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 [9], 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,

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

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 given by,

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

that is, $\mathcal{G}_{i,j} = \langle\psi_i|\psi_j\rangle$. Since all states are normalized, the diagonal elements are equal to 1, and the Gram matrix becomes,

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

By construction, the Gram matrix is Hermitian,

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

Additionally, $\mathcal{G}$ is positive semidefinite. To see this, consider an arbitrary state $|\Phi\rangle$ and an orthonormal basis $\{|i\rangle\}_{i=1}^{n}$, then,

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

The Gram matrix allows us to reformulate the exclusion problem in a more abstract, basis-independent manner. Since $\mathcal{G}$ is Hermitian and positive semidefinite, it can be factorized as,

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

for some matrix X, whose columns are the pure states,

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

Let us fix an arbitrary orthonormal basis $\{|\omega_i\rangle\}_{i=1}^{n}$. Then, the diagonal entries of X in this basis are given by,

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

[6]We define the POVM elements as projectors $\Pi_i = |\omega_i\rangle\langle\omega_i|$. Then, for the ensemble $\{(\rho_i, \eta_i)\}_{i=1}^{n}$, the corresponding semidefinite program (SDP) constraints become,

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

Thus, we can reformulate the SDP for the minimum-error (ME) protocol as,

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

[6]Note that fixing the basis $\{|\omega_i\rangle\}_{i=1}^{n}$ uniquely determines the decomposition $\mathcal{G} = X^{\dagger}X$, 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 reveals that if two ensembles A and B share the same Gram matrix, then their exclusion problems under both the ME and ZE protocols are equivalent. That is, their optimal success and error probabilities coincide. Consequently, we focus on the Gram matrix to study exclusion problems rather than the explicit state representations.

Furthermore, we note that the case of arbitrary prior probabilities η_i can be reduced to the equal prior case $\eta_i = \frac{1}{n}$ by defining non-normalized states,

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

and reformulating the problem in terms of these states. The prior probabilities are then absorbed into the state norm. Therefore, without loss of generality, in this project we will assume equal prior probabilities.

I.III GROUP GENERATED ENSEMBLES

Given a quantum state $|\psi\rangle$, referred 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 n quantum states, 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 multiplication. 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 a 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

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

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 that the Gram matrix is Hermitian, as expected, since

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

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

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

Thus, we may write,

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

This shows the circulant structure of $\mathcal{G}$, where each row is a cyclic permutation of the previous one. In other words, the Gram matrices of $\mathbb{Z}/n\mathbb{Z}$-generated ensembles are circulant matrices. This structure is particularly useful, as circulant matrices can be diagonalized by the discrete Fourier basis, greatly simplifying many computations [5].

The Fourier basis for an $n \times n$ circulant matrix consists of the set of vectors $\{\omega_i\}_{i=1}^{n}$, where

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

and

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

Moreover, we can compute the Gram matrix for any group-generated ensemble by using the Cayley table [3], also known as the *multiplication table*, of the group. For example, consider the smallest non-commutative group, S_3, consisting of the symmetries and rotations of an equilateral triangle. Denoting the identity as e, the rotations elements as s, s^2 (one being the result of 2 times the other) and the symmetries p, q, and r, the Cayley table is,

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

We now identify S_3 as a group of unitary matrices[7]. It follows that the Gram matrix of the S_3 group-generated ensemble is the matrix of expected values of the Cayley table entries with respect to the seed state $|\psi\rangle$. That is,

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

Note that $\langle e\rangle_\psi = 1$ since $e = \mathbb{1}$. Moreover, since $\mathcal{G}^{S_3}$ is Hermitian, we conclude:

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

which implies the unitary matrices corresponding to the triangle symmetries p, q, and r are Hermitian. As a matter of fact we know the eigenvalues of this matrices can only be ± 1 and at least one of them must be -1.[8] This procedure generalizes to any finite group G, showing that computing the Cayley table is equivalent to computing the Gram matrix of the corresponding group-generated ensemble.

Finally, we denote the cardinality of a finite group G (i.e., the number of its elements) as $|G|$. In scenarios with uniform prior probabilities, this implies,

$$\eta_i = \frac{1}{|G|} \quad \forall i \in \{1, ..., n\}.$$

I.IV DUAL FORMULATION OF THE PROBLEM

It is often useful to consider the *dual* version of a SDP problem, as it provides both conceptual insights and practical advantages for verifying optimality.

