Quantum state exclusion for group-generated ensembles of pure states

A. Diebra[1], S. Llorens[1], E. Bagan[1], G. Sentís[1,2], and R. Muñoz-Tapia[1,3]

[1]*Física Teòrica: Informació i Fenòmens Quàntics,*
Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
[2]*Ideaded, Carrer de la Tecnologia, 35, 08840 Viladecans, Barcelona, Spain and*
[3]*H. H. Wills Physics Laboratory, University of Bristol,*
Tyndall Avenue, Bristol, BS8 1TL, United Kingdom

Quantum state exclusion is the task of determining which states from a given set a system was not prepared in. We provide a complete solution to optimal quantum state exclusion for arbitrary sets of pure states generated by finite groups, establishing necessary and sufficient conditions for perfect (zero-error conclusive) exclusion. When perfect exclusion is impossible, we introduce two natural extensions: minimum-error and unambiguous exclusion. For both, we derive the optimal protocols and present analytical expressions for the corresponding failure probabilities and measurements, offering a new perspective on how quantum states encode information.

Introduction. In both scientific and everyday contexts, the ability to confidently exclude what did not occur, based on partial information, is often more efficient than attempting to determine what actually did. This principle is widely applied in classical scenarios, where exclusion serves as a powerful tool for narrowing possibilities and guiding decision-making. For instance, in medical diagnostics, ruling out potential diseases is crucial for refining treatment options, even when the exact disease remains unidentified [1]. Similarly, in engineering system testing, excluding certain failure modes is often more advantageous than trying to pinpoint the exact faulty process [2]. Additionally, in network security, excluding potential vulnerabilities is usually more efficient than attempting to track down the precise nature of a threat [3].

The very same principle extends into the quantum realm through a task named quantum state exclusion (QSE) [4]. Given a quantum system prepared in an unknown state drawn from a predetermined set, the goal is to exclude that the state of the given system is a particular one from that set. This task, also known as quantum antidistinguishability [5], is particularly relevant in the context of quantum state assignments, where the compatibility of different state assignments must be assessed [6, 7]. It also plays a crucial role in the debate surrounding the physical reality of quantum systems [8].

In contrast to the traditional approach of quantum state discrimination [9–11], where the goal is to identify the exact state of a system, QSE focuses on ruling out certain states, offering a different perspective on the information that can be extracted from quantum systems. QSE plays a role in quantum resource theories: any quantum resource can be quantitatively linked to the relative advantage it offers in a state exclusion task compared to free resources [12, 13]. QSE has also been shown to provide an operational interpretation of the Choi rank of a quantum channel [14]. This rank, among other properties, places bounds on the minimum number of Kraus operators required to decompose a channel. The role of contextuality in QSE have been discussed in [15]. Conversely, non-contextual inequalities have been derived from QSE [16], with implications for communication complexity [17, 18]. More recently, Chernoff error exponents for QSE have been calculated in [19]. Additionally, in quantum state discrimination with multiple copies, it has been shown that the optimal procedure may, in some cases, involve excluding specific states [20]. QSE has also been demonstrated experimentally with single photons in [21].

Just as in quantum state discrimination, finding optimal protocols for QSE in a fully general setting remains a challenging problem. Beyond the binary case (also known as hypothesis testing), multi-hypothesis quantum state discrimination has only been solved when a certain degree of symmetry can be invoked [22–31]. This same symmetry principle has been applied in the context of QSE, where it has been used to derive tight bounds for circulant sets of pure quantum states [32].

As far as we know, all existing literature on QSE has focused on perfect exclusion —that is, protocols that enable the error-free conclusive exclusion of one or more states. However, perfect QSE is only possible within a limited region of the parameter space defining the set of states (or hypotheses), with necessary and/or sufficient conditions delineating this region already established. Moreover, many existing results are non-constructive: while they confirm the existence of an error-free exclusion measurement, they do not provide its explicit form [32].

In this letter, we present a complete analytical solution to optimal QSE for group-generated sets of pure states, revealing new facets of the problem. Specifically, we derive the minimum error probability of exclusion for any finite group and across the entire parameter space, both within and outside the perfect exclusion region, provid-

ing a specific measurement that achieves this minimum. We also prove that this optimal measurement can always be taken to be sharp. Our approach relies on the Gram matrix [33] formalism, exploits the duality properties of semidefinite programming [34, 35] and makes extensive use of group representation theory [36–38].

We also investigate the zero-error (unambiguous) approach [39], which allows for inconclusive answers while forbidding errors, even outside the perfect QSE region. In this context, we provide an analytical expression for the probability of obtaining such inconclusive answers for any group-generated set of pure states.

We show that the minimum probabilities of error and inconclusive answers are both determined by the eigenvalues of the Gram matrix. The same formulas seem to provide a useful upper bound for these probabilities even in general, non-symmetric cases. This is in agreement with intuition, as symmetry inherently increases indistinguishability and reduces the ability to exclude specific objects, making discrimination and exclusion more challenging.

This letter is organized as follows. We first present the formulation and structure of the problem, followed by our main results and an outline of the proof of a central lemma, which establishes that the optimal measurements can be constructed from specific rank-one operators. We conclude with a summary of our findings.

Formulation and structure of the problem. This letter addresses the task of excluding any single preparation from a given ensemble $\mathcal{E} = \{\eta_i, \rho_i\}_i$ of possible states, where $\rho_i = |\psi_i\rangle\langle\psi_i|$ occurs with prior probability η_i. The exclusion is performed through a quantum measurement, represented by a positive operator-valued measure (POVM) $\{\Pi_j\}_j$ on the Hilbert space $\mathcal{H}$ of the states, with each outcome j indicating that the state ρ_j is ruled out. For certain ensembles of states perfect exclusion is possible, namely, there exists a POVM such that $\text{Tr}(\Pi_i \rho_i) = 0$ for all i. However, as explained in the introduction, we also consider ensembles for which this does not necessarily hold. In analogy with state discrimination, we examine two natural extensions of perfect QSE: minimum-error and unambiguous exclusion.

Minimum-error exclusion aims to minimize the average probability of incorrect exclusion, denoted by P, over the set of all possible POVMs. This optimization can be formulated as a semidefinite program (SDP):

$$P^{\min} = \min_{\{\Pi_i\}} \sum_i \eta_i \, \text{Tr}(\Pi_i \rho_i),$$
$$\text{subject to } \sum_i \Pi_i = \mathbb{1}, \quad \Pi_i \geq 0 \text{ for all } i. \quad (1)$$

Alternatively, unambiguous exclusion imposes the strict constraint that no errors occur, typically requiring

an additional POVM element, Π_Q, associated with an inconclusive outcome. When this outcome is obtained, no definitive decision can be made, so the optimal protocol seeks to minimize its average probability Q. This too can be formulated as an SDP:

$$Q^{\min} = \min_{\{\Pi_i\}} \sum_i \eta_i \, \text{Tr}(\Pi_Q \, \rho_i),$$
$$\text{subject to } \Pi_Q + \sum_i \Pi_i = \mathbb{1}, \quad \Pi_Q \geq 0,$$
$$\Pi_i \geq 0, \quad \text{Tr}(\Pi_i \rho_i) = 0 \text{ for all } i. \quad (2)$$

Perfect exclusion corresponds to $P^{\min} = Q^{\min} = 0$. We refer to P and Q as failure probabilities.

In this work, we focus on quantum ensembles that are group-generated, $\mathcal{E} = \{|\psi_g\rangle = U_g|\psi\rangle \,|\, g \in \mathcal{G}\}$, where each state in the ensemble is obtained by applying a finite-dimensional unitary (linear or projective) representation, $U : g \mapsto U_g \in \mathcal{U}(\mathcal{H})$, of a finite group $\mathcal{G}$ to a seed state $|\psi\rangle$. Furthermore, we assume that all states are equally probable, i.e., $\eta_g = 1/|\mathcal{G}|$, for all $g \in \mathcal{G}$, where $|\mathcal{G}|$ is the order of $\mathcal{G}$.

Any such representation can be decomposed into a direct sum of irreducible representations (irreps for short), $U_g = \bigoplus_\mu U_g^\mu \otimes \mathbb{1}_{m_\mu}$, where $\mathbb{1}_d$ stands for the d-dimensional identity operator, μ labels the distinct irreps, and m_μ denotes their multiplicity. Accordingly, the Hilbert space $\mathcal{H}$ breaks into orthogonal subspaces [36–38] as $\mathcal{H} = \bigoplus_\mu \mathcal{H}_\mu \otimes \mathbb{C}^{m_\mu}$, where $\mathcal{H}_\mu$ carries the irrep μ, while $\mathbb{C}^{m_\mu}$ denotes the multiplicity space, over which U acts trivially. This decomposition allows us to write the seed state as $|\psi\rangle = 1/\sqrt{|\mathcal{G}|} \sum_\mu \sqrt{d_\mu} |\psi_\mu\rangle$, where d_μ is the dimension of the irrep μ and $|\psi_\mu\rangle \in \mathcal{H}_\mu \otimes \mathbb{C}^{m_\mu}$ are non-normalized bipartite states. The factors $1/\sqrt{|\mathcal{G}|}$ and $\sqrt{d_\mu}$ have been introduced for later convenience. The states $|\psi_\mu\rangle$ can be written in a Schmidt form:

$$|\psi_\mu\rangle = \sum_{k=1}^{r_\mu} \sqrt{\alpha_k^\mu} \, |v_k^\mu\rangle |u_k^\mu\rangle, \quad (3)$$

where $r_\mu = \min\{d_\mu, m_\mu\}$, $\alpha_k^\mu \geq 0$, for all μ and k, and both $\{|v_k^\mu\rangle\}_{k=1}^{d_\mu}$ and $\{|u_k^\mu\rangle\}_{k=1}^{m_\mu}$ are orthonormal bases of $\mathcal{H}_\mu$ and $\mathbb{C}^{m_\mu}$ respectively. Using the Great Orthogonality Theorem [36–38, 40], one can show that the operator $\Omega = \sum_g U_g|\psi\rangle\langle\psi|U_g^\dagger$, which represents the (unnormalized) density matrix of the ensemble (ensemble operator for short), is diagonal in this basis:

$$\Omega = \bigoplus_\mu \mathbb{1}_{d_\mu} \otimes \sum_{k=1}^{r_\mu} \alpha_k^\mu |u_k^\mu\rangle\langle u_k^\mu|. \quad (4)$$

As in the case of quantum state discrimination, all the information required for exclusion is encoded in the Gram matrix G of the ensemble [40], whose entries are

the overlaps between the states: $G_{g,h} = \langle\psi_g|\psi_h\rangle$, with $g,h \in \mathcal{G}$. The symmetry of the problem —specifically, the representation U that generates the ensemble— determines the structure of the Gram matrix, which belongs to the algebra of the (right-)regular representation of the group [36]. Explicit examples are provided in the supplemental material [40].

