UAB

Universitat Autònoma de Barcelona

Lower bounds of the success probability in quantum state exclusion for general ensembles

Author : Sergio Castañeiras Morales
Supervisor : Ramón Muñoz Tapia
Co-Supervisor : Santiago Llorens Fernández

Final Degree Project
Bachelor's Degree in Physics

2024-2025

Ab ovo usque ad mala.

Horace

Abstract

Given a quantum state known to be prepared from an ensemble of two or more states, quantum state exclusion aims to rule out the possibility that it was prepared in a particular state from the ensemble. Using the known solution for group generated ensembles [6], we study this result as a lower bound for randomly generated ensembles via semidefinite programming.

Keywords: *SDP, Quantum state exclusion , Add keywords.*

I INTRODUCTION

In many real-world scenarios, excluding a certain hypothesis can be more practical than solving the problem entirely. For instance, in disease diagnosis, ruling out potential diseases often serves as the first step in identifying the actual condition. Similarly, when repairing a machine, it is sometimes more efficient to identify the components that are functioning correctly, which narrows down the search for the faulty part.

In this project, we project this idea into the quantum realm by focusing on Quantum State Exclusion (QSE). Rather than determining the exact state of a quantum system, we aim to eliminate one or more possible candidates from a known ensemble of states. Notice, this approach can be more suitable or efficient in certain quantum information tasks.

Given a quantum state known to be prepared from a finite ensemble, Quantum State Discrimination (QSD) seeks to identify which specific state from the ensemble corresponds to the given system. In contrast, QSE [2] adopts the opposite perspective: it aims to determine which states from the ensemble do not correspond to the prepared state. While QSD has been deeply studied in recent years[1], with significant advances since its inception [8], QSE offers a complementary framework with distinct advantages.

Although the tasks of exclusion and discrimination coincide for ensembles containing only two states [1], when dealing with ensembles of three or more states, the two problems diverge in both approach and complexity. One of the most significant features of QSE is the possibility of achieving *perfect exclusion*, where certain states can be ruled out with zero probability of error in cases where *perfect discrimination* is impossible[4].

This capability opens new frontiers in quantum information theory, particularly in the context of partial information retrieval from quantum systems. By excluding certain states, it is possible to gain insight into the encoded information without needing to fully determine the original state.

As with QSD, obtaining a general analytical solution for QSE remains an open problem. However, analytical results have been found in specific cases when the ensemble of quantum states exhibits a certain degree of symmetry. In particular, when the ensemble is generated by the action of a finite group, the problem becomes more tractable and exact solutions have been derived.

The exclusion task can be carried out under two main protocols: Minimum Error (ME) and Zero Error (ZE)[2]. In the Minimum Error scenario, the goal is to minimize the probability of mistakenly excluding the actual prepared state. In contrast, the Zero Error approach seeks to exclude a state with absolute certainty, even if that means sometimes the procedure yields an inconclusive result.

Building on recent results that provide ex-

[1] Since for the two states case excluding one necessarily implies identifying the other.

[2] Also known as *unambiguous exclusion*.

act solutions for exclusion tasks in group generated ensembles [6], this project undertakes a numerical study of such results as lower bounds for more general, randomly generated ensembles. To this end, we employ Semidefinite Program (SDP) to explore QSE performance in arbitrary settings. Furthermore, we investigate improved bounds for the general case based on how closely a given ensemble resembles a group generated one[3].

I.I FORMULATION OF THE PROBLEM

Let $\{(\rho_i, \eta_i)\}_{i=1}^n$ be an ensemble of n quantum states, where each ρ_i denotes a pure state density matrix[4], i.e., $\rho_i = |\psi_i\rangle\langle\psi_i|$, and η_i represents the prior probability of occurrence of the state ρ_i. Let ρ_j be the target state from this ensemble. Our objective is to develop a procedure to identify another state $\rho_k \in \{\rho_i\}_{i=1}^n$, such that $\rho_k \neq \rho_j$.

Quantum measurements are described by a set of Positive Operator-Valued Measures (POVMs), denoted by $\{\Pi_i\}_{i=1}^n$, acting on the Hilbert space $\mathcal{H}$ of the quantum system. Here we pewsent the two studied protocols for QSE: minimum-error (ME) and zero-error (ZE).

The goal of the ME protocol is to minimize the probability of incorrectly excluding the target state from our hypothesis. If we formulate it as an SDP, the problem reads,[5]

$$P_{\text{ME}}^e = \min_{\{\Pi_i\}} \sum_{i=1}^n \text{Tr}(\Pi_i \rho_i),$$
$$\text{subject to} \quad \sum_{i=1}^n \Pi_i = \mathbb{1}, \quad \Pi_i \geq 0 \quad \forall i \in \{1, \ldots, n\}.$$

Note the constraints $\sum_{i=1}^n \Pi_i = \mathbb{1}$ and $\Pi_i \geq 0$ ensure that the Π_i form a valid POVM, since they demand positive semi-definition and form a complete measurement. The superscript e in P_{ME}^e indicates that this is the *error probability*.

