



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 [5], 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 [6], QSE offers a complementary framework with distinct advantages.

Although the tasks of exclusion and discrimination coincide for ensembles containing

only two states¹, 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[3].

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-

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

²Also known as *unambiguous exclusion*.

act solutions for exclusion tasks in group generated ensembles [5], 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 one³.

I.1 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 matrix⁴, 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 present 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

$$P_{\text{ME}}^e = \min_{\{\Pi_i\}} \sum_{i=1}^n \text{Tr}(\Pi_i \rho_i),$$

subject to $\sum_{i=1}^n \Pi_i = \mathbb{1}, \quad \Pi_i \geq 0 \quad \forall i \in \{1, \dots, n\}.$

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,

$$P_{\text{ME}}^s = \max_{\{\Pi_i\}} \left(1 - \sum_{i=1}^n \text{Tr}(\Pi_i \rho_i) \right),$$

subject to $\sum_{i=1}^n \Pi_i = \mathbb{1}, \quad \Pi_i \geq 0 \quad \forall i \in \{1, \dots, n\}.$

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,

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

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:

$$P_{\text{ZE}}^e = \min_{\{\Pi_i\}} \sum_{i=1}^n \text{Tr}(\Pi_? \rho_i),$$

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

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

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

⁵Note 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,

$$P_{ZE}^s = \max_{\{\Pi_i\}} \left(1 - \sum_{i=1}^n \text{Tr}(\Pi_i \rho_i) \right),$$

subject to $\sum_{i=1}^n \Pi_i + \Pi_? = \mathbb{1}, \quad \Pi_? \geq 0,$

$$\text{Tr}(\Pi_i \rho_i) = 0, \quad \Pi_i \geq 0 \quad \forall i.$$

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 this matrix is Hermitian by construction,

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

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,

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

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

$$P_{ME}^e = \min_X \sum_{i=1}^n \frac{|X_{i,i}|^2}{\eta_i},$$

subject to $X^\dagger X = \mathcal{G}, \quad X \geq 0.$

Similarly, the success probability becomes,

$$P_{ME}^s = \max_X \left(1 - \sum_{i=1}^n \frac{|X_{i,i}|^2}{\eta_i} \right),$$

subject to $X^\dagger X = \mathcal{G}, \quad X \geq 0.$

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.

⁶It 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.

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,

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

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:

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

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,

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

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,

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

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

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

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[4].

Moreover we can compute the Gram matrix of a group generated ensemble by generating the Cayley table, 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 immediately 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,

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

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,

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

$$\Downarrow$$

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

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 , which implies that computing the Cayley table is equivalent to computing 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 $\eta_i = \frac{1}{|G|}$.

I.IV DUAL FORMULATION OF THE PROBLEM

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

$$\tilde{P}_{ME}^e = \max_{\Gamma} \text{Tr } \Gamma$$

$$\text{subject to } \frac{\rho_i}{n} - \Gamma \geq 0 \quad \forall i \in \{1, \dots, n\}$$

$$\Gamma^\dagger = \Gamma,$$

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

$$\tilde{P}_{ME}^s = \min_{\Gamma} (1 - \text{Tr } \Gamma)$$

$$\text{subject to } \frac{\rho_i}{n} - \Gamma \geq 0 \quad \forall i \in \{1, \dots, n\}$$

$$\Gamma^\dagger = \Gamma.$$

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

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

Add the dual version for the zero error protocol.

The dual version results specially usefull since given an POVM anatz 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*[5] 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,

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

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

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

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

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

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

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

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,

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

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 1⁹, 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 compended by those ensemble that fulfil Eq. (1).

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

I.VI 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. These solutions are independent from the intrinsic 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,

$$\mathcal{G} = UDU^\dagger \quad (2)$$

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 successful 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ¹⁰. 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 Supposing continuity on the solution and given a matrix norm and its induced topology, there exists some neighbourhoods for each matrix $\mathcal{B}(U_{\mathbb{Z}/4\mathbb{Z}})$ and $\mathcal{B}(U_{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}})$ 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. 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 immediate from Lagrange's theorem. The theorem guarantees the order of any element of the group¹¹ 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 implies it is the identity. Then every element different from the identity must be of order p for any group of p elements i.e. the group is cyclic. Since the group must be a cyclic group of p elements we are left with only one option, the group must be $\mathbb{Z}/p\mathbb{Z}$ up to isomorphism.

Therefore, for ensembles with a prime number of quantum states there only exists one unitary matrix U ¹² that leads up to a Gram matrix where the given analytical results are exact.

II METHODOLOGY

All the code is stored in the GitHub repository [9]. The workflow of the study has been the creation of the Mosek solver [7] to numer-

¹⁰This are the only two groups of 4 elements.

¹¹The 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

¹²Additionally 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 example of $\mathbb{Z}/n\mathbb{Z}$ ensembles

ically solve the SDP using the PICOS python package[8].

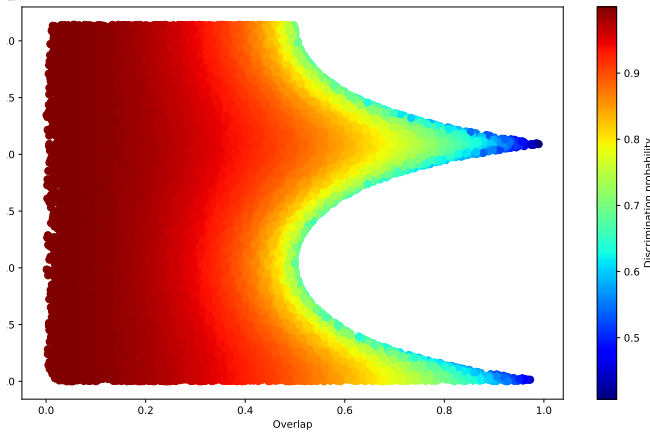
III RESULTS AND DISCUSSION

For us, is particularly interesting the case of a $\mathbb{Z}/3\mathbb{Z}$ ensemble since we know the Gram matrix to take the form of,

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

with $c \in \mathbb{C}$.

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



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] Nicola Dalla Pozza and Gianfranco Pierobon. Optimality of square-root measurements in quantum state discrimination. *Physical Review A*, 91(4), April 2015.
- [4] P.J. Davis. *Circulant Matrices*. Monographs and textbooks in pure and applied mathematics. Wiley, 1979.
- [5] Arnau Diebra, Santiago Llorens, Emili Bagan, Gael Sentís, and Ramon Muñoz-Tapia. Quantum state exclusion for group-generated ensembles of pure states, 2025.
- [6] Carl W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.
- [7] MOSEK ApS. *Semidefinite Optimization*, 2024. Version 11.0.
- [8] Guillaume Sagnol and Maximilian Stahlberg. PICOS: A Python interface to conic optimization solvers. *Journal of Open Source Software*, 7(70):3915, February 2022.
- [9] SirSergi0. Qsex_tfg-temporal_name-. https://github.com/SirSergi0/QSEx_TFG-Temporal_Name-, 2025.

LIST OF ABBREVIATIONS

| | |
|-------------|-----------------------------------|
| ME | Minimum Error. |
| POVM | Positive Operator-Valued Measure. |
| QSD | Quantum State Discrimination. |
| QSE | Quantum State Exclusion. |
| SDP | Semidefinite Program. |
| ZE | Zero Error. |