For any ensemble $\mathcal{E}$, the columns of the square root of the Gram matrix, $S = \sqrt{G}$, define an associated ensemble $\mathcal{E}_S$ from a $|\mathcal{G}|$-dimensional Hilbert space $\mathcal{H}_S$, which shares the same Gram matrix, G. If $\mathcal{E}$ is generated by a group $\mathcal{G}$, so is $\mathcal{E}_S$, with their states belonging to the (left-)regular representation of $\mathcal{G}$ [40].

The Gram matrix G and the ensemble operator Ω are closely related. Specifically, among the eigenvalues of G —denoted as λ_a, with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{|\mathcal{G}|}$ — those that are strictly positive coincide with the non-zero eigenvalues of Ω [40], which can be read off from Eq. (4).

Results. For ensembles of pure states generated by a finite group $\mathcal{G}$, the minimum error probability for excluding a state, as defined in Eq. (1), is determined by the eigenvalues $\{\lambda_a\}_{a=1}^{|\mathcal{G}|}$ of the Gram matrix:

$$P^{\min} = \left[\frac{1}{|\mathcal{G}|}\max\left(0, \sqrt{\lambda_1} - \sum_{a>1}\sqrt{\lambda_a}\right)\right]^2. \quad (5)$$

Similarly, for unambiguous QSE, the probability of the inconclusive outcome is given by

$$Q^{\min} = \frac{\mathrm{Tr}(\sqrt{G})}{|\mathcal{G}|}\max\left(0, \sqrt{\lambda_1} - \sum_{a>1}\sqrt{\lambda_a}\right). \quad (6)$$

These results establish that the condition

$$\sqrt{\lambda_1} \leq \sum_{a>1}\sqrt{\lambda_a} \quad (7)$$

is both necessary and sufficient for perfect QSE to be possible in group-generated ensembles. As a special case, Theorem 5.2 in [32] —which applies to circulant matrices— follows directly from this result, now extended to arbitrary finite groups.

Eqs. (5) and (6) follow from the lemma below. This lemma also provides the optimal measurements for the two approaches considered in this letter. Both of them are represented by rank-1 (group-)covariant POVMs.

Note that if the largest eigenvalue λ_1 has multiplicity greater than one, condition (7) is automatically satisfied, ensuring perfect QSE. This occurs whenever the largest Schmidt coefficient (or eigenvalue of Ω), α_k^μ, corresponds to an irrep μ of dimension greater than one.

The results above extend to unitary projective representations, where $U_g U_h = e^{i\theta(g,h)}U_{gh}$ for all $g,h \in \mathcal{G}$.

Such representations are not merely of academic interest: spin-$\frac{1}{2}$ particles transform under a projective representation of the 3D rotation group. For instance, the ensemble $\{|\boldsymbol{n}_\alpha\rangle\}_\alpha$, where α indexes the vertices of a regular tetrahedron in the Bloch sphere, can be viewed as generated by the Pauli matrices $\{\mathbb{1}_2, \sigma_x, \sigma_y, \sigma_z\}$, which form a nontrivial projective representation of $\mathbb{Z}_2\times\mathbb{Z}_2$ [40]. These states also define a symmetric informationally complete POVM (SIC-POVM) [41] for qubits.

When the phases $\theta(g,h)$ are non-trivial, i.e., they cannot be absorbed into the matrices $\{U_g\}_{g\in\mathcal{G}}$ themselves, the corresponding irreps necessarily have dimension two or higher [36–38, 42]. Thus, by the previous argument, perfect exclusion is always possible for sets generated by such non-trivial projective representations [40].

Lemma 1. *The optimal POVM for QSE can always be chosen to be covariant with a rank-1 seed. Specifically, it takes the form $\{\Pi_g = U_g|\omega\rangle\langle\omega|U_g^\dagger \mid g \in \mathcal{G}\}$ for minimum-error QSE, with the additional POVM element $\Pi_Q = \mathbb{1} - \sum_{g\in\mathcal{G}}\Pi_g$ for unambiguous QSE. Moreover, if $\sqrt{\lambda_1} > \sum_{a>1}\sqrt{\lambda_a}$, the optimal seed state is*

$$|\omega\rangle = \frac{1}{\sqrt{|\mathcal{G}|}}\left(\gamma|v_1^1\rangle|u_1^1\rangle - \sum_{\mu\neq 1}\sqrt{d_\mu}\sum_{k=1}^{r_\mu}|v_k^\mu\rangle|u_k^\mu\rangle\right), \quad (8)$$

where the eigenstate $|v_1^1\rangle|u_1^1\rangle$ corresponds to the largest eigenvalue of Ω in Eq. (4), with $\gamma = 1$ for minimum-error QSE, and

$$\gamma = \sum_{\mu\neq 1}\sum_{k=1}^{r_\mu}d_\mu\frac{\sqrt{\alpha_k^\mu}}{\sqrt{\alpha_1^1}} \quad (9)$$

for unambiguous QSE.

Proof. Consider a POVM of the specified form for some $|\omega\rangle \in \mathcal{H}$. It must hold that $\Phi := \sum_{g\in\mathcal{G}}U_g|\omega\rangle\langle\omega|U_g^\dagger = \mathbb{1}_\psi$, where $\mathbb{1}_\psi$ is the projector onto the span of the orbit of the seed state $|\psi\rangle$. Therefore, applying (the analog of) Eqs. (3) and (4) to Φ, we see that the state $|\omega\rangle$ must be

$$|\omega\rangle = \frac{1}{\sqrt{|\mathcal{G}|}}\sum_\mu\sqrt{d_\mu}\sum_{j=1}^{r_\mu}|e_j^\mu\rangle|f_j^\mu\rangle, \quad (10)$$

where $\{|e_j^\mu\rangle\}_{j=1}^{d_\mu}$ and $\{|f_j^\mu\rangle\}_{j=1}^{m_\mu}$ are orthonormal bases of $\mathcal{H}_\mu$ and $\mathbb{C}^{m_\mu}$, respectively, with the extra condition that $\mathrm{span}\{|f_j^\mu\rangle\}_j = \mathrm{span}\{|u_k^\mu\rangle\}_k$ for all μ. The average error probability becomes

$$P = |\langle\omega|\psi\rangle|^2 =$$
$$\frac{1}{|\mathcal{G}|^2}\left|\sum_\mu d_\mu\sum_{j,k=1}^{r_\mu}\sqrt{\alpha_j^\mu}\,|\langle v_j^\mu|e_k^\mu\rangle\langle u_j^\mu|f_k^\mu\rangle|\,e^{i\theta_{j,k}^\mu}\right|^2, \quad (11)$$

where we have written the overlaps in polar form.

To minimize the error probability, we can replace the original ensemble $\mathcal{E}$ by its associated ensemble $\mathcal{E}_S$ and, hence, without loss of generality, take U to be the regular representation. In the decomposition of this representation, all the irreps of $\mathcal{G}$ appear, each with multiplicity equal to its dimension [36–38], i.e., $d_\mu = m_\mu = r_\mu$. Thus, we can always choose mutually unbiased bases $\{|e_j^\mu\rangle\}_j$ and $\{|v_j^\mu\rangle\}_j$, as well as $\{|f_j^\mu\rangle\}_j$ and $\{|u_j^\mu\rangle\}_j$ [43], for the spaces $\mathcal{H}_\mu$ and $\mathbb{C}^{m_\mu}$, respectively, such that

$$|\langle e_j^\mu|v_k^\mu\rangle| = |\langle f_j^\mu|u_k^\mu\rangle| = \frac{1}{\sqrt{d_\mu}}, \quad 1 \le j,k \le d_\mu. \quad (12)$$

With this choice, the average error probability can be expressed as

$$P = \frac{1}{|\mathcal{G}|^2}\left| \sum_\mu \sum_{j,k=1}^{d_\mu} \sqrt{\alpha_j^\mu} e^{i\theta_{k,j}^\mu} \right|^2. \quad (13)$$

Since each eigenvalue α_k^μ appears in Ω with multiplicity d_μ —see Eq. (4), we can rewrite the error probability as

$$P = \frac{1}{|\mathcal{G}|^2}\left| \sum_{a=1}^{|\mathcal{G}|} \sqrt{\lambda_a} e^{i\theta_a} \right|^2. \quad (14)$$

If $\sqrt{\lambda_1} \le \sum_{a>1} \sqrt{\lambda_a}$, the phases in Eq. (14) can be chosen such that the error probability vanishes. This implies that $\text{Tr}(\Pi_g \rho_g) = 0$ for all $g \in \mathcal{G}$, and therefore, the probability of obtaining an inconclusive outcome also vanishes. This completes the proof of Lemma 1 when the above condition holds. Note that the optimal seed is infinitely degenerate, as there are infinitely many phase choices that yield $P^{\min} = Q^{\min} = 0$, corresponding to perfect exclusion.

In contrast, when $\sqrt{\lambda_1} > \sum_{a>1} \sqrt{\lambda_a}$, the error probability P in Eq. (14) does not vanish. Its minimum occurs when $\theta_a = \theta_1 + \pi$ for all $a > 1$. In this case, we adopt the ansatz from Eq. (10), with $|e_j^\mu\rangle \propto |u_j^\mu\rangle$ and $|f_j^\mu\rangle \propto |v_j^\mu\rangle$, replacing the unbiased bases used previously. Under this choice of bases and phases, Eq. (10) gives Eq. (8) with $\gamma = 1$, and Eq. (11) simplifies to the right-hand side of Eq. (5), denoted as P^{primal}.

The optimality of this ansatz follows from the dual formulation of Eq. (1),

$$P^{\text{dual}} = \max_{Y \ge 0} \text{Tr}(Y),$$
$$\text{subject to } \frac{\rho_g}{|\mathcal{G}|} - Y \ge 0, \text{ for all } g \in \mathcal{G}. \quad (15)$$

To maximize $\text{Tr}(Y)$, we propose a natural choice for the dual operator: $Y = (1/|\mathcal{G}|)\sum_{g\in\mathcal{G}} U_g|\omega\rangle\langle\omega|\psi\rangle\langle\psi|U_g^\dagger$, ensuring $\text{Tr}(Y) = P^{\text{primal}}$. With this choice, the (Holevo-like) constraint in Eq. (15) simplifies to $|\psi\rangle\langle\psi| - |\mathcal{G}|Y \ge 0$,

invoking group covariance. This inequality holds since the left-hand side can be written as a convex combination of positive semidefinite operators [40]. This confirms that our choice provides a feasible solution to the dual problem, proving $P^{\text{dual}} = P^{\text{primal}}$ and, in turn, validating Eq. (5).