Alternatively, we may formulate the problem in terms of the *success probability*, denoted by P_{ME}^s, which quantifies the probability of a correct exclusion. This equivalent formulation reads,

$$P_{\text{ME}}^s = \max_{\{\Pi_i\}} \left(1 - \sum_{i=1}^n \text{Tr}(\Pi_i \rho_i)\right),$$
$$\text{subject to} \quad \sum_{i=1}^n \Pi_i = \mathbb{1}, \quad \Pi_i \geq 0 \quad \forall i \in \{1, \ldots, n\}.$$

Naturally, both formulations are related via:

$$P_{\text{ME}}^s + P_{\text{ME}}^e = 1.$$

In the case of the ZE protocol, the POVMs must also satisfy an unambiguity condition, i.e. each measurement operator Π_i must be orthogonal to the corresponding state ρ_i. In other words,

$$\text{Tr}(\Pi_i \rho_i) = 0 \quad \forall i \in \{1, \ldots, n\}.$$

To ensure completeness, we introduce an additional POVM element $\Pi_?$ representing an inconclusive result,

$$\Pi_? = \mathbb{1} - \sum_{i=1}^n \Pi_i.$$

If the measurement yields the outcome $\Pi_?$ (i.e., the "?" symbol), the result is inconclusive.

The corresponding SDP for minimizing the probability of an inconclusive result (i.e., error) in the ZE protocol is:

$$P_{\text{ZE}}^e = \min_{\{\Pi_i\}} \sum_{i=1}^n \text{Tr}(\Pi_? \rho_i),$$
$$\text{subject to} \quad \sum_{i=1}^n \Pi_i + \Pi_? = \mathbb{1}, \quad \Pi_? \geq 0,$$
$$\text{Tr}(\Pi_i \rho_i) = 0, \quad \Pi_i \geq 0 \quad \forall i.$$

[3] The notion of "how close" will be formally defined in Section add section.

[4] This formulation hols true for mixed states but the project will only discuss the pure state scenario.

[5] Note that the SDP formulations of quantum state discrimination may differ from the exclusion ones by interchanging minimization and maximization problems.

The corresponding success probability is naturally given by,

$$P^s_{\text{ZE}} = \max_{\{\Pi_i\}} \left(1 - \sum_{i=1}^{n} \text{Tr}(\Pi_? \rho_i)\right),$$
$$\text{subject to} \quad \sum_{i=1}^{n} \Pi_i + \Pi_? = \mathbb{1}, \quad \Pi_? \geq 0,$$
$$\text{Tr}(\Pi_i \rho_i) = 0, \quad \Pi_i \geq 0 \quad \forall i.$$

This formulation is analogous to the ME protocol, with the crucial difference being the constraint $\text{Tr}(\Pi_i \rho_i) = 0$, enforcing unambiguous discrimination.

I.II GRAM MATRIX FORMULATION

Let $\mathcal{G} \in \mathbb{C}^{n\times n}$ be the *Gram matrix* of the system, defined as the $n \times n$ positive semidefinite hermitian matrix such that,

$$\mathcal{G} = \begin{pmatrix} \langle\psi_1|\psi_1\rangle & \langle\psi_1|\psi_2\rangle & \dots & \langle\psi_1|\psi_n\rangle \\ \langle\psi_2|\psi_1\rangle & \langle\psi_2|\psi_2\rangle & \dots & \langle\psi_2|\psi_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle\psi_n|\psi_1\rangle & \langle\psi_n|\psi_2\rangle & \dots & \langle\psi_n|\psi_n\rangle \end{pmatrix},$$

i.e., $\mathcal{G}_{i,j} = \langle\psi_i|\psi_j\rangle$. Since all states are normalized, we have,

$$\mathcal{G} = \begin{pmatrix} 1 & \langle\psi_1|\psi_2\rangle & \dots & \langle\psi_1|\psi_n\rangle \\ \langle\psi_2|\psi_1\rangle & 1 & \dots & \langle\psi_2|\psi_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle\psi_n|\psi_1\rangle & \langle\psi_n|\psi_2\rangle & \dots & 1 \end{pmatrix}.$$

Notice the Gram matrix is Hermitian by construction,

$$\mathcal{G}^*_{i,j} = (\langle\psi_i|\psi_j\rangle)^* = \langle\psi_j|\psi_i\rangle = \mathcal{G}_{j,i},$$

additionally is a positive semi-definite matrix since for an arbitrary state $|\Phi\rangle$ and a basis $\{|i\rangle\}_{i=1}^n$ we can prove that,

$$\begin{aligned}\langle\Phi|\mathcal{G}|\Phi\rangle &= \langle\Phi| \left(\sum_{i,j=1}^{n} \langle\psi_i|\psi_j\rangle |i\rangle \langle j|\right) |\Phi\rangle \\ &= \sum_{i,j=1}^{n} \langle\psi_i|\psi_j\rangle \langle\Phi|i\rangle \langle j|\Phi\rangle \\ &= \left|\left|\sum_{i=1}^{n} \langle i|\Phi\rangle |\psi_i\rangle\right|\right|^2 \\ &\geq 0.\end{aligned}$$

The Gram matrix allows us to reframe the exclusion problem in a more abstract and basis-independent form. Since $\mathcal{G}$ is hermitian and positive semi-definite, we can write,

$$\mathcal{G} = X^\dagger X,$$

for some matrix X whose columns are the pure states,

$$X = \begin{pmatrix} | & | & & | \\ |\psi_1\rangle & |\psi_2\rangle & \dots & |\psi_n\rangle \\ | & | & & | \end{pmatrix}.$$

Notice the diagonal elements of X are,

$$X_{i,i} = \langle\omega_i|\psi_i\rangle$$

For an arbitrary orthonormal basis $\{|\omega_i\rangle\}_{i=1}^n$. [6]

