_x^{A\sigma}}\sum_{j=1}^{d_{B'}^2-1}\mathrm{Tr}\left[\bar{A}_x\varrho_x^A \otimes \left(\tfrac{\beta_j^{B'}}{d_{A'}}\mathbb{I}_{A'} + \tfrac{1}{2}\sum_{i=1}^{d_{A'}^2-1}\mathcal{C}_{ij}\boldsymbol{\sigma}_i^{A'}\right)\right]\varrho_x^B \otimes \boldsymbol{\sigma}_j^{B'}. \tag{152}$$

The expression in the parentheses is, for every $j \in [d_{B'}^2 - 1]$ some operator, we denote $\tau_j^{A'}$, on $\mathcal{H}_{A'}$. We get therefore,

$$\varrho_x^B \otimes \left(\tfrac{1}{d'_B} \mathbb{I}_{B'} + \tfrac{1}{2} \sum_{j=1}^{d_{B'}^2 - 1} \frac{\mathrm{Tr}\left[\bar{A}_x \varrho_x^A \otimes \tau_j^{A'} \right]}{P_x^{\mathcal{A}\sigma}} \boldsymbol{\sigma}_j^{B'} \right). \tag{153}$$

We define the expression in the parentheses as $\chi_x^{B'}$. This is a state on $\mathcal{H}_B$ with Bloch vector components given by

$$\frac{\mathrm{Tr}\left[\bar{A}_x \varrho_x^A \otimes \tau_j^{A'} \right]}{P_x^{\mathcal{A}\sigma}} \tag{154}$$

And we find that the states left for Bob are given by

$$\kappa_x^{\bar{B}} = \varrho_x^B \otimes \chi_x^{B'}. \tag{155}$$

Unlike the non-assisted case Alice can now alternate both the prior and the states that Bob has to discriminate. This would lead one to think that there could be a possibility of a strict separation between the non-assisted and the entanglement assisted optimal winning probabilities. However, we have not found any such examples.

Example 18. (Unsuccessful attempt at finding separation with non-assisted case) In this example we investigate if Alice and Bob can enhance the optimal winning probability if they are allowed to share a maximally entangled state in $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$. We assume $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$ both to have dimension n for some $n \geq 2$. In other words, let

$$\sigma^{A'B'} = |\Psi\rangle \langle \Psi| \tag{156}$$

where

$$|\Psi\rangle = \tfrac{1}{\sqrt{n}} \sum_{i=1}^{n} |ii\rangle \tag{157}$$

Consider the LSSD problem, as in the previous section, involving $|00\rangle$ and $|\varphi\varphi\rangle$ where $\omega > \frac{\pi}{6}$. As we have seen, the optimal strategy for Alice and Bob is a $\mathfrak{H}$ class measurement locally for both of them. Lemma 11 therefore tells us that if there exists an entanglement assisted strategy $\{\mathcal{A}_\sigma, \mathcal{B}_\sigma\}$ such that $P^{\mathcal{A}_\sigma \mathcal{B}_\sigma} > P^{\mathcal{A}\mathcal{B}}$ then $\mathcal{A}_\sigma$ is not $\mathfrak{H}^{\bar{A}}$ class.

Notice that the reduced states of the maximally entangled state $\sigma^{A'B'}$ are maximally mixed i. e. $\sigma^{A'} = \frac{1}{n}\mathbb{I}^{A'}$. We will consider the following non - $\mathfrak{H}^{\bar{A}}$ class measurements: Let $\{Q, Q'\}$ be a projective measurement in $\mathcal{H}_{A'}$ where Q has rank $0 < r < n$ and let

$$\bar{A}_0 = A_0 \otimes Q \quad \text{and} \quad \bar{A}_1 = \mathbb{I}^{\bar{A}} - A_0 \otimes Q. \tag{158}$$