Consider the ensemble $\left\{\left(\rho_i, \frac{1}{n}\right)\right\}_{i=1}^{n}$, where each state ρ_i appears with uniform prior probability $1/n$. The dual SDP corresponding to the Minimum Error (ME) exclusion protocol,

[7] We treat each group element as a unitary matrix, and the group operation as matrix multiplication.

[8] Otherwise, they would be the identity and we know them to be different by construction.

when expressed in terms of the error probability, is given by,

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

where $\tilde{P}$ denotes the dual version of the problem.

Similarly, the dual SDP for the success probability in the same protocol reads:

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

Add the dual version for the zero error protocol.

In the case of the zero-error exclusion protocol, the dual SDP formulation becomes

One of the primary uses of the dual formulation is in establishing optimality. If a POVM ansatz yields equal objective values for both the primal and dual problems, i.e., $P = \tilde{P}$, then strong duality holds and the measurement is guaranteed to be optimal.

This duality principle not only provides a tool for verification but also suggests constructive approaches to discovering optimal measurements, especially in structured ensembles such as those generated by group actions.

I.V PREVIOUS RESULTS

Significant progress has been made in the study of the state exclusion task for group-generated ensembles. In particular, the work *Quantum State Exclusion for Group-Generated Ensembles of Pure States*[6] presents exact analytical expressions for the success and error probabilities under both the Minimum Error ME and Zero Error ZE exclusion protocols.

Let $\mathcal{G}^G$ denote the Gram matrix of a group-generated ensemble $\left\{\left(\rho_i, \frac{1}{|G|}\right)\right\}_{i=1}^{|G|}$, where G is a finite group of size $|G|$, and let $\{\lambda_i\}_{i=1}^{|G|}$ be the set of eigenvalues of $\mathcal{G}^G$. Assume the eigenvalues are ordered increasingly,

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

i.e., λ_1 is the smallest and $\lambda_{|G|}$ the largest eigenvalue.

The exclusion probabilities under the Minimum Error protocol are given by,

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

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

For the Zero Error protocol, the corresponding expressions arem

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

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

A key feature of these results is their independence from the specific group generating the ensemble. That is, for any two group-generated ensembles A and B corresponding to groups G_A and G_B (with $G_A \neq G_B$ but $|G_A| = |G_B|$), if their respective Gram matrices $\mathcal{G}^{G_A}$ and $\mathcal{G}^{G_B}$ share the same eigenvalues, then the exclusion probabilities for both ME and ZE protocols are identical. This group-independence property is a cornerstone of the present study.

Another important outcome from [6] is the identification of conditions under which perfect exclusion is achievable, i.e., the exclusion can be carried out with zero error. This occurs if the eigenvalues satisfy the inequality,

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

We refer to the regime satisfying this inequality as the *perfect exclusion zone*. Within this regime, the success probability of the exclusion task reaches one, implying that exclusion can be performed perfectly.

In this project, we will extend this result by demonstrating that the perfect exclusion condition Eq. (1) provides a lower bound for the success probability of exclusion even for non-group-generated ensembles. Since this bound equals 1, it implies that any ensemble whether or not group-generated that satisfies condition Eq. (1) can achieve perfect exclusion. Thus, the perfect exclusion zone is not exclusive to group-generated ensembles, but also includes all ensembles that fulfill the given condition.

I.VI LIMIT CASE SCENARIOS

Let us study the Gram matrix of a limit ensemble composed of n identical quantum states (i.e., the same state is repeated n times in the ensemble).[9] The Gram matrix reads:

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

The eigenvalues of this matrix are:

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

Clearly, this set of eigenvalues does not satisfy Eq. (1), i.e., we are in the non-perfect exclusion regime. In fact, we can interpret this ensemble as a group-generated ensemble from the *trivial group*,[10] which generates no variation.

Thus, the success and error probabilities for both the ME protocol is,

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

The intuition behind this result is clear. If there is no physical way to distinguish between states, the exclusion must be made randomly, with uniform probability. This observation also extends naturally to QSD.

Since this is a limiting case scenario, the success probability for either QSE or QSD must be strictly greater than $\frac{n-1}{n}$ (i.e., the error probability must be less than $\frac{1}{n}$). Notice this result holds only for the ME protocol. Otherwise, since the exclusion cannot be accomplished without ambiguity, the successfull exclusion probability for the ZE protocol is 0 for either QSE or QSD (i.e., the error exclusion probability is 1),

$$\begin{aligned} P^e_{ZE} &= 1, \\ P^s_{ZE} &= 0. \end{aligned}$$

The opposite limiting case is an ensemble of n orthogonal quantum states $\{\rho_i\}_{i=1}^n$. In this case, the Gram matrix becomes the identity,

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

Under these conditions, both QSE and QSD are trivial, as the states form an orthonormal basis. In particular, in the space spanned by these states, we have,

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

which means that the set $\{\rho_i\}$ is itself a POVM. The measurement corresponding to this POVM allows perfect identification (or exclusion), hence both QSE and QSD can be performed without error.