Let us consider an arbitrary orthonormal basis $\{|\omega_i\rangle\}_{i=1}^n$, and define the POVM elements as projectors $\Pi_i = |\omega_i\rangle \langle\omega_i|$. Then, the SDP formulation for the ensemble $\{(\rho_i, \eta_i)\}_{i=1}^n$ can be expressed as the following,

$$\begin{aligned}\text{Tr}(\Pi_i \rho_i) &= \text{Tr}\left(|\omega_i\rangle \langle\omega_i| \, |\psi_i\rangle \langle\psi_i|\right) \\ &= |\langle\omega_i|\psi_i\rangle|^2 \\ &= |X_{i,i}|^2.\end{aligned}$$

Therefore, we can reformulate the SDP for the ME protocol as,

$$P^e_{ME} = \min_X \sum_{i=1}^{n} \frac{|X_{i,i}|^2}{\eta_i},$$
$$\text{subject to} \quad X^\dagger X = \mathcal{G}, \quad X \geq 0.$$

[6] It is important to remark that fixing the basis $\{|\omega_i\rangle\}_{i=1}^n$ fixes the decomposition of $G = X^\dagger X$ and vice versa.

Similarly, the success probability becomes,

$$P^s_{ME} = \max_X \left(1 - \sum_{i=1}^{n} \frac{|X_{i,i}|^2}{\eta_i}\right),$$
$$\text{subject to} \quad X^\dagger X = \mathcal{G}, \quad X \geq 0.$$

This reformulation highlights that if two ensembles A and B share the same Gram matrix, then their exclusion problems, in both ME and ZE protocols, are equivalent. That is, the optimal success and error probabilities are identical in both systems. Hence, we focus on the Gram matrix to analyze exclusion problems, rather than relying on explicit state representations.

Moreover, we remark we are not especially interested in the arbitrary prior probabilities η_i scenario, since the result for equal prior probabilities $\eta_i = \frac{1}{n}$ can be easily extended to the previous case, with n as the number of states. This extension can be performed by considering the non-normalized states

$$|\tilde{\psi}_i\rangle = \frac{1}{\sqrt{\eta_i}} |\psi_i\rangle$$

and reformulate the problem in terms of this new states forgetting about the prior probabilities since they are encoded inside the states. Thus, for simplicity we will consider the equal probabilities case.

I.III GROUP GENERATED ENSEMBLES

Given a quantum state $|\psi\rangle$, which we refer to as the *seed state*, we define a *group generated ensemble* as the set of states obtained by applying a group of unitary transformations to $|\psi\rangle$. Specifically, if the ensemble consists of a total of n quantum states, then its elements are of the form,

$$U_i |\psi\rangle, \quad i \in \{1, \ldots, n\},$$

where the set of unitary matrices $\{U_i\}_{i=1}^n$ forms a finite group under standard matrix product. In terms of density matrices, the ensemble can equivalently be written as:

$$\rho_i = U_i \rho U_i^\dagger, \quad i \in \{1, \ldots, n\},$$

where $\rho = |\psi\rangle\langle\psi|$ is the density matrix corresponding to the seed state.

For instance, let $\mathcal{U}$ be a unitary operator such that $\mathcal{U}^n = \mathbb{1}$ (i.e., $\mathcal{U}$ generates a cyclic group of order n). Then, the set of states

$$\{\mathcal{U}^i |\psi\rangle\}_{i=0}^{n-1}$$

forms a group generated ensemble based on the cyclic group $\mathbb{Z}/n\mathbb{Z}$. This type of ensemble is of particular interest in our study and will be explored in more detail in subsequent section.

Example: The $\mathbb{Z}/n\mathbb{Z}$ group generated ensemble: Let $\mathcal{U} \in U(n)$ be an $n \times n$ unitary matrix satisfying $\mathcal{U}^n = \mathbb{1}$, and let $|\psi\rangle$ be the seed state. The Gram matrix $\mathcal{G}^{\mathbb{Z}/n\mathbb{Z}}$ elements associated with the ensemble $\{\mathcal{U}^i |\psi\rangle\}_{i=0}^{n-1}$ are nothing but,

$$\mathcal{G}^{\mathbb{Z}/n\mathbb{Z}}_{i,j} = \langle \mathcal{U}^i \psi | \mathcal{U}^j \psi \rangle = \langle \psi | \mathcal{U}^{j-i} | \psi \rangle = \langle \mathcal{U}^{j-i} \rangle_\psi,$$

where we use the shorthand notation

$$\langle \mathcal{U}^k \rangle_\psi := \langle \psi | \mathcal{U}^k | \psi \rangle.$$

Using this, the Gram matrix $\mathcal{G}^{\mathbb{Z}/n\mathbb{Z}}$ can be expressed as a circulant matrix,

$$\mathcal{G}^{\mathbb{Z}/n\mathbb{Z}} = \begin{pmatrix} 1 & \langle \mathcal{U} \rangle_\psi & \langle \mathcal{U}^2 \rangle_\psi & \cdots & \langle \mathcal{U}^{n-1} \rangle_\psi \\ \langle \mathcal{U}^{n-1} \rangle^*_\psi & 1 & \langle \mathcal{U} \rangle_\psi & \cdots & \langle \mathcal{U}^{n-2} \rangle_\psi \\ \langle \mathcal{U}^{n-2} \rangle^*_\psi & \langle \mathcal{U}^{n-1} \rangle^*_\psi & 1 & \cdots & \langle \mathcal{U}^{n-3} \rangle_\psi \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \langle \mathcal{U} \rangle^*_\psi & \langle \mathcal{U}^2 \rangle^*_\psi & \langle \mathcal{U}^3 \rangle^*_\psi & \cdots & 1 \end{pmatrix}.$$