We will first derive the states and the prior left for Bob. One easily finds

$$P_0^{\mathcal{A}_\sigma} = \tfrac{r}{n} P_0^{\mathcal{A}} = \tfrac{r}{2n} \left(1 + \sin(\omega) \right) \tag{159}$$

and

$$P_1^{\mathcal{A}_\sigma} = 1 - \tfrac{r}{n} + \tfrac{r}{n} P_1^{\mathcal{A}} = 1 - \tfrac{r}{2n}\left(1 - \sin(\omega)\right) \tag{160}$$

such that Alice can skew Bob's prior by varying r. We have

$$P^{\mathcal{A}_\sigma} = \tfrac{1}{2} P_0^{\mathcal{A}_\sigma} + \tfrac{1}{2} P_1^{\mathcal{A}_\sigma} = \tfrac{1}{2} + \tfrac{r}{2n}\sin(\omega). \tag{161}$$

As expected we see that $P^{\mathcal{A}_\sigma} \leq P^{\mathcal{A}}$ with equality if and only if $r = n$. When calculating the states left for Bob it is useful to notice the following

$$\begin{aligned}
\mathrm{Tr}_{A'}\left[Q \otimes \mathbb{I}^{B'} \sigma^{A'B'}\right] =& \tfrac{1}{n} \sum_{i=1}^{n} \mathrm{Tr}_{A'}\left[Q \otimes \mathbb{I}^{B'} |ii\rangle \langle ii|\right] && (162)\\
=& \tfrac{1}{n} \sum_{i=1}^{n} Q_{ii} |i\rangle \langle i| && (163)\\
=& \tfrac{1}{n} \mathrm{diag}(Q_{ii}). && (164)
\end{aligned}$$

The states left for Bob are

$$\begin{aligned}
\kappa_0^{\bar{B}} =& \tfrac{1}{P_0^{\mathcal{A}_\sigma}} \mathrm{Tr}_{\bar{A}}\left[A_0 \otimes \mathbb{I}^B \otimes Q \otimes \mathbb{I}^{B'} \varrho_0^{AB} \otimes \sigma^{A'B'}\right] && (165)\\
=& \tfrac{1}{P_0^{\mathcal{A}_\sigma}} \mathrm{Tr}_{A}\left[A_0 \otimes \mathbb{I}^B \varrho_0^A \otimes \varrho_0^B\right] \otimes \mathrm{Tr}_{A'}\left[Q \otimes \mathbb{I}^{B'} \sigma^{A'B'}\right] && (166)\\
=& \tfrac{P_0^{\mathcal{A}}}{n P_0^{\mathcal{A}_\sigma}} \varrho_0^B \otimes \mathrm{diag}(Q_{ii}) && (167)\\
=& \tfrac{1}{P_0^{\mathcal{A}_\sigma}} \varrho_0^B \otimes K && (168)
\end{aligned}$$

where $K \coloneqq P_0^{\mathcal{A}} \mathrm{diag}(\frac{Q_{ii}}{n})$. In a similar fashion one finds

$$\kappa_1^{\bar{B}} = \tfrac{1}{P_1^{\mathcal{A}_\sigma}}\left(\varrho_1^B \otimes \mathrm{diag}\left(\tfrac{Q'_{ii}}{n}\right) + \varrho_1^B \otimes K\right) \tag{169}$$

using $P_0^{\mathcal{A}} = P_1^{\mathcal{A}}$. Owing to 75 we get therefore an upper bound of the winning probability as

$$\tfrac{1}{2} P^{\mathcal{A}_\sigma} + \tfrac{1}{4}\left\|(\varrho_0^B - \varrho_1^B) \otimes K - \varrho_1^B \otimes \mathrm{diag}(\tfrac{Q'_{ii}}{n})\right\|_{\mathrm{Tr}}. \tag{170}$$