Next, we address unambiguous QSE, also when the condition $\sqrt{\lambda_1} > \sum_{a>1} \sqrt{\lambda_a}$ holds. With the ansatz (8) and choice (9), the inconclusive POVM element reads $\Pi_Q = \mathbb{1} - \sum_{g\in\mathcal{G}} U_g|\omega\rangle\langle\omega|U_g^\dagger$. This specific choice of the seed state $|\omega\rangle$ ensures that $\text{Tr}(\Pi_g \rho_g) = |\langle\omega|\psi\rangle|^2 = 0$, and $\Pi_Q = (1 - \gamma^2)|v_1^1\rangle\langle v_1^1| \otimes |u_1^1\rangle\langle u_1^1| \ge 0$, since we can alternatively write $\gamma = (1/\sqrt{\lambda_1})\sum_{a\ne 1} \sqrt{\lambda_a} < 1$. Thus our ansatz is a feasible solution of the (primal) SDP in Eq. (2), with the probability of an inconclusive outcome given by $Q^{\text{primal}} = (\alpha_1^1/|\mathcal{G}|)(1 - \gamma^2)$, which simplifies to our main result in Eq. (6).

To show the optimality of this ansatz, we consider the dual formulation of Eq. (2),

$$Q^{\text{dual}} := \max_{X \ge 0} 1 - \text{Tr}(X), \text{ subject to}$$
$$\sum_{g\in\mathcal{G}} U_g X U_g^\dagger + \nu|\psi\rangle\langle\psi| - \Omega \ge 0, \ \nu \in \mathbb{R}, \quad (16)$$

which has been particularized for the problem at hand and simplified by exploiting its symmetries. This maximum is not strictly achievable, as the optimal solution lies on the boundary of the feasibility set, which is not contained within the feasibility set itself [34, 35]. As a result, unlike in the minimum-error case, there is no natural choice for the dual operator X.

Nevertheless, strong duality holds, and it is possible to construct X such that the dual problem yields an inconclusive probability satisfying $Q^{\text{dual}} = Q^{\text{primal}} - \varepsilon$, where ε is an arbitrary positive real number [40]. This construction ensures that for any such ε, there exists a corresponding ν in Eq. (16) that makes the solution feasible. Hence, taking the limit $\varepsilon \to 0^+$, we obtain $Q^{\text{dual}} = Q^{\text{primal}} = Q$, proving the optimality of the ansatz (8) with the specified γ. ∎

Conclusions. We have obtained the optimal minimum-error and unambiguous quantum state exclusion (QSE) protocols for any (finite-)group-generated set of states, offering a constructive proof that provides the explicit form of the optimal POVM in both cases. Several previously known results emerge as particular instances of our findings. A key aspect of our approach is the systematic use of the Gram matrix, which encodes all the information required for discrimination and exclusion, regardless of whether the set is symmetric or not. Our expressions for the failure probabilities, Eqs. (5) and (6), depend solely on the Gram matrix eigenvalues, making them applicable even to non-symmetric sets. Numerical

analysis further suggests that these expressions provide upper bounds on the corresponding probabilities for the optimal QSE protocols, aligning with the heuristic expectation that discrimination and exclusion become more challenging as the states share more symmetries. We are currently exploring these ideas further.

[1] S. McGee, *Evidence-Based Physical Diagnosis* (Elsevier, 2012).

[2] A. Birolini, *Reliability Engineering: Theory and Practice*, 8th ed. (Springer, Berlin, Germany, 2017).

[3] W. Stallings, *Network Security Essentials: Applications and Standards*, 7th ed. (Pearson, Boston, MA, 2020).

[4] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Physical Review A **89**, 022336 (2014).

[5] T. Heinosaari and O. Kerppo, Journal of Physics A: Mathematical and Theoretical **51**, 365303 (2018).

[6] T. A. Brun, J. Finkelstein, and N. D. Mermin, Physical Review A **65**, 032315 (2002).

[7] C. M. Caves, C. A. Fuchs, and R. Schack, Physical Review A **66**, 062111 (2002).

[8] M. F. Pusey, J. Barrett, and T. Rudolph, Nature Physics **8**, 475 (2012).

[9] A. Chefles, Contemporary Physics **41**, 401 (2000).

[10] J. A. Bergou, Journal of Modern Optics **57**, 160 (2010).

[11] J. Bae and L.-C. Kwek, Journal of Physics A: Mathematical and Theoretical **48**, 083001 (2015).

[12] A. F. Ducuara and P. Skrzypczyk, Physical Review Letters **125**, 110401 (2020).

[13] R. Uola, T. Bullock, T. Kraft, J.-P. Pellonpää, and N. Brunner, Physical Review Letters **125**, 110402 (2020).

[14] B. Stratton, C.-Y. Hsieh, and P. Skrzypczyk, Phys. Rev. A **110**, L050601 (2024).

[15] A. K. Maiyuren Srikumar, Stephen D. Bartlett, arXiv preprint arXiv:2411.09919 (2024).

[16] M. Leifer and C. Duarte, Physical Review A **101**, 062113 (2020).

[17] V. Havlíček and J. Barrett, Physical Review Research **2**, 013326 (2020).

[18] T. Heinosaari, O. Kerppo, L. Leppäjärvi, and M. Plávala, Physical Review A **109**, 032627 (2024).

[19] H. K. Mishra, M. Nussbaum, and M. M. Wilde, Letters in Mathematical Physics **114**, 76 (2024).

[20] G. Sentís, E. Martínez-Vargas, and R. Muñoz-Tapia, Quantum **6**, 658 (2022).

[21] J. W. Webb, I. V. Puthoor, J. Ho, J. Crickmore, E. Blakely, A. Fedrizzi, and E. Andersson, Phys. Rev. Res. **5**, 023094 (2023).

[22] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, and O. Hirota, Physical Review A **59**, 3325 (1999).

[23] S. M. Barnett, Physical Review A **64**, 030303 (2001).

[24] Y. C. Eldar and G. D. Forney, IEEE Transactions on Information Theory **47**, 858 (2001).

[25] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Transactions on Information Theory **50**, 1198 (2004).

[26] K. Nakahira and T. S. Usuda, Physical Review A—Atomic, Molecular, and Optical Physics **86**, 062305 (2012).

[27] K. Nakahira and T. S. Usuda, Physical Review A—Atomic, Molecular, and Optical Physics **87**, 012308 (2013).

[28] G. Sentís, E. Bagan, J. Calsamiglia, G. Chiribella, and R. Munoz-Tapia, Physical Review Letters **117**, 150502 (2016).

[29] G. Sentís, J. Calsamiglia, and R. Munoz-Tapia, Physical review letters **119**, 140506 (2017).

[30] S. Llorens, G. Sentís, and R. Muñoz-Tapia, Quantum **8**, 1452 (2024).

[31] M. Skotiniotis, S. Llorens, R. Hotz, J. Calsamiglia, and R. Muñoz Tapia, Phys. Rev. Res. **6**, 033329 (2024).

[32] N. Johnston, V. Russo, and J. Sikora, Quantum **9**, 1622 (2025).

[33] R. A. Horn and C. R. Johnson, *Matrix analysis* (Cambridge university press, 2012).

[34] S. Boyd and L. Vandenberghe, *Convex optimization* (Cambridge university press, 2004).

[35] J. Watrous, *The theory of quantum information* (Cambridge university press, 2018).

[36] M. Hamermesh, *Group Theory and Its Application to Physical Problems*, Addison Wesley Series in Physics (Dover Publications, 1989).

[37] B. Steinberg, *Representation Theory of Finite Groups: An Introductory Approach*, Universitext (Springer New York, 2011).

[38] M. Christandl, The structure of bipartite quantum states —insights from group theory and cryptography (2006), arXiv:quant-ph/0604183 [quant-ph].

[39] J. Crickmore, I. V. Puthoor, B. Ricketti, S. Croke, M. Hillery, and E. Andersson, Physical Review Research **2**, 013256 (2020).

[40] See supplemental material below.

[41] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Journal of Mathematical Physics **45**, 2171 (2004).

[42] C. Cheng, Linear Algebra and its Applications **469**, 230 (2015).

[43] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, International Journal of Quantum information **8**, 535 (2010).

Quantum state exclusion for group-generated ensembles of pure states

A. Diebra[1], S. Llorens[1], E. Bagan[1], G. Sentís[1,2], and R. Muñoz-Tapia[1,3]

[1]*Física Teòrica: Informació i Fenòmens Quàntics,*
Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
[2]*Ideaded, Carrer de la Tecnologia, 35, 08840 Viladecans, Barcelona, Spain and*
[3]*H. H. Wills Physics Laboratory, University of Bristol,*
Tyndall Avenue, Bristol, BS8 1TL, United Kingdom

All equations in this supplementary note are numbered with the prefix 'S'. Equations referenced without this prefix correspond to those in the main text.

I. GRAM MATRIX AS A COMPLETE DESCRIPTOR OF PURE STATE ENSEMBLES

In this section, we provide a formal proof that, in the context of state discrimination and exclusion, the Gram matrix encapsulates all the information needed to compute averaged cost functions and figures of merit, as well as to determine the corresponding optimal measurements.

More precisely, we consider the task of discriminating or excluding pure states drawn from a given ensemble $\mathcal{E} := \{\eta_k, |\psi_k\rangle\}_{k=1}^N$, where the states have prior probabilities η_k and may or may not be linearly independent. We assume that the states belong to a d-dimensional Hilbert space, i.e., $|\psi_k\rangle \in \mathbb{C}^d$. The Gram matrix G associated with $\mathcal{E}$ is defined as

$$G_{k,l} = \sqrt{\eta_k \eta_l} \langle \psi_k | \psi_l \rangle. \tag{S1}$$

It can be viewed as an operator on $\mathbb{C}^N$, given by

$$G = \sum_{k,l=1}^N \sqrt{\eta_k \eta_l} \langle \psi_k | \psi_l \rangle |k\rangle \langle l|, \tag{S2}$$

where $\{|k\rangle\}_{k=1}^N$ is an arbitrary orthonormal basis, which may be chosen to suit the specific problem at hand.

The cost functions relevant to discrimination and exclusion tasks generically take the form

$$\mathcal{F} = \sum_{l,k=1}^N \eta_k f_{k,l} \langle \psi_k | \Pi_l | \psi_k \rangle, \tag{S3}$$

where $\{\Pi_k\}_{k=1}^N$ defines the Positive Operator-Valued Measure (POVM) describing the quantum measurement performed on $|\psi_k\rangle$ to carry out the task. The joint probability of preparing the state $|\psi_k\rangle$ from $\mathcal{E}$ and obtaining measurement outcome l is given by $\eta_k \langle \psi_k | \Pi_l | \psi_k \rangle$. Thus, the choice of coefficients $f_{k,l}$ determines the (averaged) cost function; for instance, in the exclusion problem, the average error probability is obtained by setting $f_{k,l} = \delta_{k,l}$. The operators Π_k are positive semidefinite and satisfy

$$\mathbb{1}_d - \sum_{k=1}^N \Pi_k \geq 0, \tag{S4}$$

where $\mathbb{1}_d$, the d-dimensional identity operator (or matrix), may be replaced by the projector onto the span of $\mathcal{E}$, denoted $\mathbb{1}_{\text{span}(\mathcal{E})}$ (obviously, $\mathbb{1}_d - \mathbb{1}_{\text{span}(\mathcal{E})} \geq 0$). Additional constraints of the form

$$\sum_{k,l=1}^N c_{l,k}^a \langle \psi_k | \Pi_l | \psi_k \rangle = 0, \qquad a = 1, 2, \ldots \tag{S5}$$

may apply depending on the problem, where $c_{l,k}^a$ are fixed coefficients. For instance, in unambiguous exclusion, one requires $\mathrm{Tr}(\Pi_k \rho_k) = \langle \psi_k | \Pi_k | \psi_k \rangle = 0$ for all k; see Eq. (2).