Note the Gram matrix is Hermitian, as required, since,

$$\langle \mathcal{U}^{-j} \rangle_\psi = \langle \psi | U^{-j} | \psi \rangle = \left(\langle \psi | U^j | \psi \rangle\right)^* = \langle \mathcal{U}^j \rangle^*_\psi.$$

Additionally, by using the identity $\mathcal{U}^n = \mathbb{1}$, we can simplify terms such as,

$$\langle \mathcal{U}^{-n+i} \rangle_\psi = \langle \psi | \mathcal{U}^{-n+i} | \psi \rangle = \langle \psi | \mathcal{U}^i | \psi \rangle = \langle \mathcal{U}^i \rangle_\psi.$$

Therefore we may write,

$$\mathcal{G}^{\mathbb{Z}/n\mathbb{Z}_\psi} = \begin{pmatrix} 1 & \langle\mathcal{U}\rangle_\psi & \langle\mathcal{U}^2\rangle_\psi & \dots & \langle\mathcal{U}\rangle^*_\psi \\ \langle\mathcal{U}\rangle^*_\psi & 1 & \langle\mathcal{U}\rangle_\psi & \dots & \langle\mathcal{U}^2\rangle^*_\psi \\ \langle\mathcal{U}^2\rangle^*_\psi & \langle\mathcal{U}\rangle^*_\psi & 1 & \dots & \langle\mathcal{U}^3\rangle^*_\psi \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \langle\mathcal{U}\rangle_\psi & \langle\mathcal{U}^2\rangle_\psi & \langle\mathcal{U}^3\rangle_\psi & \dots & 1 \end{pmatrix}.$$

This confirms the circulant structure of $\mathcal{G}$, where each row is a cyclic permutation of the one above it. In other words the Gram matrix of $\mathbb{Z}/n\mathbb{Z}$ matrices are circulant matrixes. This result is especially useful, as they can be diagonalized by the discrete Fourier basis, which simplifies many tasks[5].

Note the Fourier basis for a $n \times n$ circulant matrix is conformed by the set of vectors $\{\omega_i\}_{i=1}^n$, such that,

$$\omega_i = \frac{1}{\sqrt{n}}(1, \gamma^i, \gamma^{2i}, ..., \gamma^{i(n-1)})^T,$$

where,

$$\gamma = e^{\frac{2\pi i}{n}}.$$

Moreover we can compute the Gram matrix for any group generated ensemble by generating the Cayley table[3], also known as the *multiplication table*, of the group. For instance, let us consider the smallest non-commutative group S_3 composed by the rotations and symmetries of the triangle. If we denote the identity as e, the 3 symmetries as p, q and s and a rotation as s, we know the Cayley table to be,

Table 1: Cayley table of the S_3 group.

S_3	e	s	s^2	p	q	r
e	e	s	s^2	p	q	r
s^2	s^2	e	s	r	p	q
s	s	s^2	e	q	r	p
p	p	r	q	e	s^2	s
q	q	p	r	s	e	s^2
r	r	q	p	s^2	s	e

where we have enforced the diagonal elements to be the identity. Subsequently if we identify S_3 as a group of unitary matrices [7] we immediatelly realize the Gram matrix of the S_3 group generated ensemble is the matrix corresponding to the expected values of the Cayley table respect a certain seed state $|\psi\rangle$. In other words the Gram matrix is nothing but,

$$\mathcal{G}^{S_3}_\psi = \begin{pmatrix} 1 & \langle s\rangle_\psi & \langle s^2\rangle_\psi & \langle p\rangle_\psi & \langle q\rangle_\psi & \langle r\rangle_\psi \\ \langle s^2\rangle_\psi & 1 & \langle s\rangle_\psi & \langle r\rangle_\psi & \langle p\rangle_\psi & \langle q\rangle_\psi \\ \langle s\rangle_\psi & \langle s^2\rangle_\psi & 1 & \langle q\rangle_\psi & \langle r\rangle_\psi & \langle p\rangle_\psi \\ \langle p\rangle_\psi & \langle r\rangle_\psi & \langle q\rangle_\psi & 1 & \langle s^2\rangle_\psi & \langle s\rangle_\psi \\ \langle q\rangle_\psi & \langle p\rangle_\psi & \langle r\rangle_\psi & \langle s\rangle_\psi & 1 & \langle s^2\rangle_\psi \\ \langle r\rangle_\psi & \langle q\rangle_\psi & \langle p\rangle_\psi & \langle s^2\rangle_\psi & \langle s\rangle_\psi & 1 \end{pmatrix}.$$

Notice that, $\langle e\rangle_\psi = 1$ since e is the neutral element of the matrix product operation, i.e. $e = \mathbb{1}$. Moreover in this particular example we can observe since $\mathcal{G}^{S_3}$ is hermitian we know that,

$$\begin{cases} \langle p\rangle_\psi = & \langle p\rangle^*_\psi \\ \langle q\rangle_\psi = & \langle q\rangle^*_\psi \\ \langle r\rangle_\psi = & \langle r\rangle^*_\psi \end{cases} \quad \forall\,|\psi\rangle \in \mathcal{H}$$

$$\Updownarrow$$

$$\langle p\rangle_\psi, \langle q\rangle_\psi, \langle r\rangle_\psi \in \mathbb{R} \quad \forall\,|\psi\rangle \in \mathcal{H}.$$

Therefore the unitary matrices corresponding to the triangle symmetries p, q and r are hermitian. It is immediate this procedure can be applied for any group G, whic implies that computing the Cayley table is equivalent to computin the Gram matrix of the group generated ensemble.