[9] This case may appear paradoxical, since there is no way to distinguish between identical states. Nevertheless, we present it as a limiting scenario.

[10] The trivial group is the group consisting solely of the neutral/identity element.

I.VII ENSEMBLES WITH A PRIME NUMBER OF ELEMENTS

As previously discussed, analytical solutions have been found for the exclusion task under both the ME and ZE protocols. These solutions depend solely on the eigenvalues of the Gram matrix and are independent of the specific group structure generating the ensemble.

Let the Gram matrix of an ensemble decompose as,

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

where U is a unitary matrix and D is the diagonal matrix of eigenvalues. We then encounter two possibilities,

- The eigenvalues satisfy Eq. (1), placing the ensemble in the *perfect exclusion* regime.
- The eigenvalues do not satisfy Eq. (1), placing the ensemble in the *non-perfect exclusion* regime.

In the perfect exclusion regime, the existence of a POVM, such that the measurement outcome allows exclusion of a hypothesis without error, is guaranteed.

In the non-perfect exclusion regime, the analytical results for group-generated ensembles provide lower bounds on the success probabilities (and upper bounds on the error probabilities) for general ensembles.

Consider, for example, the case of an ensemble of 4 quantum states. There are exactly two groups of four elements: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.[11] This implies that there exist two specific unitary matrices, $U_{\mathbb{Z}/4\mathbb{Z}}$ and $U_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}}$ (up to permutation of rows and columns), for which the analytical solution holds exactly.

Since $U(n)$ is compact, and assuming continuity of the exclusion probabilities with respect to U under a given matrix norm, for each of these unitary matrices there exist arbitrarily small neighborhoods $\mathcal{B}(U_{\mathbb{Z}/4\mathbb{Z}})$ and $\mathcal{B}(U_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}})$ such that the exclusion probabilities within these neighborhoods approximate the analytical result as closely as desired. However, the existence of multiple such matrices (and intersecting neighborhoods) can complicate numerical optimization and analysis.

In contrast, it is usefull to consider the case where the ensemble contains a prime number p of states. In this scenario, the situation simplifies considerably, since there exists only one group (up to isomorphism) of order p, namely $\mathbb{Z}/p\mathbb{Z}$.

This result follows immediately from Lagrange's theorem. The theorem guarantees that the order of any element in a finite group[12] must divide the order of the group. Since p is a prime number, the only positive integers dividing p are either 1 or p itself. Therefore, the order of any group element must be either 1 or p. An element of order 1 must be the identity, so every non-identity element in the group must have order p. This implies that all non-identity elements generate the entire group, i.e., the group is cyclic. As a result, any group of prime order p is necessarily cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Consequently, for an ensemble of p quantum states, there exists a unique unitary matrix $U_{\mathbb{Z}/p\mathbb{Z}}$ (up to reordering) that diagonalizes the Gram matrix in such a way that the analytical results are exact. [13]

Ensembles of prime cardinality are thus of particular interest and will be further explored in the Results and Discussion section. Add reference to Results section

[11] These are the only non-isomorphic groups of order 4.

[12] The order of an element τ in a group G is the smallest positive integer m such that $\tau^m = e$, where e denotes the identity/neutral element of the group.

[13] Moreover, the columns of this matrix correspond to the elements of the Fourier basis, as discussed in Section I.III, particularly in the example involving $\mathbb{Z}/n\mathbb{Z}$.

II METHODOLOGY

All the code used in this project is hosted in the GitHub repository [13], where additional documentation is available detailing the functionality and structure of each script and class involved in the implementation.

II.I SDP SOLVER

The core of the numerical analysis is the implementation of a Semi-Definite Programming (SDP) solver based on the MOSEK optimization suite [11], interfaced through the Python-based PICOS optimization library [12].

II.II GENERATION OF RANDOM GRAM MATRICES

To analyze both group-generated and generic quantum state ensembles, we developed a method for generating random Gram matrices with prescribed spectral properties.