The following theorem formalizes the claim that the Gram matrix fully describes a pure state ensemble for computing averages in state discrimination and exclusion:

Theorem I. *For any POVM $\{\Pi_k\}_{k=1}^{N}$ on $\mathbb{C}^d$, there exists a set of positive operators $\{\Xi_k\}_{k=1}^{N}$ acting on $\mathbb{C}^N$ satisfying*

$$G - \sum_{k=1}^{N} \Xi_k \geq 0, \tag{S6}$$

such that

$$\eta_k \langle \psi_k | \Pi_l | \psi_k \rangle = \langle k | \Xi_l | k \rangle. \tag{S7}$$

Conversely, given a set of positive operators $\{\Xi_k\}_{k=1}^{N}$ on $\mathbb{C}^N$ satisfying Eq. (S6), there exists a POVM on $\mathbb{C}^d$ for which Eq. (S7) holds.

Proof. Define the operator

$$X = \sum_{k=1}^{N} \sqrt{\eta_k} |\psi_k\rangle\langle k|, \tag{S8}$$

which satisfies $G = X^\dagger X$. Given a POVM $\{\Pi_k\}_{k=1}^{N}$, define $\Xi_k = X^\dagger \Pi_k X \geq 0$. Then, the POVM condition in Eq. (S4) becomes

$$X^\dagger X - \sum_{k=1}^{N} X^\dagger \Pi_k X \geq 0, \tag{S9}$$

proving Eq. (S6). On the other hand, since $X|k\rangle = \sqrt{\eta_k}|\psi_k\rangle$, it follows that

$$\eta_k \langle \psi_k | \Pi_l | \psi_k \rangle = \langle k | X^\dagger \Pi_l X | k \rangle = \langle k | \Xi_l | k \rangle. \tag{S10}$$

This completes the proof of the direct statement.

To prove the converse, let X^+ denote the Moore-Penrose pseudoinverse of X. Given positive semidefinite operators $\{\Xi_k\}_{k=1}^{N}$ that satisfy Eq. (S6), define

$$\Pi_k := (X^+)^\dagger \Xi_k X^+ \geq 0. \tag{S11}$$

Multiplying Eq. (S6) by $(X^+)^\dagger$ from the left and by X^+ from the right yields

$$(X^+)^\dagger X^\dagger X X^+ - \sum_{k=1}^{N} (X^+)^\dagger \Xi_k X^+ \geq 0. \tag{S12}$$

Noticing that $XX^+ = \mathbb{1}_{\mathrm{range}(X)}$ is the projector onto $\mathrm{range}(X) = \mathrm{span}(\mathcal{E})$, one obtains that the first term of this expression equals $\mathbb{1}_{\mathrm{span}(\mathcal{E})} \leq \mathbb{1}_d$, recovering the POVM condition (S4). Additionally

$$\eta_k \langle \psi_k | \Pi_l | \psi_k \rangle = \langle k | X^\dagger \Pi_l X | k \rangle = \langle k | \left[(X^+ X)^\dagger \Xi_l X^+ X \right] | k \rangle = \langle k | \Xi_l | k \rangle, \tag{S13}$$

where, in the final equality, we used $X^+ X = \mathbb{1}_{\mathrm{range}(X^\dagger)}$, $\mathrm{range}(X^\dagger) = \mathrm{range}(G)$, and the fact that $\Xi_k \mathbb{1}_{\mathrm{range}(G)} = \Xi_k$, which follows from condition (S6). This completes the proof $\blacksquare$

Using Theorem I, we can rewrite the averaged cost function in Eq. (S3) as

$$\mathcal{F} = \sum_{l,k=1}^{N} f_{k,l} \langle k | \Xi_l | k \rangle, \tag{S14}$$

with the POVM condition (S4) reexpressed in terms of the positive semidefinite operators $\{\Xi_k\}_{k=1}^N$ as in Eq. (S6). Similarly, if additional constraints such as those in Eq. (S5) are imposed, they can be written as

$$\sum_{k,l=1}^N \tilde{c}_{l,k}^a \langle k|\Xi_l|k\rangle = 0, \qquad a = 1, 2, \dots \tag{S15}$$

for some new coefficients $\tilde{c}_{l,k}^a$. Thus, the various elements needed to formulate the discrimination or exclusion problem, originally expressed in Eqs. (S3)–(S5), can be equivalently reformulated as Eqs. (S14)–(S15), where the full description of the ensemble $\mathcal{E}$ is encoded in the Gram matrix G.

Although not widely used in the context of discrimination and exclusion, it also follows from Theorem I that the Gram matrix remains a sufficient descriptor of ensembles even for non-linear cost functions, such as mutual information, and for non-linear constraints, as long as both depend solely on the joint probabilities $\eta_k \langle \psi_k | \Pi_l | \psi_k \rangle$.

Another direct consequence of Theorem I is that any two ensembles $\mathcal{E} = \{\eta_k, |\psi_k\rangle\}_{k=1}^N$ and $\tilde{\mathcal{E}} = \{\tilde{\eta}_k, |\tilde{\psi}_k\rangle\}_{k=1}^N$, that share the same Gram matrix, will exhibit identical discrimination and exclusion properties. Moreover, for any given POVM $\{\Pi_k\}_{k=1}^N$, there exists an alternative one $\{\tilde{\Pi}_k\}_{k=1}^N$ such that

$$\eta_k \langle \psi_k | \Pi_l | \psi_k \rangle = \tilde{\eta}_k \langle \tilde{\psi}_k | \tilde{\Pi}_l | \tilde{\psi}_k \rangle \quad \text{for all} \quad k, l. \tag{S16}$$

Such a POVM can be constructed as

$$\tilde{\Pi}_k := (X\tilde{X}^+)^\dagger \Pi_k X\tilde{X}^+, \tag{S17}$$

where X is defined in Eq. (S8) and $\tilde{X}$ is defined similarly as

$$\tilde{X} = \sum_{k=1}^N \sqrt{\tilde{\eta}_k} |\tilde{\psi}_k\rangle\langle k|. \tag{S18}$$

Lastly, noticing that the ensemble operator $\Omega := \sum_k \eta_k |\psi_k\rangle\langle\psi_k|$ can be written as $\Omega = XX^\dagger$, one concludes that both the Gram matrix G and the ensemble operator Ω share the same non-zero eigenvalues —a result that has been extensively used in the main text.

II. REPRESENTATION THEORY OF FINITE GROUPS: A CONCISE SUMMARY

This section provides an overview of key concepts in representation theory extensively used throughout the letter. The results summarized here can be found in standard textbooks [36, 37] and also in review articles such as [38, 42].

A. Linear representations

A *representation* of a group $\mathcal{G}$ is a homomorphism from $\mathcal{G}$ to the group of invertible linear transformations (matrices) acting on a vector space V. Representations provide a powerful way to study the structure and properties of abstract groups through linear algebra. In addition, unitary representations are central in quantum physics, as they describe transformations of physical systems.

Formally, if $GL(V)$ denotes the general linear group on V, a representation is a map $D : \mathcal{G} \to GL(V)$ satisfying

$$D(g)D(h) = D(gh), \quad D(e) = \mathbb{1}, \tag{S19}$$

for all $g, h \in \mathcal{G}$, where $e \in \mathcal{G}$ is the identity element and $\mathbb{1}$ is the identity matrix in $GL(V)$.

In these notes, we focus exclusively on *unitary representations*, where each group element is mapped to a unitary matrix. That is, we consider maps $U : \mathcal{G} \to \mathcal{U}(V)$, where $\mathcal{U}(V) \subset GL(V)$ is the group of unitary transformations on V, which is typically a Hilbert space $\mathcal{H}$ in quantum mechanical applications. In this case, it is customary to write U instead of D and use the subscript notation $U_g := U(g) \in \mathcal{U}(V)$.

A central concept in representation theory is irreducibility. A representation U is said to be *irreducible* if the only subspaces $W \subseteq V$ that remain invariant under the action of all U_g are the trivial subspaces, namely the zero subspace $W = \{0\}$ and the entire space $W = V$. Irreducible representations, often referred to as irreps, are fundamental because any representation U of a finite group $\mathcal{G}$ is either irreducible or can be decomposed into a direct sum of irreps, in which case it is called *reducible*. Specifically, we have

$$U \cong \bigoplus_\mu m_\mu U^\mu, \tag{S20}$$

where μ labels the distinct irreps U^μ of $\mathcal{G}$ and m_μ denotes their multiplicity. In matrix terms, this means that by choosing an appropriate basis, each group element U_g can be written as

$$U_g = \bigoplus_\mu U_g^\mu \otimes \mathbb{1}_{m_\mu}, \tag{S21}$$

where $\mathbb{1}_{m_\mu}$ accounts for the multiplicity of the irreps. The irreps of a group are fundamentally determined by its structure. Each finite group has a finite set of irreps, with each irrep corresponding to a conjugacy class of the group.

A fundamental result in the classification of irreducible representations is *Schur's lemma*. In its matrix form, it states that given two irreps, U_g^μ and U_g^ν, if a matrix T satisfies $TU_g^\mu = U_g^\nu T$ for all $g \in \mathcal{G}$, then T is either invertible —implying that the two representations are isomorphic— or zero. Moreover, in the special case where both irreps coincide, $\mu = \nu$, i.e., when T commutes with U_g^μ for all $g \in \mathcal{G}$, T must be a scalar multiple of the identity in the corresponding irreducible subspace. In other words, $T = \lambda \mathbb{1}_{d_\mu}$ for some $\lambda \in \mathbb{C}$, where d_μ is the dimension of the irrep.

A direct consequence of Schur's lemma is that the matrix elements of two irreps satisfy the following orthogonality relation, known as the *Great Orthogonality Theorem*,

$$\sum_{g \in \mathcal{G}} \left(U_g^\mu\right)_{n,m} \left(U_g^\nu\right)_{n',m'}^* = \delta_{\mu,\nu}\delta_{n,n'}\delta_{m,m'} \frac{|\mathcal{G}|}{d_\mu}, \tag{S22}$$

where $*$ denotes complex conjugation, the sum extends over all group elements $g \in \mathcal{G}$, and $|\mathcal{G}|$ is the order of the group.