Additionally, we will denote the cardinality of a finite group G[8], as $|G|$ which implies that for our case of interest of the prior probabilities scenario we may write $\eta_i = \frac{1}{|G|}$.

[7] we think of each element of the group as an unitary matrix and the operation of the group as the matrix product.

[8] The cardinality of a group is the same as the number elements of the group.

I.IV DUAL FORMULATION OF THE PROBLEM

Sometimes it is usefull to consider the dual version of each *sdp* problem. The dual version of the exclusion task for the $\left\{\left(\rho_i, \frac{1}{n}\right)\right\}_{i=1}^{n}$ ensemble for the error probability with the Minimum Error (ME) protocol is,

$$\begin{aligned}\tilde{P}^e_{ME} = &\max_{\Gamma} \operatorname{Tr}\Gamma \\ &\text{subject to } \frac{\rho_i}{n} - \Gamma \geq 0 \quad \forall i \in \{1, ..., n\} \\ &\Gamma^\dagger = \Gamma,\end{aligned}$$

where $\tilde{P}$ stands for the dual version of the problem. Naturally, for the success probability the problem reads,

$$\begin{aligned}\tilde{P}^s_{ME} = &\min_{\Gamma} (1 - \operatorname{Tr}\Gamma) \\ &\text{subject to } \frac{\rho_i}{n} - \Gamma \geq 0 \quad \forall i \in \{1, ..., n\} \\ &\Gamma^\dagger = \Gamma.\end{aligned}$$

Add the dual version for the zero error protocol.

The dual version results specially usefull since given an POVM anzatz if the probabilities of the primal and dual problems coincide, i.e. $P = \tilde{P}$ we know we have found the optimal measurement.

I.V PREVIOUS RESULTS

Enormous advances have been made in the exclusion task for group generated ensembles. The publication *Quantum state exclusion for group-generated ensembles of pure states*[6] yields a result of the actual exact success and/or error probabilities for both ME and ZE protocols for group generated ensembles. The result reads, let $\mathcal{G}^G$ the Gram matrix of the group generated ensemble $\left\{\left(\rho_i, \frac{1}{|G|}\right)\right\}_{i=1}^{|G|}$ corresponding to a finite group G, where $|G|$ denotes the number of the group's elements, let also $\{\lambda_i\}_{i=1}^{|G|}$ be the set of eigenvalues of the Gram matrix. Additionally let us consider the set of eigenvalues $\{\lambda_i\}_{i=1}^{|G|}$ to be an ordered group, such that,

$$i \leq j \quad \forall i, j \in \{1, ..., |G|\} \Leftrightarrow \lambda_i \geq \lambda_j \forall i, j \in \{1, ..., |G|\},$$

or equivalently, the set is ordered from the lowest to highest eigenvalue. Hence, the exclusion probabilities for the minimum error (ME) protocol are,

$$P^e_{ME} = \max\left\{0, \left(\frac{\sqrt{\lambda_{|G|}} - \sum_{i<|G|}\sqrt{\lambda_i}}{|G|}\right)^2\right\}$$

$$P^s_{ME} = \min\left\{1, 1 - \left(\frac{\sqrt{\lambda_{|G|}} - \sum_{i<|G|}\sqrt{\lambda_i}}{|G|}\right)^2\right\}.$$

Additionally, the results for the zero error (ZE) protocol are,

$$P^e_{ZE} = \max\left\{0, \frac{\sum_{i=1}^{|G|}\sqrt{\lambda_i}\left(\sqrt{\lambda_{|G|}} - \sum_{j<|G|}\sqrt{\lambda_j}\right)}{|G|}\right\}$$

$$P^s_{ZE} = \min\left\{1, 1 - \frac{\sum_{i=1}^{|G|}\sqrt{\lambda_i}\left(\sqrt{\lambda_{|G|}} - \sum_{j<|G|}\sqrt{\lambda_j}\right)}{|G|}\right\}.$$

For us is crucial to remark one of the results' traitmarks: the probabilities are independent of the group. In other words, given two group generated ensembles A and B for 2 differnt groups G_A and G_b ($G_A \neq G_B$) with the same cardinality, i.e. $|G_A| = |G_B|$, we know that if the respective Gram matrices $\mathcal{G}^{G_A}$ and $\mathcal{G}^{G_b}$ have the same eigenvalues, then the exclusion probability for both protocols ME and ZE is the same. This matter is one of the cornersotnes of this project study.

Additionally we do also notice the exstence of some conditions where the exclusion can be performed with no error what so ever. This can be done if,

$$\lambda_{|G|} \leq \left(\sum_{i=1}^{|G|}\sqrt{\lambda_i}\right)^2. \tag{1}$$

The regime corresponding to this conditions is denoted as the *perfect exclusion zone*. In this

project we will prove this results to be a lower bound for the exclusion success probability for the non group generated ensembles. However since the lower bound for the *perfect exclusion zone* it is equal to 1[9], then a perfect exclusion can be performed for a non group generated ensemble if it fulfils the perfect exclusion condition Eq. (1). Subsequently, the perfect exclusion regime exists for a general ensemble and at least is comphended by those ensemble that fulfil Eq. (1).