A Numpy Random Number Generator (RNG)[8] produces a set of n non-negative real numbers $\{\lambda_i\}_{i=1}^n$ that are normalized to satisfy the trace condition,

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

These values are used as the eigenvalues of the Gram matrix, forming the diagonal matrix $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$.

Next, we generate a unitary matrix U and construct the Gram matrix as,

$$\mathcal{G} = UDU^\dagger.$$

At this point, we choose whether the ensemble is to be group-generated or generic.

For a generic ensemble, the unitary matrix U is drawn randomly according to the Haar measure [7], which defines the unique uniform probability measure on the unitary group $U(n)$ that is invariant under group multiplication. To ensure this uniformity, we use the algorithm introduced by Francesco Mezzadri in [10], which provides an efficient and accurate way of sampling unitary matrices while uniformly covering $U(n)$.

In the case of a group-generated ensemble, we restrict ourselves to ensembles generated by the cyclic group $\mathbb{Z}/n\mathbb{Z}$. The corresponding unitary matrix U is constructed such that its columns are the vectors of the discrete Fourier basis, as discussed in Section I.III (*Group-Generated Ensemble*).

Other groups are omitted in our analysis since we can always choose n to be a prime number, in which case the only group of order n (up to isomorphism) is the cyclic group $\mathbb{Z}/n\mathbb{Z}$. This significantly simplifies the group structure and ensures that the only group-generated ensemble under consideration corresponds to a well-defined, unique construction.

This methodology provides a flexible yet rigorous foundation for both exploring generic quantum ensembles and benchmarking them against analytically tractable group-generated cases.

III RESULTS AND DISCUSSION

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

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

with $c \in \mathbb{C}$. Note that, with respect to previous notation, we write $c = \langle U \rangle_\psi$, where c and c^* denote the overlap between different states. We can parametrize c as $c = |c|e^{i\phi}$, and since we are analyzing normalized states,

$$|c| \in [0, 1], \quad \phi \in [0, 2\pi]$$

we observe two Degrees of Freedom (DoF).

Since 3 is a prime number, the only group of order 3 is $\mathbb{Z}/3\mathbb{Z}$, as discussed in Section (I.VII).

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 $U_{\mathbb{Z}/3\mathbb{Z}}$ is the unitary matrix with Fourier basis vectors as columns. The eigenvalues of the matrix are denoted as $\{\lambda_1, \lambda_2, \lambda_3\}$ with $\lambda_1 \leq \lambda_2 \leq \lambda_3$. Since,

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

we again find only two DoFs, consistent with our earlier parameterization. Furthermore, since $\mathcal{G}^{\mathbb{Z}/3\mathbb{Z}} \geq 0$, we have,

$$\lambda_i \geq 0 \quad \forall i \in \{1, 2, 3\},$$

implying the eigenvalues must lie in the interval $[0, 3]$.[14] Therefore,

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

This scenario is particularly interesting as it is the only ensemble with a small enough dimension to fully visualize all parameter dependencies and study the ensemble structure.[15] Higher-dimensional cases are too complex for full representation, while two-state cases reduce to standard quantum state discrimination (QSD) as previously discussed.

III.I COMPARISON QSD VS. QSE, AND ME VS. ZE

We first present results for the Quantum State Discrimination (QSD) task to motivate the problem and highlight contrasts with the Quantum State Exclusion (QSE) task, which is the focus of this study.

Figure (III.I) shows a heatmap of the average successful discrimination probability under the Minimum Error (ME) protocol for a $\mathbb{Z}/3\mathbb{Z}$ group-generated ensemble. Probabilities are shown as functions of the modulus (x-axis) and phase (y-axis) of the overlap c, which fully determine the Gram matrix. We assume equal prior probabilities, as generalization to arbitrary priors is discussed in Section (I.II). Note, equal priors are presuposed throughout this work unless stated otherwise.

The colorless regions correspond to parameters where $\mathcal{G}^{\mathbb{Z}/3\mathbb{Z}}$ is not positive semi-definite, and leading up yo non-valid Gram matrices, since positive semi-definition is inherent to a Gram matrix.