Using the triangle inequality we get

$$\begin{aligned}
\leq& \tfrac{1}{2} P^{\mathcal{A}_\sigma} + \tfrac{1}{4}\left\|(\varrho_0^B - \varrho_1^B) \otimes K\right\|_{\mathrm{Tr}} + \tfrac{1}{4}\left\|\varrho_1^B \otimes \mathrm{diag}(\tfrac{Q'_{ii}}{n})\right\|_{\mathrm{Tr}} && (171)\\
=& \tfrac{1}{2} P^{\mathcal{A}_\sigma} + \tfrac{1}{4} P_0^{\mathcal{A}}\left\|(\varrho_0^B - \varrho_1^B)\right\|_{\mathrm{Tr}}\left\|\mathrm{diag}(\tfrac{Q_{ii}}{n})\right\|_{\mathrm{Tr}} + \tfrac{1}{4}\left\|\mathrm{diag}(\tfrac{Q'_{ii}}{n})\right\|_{\mathrm{Tr}} && (172)\\
=& \tfrac{1}{2} P^{\mathcal{A}_\sigma} + \tfrac{1}{4} \tfrac{r}{n} P_0^{\mathcal{A}}\left\|(\varrho_0^B - \varrho_1^B)\right\|_{\mathrm{Tr}} + \tfrac{1}{4} \tfrac{n-r}{n} && (173)
\end{aligned}$$

This bound is reached if and only if

$$\mathrm{diag}(Q_{ii})\mathrm{diag}(Q'_{ii}) = \mathrm{diag}\left(Q_{ii}(1 - Q_{ii})\right) = 0. \tag{174}$$

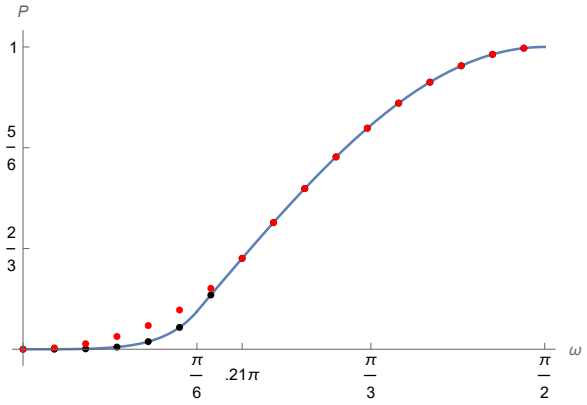


Figure 2: Graph of upper bound on winning of LSSD problem involving $|00\rangle$ and $|\varphi\varphi\rangle$ with uniform prior. Black points are numerically obtained using method described in section 4.4. Red points correspond with no-signaling strategies obtained numerically.

This, in turn, is the case if and only if Q is diagonal. To see why, recall that it is a standing assumption that Q is a projection so $Q^2 - Q = 0$ which implies

$$Q_{ii} = Q_{ii}^2 + \sum_{j \neq i} |Q_{ij}|^2 \tag{175}$$

so 174 is fulfilled if and only if $Q_{ij} = 0$ for all $i \neq j$ which is equavalent to Q being diagonal.

If one writes out 173 explicitly in terms of ω one gets:

$$\tfrac{1}{2} + \tfrac{r}{4n}\left(2\sin(\omega) - \cos^2(\omega)\right) \tag{176}$$

for the values of ω that we are considering the expression in the parentheses is larger that 0 and hence the winning probability is upper bounded by

$$\tfrac{1}{2} + \tfrac{1}{4}\left(2\sin(\omega) - \cos^2(\omega)\right) = \left(\tfrac{1+\sin(\omega)}{2}\right)^2 \tag{177}$$

and we have therefore recovered the original expression for the upper bound in the non-assisted case. •

5.3 Strict no-signaling separation

Since we have explicitly derived an upper bound on the winning probability for product states of the form $|00\rangle$ and $|\varphi\varphi\rangle$ with uniform prior in the non-assisted case, we can investigate whether it is possible to increase the winning probability with additional resources. As already mentioned we have not been able to find any example of 2-LSSD problems for which

$$P^{\mathcal{A}_\sigma \mathcal{B}_\sigma} > \sup_{\mathcal{A},\mathcal{B}} P^{\mathcal{A}\mathcal{B}}. \tag{178}$$

However, interestingly, we have for small angles (ω less that $\approx .21\pi$) by using a standard SDP solver, found a strict no-signaling separation. More specifically we have a lower bound on $\sup_{\Omega} P^{\Omega}$ which is strictly larger than $\sup_{\mathcal{A},\mathcal{B}} P^{\mathcal{AB}}$. This, in particular means that Proposition 3.3 in [12] does not generalize to quantum states. In Figure 2 we have included an overview of the results of this chapter.