A well-known example of a reducible representation is the *regular representation*, which plays an importantl role in the proof of the lemma in the main text. This representation arises from the natural action of $\mathcal{G}$ on itself. Specifically, each element $g \in \mathcal{G}$ is associated with an orthonormal basis $\{|g\rangle\}_{g \in \mathcal{G}}$ of a $|\mathcal{G}|$-dimensional Hilbert space, commonly denoted as $\mathbb{C}[\mathcal{G}]$ and referred to as the *group algebra*. The *left-(right-)regular representation* is then defined by left (right) translations:

$$L_g|c\rangle = |gc\rangle, \quad R_g|c\rangle = |cg^{-1}\rangle. \tag{S23}$$

The matrices of L_g and R_g are $(0,1)$-matrices (i.e., matrices with binary entries). Their matrix elements are given by

$$(L_g)_{r,c} = \delta_{g,rc^{-1}}, \qquad (R_g)_{r,c} = \delta_{g,r^{-1}c}, \tag{S24}$$

where $\delta_{g,h}$ is the Kronecker delta over the elements of $\mathcal{G}$.

These matrices can be directly constructed from the group's multiplication table. Specifically, consider a Cayley table $\mathcal{L}$ where the column headings list the inverses of the group elements instead of the elements themselves. In this table, each entry is given by $\mathcal{L}_{r,c} = rc^{-1}$. Similarly, define $\mathcal{R}$ as a Cayley table where the row headings list the inverses, so that $\mathcal{R}_{r,c} = r^{-1}c$. Comparing with Eq. (S24), we see that the matrix L_g (resp. R_g) is obtained by replacing every occurrence of g in $\mathcal{L}$ (resp. $\mathcal{R}$) with 1, while all other entries are replaced by 0.

Both regular representations are unitary, and their traces satisfy $\text{Tr}(L_g) = \text{Tr}(R_g) = |\mathcal{G}|\delta_{g,e}$, meaning that they are traceless matrices except for the identity element e. As a result, it can be shown from character theory that the decomposition of the regular representations contains all the distinct irreps of the group, each appearing with multiplicity equal to its dimension:

$$L \cong \bigoplus_\mu d_\mu U^\mu, \quad R \cong \bigoplus_\mu d_\mu U^\mu. \tag{S25}$$

Taking traces, we obtain the well-known result

$$|\mathcal{G}| = \sum_\mu d_\mu^2, \tag{S26}$$

which relates the order of the group to the dimensions of its irreps. An immediate consequence is that all irreps of a finite abelian group are one-dimensional: since all elements of an abelian group commute, the number of conjugacy classes —and hence the number of distinct irreps— equals the order of the group, which, by Eq. (S26), forces $d_\mu = 1$ for all μ.

B.   Projective representations

Projective representations generalize linear representations by allowing multiplicative prefactors in the composition rule of D. Specifically, a *projective representation* of a group $\mathcal{G}$ on a vector space V is a map $D : \mathcal{G} \to GL(V)$ satisfying

$$D(g)D(h) = \omega(g,h)D(gh), \quad D(e) = \mathbb{1}, \tag{S27}$$

for all $g, h \in \mathcal{G}$, where $\omega(g,h) \in \mathbb{C}^\times$ are nonzero complex functions of the group elements.

Such prefactors are not arbitrary; the map $\omega : \mathcal{G} \times \mathcal{G} \to \mathbb{C}^\times$ must satisfy

$$\omega(g,h)\omega(gh,f) = \omega(g,hf)\omega(h,f), \quad \omega(g,e) = \omega(e,g) = 1, \quad \text{for all } g, h, f \in \mathcal{G}, \tag{S28}$$

where the first relation ensures associativity. The map ω is commonly referred to as a *multiplier* (or 2-cocycle in topology terminology). A projective representation is then completely determined by the tuple (D, ω).

The introduction of multipliers broadens the concept of equivalence between representations. We say that *two multipliers ω and ω' are equivalent* if there exists a map $\mu : \mathcal{G} \to \mathbb{C}^\times$ with $\mu(e) = 1$ such that

$$\omega(g,h) = \frac{\mu(g)\mu(h)}{\mu(gh)}\omega'(g,h), \qquad \text{for all } g, h \in \mathcal{G}. \tag{S29}$$

It is straightforward to verify that Eq. (S29) defines an equivalence relation. *Two projective representations (D, ω) and (D', ω') are said to be equivalent* if D and D' are isomorphic, meaning that there exists an invertible matrix T such that $D'(g) = TD(g)T^{-1}$ for all $g \in \mathcal{G}$, and their corresponding multipliers are equivalent. Then, $D'(g) = [1/\mu(g)]TD(g)T^{-1}$.

It is sometimes possible to reduce a projective representation (D, ω) to a linear representation. This is always the case if there exists a map $\mu : \mathcal{G} \to \mathbb{C}^\times$ with $\mu(e) = 1$ such that ω takes the form

$$\omega(g,h) = \frac{\mu(g)\mu(h)}{\mu(gh)}, \qquad \text{for all } g, h \in \mathcal{G}. \tag{S30}$$

When ω has this form, we say that ω is a *2-coboundary*. From Eq. (S29), we immediately see that such an ω is equivalent to the trivial multiplier $\omega'(g,h) = 1$ for all $g, h \in \mathcal{G}$. A projective representation (D, ω) where ω is a 2-coboundary is referred to as a *trivial (projective) representation*, as it can be reduced to a linear representation D' defined by $D'(g) = [1/\mu(g)]D(g)$:

$$D'(g)D'(h) = \frac{1}{\mu(g)\mu(h)}D(g)D(h) = \frac{1}{\mu(gh)}D(gh) = D'(gh). \tag{S31}$$

Consequently, all one-dimensional projective representations $\chi : \mathcal{G} \to \mathbb{C}$, for which $\chi(g)\chi(h) = \omega(g,h)\chi(gh)$, are trivial, as the corresponding multiplier ω is clearly a 2-coboundary, with $\mu(g) = \chi(g)$.

As with linear representations, we focus exclusively on *unitary projective representations* $U : \mathcal{G} \to \mathcal{U}(V)$, where the corresponding multipliers are pure phases (unitary), i.e., $\omega(g,h) = e^{i\theta(g,h)}$, $\theta(g,h) \in \mathbb{R}$ for all $g, h \in \mathcal{G}$. Given any projective representation D, one can always find an equivalent unitary projective representation.

In quantum mechanics, where we are primarily concerned with the action of unitary representations on quantum states $|\psi\rangle \in \mathcal{H}$, global phases are irrelevant since physical states correspond to rays in Hilbert space. This freedom

implies that U_g and $U'_g = \mu(g)U_g$ are physically equivalent for any pure phase $\mu(g)$. Consequently, equivalent projective unitary representations, as defined in Eq. (S29), induce the same physical transformations on a quantum system.

Most properties of linear representations naturally extend to projective representations when properly accounting for the multiplier ω. In particular, a reducible projective representation (U, ω) decomposes as a direct sum of irreducible projective representations, as in Eqs. (S20) and (S21), satisfying $U_g^\mu U_h^\mu = \omega(g, h)U_{gh}^\mu$ with the same multiplier ω for all μ. Furthermore, Schur's lemma applies to projective representations without modification, while the Great Orthogonality Theorem now reads

$$\sum_{g \in \mathcal{G}} \omega^*(g, g^{-1}) \left(U_g^\mu\right)_{n,m} \left(U_{g^{-1}}^\nu\right)_{m',n'} = \delta_{\mu,\nu}\delta_{n,n'}\delta_{m,m'} \frac{|\mathcal{G}|}{d_\mu}. \tag{S32}$$

Note that while Eq. (S22) involves $U_g^\dagger$, for projective representations, $U_{g^{-1}}$ appears instead, and in general, $U_{g^{-1}} \neq U_g^\dagger$.

Having provided a general overview of projective representations of groups, we now turn to considerations specific to the objectives of the main text. In particular, we aim to derive a canonical form for the Gram matrix (Sec. III B below) and show that our results, especially Eqs. (5) and (6), also hold in the case of projective representations.

For general unitary projective representations, it has been noted that $U_{g^{-1}} \neq U_g^\dagger$, meaning that the inverse of a matrix does not necessarily belong to the representation. However, the two matrices are related by

$$U_g^\dagger = \omega^*(g, g^{-1})U_{g^{-1}} = \omega^*(g^{-1}, g)U_{g^{-1}}, \tag{S33}$$

which follows from the relation $U_g U_{g^{-1}} = \omega(g, g^{-1})U_{gg^{-1}} = \omega(g, g^{-1})\mathbb{1}$ and the analogous expression for $U_{g^{-1}}U_g$. Defining the map $\mu : \mathcal{G} \to \mathbb{C}^\times$ by

$$\mu(g) = \frac{1}{\sqrt{\omega(g, g^{-1})}} \tag{S34}$$

(choosing either branch of the square root), we see that the equivalent representation $U'_g = \mu(g)U_g$ satisfies $U'_g U'_{g^{-1}} = \mathbb{1}$, i.e., $(U'_g)^\dagger = U'_{g^{-1}}$. Thus, when the multipliers are unitary (pure phases), we may assume without loss of generality that

$$\omega(g, g^{-1}) = \omega(g^{-1}, g) = 1, \qquad \text{for all } g \in \mathcal{G}. \tag{S35}$$

Under this assumption, the Great Orthogonality Theorem in Eq. (S32) takes the same form as its counterpart for linear representations in Eq. (S22).

The concept of the regular representation extends to projective representations. In analogy with linear representations, the *projective left- and right-regular representations* with multiplier ω are defined by left and right translations over the group algebra:

$$L_g|h\rangle = \omega(g, h)|gh\rangle, \quad R_g|h\rangle = \omega(g, h^{-1})|hg^{-1}\rangle. \tag{S36}$$

For unitary ω, both representations are unitary, though they are no longer $(0, 1)$-matrices; instead, their entries are pure phases:

$$(L_g)_{r,c} = \omega(rc^{-1}, c)\delta_{g,rc^{-1}} = [\omega(r, c^{-1})]^*\delta_{g,rc^{-1}}, \quad (R_g)_{r,c} = \omega(r^{-1}c, c^{-1})\delta_{g,r^{-1}c} = [\omega(r^{-1}, c)]^*\delta_{g,r^{-1}c}, \tag{S37}$$

where we have used Eq. (S28) and assumption (S35). The traces of these matrices satisfy $\text{Tr}(L_g) = \text{Tr}(R_g) = |\mathcal{G}|\delta_{g,e}$, implying that the projective regular representations obeys Eqs. (S25) and (S26).