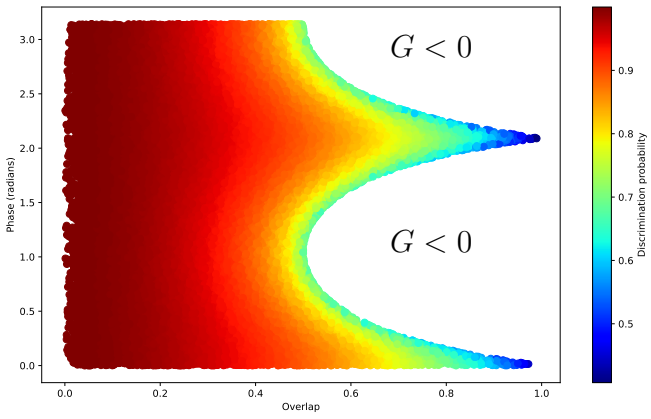

Figure 1: Heatmap of the success probability for minimum error (ME) quantum state discrimination for a $\mathbb{Z}/3\mathbb{Z}$ group-generated ensemble.

In these conditions, the Square Root Measurement (SRM)[16] is optimal, i.e. the result of the SDP matches the one obtained from the SRM. In particular, the SRM is obtained from the square root decomposition of the Gram matrix,

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

and is the standard in QSD under the ME protocol [4].

[14] In general, eigenvalues lie in $[0, n]$ for an n-dimensional ensemble, even for non-group-generated ensembles.
[15] Visualizations include two parameters along with the success/exclusion probability of the respective protocol.
[16] Also known as the Pretty Good Measurement.

As expected, no ensemble yields a success probability below 1/3, consistent with the discussion in Section (I.VI). Moreover, as the modulus of the overlap approaches zero, the success probability approaches one, corresponding to orthogonal states, again matching expectations.

Figure (III.I) shows results for the Zero Error (ZE) protocol under the same conditions.

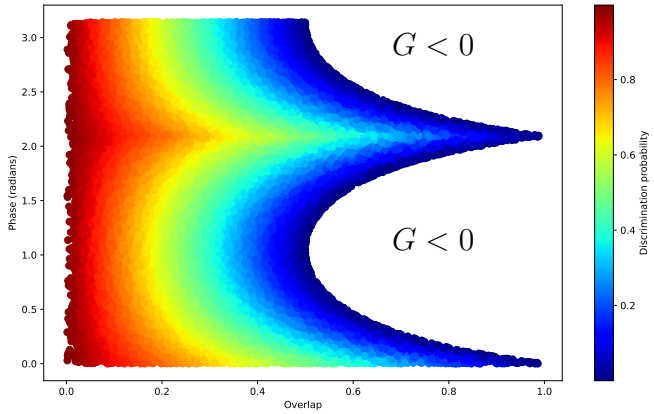

Figure 2: Heatmap of the success probability for zero-error (ZE) quantum state discrimination for a $\mathbb{Z}/3\mathbb{Z}$ group-generated ensemble.

Both limiting behaviors remain valid. However, the ZE success probabilities are lower than those of the ME protocol. This is explained by the stricter constraints imposed in the ZE scenario, where $\mathrm{Tr}(\Pi_i \rho_i) = 0$ is enforced for all POVM elements except one. 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 success probabilities for ME are greater than the ones obtained with the ZE protocol.

Figure (III.I) compares the performance of the ME, ZE, and SRM protocols.

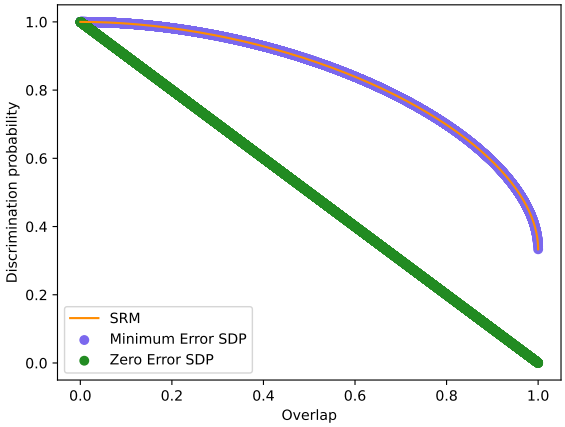

Figure 3: Comparison of successful discrimination probabilities for ME, ZE, and SRM protocols in a $\mathbb{Z}/3\mathbb{Z}$ ensemble.

As expected, perfect discrimination is only achieved when the overlap is zero (orthogonal states), and the SRM success probability matches the one obtained from the numerical SDP. This highlights the motivation behind the study of QSE, which allows for perfect exclusion in cases where discrimination is impossible.

Figure (III.I) presents the ME protocol results for the QSE task, analogous to Figure (III.I).