6 LSSD involving entangled states

In this section we investigate a particular LSSD problem introduced in [13]. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be d'-dimensional complex Euclidean spaces i. e. $\mathbb{C}^{d'}$. Let X be a $d := d' - 1$ dimensional complex Euclidean space i. e. $\mathbb{C}^d$ and consider the following map

$$V_{X\to AB} : X \longrightarrow \mathcal{H}_A \otimes \mathcal{H}_B \tag{179}$$

defined by

$$|\varphi\rangle \longmapsto \tfrac{1}{\sqrt{2}} \left(|\varphi\rangle_A \otimes |d'\rangle_B + |d'\rangle_A \otimes |\varphi\rangle_B \right). \tag{180}$$

where $|d'\rangle$ is orthogonal to X. Now consider two perfectly distinguishable states, σ_0 and σ_1 in X. We wish, in this example to investigate Alice and Bob's maximal success probability of discriminating the states

$$\varrho_0^{AB} := V\sigma_0 V^\dagger \quad \text{and} \quad \varrho_1^{AB} := V\sigma_1 V^\dagger \tag{181}$$

with uniform prior.

This problem has been studied in the context of uncloneable quantum encryption schemes for classical messages in [13]. Previously, in [3] certain security notions have been considered, in particular that of *uncloneable-indistinguishability* and *cloning attacks*. The example that we study in this section can be viewed as a particular instance of a cloning attack. If we think of the input state $|x\rangle$ as the quantum encryption of a classical message, we can consider the operator V as a cloning operator, outputting the state $V|x\rangle$ which is given to Alice and Bob. If Alice and Bob are able to recover the original message (using a classical key) with a probability that is only negligibly above the trivial guessing probability, the encryption scheme under consideration is said to be *secure*.

In [13] the authors show the impossibility of uncloneable encryption using pure states as ciphertext (see also [12]). They do this by showing that the optimal winning probability in the LSSD problem described above has a lower bound of

$$\tfrac{1}{2} + \tfrac{m}{16} \tag{182}$$

where m is the maximum of the eigenvalues of σ_0 and σ_1. In what follows we will show that for pure states, $\frac{9}{16}$ is in fact an upper bound.

We begin by making a few general observations. Recall, that by assumption $\sigma_0\sigma_1 = 0$, so they can be simultaneously diagonalized in the basis $\{|\psi_i\rangle\}_{i=1}^d$. We then have eigen-decompositions,

$$\sigma_0 = \sum_{i=1}^d \nu_i^0 |\psi_i\rangle\langle\psi_i| \quad \text{and} \quad \sigma_1 = \sum_{i=1}^d \mu_i^1 |\psi_i\rangle\langle\psi_i| \tag{183}$$

with $1 \geq \nu_1 \geq ... \geq \nu_d = 0$ and $0 = \mu_1 \leq ... \leq \mu_d \leq 1$ and $\nu_i = 0$ if $\mu_i \neq 0$ and vice versa. Then $|\psi_i\rangle_{i=1}^d$ along with $|\psi_{d'}\rangle := |d'\rangle$ defines an orthonormal basis. We find the state ϱ_0^{AB} explicitly as,

$$\begin{aligned}\varrho_0^{AB} = \tfrac{1}{2}\sum_{i=1}^d \nu_i\big(&|\psi_i\psi_{d'}\rangle\langle\psi_i\psi_{d'}| + |\psi_i\psi_{d'}\rangle\langle\psi_{d'}\psi_i| \\ &+ |\psi_{d'}\psi_i\rangle\langle\psi_i\psi_{d'}| + |\psi_{d'}\psi_i\rangle\langle\psi_{d'}\psi_i|\big)\end{aligned} \tag{184}$$