As in the case of linear representations, the matrices of the two regular representations can be systematically derived from "Cayley-like tables" that also incorporate the multipliers:

$$\mathcal{L}_{r,c} = \omega(r, c^{-1})rc^{-1}, \quad \mathcal{R}_{r,c} = \omega(r^{-1}, c)r^{-1}c, \tag{S38}$$

where the right-hand sides are formal expressions used for bookkeeping purposes. Comparing with Eq. (S37), the matrix of L_g^*—the complex conjugate of the left-regular representation, as defined in Eq. (S36)— can be obtained from the table $\mathcal{L}$ by replacing all occurrences of g with 1 and setting the remaining entries to 0. To construct L_g, we then take the complex conjugate of the resulting matrix. Similarly, applying the same procedure to the multiplication table $\mathcal{R}$ yields R_g^* and R_g. The sets $\{L_g^*\}_{g \in \mathcal{G}}$ and $\{R_g^*\}_{g \in \mathcal{G}}$ themselves form regular representations.

III. GROUP-GENERATED GRAM MATRICES

This section discusses the structure and construction of Gram matrices associated with group-generated pure state ensembles. The key insight is that the symmetry group generating the ensemble fully determines the structure of its Gram matrix. We illustrate our findings with concrete examples.

A. Linear representations

Consider the ensemble $\mathcal{E} = \{|\psi_g\rangle = U_g|\psi\rangle \,|\, g \in \mathcal{G}\}$ of equiprobable states generated by a group $\mathcal{G}$. To simplify the analysis, we omit the prior probability $\eta_g = 1/|\mathcal{G}|$ from the definition of the associated Gram matrix, Eq. (S1), and instead define $G_{g,h} = \langle \psi_g|\psi_h\rangle$. Identifying the orthonormal basis in Eq. (S2) with the basis of the group algebra, we obtain

$$G = \sum_{g,h\in\mathcal{G}} \langle \psi_g|\psi_h\rangle |g\rangle\langle h| = \sum_{g,h\in\mathcal{G}} \langle \psi|\psi_{g^{-1}h}\rangle |g\rangle\langle h| = \sum_{l,h\in\mathcal{G}} \langle \psi|\psi_l\rangle |hl^{-1}\rangle\langle h| = \sum_{l,h\in\mathcal{G}} \langle \psi|\psi_l\rangle R_l|h\rangle\langle h| = \sum_{l\in\mathcal{G}} \langle \psi|\psi_l\rangle R_l. \quad \text{(S39)}$$

Thus, the Gram matrix G is contained in the associative algebra spanned by the right-regular representation of the group that generates the ensemble, fully determining its structure.

The above provides a direct and systematic procedure for constructing Gram matrices with a desired symmetry inherited from the group $\mathcal{G}$, bypassing the explicit construction of the associated ensemble $\mathcal{E}$. The steps are as follows:

(a) Construct the group's multiplication table $\mathcal{R}$ (see Sec. II A) listing the elements of $\mathcal{G}$ as column headings and their inverses as row headings.
(b) Define a matrix $\tilde{G}$ by replacing each distinct entry of the table $\mathcal{R}$ with a complex coefficient c_g, assigning $c_e = 1$ for the identity element e.
(c) Impose semidefiniteness constraints on $\tilde{G}$ to ensure it represents a valid Gram matrix.

The resulting matrix G has the desired group symmetry. This procedure is illustrated in the following example.

Example. Consider the smallest non-abelian group: the dihedral group D_3. It is the symmetry group of an equilateral triangle with vertices A, B, C. The group consists of six elements: three (clockwise) rotations, e, r, and r^2, by angles 0, $2\pi/3$, and $4\pi/3$ radians, respectively ($r^3 = e$), and three reflections, s_A, s_B, and s_C, along the lines passing through vertex A, B, or C, respectively, and the midpoint of the opposite side. Step (a) yields the following multiplication table:

D_3	e	r	r^2	s_A	s_B	s_C
e	e	r	r^2	s_A	s_B	s_C
r^2	r^2	e	r	s_C	s_A	s_B
r	r	r^2	e	s_B	s_C	s_A
s_A	s_A	s_C	s_B	e	r^2	r
s_B	s_B	s_A	s_C	r	e	r^2
s_C	s_C	s_B	s_A	r^2	r	e

In step (b), we substitute $r^k \mapsto c_k \in \mathbb{C}$ and $e \mapsto 1$, along with $s_\alpha \mapsto c_\alpha \in \mathbb{C}$, yielding:

$$\tilde{G} = \begin{pmatrix} 1 & c_1 & c_2 & c_A & c_B & c_C \\ c_2 & 1 & c_1 & c_C & c_A & c_B \\ c_1 & c_2 & 1 & c_B & c_C & c_A \\ c_A & c_C & c_B & 1 & c_2 & c_1 \\ c_B & c_A & c_C & c_1 & 1 & c_2 \\ c_C & c_B & c_A & c_2 & c_1 & 1 \end{pmatrix}. \quad \text{(S40)}$$

Finally, in step (c), we enforce the conditions required for G to be a valid Gram matrix: hermiticity imposes $c_2 = c_1^*$ and $c_A, c_B, c_C \in \mathbb{R}$, while positive semidefiniteness further constrains the coefficients. Thus,

$$G = \begin{pmatrix} 1 & c_1 & c_1^* & c_\mathrm{A} & c_\mathrm{B} & c_\mathrm{C} \\ c_1^* & 1 & c_1 & c_\mathrm{C} & c_\mathrm{A} & c_\mathrm{B} \\ c_1 & c_1^* & 1 & c_\mathrm{B} & c_\mathrm{C} & c_\mathrm{A} \\ c_\mathrm{A} & c_\mathrm{C} & c_\mathrm{B} & 1 & c_1^* & c_1 \\ c_\mathrm{B} & c_\mathrm{A} & c_\mathrm{C} & c_1 & 1 & c_1^* \\ c_\mathrm{C} & c_\mathrm{B} & c_\mathrm{A} & c_1^* & c_1 & 1 \end{pmatrix} ; \quad c_1 \in \mathbb{C}, \quad c_\mathrm{A}, c_\mathrm{B}, c_\mathrm{C} \in \mathbb{R}, \quad \text{such that} \quad G \geq 0. \tag{S41}$$

Since the Gram matrix G belongs to the associative algebra spanned by the set $\{R_g\}_{g \in \mathcal{G}}$, any function of G, including its square root $S = \sqrt{G}$, also lies in the same algebra. Consequently,

$$S = \sum_{g \in \mathcal{G}} s_g R_g, \tag{S42}$$

for some complex coefficients $\{s_g\}_{g \in \mathcal{G}}$.

Associated with any ensemble $\mathcal{E}$ that can be represented by the Gram matrix G, one can always construct a new ensemble $\mathcal{E}_S = \{|\phi_g\rangle, g \in \mathcal{G}\}$ by regarding each column of S as a state, $|\phi_g\rangle = \sum_{h \in \mathcal{G}} S_{h,g}|h\rangle \in \mathbb{C}^{|\mathcal{G}|}$. By construction, the ensemble $\mathcal{E}_S$ is represented by the same Gram matrix, i.e., $G_{g,h} = \langle \psi_g | \psi_h \rangle = \langle \phi_g | \phi_h \rangle$. Consequently, $\mathcal{E}$ and $\mathcal{E}_S$ share the same (anti-)distinguishability properties, as discussed in Sec. I. The ensemble $\mathcal{E}_S$ is also group-generated by $\mathcal{G}$ and transforms under the left regular representation:

$$L_g |\phi_h\rangle = \sum_{l \in \mathcal{G}} S_{l,h} L_g |l\rangle = \sum_{l \in \mathcal{G}} S_{l,h} |gl\rangle = \sum_{l \in \mathcal{G}} S_{g^{-1}l,h} |l\rangle = |\phi_{gh}\rangle, \tag{S43}$$

where the last equality follows from $S_{g^{-1}l,h} = S_{l,gh}$, since S belongs to the algebra of the right-regular representation:

$$S_{g^{-1}l,h} = \sum_{f \in \mathcal{G}} s_f (R_f)_{g^{-1}l,h} = \sum_{f \in \mathcal{G}} s_f \delta_{f,l^{-1}gh} = \sum_{f \in \mathcal{G}} s_f (R_f)_{l,gh} = S_{l,gh}. \tag{S44}$$

In particular, the above proves that any matrix constructed by the above procedure is the Gram matrix of at least one group-generated ensemble.

B.   Projective representations

When the ensemble $\mathcal{E} = \{|\psi_g\rangle = U_g|\psi\rangle \mid g \in \mathcal{G}\}$ is generated by a projective representation of a group $\mathcal{G}$ with multiplier ω, the associated Gram matrix can be brought into a canonical form that also exhibits a well-defined structure determined by the representation.

We first write the Gram matrix in the basis of the group algebra, obtaining

$$G = \sum_{g,h \in \mathcal{G}} \langle \psi_g | \psi_h \rangle |g\rangle\langle h| = \sum_{g,h \in \mathcal{G}} \omega(g^{-1},h) \langle \psi | \psi_{g^{-1}h} \rangle |g\rangle\langle h|$$

$$= \sum_{l,h} \omega(lh^{-1},h) \langle \psi | \psi_l \rangle |hl^{-1}\rangle\langle h| = \sum_{l,h} \omega^*(l,h^{-1}) \langle \psi | \psi_l \rangle |hl^{-1}\rangle\langle h| = \sum_l \langle \psi | \psi_l \rangle R_l^*, \tag{S45}$$

where the second-to-last equality follows from Eq. (S28) and assumption (S35). Thus, in a manner analogous to the linear case, the Gram matrix G is seen to belong to the associative algebra spanned by $\{R_g^*\}_{g \in \mathcal{G}}$. Consequently, any function of G must also lie within this algebra. In particular, its square root $S = \sqrt{G}$ takes the form

$$S = \sum_{g \in \mathcal{G}} s_g R_g^* \tag{S46}$$

where $\{s_g\}_{g \in \mathcal{G}}$ are complex coefficients.

Consider now the ensemble $\mathcal{E}_S = \{|\phi_g\rangle, g \in \mathcal{G}\}$ constituted by the columns of S, i.e., $|\phi_g\rangle = \sum_{h \in \mathcal{G}} S_{h,g}|h\rangle$. This ensemble is also group-generated by $\mathcal{G}$ and transforms under the projective left-regular representation, as shown by the following:

$$L_g|\phi_h\rangle = \sum_{l \in \mathcal{G}} S_{l,h} L_g |l\rangle = \sum_{l \in \mathcal{G}} \omega(g,l) S_{l,h} |gl\rangle = \sum_{l \in \mathcal{G}} \omega(g, g^{-1}l) S_{g^{-1}l,h} |l\rangle = \omega(g,h)|\phi_{gh}\rangle, \tag{S47}$$

where the identity $\omega(g, g^{-1}l) S_{g^{-1}l,h} = \omega(g,h) S_{l,gh}$, used in the last equality, is analogous to Eq. (S44) and follows from the fact that S belongs to the algebra spanned by $\{R_g^*\}_{g \in \mathcal{G}}$.