I.VI LIMIT CASE SCENARIOS

Let us study the Gram matrix of the limit ensemble of n states, all of them beeing the same state (the state is repeated in the ensemble n times)[10], reads,

$$\mathcal{G}^{\text{limit}} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Therefore the eigenvalues of the Gram matrix are,

$$\begin{aligned} \lambda_n &= n \\ \lambda_{n-1} &= 0 \\ &\vdots \\ \lambda_1 &= 0 \end{aligned}$$

which clearly fulfil Eq.(1) i.e. we are in the non-perfect exclusion regime. As a matter of fact, we can think of this set of states as a gorup generated ensemble by the trivial gorup[11]. Hence the probability of successfull exclusion and mistakenly exclusion in both protocols is,

$$\begin{aligned} P^e_{ME} = P^e_{ZE} &= \frac{1}{n} \\ P^s_{ME} = P^s_{ZE} &= \frac{n-1}{n}. \end{aligned}$$

This result is the expected, if there is no physical way to distinguish between states the selection of the excluded state must be taken randomly with homogenious probability. Notice this idea is also extensible to QSD.

This result is result is the limit plausible scenario, therefore all the computed success probabilities for eighter QSE or QSD for any protocol must be greater to $\frac{n-1}{n}$ (i.e. the error probabilities must be lower than $\frac{1}{n}$).

The counterpart scenario is the ensemble comformed by a set of orthogonal states $\{\rho_i\}_{i=i}^n$. In this conditions the Gram matrix of the ensemble is the identity,

$$\mathcal{G} = \mathbb{1}.$$

In this conditions, both QSE and QSD are trivial since the set of states comformes a basis. In particular, in the space generated by the linear span of states we know that,

$$\sum_{i=1}^{n} \rho_i = \mathbb{1},$$

i.e. the set of states is a POVM set itself. The outcome of this measurement will lead up to distinguishing the target state with no error, then QSE and QSD can be performed perfectly.

I.VII ENSEMBLES WITH A PRIME NUMBER OF ELEMENTS

As we have discussed, analytical solutions have been found for the exclusion task in ME and ZE protocols. This solutions are independent from

[9] The exclusion can always be performed successfully in this context.

[10] This case might seem paradogic since there is no way to distinguish the same thing. Nevertheless, we present it as a limit case scenario.

[11] The trivial group is the one entirely comformed by the identity.

the intrinsc group of the ensemble and only depend on the eigenvalues of the Gram matrix.

Hence if the Gram matrix for a general ensemble decomposes as,

$$\mathcal{G} = UDU^\dagger \tag{2}$$

where U stands for an unitary matrix, and D for a the eigenvalues diagonal matrix. Then, we are left with two options:

- We are in the perfect exclusion regime, i.e. the eigenvalues composing the D matrix fulfil Eq.(1).
- We are not in the perfect exclusion regime, i.e. the eigenvalues composing the D matrix do not fulfil Eq.(1).

If we are in the perfect exclusion scenario we know we can find a set of POVMs that the outcome of the measurement allows us to exclude one hypothesis from the ensemble with no mistake.

Otherwise we are in the non-perfect exclusion zone. In this regime the solution for group generated ensembles are lower bounds of the successfull exclusion probability in both protocols (i.e. upperbound of the error probability of exclusion).

Let us consider the 4 states ensemble case. In this scenario we know the result to be an exact solution for the groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$[12]. Then we know there are two unitary matrices $U_{\mathbb{Z}/4\mathbb{Z}}$ and $U_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}}$ (up to a flip of columns and/or rows) where the solution is exact. Since $U(n)$ is a compact set, supposing contonuity on the solution and given a matix norm and its induced topology, there exists some neighbourhoods for each matrix $\mathcal{B}(U_{\mathbb{Z}/4\mathbb{Z}})$ and $B(U_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}})$ arbitrarily small such that the success probabilities approaches the analytical solution as much as desired. However the existence of two unitary matrices that lead up to the same solution complicates the numerical analysis since the neighbourhoods can intersect. As a matter of fact, given an ensemble of n quantum states, there exist as many unitary matrices as number of groups of n elements where the solution is exact.

Nevertheless, if we consider the case of a prime number of states $n = p$ the task simplifies drastically since we know there only exists one group of p elements and it is $\mathbb{Z}/p\mathbb{Z}$.

This result is inmediate from Lagrange's theoreme. The theoreme garanties the order of any element of the group[13] must divide the order of the group. Since p is prime the order of any element is either 1 or p, but if the order of an element is 1 this emplies it is the identity. Then every element different from the identity must of order p for any group of p elements i.e. the group is cyclic. Since the group must be a cyclic gorup of p elements we are left with only one option, the group must be $\mathbb{Z}/p\mathbb{Z}$ up to ismorfism.

Therefore, for ensembles with a prime number of quantum states there only exists one unitary matrix U[14] that leads up to a Gram matrix where the given analytical results are exact. This ensembles are particularly interesting and will be discussed in the Results and Discussion sestion Add reference.

II METHODOLOGY

All the code is stored in the GitHub repository [12]. Here you can find extra documentation on the functionality of each script and class.

[12] This are the only two groups of 4 elements.

[13] The order of an element τ that belongs to a group G is the minimum natural number m such that $\tau^m = e$ where e stands for the neutral element of the group

[14] Additionally we know the columns of this matrix are the elements of the Fourier's basis from the discussion in section *Group Generated Ensembles* (I.III) in the examble of $\mathbb{Z}/n\mathbb{Z}$ ensembles

II.I SDP SOLVER

The workflow of the study has been the creation of the Mosek solver [10] to numerically solve the SDP using the PICOS python package[11].