and similarly for ϱ_1^{AB}. The reduced state ϱ_x^A is

$$\varrho_x^A = \tfrac{1}{2}|\psi_{d'}\rangle\langle\psi_{d'}| + \tfrac{1}{2}\sigma_x. \tag{185}$$

where σ_x has been given an appropriate domain extension. Hence for some POVM $\mathcal{A} = \{A_0, A_1\}$, we have

$$P_x^{\mathcal{A}} = \tfrac{1}{2}(A_x)_{d'd'} + \tfrac{1}{2}\mathrm{Tr}[\sigma_x' A_x] \tag{186}$$

where $(A_x)_{d'd'} := \langle\psi_{d'}| A_x |\psi_{d'}\rangle$. Using $(A_1)_{ii} = 1 - (A_0)_{ii}$ one finds

$$P^{\mathcal{A}} = \tfrac{1}{2} + \tfrac{1}{4}\mathrm{Tr}[A_0(\sigma_0 - \sigma_1)] \tag{187}$$

which is upper bounded by $\frac{3}{4}$ corresponding to an $\mathfrak{H}^A$ class measurement.

Observation 19. *Let $\mathcal{A}$ be $\mathfrak{H}^A$ class. Then the winning probability is upper bounded by $\frac{1}{2}$.*

Proof. Suppose Alice chooses an $\mathfrak{H}^A$ class measurement. Since it is a standing assumption that $\mathcal{A}$ is projective, we may assume that A_0 has 1 in the diagonal entries for which $\nu_i > 0$ and zeros in the entries of the same rows and columns. For such a measurement the states left for Bob can be found as

$$\kappa_x^B = \tfrac{1}{2P_x^{\mathcal{A}}}\left(|\psi_{d'}\rangle\langle\psi_{d'}| + (A_x)_{d'd'}\sigma_x\right) \tag{188}$$

We have therefore an upper bound on the winning probability as

$$\begin{aligned}\tfrac{1}{2}P^{\mathcal{A}}\left(1 + \left\|p_0\tfrac{P_0^{\mathcal{A}}}{P^{\mathcal{A}}}\kappa_0^B - p_1\tfrac{P_1^{\mathcal{A}}}{P^{\mathcal{A}}}\kappa_1^B\right\|_{\mathrm{Tr}}\right) &= \tfrac{1}{2}P^{\mathcal{A}} + \tfrac{1}{4}\left\|P_0^{\mathcal{A}}\kappa_0^B - P_1^{\mathcal{A}}\kappa_1^B\right\|_{\mathrm{Tr}} && (189)\\ &= \tfrac{3}{8} + \tfrac{1}{4}\left\|\tfrac{1}{2}(A_0)_{d'd'}\sigma_0 - \tfrac{1}{2}(A_1)_{d'd'}\sigma_1\right\|_{\mathrm{Tr}} && (190)\\ &= \tfrac{3}{8} + \tfrac{1}{8}\left((A_0)_{d'd'} + (A_1)_{d'd'}\right) = \tfrac{1}{2} && (191)\end{aligned}$$

using the orthogonality of σ_0 and σ_1 in the third equality. □

Lemma 20. *Consider the 2-LSSD problem involving $V\sigma_0V^\dagger$ and $V\sigma_1V^\dagger$ (defined in (181)) with uniform prior. When upper bounding the winning probability it suffices to consider joint strategies*

$$\{A, \mathbb{I} - A\} \quad \textit{and} \quad \{B, \mathbb{I} - B\} \tag{192}$$

for which

$$(\dagger) : A = B \quad \text{or} \quad (\ddagger) : B = \begin{pmatrix} A_{11} & \cdots & A_{1d'} \\ \vdots & \ddots & \\ A_{d'1} & \cdots & 1 - A_{d'd'} \end{pmatrix}. \tag{193}$$