The above discussion shows that the systematic procedure used to derive the structure of the Gram matrix from the Cayley table $\mathcal{R}$ in the linear case also applies to projective representations, provided that condition (S35) holds. As noted, for any given representation, one can always find an equivalent one —corresponding to the same physical situation— in which this condition is satisfied. Therefore, the procedure can always be applied, yielding the Gram matrix of any group-generated ensemble in a specific (canonical) form, with its structure entirely determined by the symmetry of the ensemble.

To illustrate our findings, we conclude the section with a detailed, physically motivated example of a group-generated set of four states that defines a Symmetric Informationally Complete POVM (SIC-POVM) with the symmetries of a regular tetrahedron.

Example. Consider the group of 3D rotation matrices $\mathfrak{G} = \{\mathbb{1}_3, \mathcal{R}_x(\pi), \mathcal{R}_y(\pi), \mathcal{R}_z(\pi)\}$, where $\mathcal{R}_j(\theta)$ represents a rotation by an angle θ about the j-axis. By acting on the vector $\boldsymbol{v}_A = (1,1,1)$, the group $\mathfrak{G}$ generates the vertices A, B, C, and D of a regular tetrahedron, with corresponding position vectors $\{\boldsymbol{v}_\alpha\}_\alpha$ ($\alpha = A, B, C, D$), represented in Fig. 1. The group $\mathfrak{G}$ forms a subgroup of the tetrahedral group T_d —the full symmetry group of a regular tetrahedron, including both rotations and reflections. The three elements $\mathcal{R}_j(\pi)$ for $j = x, y, z$ correspond to 180-degree rotations about the axes passing through the midpoints of pairs of opposite edges: (AB, CD), (AC, BD), and (AD, BC), respectively.
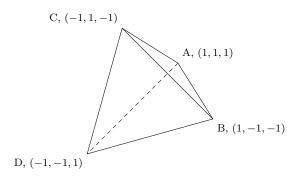

FIG. 1. Regular tetrahedron generated by $\mathfrak{G} = \{\mathbb{1}, \mathcal{R}_x(\pi), \mathcal{R}_y(\pi), \mathcal{R}_z(\pi)\}$ acting on $(1,1,1)$.

This group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, also known as the Klein four-group, with the following multiplication table:

$\mathbb{Z}_2 \times \mathbb{Z}_2$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Explicitly, the isomorphism between the two groups is given by $\mathbb{1} \mapsto e$ and $\mathcal{R}_j(\pi) \mapsto j$, for $j = x, y, z$. To avoid unnecessary proliferation of symbols, we will use the same letters introduced in this table to denote the rotations themselves, as well as the elements of other equivalent representations that will be introduced below.

The family of spin-$\frac{1}{2}$ states, $\{|\boldsymbol{n}_\alpha\rangle \in \mathbb{C}^2\}_\alpha$, where $\boldsymbol{n}_\alpha = \boldsymbol{v}_\alpha/|\boldsymbol{v}_\alpha|$, consists of four qubits whose Bloch vectors point towards the vertices of a regular tetrahedron. These states are important in quantum information theory, as they define a SIC-POVM [41] for qubits, with the corresponding POVM elements given by $\{E_\alpha = (1/2)|\boldsymbol{n}_\alpha\rangle\langle\boldsymbol{n}_\alpha|\}_\alpha$.

The family also defines an ensemble of pure states generated by the action of the group $\mathfrak{G}$, given by $\mathcal{E} = \{U_g|\boldsymbol{n}_A\rangle : g \in \mathcal{G}\}$, where $U_g \in SU(2)$ represents the standard spin-$\frac{1}{2}$ representation of the 3D rotations in $\mathfrak{G}$. Specifically,

$$U_e = \mathbb{1}_2, \quad U_j = -i\sigma_j, \quad j = x, y, z, \tag{S48}$$

with σ_j, $j = x, y, z$, being the Pauli matrices. In terms of the standard $\mathbb{C}^2$ (qubit) basis, the seed state is given by

$$|\boldsymbol{n}_{\mathrm{A}}\rangle = a_- |0\rangle + e^{i\pi/4} a_+ |1\rangle, \tag{S49}$$

where $a_\pm = \left[(3 \pm \sqrt{3})/6 \right]^{1/2}$.

The set $\{ \mathbb{1}_2, -i\sigma_x, -i\sigma_y, -i\sigma_z \}$, more conveniently written as $\{ e, x, y, z \}$, where

$$e := \mathbb{1}_2, \quad j := -i\sigma_j, \quad j = x, y, z, \tag{S50}$$

constitutes a projective representation of the group $\mathfrak{G}$ on $\mathbb{C}^2$. The corresponding multiplication table, $\mathcal{R}$, as defined in Eq. (S38), is given by

$\mathbb{Z}_2 \times \mathbb{Z}_2$	e	x	y	z
e	e	x	y	z
x	x	$-e$	z	$-y$
y	y	$-z$	$-e$	x
z	z	y	$-x$	$-e$

This table clearly reveals that $\omega(g, g^{-1}) = -1$ for $g \neq e$, and thus condition (S35) does not hold in this representation.

We now define an equivalent representation through the map given in Eq. (S34), so that condition (S35) is satisfied. Choosing $\sqrt{-1} = -i$, we obtain the mapping:

$$e \mapsto \mathbb{1}_2, \qquad j \mapsto \frac{-i\sigma_j}{\sqrt{-1}} = \sigma_j, \quad j = x, y, z. \tag{S51}$$

The set $\{ \mathbb{1}_2, \sigma_x, \sigma_y, \sigma_z \}$ is a well-known two-dimensional projective irrep of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. This representation, often referred to as the Pauli representation, is closely related to the quaternion group, as the Pauli matrices satisfy multiplication rules analogous to those of the quaternions.

In the example at hand, the use of the Pauli representation is equivalent to assigning phase factors to three of the original states in the ensemble $\mathcal{E}$. Specifically, it replaces the states $|\boldsymbol{n}_{\mathrm{B}}\rangle$, $|\boldsymbol{n}_{\mathrm{C}}\rangle$, and $|\boldsymbol{n}_{\mathrm{D}}\rangle$ from the original ensemble by the physically equivalent states $i|\boldsymbol{n}_{\mathrm{B}}\rangle$, $i|\boldsymbol{n}_{\mathrm{C}}\rangle$, and $i|\boldsymbol{n}_{\mathrm{D}}\rangle$, respectively.

Denoting $\{ \mathbb{1}_2, \sigma_x, \sigma_y, \sigma_z \}$ by the symbols e, x, y, and z for conciseness, the table $\mathcal{R}$ of the Pauli representation is given by

$\mathbb{Z}_2 \times \mathbb{Z}_2$	e	x	y	z
e	e	x	y	z
x	x	e	iz	$-iy$
y	y	$-iz$	e	ix
z	z	iy	$-ix$	e

From this table, we immediately obtain the canonical Gram matrix structure of any ensemble generated by any projective representation equivalent to the Pauli matrices:

$$G = \begin{pmatrix} 1 & c_x & c_y & c_z \\ c_x & 1 & ic_z & -ic_y \\ c_y & -ic_z & 1 & ic_x \\ c_z & ic_y & -ic_x & 1 \end{pmatrix}, \qquad c_j \in \mathbb{R}, \ j = x, y, z, \quad G \geq 0. \tag{S52}$$

For the SIC-POVM set of equiprobable pure states $\{ |\boldsymbol{n}_{\mathrm{A}}\rangle, i|\boldsymbol{n}_{\mathrm{B}}\rangle, i|\boldsymbol{n}_{\mathrm{C}}\rangle, i|\boldsymbol{n}_{\mathrm{D}}\rangle \}$, the Gram matrix takes the specified form with $c_x = c_y = c_z = 1/\sqrt{3}$. A different choice of seed state would result in different values for the real coefficients c_j, but the overall structure of the Gram matrix is determined solely by the symmetry group and the projective representation that generates the ensemble.

For completeness, we provide the matrices of the right-regular representation, derived from the last table as discussed in Sec. II B:

$$R_e = \mathbb{1}_4, \quad R_x = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}, \quad R_y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \\ 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}, \quad R_z = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{S53}$$

This representation decomposes into two copies of the irreducible 2-dimensional Pauli representation. The unitary matrix that achieves this block diagonalization of the right-regular representation is

$$\mathcal{U} = -\frac{i}{2} \begin{pmatrix} 1 & -1 & i & 1 \\ -1 & 1 & i & 1 \\ -1 & -1 & i & -1 \\ -1 & -1 & -i & 1 \end{pmatrix}. \tag{S54}$$

More explicitly,

$$\mathcal{U} R_j \mathcal{U}^\dagger = \sigma_j \oplus \sigma_j, \quad j = x, y, z. \tag{S55}$$

Since this irrep has dimension 2, the results from the main text imply that the maximum eigenvalue of G is doubly degenerate, ensuring that perfect exclusion is possible for the ensemble $\mathcal{E}$.

IV. OPTIMALITY OF MINIMUM-ERROR EXCLUSION MEASUREMENT

To prove the optimality of the POVM in Eq.(8) for minimum-error QSE ($\gamma = 1$) outside the region of perfect exclusion, we need to check that the operators $\rho_g/|\mathcal{G}| - Y$, introduced in Eq. (15), with $Y = (1/|\mathcal{G}|) \sum_{g \in \mathcal{G}} U_g |\omega\rangle\langle\omega|\psi\rangle\langle\psi|U_g^\dagger$, are positive semidefinite for all $g \in \mathcal{G}$. Due to group covariance, it suffices to check that positive semidefiniteness holds for $|\psi\rangle\langle\psi| - |\mathcal{G}|Y$, since

$$U_g \left(|\psi\rangle\langle\psi| - |\mathcal{G}|Y\right) U_g^\dagger = |\mathcal{G}| \left(\frac{|\psi_g\rangle\langle\psi_g|}{|\mathcal{G}|} - Y \right) = |\mathcal{G}| \left(\frac{\rho_g}{|\mathcal{G}|} - Y \right). \tag{S56}$$