II.II GENERATION OF RANDOM GRAM MATRICES

The Random Number Generator (RNG) provides a set of n random numbers $\{\lambda_i\}_{i=1}^n$ that are normalized such that their sum is equal to n,

$$\sum_{i=1}^{n} \lambda_i = n,$$

this will be the eigenvalues of the gram matrix comforming the diagonal matrix D. Then we generate a matrix U such that $\mathcal{G} = UDU^\dagger$. At this stage we choose between a group generated enseble or a generic one.

The generic ensemble is generated by a random unitary matrix U such that distribution the unique measure is invariant under group multiplication, known as Haar measure[7]. This is acomplished by using the Francesco Mezzadri's algorithm presented in [9]. This way we ensure the $U(n)$ set is covered homogeniously by our random unitary matrices.

For a $\mathbb{Z}/n\mathbb{Z}$ group generated ensemble the unitary matix U is the one that encodes the vectors of the Fourier basis as columns as discussed in section (I.III) Group Generated Esnemble.

Other gorus are obviated since we can always set n to be a prime number and impossing $\mathbb{Z}/n\mathbb{Z}$ to be the only possibile group generated ensemble.

III RESULTS AND DISCUSSION

Let us analyze the case of a $\mathbb{Z}/3\mathbb{Z}$ ensemble. We know the Gram matrix takes the form of,

$$\mathcal{G}^{\mathbb{Z}/3\mathbb{Z}} = \begin{pmatrix} 1 & c & c^* \\ c^* & 1 & c \\ c & c^* & 1 \end{pmatrix}$$

with $c \in \mathbb{C}$. Notice that respect the previous notation, we are writting $c = \langle U \rangle_\psi$, where c and c^* denotes the overlap between different states. Therefore we notice if we write $c = |c|e^{i\phi}$, and since we are analyzing an overlap of normalized states,

$$|c| \in [0, 1] \quad \text{and} \quad \theta \in [0, 2\pi]$$

we have two Degrees of Freedom (DoF).

Since 3 is a prime number the only group of 3 elements is $\mathbb{Z}/3\mathbb{Z}$ as discussed in the section *Ensembles with a prime number of elements* (I.VII), then the Gram matrix can be diagonalized as,

$$\mathcal{G}^{\mathbb{Z}/3\mathbb{Z}} = U_{\mathbb{Z}/3\mathbb{Z}} D U^\dagger_{\mathbb{Z}/3\mathbb{Z}},$$

where, $U_{\mathbb{Z}/3\mathbb{Z}}$ stands for the unitary matrix with the Fourier basis as columns. Then the eigenvalues of the matrix are $\{\lambda_1, \lambda_2, \lambda_3\}$ where $\lambda_1 \leq \lambda_2 \leq \lambda_3$. Notice that,

$$3 = \operatorname{Tr} \mathcal{G}^{\mathbb{Z}/3\mathbb{Z}} = \operatorname{Tr} D = \sum_{i=1}^{3} \lambda_i$$

which constraints the system two only 2 DoF, as expected concording with the DoF of the previous picture of the Gram matrix, where we were looking directly at the elements instead of the eigenvalues. Additionally, we know that,

$$\mathcal{G}^{\mathbb{Z}/3\mathbb{Z}} \geq 0 \Rightarrow \lambda_i \geq 0 \quad \forall i \in \{1, 2, 3\}.$$

Which implies the eigenvalues are constrained to be number between 0 and 3.[15] Then,

$$\lambda_3 \in [0, 3] \quad \lambda_2 \in [0, \lambda_3] \quad \lambda_1 = 3 - \lambda_3 - \lambda_2$$

[15] For the general case scenario the eigenvalues are numbers between 0 and n. Also notice, this holds true even in the non-group generated ensembles.

[16] The plots consists in 2 parameters plus the success/error exclusion probability for the respective protocol.

This case is particularly interesting since it is the only ensemble that allows us to represent all the dependencies in each DoF and visually analyze the hole ensemble[16]. For scenarios with more quantum states it is impossible to represent the hole picture, and for the two quantum states case we have already discussed its equivalentcy to the discrimination task in QSD.

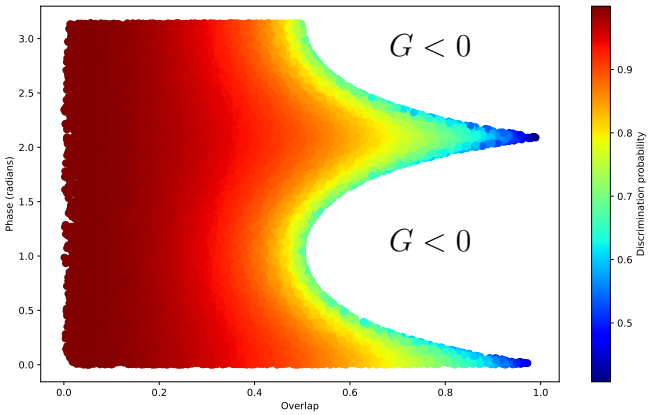

Figure 1: Representation of the probability of successfull discrimination for a $\mathbb{Z}/3\mathbb{Z}$ group generated ensemble with Minimum Error (ME) protocol.