Proof. Let $\{A, \mathbb{I} - A\}$ and $\{B, \mathbb{I} - B\}$ be a joint strategy. One readily finds

$$\operatorname{Tr}[A \otimes B\varrho_0^{AB}] = \tfrac{1}{2}\sum_{i=1}^{d} \nu_i \left[A_{ii}B_{d'd'} + A_{id'}B_{d'i} + A_{d'i}B_{id'} + B_{ii}A_{d'd'}\right] \tag{194}$$

Let us write the numbers $A_{id'}$ and $B_{id'}$ in their polar form

$$A_{jd'} = \left|A_{jd'}\right| \mathrm{e}^{i\alpha_j} \quad \text{and} \quad B_{jd'} = \left|B_{jd'}\right| \mathrm{e}^{i\beta_j}. \tag{195}$$

Then the law of cosines implies

$$\begin{aligned} A_{id'}B_{d'i} + A_{id'}B_{d'i} &= 2|A_{id'}||B_{id'}|\cos(\alpha_i - \beta_i) && (196)\\ &= |A_{id'}|^2 + |B_{id'}|^2 - |A_{id'} - B_{id'}|^2 && (197)\\ &\leq |A_{id'}|^2 + |B_{id'}|^2 && (198) \end{aligned}$$

with equality if and only if $A_{id'} = B_{id'}$ for all $i \leq d$. We thus have the bound

$$\operatorname{Tr}[A \otimes B\varrho_0^{AB}] \leq \tfrac{1}{2}\sum_{i=1}^{d} \nu_i \left[A_{ii}B_{d'd'} + |A_{id'}|^2 + |B_{id'}|^2 + B_{ii}A_{d'd'}\right] \tag{199}$$

We find similarly

$$\begin{aligned} &\operatorname{Tr}[(\mathbb{I} - A) \otimes (\mathbb{I} - B)\varrho_1^{AB}] && (200)\\ \leq &\tfrac{1}{2}\sum_{i=1}^{d} \mu_i \big[(1 - A_{ii})(1 - B_{d'd'}) + |A_{id'}|^2 + |B_{id'}|^2 + (1 - B_{ii})(1 - A_{d'd'})\big] && (201)\\ = 1 + &\tfrac{1}{2}\sum_{i=1}^{d} \mu_i \big[A_{ii}B_{d'd'} + B_{ii}A_{d'd'} + |A_{id'}|^2 + |B_{id'}|^2 - A_{ii} - B_{d'd'} - B_{ii} - A_{d'd'}\big] && (202) \end{aligned}$$

using that the eigenvalues sum to 1. We hence have the following bound on the winning probability

$$\begin{aligned} P^{\mathcal{AB}} \leq &\tfrac{1}{2} + \tfrac{1}{4}\sum_{i=1}^{d} \nu_i \left[A_{ii}B_{d'd'} + |A_{id'}|^2 + |B_{id'}|^2 + B_{ii}A_{d'd'}\right] && (203)\\ &+ \mu_i \left[A_{ii}B_{d'd'} + B_{ii}A_{d'd'} + |A_{id'}|^2 + |B_{id'}|^2 - A_{ii} - B_{d'd'} - B_{ii} - A_{d'd'}\right]. && (204) \end{aligned}$$

Using the idempotency of A and B we have

$$A_{d'd'}^2 + \sum_{i=1}^{d} |A_{id'}|^2 = A_{d'd'} \tag{205}$$

and similarly for B. Hence

$$A_{d'd'} - A_{d'd'}^2 = B_{d'd'} - B_{d'd'}^2 \tag{206}$$

and we obtain two cases:

$$(\dagger): \ B_{d'd'} = A_{d'd'}, \quad (\ddagger): \ B_{d'd'} = 1 - A_{d'd'}. \tag{207}$$

Upon insertion into the expression in (203) one easily sees that the sum in (203) splits up in two terms involving A and B individually. This is sufficient to conclude that we only have to consider the case where upper left d-by-d blocks of A and B are equal. We conclude therefore the desired.

□

We are now ready to prove the main result of this section.