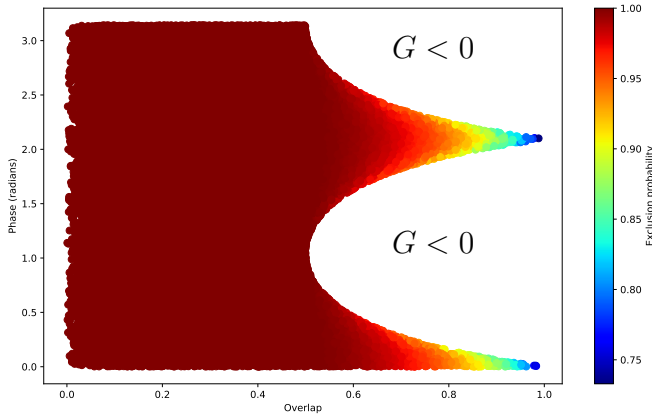

Figure 4: Heatmap of the success probability for minimum error (ME) quantum state exclusion in a $\mathbb{Z}/3\mathbb{Z}$ ensemble.

The ZE protocol for QSE is shown in Figure (III.I).

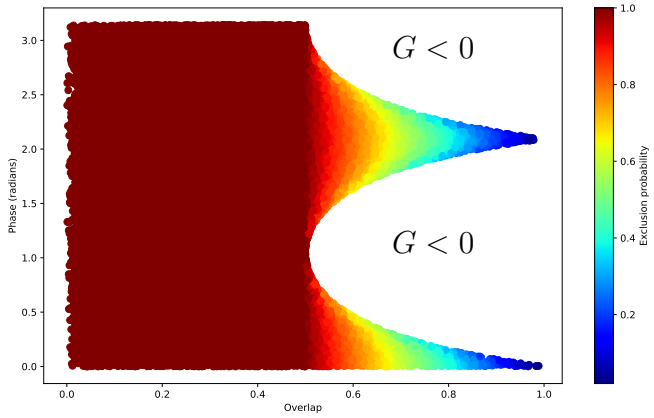

Figure 5: Heatmap of the success probability for zero-error (ZE) quantum state exclusion in a $\mathbb{Z}/3\mathbb{Z}$ ensemble.

Again, the ZE protocol yields lower probabilities due to its constraints and the limit case scenarios match with the previos discussion in Section (I.VI). However, crucially, perfect exclusion is possible even when perfect discrimination is not. Figure (III.I) highlights the regions where perfect exclusion is achieved, even outside the perfect discrimination regime.

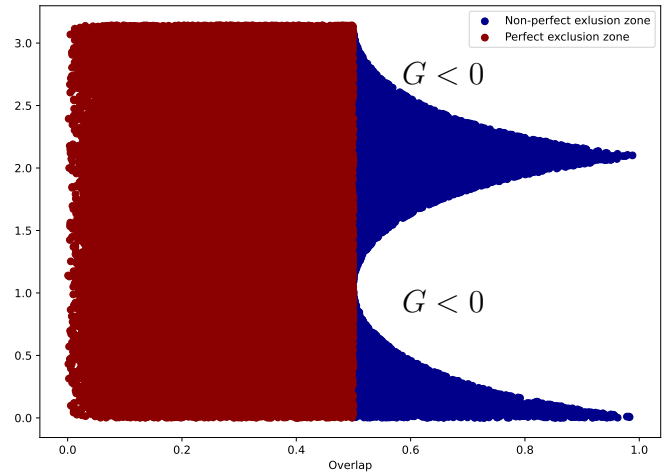

Figure 6: Perfect exclusion zone for a $\mathbb{Z}/3\mathbb{Z}$ ensemble under the minimum error (ME) protocol.

This property of QSE is a major motivation for its study. For example, in a regime where perfect exclusion is possible, having access to multiple copies of a target state enables hybrid exclusion-discrimination protocols that can outperform purely discriminative strategies. Even partial information, such as the exclusion of a single quantum state, has value in certain quantum information theories. These features make QSE a fertile ground for further theoretical and applied research.

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] Charles R Harris, K Jarrod Millman, Stéfan J van der Walt, Ralf Gommers, Pauli Virtanen, David Cournapeau, Eric Wieser, Julian Taylor, Sebastian Berg, Nathaniel J Smith, et al. Array programming with NumPy. *Nature*, 585(7825):357–362, 2020.

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

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

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

[12] Guillaume Sagnol and Maximilian Stahlberg. PICOS: A Python interface to conic optimization solvers. *Journal of Open Source Software*, 7(70):3915, February 2022.

[13] 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.