III.I COMPARATION QSD VS. QSE AND ME VS. ZE

First of all, let us present some results for the Quantum State Discrimination (QSD) task, in order to motivate the problem and discuss the advantages and disadvantages respect its counterpart, the QSD, the main object of study for this project. In Figure (III.I) we can find a heatmap of the average successfull discrimination probability for the minimum error ME protocol for a $\mathbb{Z}/3\mathbb{Z}$ group generated ensemble. The probabilities are represented in terms of the modolus of the overlap (x-axis) and the phase (y-axis) that completely determine the Gram matrix of the ensemble, as discussed previousl. Additionally we present the case for equal prior probabilities since the results can be easily generaliced to arbitrary prior probabilities as discussed in section (I.II) Gram Matrix Formulation. The prior probabilities scenario will the standard procedure for all the project.

The colorless region comprehends the overlap values c (i.e. $c = overlap \cdot e^{iphase}$) such that $\mathcal{G}^{\mathbb{Z}/3\mathbb{Z}}$ has negative eigenvalues values. The matrix generated in this region are no Gram matrices *per se* since positive semi-definiteness is required as discussed in section (I.II) Gram Matrix Formulation.

In this conditions we know the known as Square Root Measurement (SRM) [17] to be optimal, i.e. the result of the SDP is the same as the SRM. This measurement is the one obtained by the decomposition of the Gram matrix the square root of an hermitian matrix S as the following,

$$\mathcal{G} = S^\dagger S = S^2.$$

this measurement is the estandard in QSD for the ME protocol [4].

As expected no ensemble leads to probabilities under $\frac{1}{3}$ acording to the previous discussion in section (I.VI) Limit Case Scenarios.

Moreover we observe when the modolus of the overlap tends to 0 the success probability tends to 1. Naturally the observation is consistent since this limit is the one obtained with ensembles of orthogonal states and we obtain

[17] a.k.a. pretty good measurement.

the expected result discussed in section (I.VI) Limit Case Scenarios.

Additionally we can consider the same condition but using the Zero Error (ZE), the result are shown in Figure (III.I).

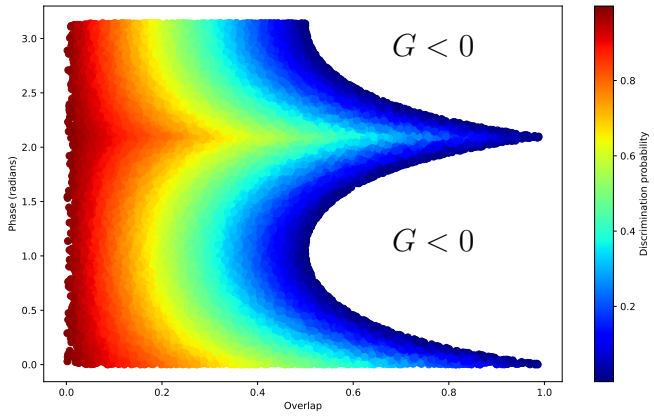

Figure 2: Representation of the probability of successfull discrimination for a $\mathbb{Z}/3\mathbb{Z}$ group generated ensemble with Zero Error (ZE) protocol.

We observe both limit scenarios are preserved in this protocol too as expected. Additionally, notice the successfull exclusion probabilities are lower than the ones obtained with the Minimum Error (ME) protocol. This observation is explained by the SDP construction of the problem in section (I.I) Formulation Of The Problem. Notice both probabilities are computed in a completely symmetric way,

$$P^s_{ME} \sim P^s_{ZE} \sim 1 - \sum_{POVM} \mathrm{Tr}\left(\Pi_i \rho_i\right).$$

Nevertheless, in the ZE case we enforce $\mathrm{Tr}\left(\Pi_i \rho_i\right) = 0$ for all the POVMs except one. Thus, the system is more constrained in the ZE protocol, then the optimization of the probability cannot be performed up to the same point as in the ME protocol. Hence, the probabilities for

REFERENCES

[1] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, January 2015.

[2] Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim, and Christopher Perry. Conclusive exclusion of quantum states. *Phys. Rev. A*, 89:022336, Feb 2014.

[3] Prof. Cayley. On the theory of groups. *American Journal of Mathematics*, 11(2):139–157, 1889.

[4] Nicola Dalla Pozza and Gianfranco Pierobon. Optimality of square-root measurements in quantum state discrimination. *Physical Review A*, 91(4), April 2015.

[5] P.J. Davis. *Circulant Matrices*. Monographs and textbooks in pure and applied mathematics. Wiley, 1979.

[6] Arnau Diebra, Santiago Llorens, Emili Bagan, Gael Sentís, and Ramon Muñoz-Tapia. Quantum state exclusion for group-generated ensembles of pure states, 2025.

[7] Alfréd Haar. Der Maßbegriff in der Theorie der kontinuierlichen Gruppen. *Annals of Mathematics*, 34(1):147–169, 1933.

[8] Carl W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.

[9] Francesco Mezzadri. How to generate random matrices from the classical compact groups, 2007.

[10] MOSEK ApS. *Semidefinite Optimization*, 2024. Version 11.0.

[11] Guillaume Sagnol and Maximilian Stahlberg. PICOS: A Python interface

to conic optimization solvers. *Journal of Open Source Software*, 7(70):3915, February 2022.

[12] SirSergi0. Qsex_tfg-temporal_name-. `https://github.com/SirSergi0/QSEx_TFG-Temporal_Name-`, 2025.

LIST OF ABBREVIATIONS

DoF	Degrees of Freedom.
ME	Minimum Error.
POVM	Positive Operator-Valued Measure.
QSD	Quantum State Discrimination.
QSE	Quantum State Exclusion.
RNG	Random Number Generator.
SDP	Semidefinite Program.
SRM	Square Root Measurement.
ZE	Zero Error.