Proposition 21. *Let σ_0 and σ_1 be pure states. For the 2-LSSD problem involving involving $V\sigma_0 V^\dagger$ and $V\sigma_1 V^\dagger$ with uniform prior the winning probability is upper bounded by $\frac{9}{16}$.*

Proof. Since σ_0 and σ_1 are assumed to be pure states, all eigenvalues except one vanish and we can without loss of generality assume that $d = 2$ and $\nu_1 = 1$ and $\mu_2 = 1$. The expression (203) then becomes

$$P^{\mathcal{AB}} \leq \tfrac{1}{2} + \tfrac{1}{4}\Big(A_{11}B_{33} + |A_{13}|^2 + |B_{13}|^2 + B_{11}A_{33} + A_{22}B_{33} + B_{22}A_{33} \tag{208}$$

$$+ |A_{23}|^2 + |B_{23}|^2 - A_{22} - B_{33} - B_{22} - A_{33}\Big) \tag{209}$$

By using the idempotency of A and B to write

$$|A_{13}|^2 + |A_{23}|^2 = A_{33} - A_{33}^2 \tag{210}$$

and similarly fo B we get the upper bound

$$\tfrac{1}{2} + \tfrac{1}{4}\left((A_{11} + A_{22})B_{33} - A_{22} - A_{33}^2\right) + \tfrac{1}{4}\left((B_{11} + B_{22})A_{33} - B_{22} - B_{33}^2\right) \tag{211}$$

The two cases $(\dagger)$ and $(\ddagger)$ therefore become

$$(\dagger): \quad P_1(A) := \tfrac{1}{2} + \tfrac{1}{2}\big[(A_{11} + A_{22})A_{33} - A_{33}^2 - A_{22}\big] \tag{212}$$

$$(\ddagger): \quad P_2(A) := \tfrac{1}{2} + \tfrac{1}{2}\big[(A_{11} + A_{22})(1 - A_{33}) - (1 - A_{33})^2 - a_{22}\big] \tag{213}$$

The rank of A is equal to $A_{11} + A_{22} + A_{33}$ which belongs to the set $\{0, 1, 2, 3\}$. If $\mathrm{rank}(A) \in \{0, 3\}$ then we have either $A_{11} = A_{22} = A_{33} \in \{0, 1\}$ and one easily finds the success probability in both cases to be less than or equal to $\frac{1}{2}$.

We consider now the case $(\ddagger)$:

- rank$(A) = 1$: We then have $1 - A_{33} = A_{11} + A_{22}$ so we have

$$P_2(A) = \tfrac{1}{2} - \tfrac{1}{2}A_{22} \leq \tfrac{1}{2} \tag{214}$$

- rank$(A) = 2$: We then get

$$P_2(A) = 1 - \tfrac{1}{2}(A_{22} + A_{33}) \tag{215}$$

  and since rank$(A) = 2$ we must have $A_{22} + A_{33} \geq 1$ so we get again an upper bounded of $\frac{1}{2}$.

Next, we consider case the (†):

- rank$(A) = 1$: We find

$$P_1(A) = \tfrac{1}{2} + \tfrac{1}{2}\big[A_{33} - 2A_{33}^2 - A_{22}\big] \tag{216}$$

  which is upper bounded by

$$\tfrac{1}{2} + \tfrac{1}{2}A_{33}\big[1 - 2A_{33}\big] \leq \tfrac{9}{16}. \tag{217}$$

  for $A_{22} = 0$.

- rank$(A) = 2$: We add and subtract A_{33} in the parentheses in (212) to get

$$\tfrac{1}{2} + \tfrac{1}{2}\big[3A_{33} - 2A_{33}^2 - (A_{22} + A_{33})\big] \tag{218}$$

  Now we use the fact that $A_{22} + A_{33} \geq 1$ (which is the case since the rank is equal to 2) to get the upper bound

$$\tfrac{1}{2} + \tfrac{1}{2}\big[3a_{22} - 2a_{22}^2 - 1\big] = \tfrac{1}{2}a_{22}\big[3 - 2a_{22}\big] \leq \tfrac{9}{16}. \tag{219}$$

We are done. □

Once again we have analytically determined an upper bound for an LSSD problem, which makes it possible to search for strict separations in the assisted problems in the same sense as for the product states. We have not been able to find examples of strict separation for the entanglement assisted problem. However, once again we have a strict separation with respect to the no-signaling assisted problem. Numerically we have determined a no signaling assisted strategy with a winning probability of $0.58579 \approx 2 - \sqrt{2} > \frac{9}{16}$.