To do so, we define

$$\beta_k^\mu := \sqrt{\frac{\alpha_k^\mu}{|\mathcal{G}|}}; \quad \zeta := \sqrt{|\mathcal{G}|} \langle\psi|\omega\rangle = \beta_1^1 - \sum_{\mu \neq 1} \sum_{k=1}^{r_\mu} d_\mu \beta_k^\mu; \quad |\xi_k^\mu\rangle := |v_k^\mu\rangle|u_k^\mu\rangle; \tag{S57}$$

where $\{|v_k^\mu\rangle\}_{k=1}^{d_\mu}$, $\{|u_k^\mu\rangle\}_{k=1}^{m_\mu}$ are the (Schmidt) bases introduced in Eq. (3). Recall that the irrep $\mu = 1$ corresponds to the largest eigenvalue of the ensemble operator Ω, see Eq. (4), and necessarily has dimension $d_1 = 1$ in the region considered, so $\zeta > 0$. By the Great Orthogonality Theorem, Eq.(S22), the operator $|\mathcal{G}|Y$ can be express as

$$|\mathcal{G}|Y = \left(\beta_1^1\right)^2 |\xi_1^1\rangle\langle\xi_1^1| - \zeta \sum_{\mu \neq 1} \sum_{k=1}^{r_\mu} \beta_k^\mu \left(d_\mu |\xi_1^1\rangle\langle\xi_1^1| + |\xi_k^\mu\rangle\langle\xi_k^\mu| \right) - \left(\sum_{\mu \neq 1} \sum_{k=1}^{r_\mu} d_\mu \beta_k^\mu \right)^2 |\xi_1^1\rangle\langle\xi_1^1| - \zeta Z, \tag{S58}$$

where Z is the positive semidefinite operator

$$Z = \sum_{\mu \neq 1} \sum_{j=1}^{r_\mu} \sum_{\substack{k=1 \\ k \neq j}}^{d_\mu} \beta_j^\mu |v_k^\mu\rangle\langle v_k^\mu| \otimes |u_j^\mu\rangle\langle u_j^\mu|. \tag{S59}$$

The seed state of the ensemble is $|\psi\rangle = \sum_\mu \sqrt{d_\mu}(|\psi_\mu\rangle/\sqrt{|\mathcal{G}|})$, and from Eq. (3), $|\psi_\mu\rangle/\sqrt{|\mathcal{G}|} = \sum_{k=1}^{r_\mu} \beta_k^\mu |\xi_k^\mu\rangle$. Using this and Eq. (S58) we obtain

$$|\psi\rangle\langle\psi| - |\mathcal{G}|Y = \zeta Z + \zeta \sum_{\mu \neq 1} \sum_{k=1}^{r_\mu} \beta_k^\mu |\phi_k^\mu\rangle\langle\phi_k^\mu| + |\Psi\rangle\langle\Psi|, \tag{S60}$$

where

$$|\phi_k^\mu\rangle := \sqrt{d_\mu}|\xi_1^1\rangle + |\xi_k^\mu\rangle; \quad |\Psi\rangle := \sum_{\mu \neq 1} \sum_{k=1}^{r_\mu} \sqrt{d_\mu} \beta_k^\mu |\phi_k^\mu\rangle. \tag{S61}$$

Since each term on the right-hand side of Eq. (S60) is positive semidefinite, it follows that $|\psi\rangle\langle\psi| - |\mathcal{G}|Y \geq 0$, proving the optimality of the POVM generated by the seed state $|\omega\rangle$ in Eq. (8). ∎

V. OPTIMALITY OF UNAMBIGUOUS EXCLUSION POVM

In this section, we prove that the POVM seed state given in Eqs. (8) and (9) is optimal, i.e., it minimizes the failure probability Q.

The primal SDP in Eq. (2) specializes to the group-covariant scenario at hand as

$$\min_{E \geq 0} \ 1 - \mathrm{Tr}(\Omega E), \quad \text{subject to } \mathbb{1} - \sum_{g \in \mathcal{G}} U_g E U_g^\dagger \geq 0, \ \langle \psi | E | \psi \rangle = 0, \tag{S62}$$

where E is the POVM seed operator, satisfying $\Pi_g = U_g E U_g^\dagger$ for all $g \in \mathcal{G}$, with no assumption on the rank of E at this stage. The corresponding dual SDP is given in Eq. (16):

$$\max_{X \geq 0} \ 1 - \mathrm{Tr}(X), \quad \text{subject to } \sum_{g \in \mathcal{G}} U_g X U_g^\dagger + \nu |\psi\rangle\langle\psi| - \Omega \geq 0, \ \nu \in \mathbb{R}. \tag{S63}$$

It can be verified that the dual problem satisfies the Slater conditions [34, 35], i.e., the constraint set in Eq. (S63) has a strictly feasible point, ensuring strong duality. In other words, the primal and dual problem yield the same objective value. However, the primal problem lacks a strictly feasible solution due to the rank-deficient constraint on E, creating an asymmetry in the Slater conditions between the two programs. As noted in [35], such asymmetry can result in situations where the solution to one problem may not be strictly attainable. This is the case here, and complementary slackness cannot be used to derive the dual solution from the primal one.

To address this, we propose an ansatz for X that provides a lower bound on the optimal inconclusive probability. We show below that this lower bound matches the upper bound Q^{prim} from Eq. (6) in a specific limit. Our ansatz is

$$X = \bigoplus_{\mu \neq 1} \mathbb{1}_{d_\mu} \otimes \sum_{k=1}^{r_\mu} \left[\beta_k^\mu \left(\beta_k^\mu + \Delta \right) + \frac{\varepsilon}{d_\Lambda} \delta_{\mu,\Lambda} \delta_{k,r_\Lambda} \right] |u_k^\mu\rangle\langle u_k^\mu|, \tag{S64}$$

where $\Delta := \sum_{\mu \neq 1} \sum_{k=1}^{r_\mu} d_\mu \beta_k^\mu$, ε is an arbitrary positive constant, and the coefficients β_k^μ are defined in Eq. (S57). We adhere to the notation of the main text and order the eigenvalues of the ensemble operator Ω (and the Gram matrix G) in decreasing order, from largest to smallest. Following this convention, the indices $\mu = \Lambda$, $k = r_\Lambda$ correspond to (any of) the smallest nonzero eigenvalue(s) of Ω. We obtain

$$1 - \mathrm{Tr}(X) = 1 - \sum_{\mu \neq 1} d_\mu \sum_{k=1}^{r_\mu} \beta_k^\mu (\beta_k^\mu + \Delta) - \varepsilon = (\beta_1^1)^2 - \Delta^2 - \varepsilon = Q^{\mathrm{prim}} - \varepsilon, \tag{S65}$$

where we have used the normalization condition of the seed state $|\psi\rangle$:

$$1 = \sum_\mu d_\mu \sum_{k=1}^{r_\mu} (\beta_k^\mu)^2. \tag{S66}$$

We next prove that for any $\varepsilon > 0$, X is feasible. Since X is group-invariant, the condition in Eq. (S63) simplifies to

$$X + \nu |\psi\rangle\langle\psi| - \frac{\Omega}{|\mathcal{G}|} \geq 0, \tag{S67}$$

where we have rescaled ν to absorb the constant factor $|\mathcal{G}|$. We need to show that for any $\varepsilon > 0$, there exists ν such that Eq. (S67) holds. Since we are interested in the limit $\varepsilon \to 0^+$ and expect $\nu = \mathcal{O}(\varepsilon^{-1})$ in this limit, we write $\nu = \tilde{\nu}/\varepsilon$, where $\tilde{\nu}$ is a positive constant (of order one). Using some of the definitions introduced in Eq. (S57), we can write

$$X + \frac{\tilde{\nu}}{\varepsilon} |\psi\rangle\langle\psi| - \frac{\Omega}{|\mathcal{G}|} = \Delta Z + \frac{\varepsilon}{d_\Lambda} \left(\sum_{\substack{k=1 \\ k \neq r_\Lambda}}^{d_\Lambda} |v_k^\Lambda\rangle\langle v_k^\Lambda| \right) \otimes |u_{r_\Lambda}^\Lambda\rangle\langle u_{r_\Lambda}^\Lambda| + K, \tag{S68}$$

where

$$K := \frac{\tilde{\nu}}{\varepsilon}|\psi\rangle\langle\psi| - (\beta_1^1)^2|\xi_1^1\rangle\langle\xi_1^1| + \sum_{\mu\neq 1}\sum_{k=1}^{r_\mu}\left(\beta_k^\mu\Delta + \frac{\varepsilon}{d_\Lambda}\delta_{\mu,\Lambda}\delta_{k,r_\Lambda}\right)|\xi_k^\mu\rangle\langle\xi_k^\mu|. \tag{S69}$$

Since the first two operators on the right-hand side of Eq. (S68) are manifestly positive semidefinite, the feasibility of X reduces to proving the positive definiteness of K, which we now proceed to do.

To obtain clearer expressions, we introduce a new notation: we assign a single integer index to replace each pair (μ, k), and write, e.g., β_p and $|p\rangle$ instead of β_k^μ and $|\xi_k^\mu\rangle$, respectively. The integer indices are assigned such that $\beta_1 (= \beta_1^1) > \beta_2 \geq \beta_3 \geq \cdots \geq \beta_N (= \beta_{r_\Lambda}^\Lambda) > 0$. In this notation, Eq. (S69) becomes:

$$K = \frac{\tilde{\nu}}{\varepsilon}\sum_{p,q=1}^{N}\sqrt{d_p d_q}\,\beta_p\beta_q|p\rangle\langle q| - (\beta_1)^2|1\rangle\langle 1| + \sum_{p>1}^{N}\left(\beta_p\sum_{q>1}^{N}d_q\beta_q + \frac{\varepsilon}{d_N}\delta_{p,N}\right)|p\rangle\langle p|, \tag{S70}$$

from which the matrix of K is easily obtained. This allows us to compute its pivots through row elimination and, in turn, its leading principal minors. Denoting these minors by $\det K_l$, where l is the order of the corresponding submatrix, we obtain the following:

$$\det K_1 = \frac{\tilde{\nu}}{\varepsilon}\beta_1^2 + \mathcal{O}(1), \tag{S71}$$

$$\det K_l = \frac{\tilde{\nu}}{\varepsilon}\beta_1^2\left(\prod_{p=2}^{l}\beta_p\right)\left(\sum_{p=l+1}^{N}d_p\beta_p\right)\left(\sum_{p=2}^{N}d_p\beta_p\right)^{l-2} + \mathcal{O}(1), \quad 2 \leq l \leq N-1, \tag{S72}$$

$$\det K_N = \tilde{\nu}\beta_1^2\left(\prod_{p=2}^{N}\beta_p\right)\left(\sum_{p=2}^{N}d_p\beta_p\right)^{N-3} + \mathcal{O}(1), \tag{S73}$$

where the terms that depend on $\tilde{\nu}$ are explicitly shown. Thus, for any $\varepsilon > 0$, and independently of the $\mathcal{O}(1)$ terms, these minors can be made strictly positive by choosing $\tilde{\nu}$ sufficiently large. Hence, by Sylvester's criterion [33], K is positive definite for this choice of $\tilde{\nu}$.

In summary, we have shown that for any $\varepsilon > 0$, the following inequality holds:

$$Q^{\text{prim}} - \varepsilon \leq Q^* \leq Q^{\text{prim}}, \tag{S74}$$

where Q^* denotes the optimal probability of obtaining an inconclusive outcome. Taking the limit $\varepsilon \to 0^+$, we obtain the final result: $Q^* = Q^{\text{prim}} = Q^{\text{min}}$. ∎