7 Conclusion

As a general result we have shown that the winning probability in any N-LSSD problem has the form of a product of individual success probabilities of two different but interdependent QSD problems.

We have determined upper bounds on the winning probability of non-assisted 2-LSSD problems involving both product states and one example involving entangled states. This has made it possible to show a strict no-signaling assisted separation. Whether there exist strict entanglement assisted separations for 2-LSSD problems is left open.

Furthermore, we have proposed a numerical method for studying LSSD problems. Testing this method against the LSSD problems with the upper bounds that we have found shows the efficiency of this numerical procedure.

We have seen that if the optimal non-assisted strategy consists of Local Helstrom measurements then any entanglement assisted strategy that beats this uses non-Helstrom measurements locally.

References

[1] J. Bae and L.-C. Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, jan 2015. doi:10.1088/1751-8113/48/8/083001.

[2] S. M. Barnett and S. Croke. Quantum state discrimination. *Adv. Opt. Photon.*, 1(2):238–278, Apr 2009. doi:10.1364/AOP.1.000238.

[3] A. Broadbent and S. Lord. Uncloneable Quantum Encryption via Oracles. In S. T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:22, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.TQC.2020.4.

[4] E. Chitambar, D. Leung, L. Mančinska, and et al. Everything you always wanted to know about locc (but were afraid to ask). *Commun. Math. Phys.*, 328:303–326, 2014. doi:https://doi.org/10.1007/s00220-014-1953-9.

[5] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975. doi:https://doi.org/10.1016/0024-3795(75)90075-0.

[6] M. E. Deconinck and B. M. Terhal. Qubit state discrimination. *Physical Review A*, 81(6), Jun 2010. doi:10.1103/physreva.81.062304.

[7] R. Duan and A. Winter. No-signalling-assisted zero-error capacity of quantum channels and an information theoretic interpretation of the lovász number. *IEEE Transactions on Information Theory*, 62(2):891–914, 2016. doi:10.1109/TIT.2015.2507979.

[8] P. Hausladen and W. K. Wootters. A 'pretty good' measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385–2390, 1994, https://doi.org/10.1080/09500349414552221. doi:10.1080/09500349414552221.

[9] C. W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

[10] A. S. Holevo. "remarks on optimal quantum measurements". *Probl. Peredachi Inf.*, 10(4):317–320, 1974.

[11] T. Imamichi and R. Raymond. 'Constructions of Quantum Random Access Codes'. *Asian Quantum Information Symposium (AQIS)*, 2018. URL `http://www.ngc.is.ritsumei.ac.jp/~ger/static/AQIS18/OnlineBooklet/122`.

[12] C. Majenz, M. Ozols, C. Schaffner, and M. Tahmasbi. Local simultaneous state discrimination, 2021, 2111.01209.

[13] C. Majenz, C. Schaffner, and M. Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding, 2021, 2103.14510.

[14] L. Mančinska and S. A. L. Storgaard. The geometry of bloch space in the context of quantum random access codes, 2021, 2106.00155.

[15] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[16] I. G. Todorov and L. Turowska. Quantum no-signalling correlations and non-local games, 2020, 2009.07016.

[17] J. Watrous. *The theory of quantum information*. Cambridge University Press, Cambridge, 2018.

[18] J.-H. Zhang, F.-L. Zhang, Z.-X. Wang, L.-M. Lai, and S.-M. Fei. Discriminating bipartite mixed states by local operations. *Phys. Rev. A*, 101:032316, Mar 2020. doi:10.1103/PhysRevA.101.032316.