Conclusive exclusion of quantum states

Somshubhro Bandyopadhyay,[1] Rahul Jain,[2] Jonathan Oppenheim,[2,3] and Christopher Perry[3,*]

[1]*Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Block EN, Sector V, Bidhan Nagar, Kolkata 700091, India*

[2]*Department of Computer Science and Centre for Quantum Technologies, National University of Singapore, Singapore 119615*

[3]*Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom*

(Received 21 June 2013; published xxxxxx)

In the task of quantum state exclusion, we consider a quantum system prepared in a state chosen from a known set. The aim is to perform a measurement on the system which can conclusively rule that a subset of the possible preparation procedures cannot have taken place. We ask what conditions the set of states must obey in order for this to be possible and how well we can complete the task when it is not. The task of quantum state discrimination forms a subclass of this set of problems. Within this paper, we formulate the general problem as a semidefinite program (SDP), enabling us to derive sufficient and necessary conditions for a measurement to be optimal. Furthermore, we obtain a necessary condition on the set of states for exclusion to be achievable with certainty, and we give a construction for a lower bound on the probability of error. This task of conclusively excluding states has gained importance in the context of the foundations of quantum mechanics due to a result from Pusey, Barrett, and Rudolph (PBR). Motivated by this, we use our SDP to derive a bound on how well a class of hidden variable models can perform at a particular task, proving an analog of Tsirelson's bound for the PBR experiment and the optimality of a measurement given by PBR in the process. We also introduce variations of conclusive exclusion, including unambiguous state exclusion, and state exclusion with worst-case error.

DOI: 10.1103/PhysRevA.00.002300 PACS number(s): 03.67.Ac, 03.65.Ta, 03.65.Ud

I. INTRODUCTION

Suppose we are given a single-shot device, guaranteed to prepare a system in a quantum state chosen at random from a finite set of k known states. In the quantum state discrimination problem, we would attempt to identify the state that has been prepared. It is a well-known result [1] that this can be done with certainty if and only if all of the states in the set of preparations are orthogonal to one another. By allowing inconclusive measurement outcomes [2–4] or accepting some error probability [5–7], strategies can be devised to tackle the problem of discriminating between nonorthogonal states. For a recent review of quantum state discrimination, see [8]. What, however, can we deduce about the prepared state with certainty?

Through state discrimination we effectively attempt to increase our knowledge of the system so that we progress from knowing it is one of k possibilities to knowing it is one particular state. We reduce the size of the set of possible preparations that could have occurred from k to 1. A related and less ambitious task would be to exclude m preparations from the set, reducing the size of the set of potential states from k to $k-m$. If we rule out the m states with certainty, we say that they have been conclusively excluded. Conclusive exclusion of a single state is not only interesting from the point of view of the theory of measurement, but it is becoming increasingly important in the foundations of quantum theory. It has previously been considered with respect to quantum state compatibility criteria between three parties [9], where Caves *et al.* derive necessary and sufficient conditions for conclusive exclusion of a single state from a set of three pure states to be possible. More recently, it has found use in investigating the plausibility of ψ-epistemic theories describing quantum mechanics [10].

As recognized in [10] for the case of single state exclusion, the problem of conclusive exclusion can be formulated in the framework of semidefinite programs (SDPs). As well as being efficiently numerically solvable, SDPs also offer a structure that can be exploited to derive statements about the underlying problem they describe [11,12]. This has already been applied to the problem of state discrimination [13–15]. Given that minimum error state discrimination forms a subclass ($m = k-1$) of the general exclusion framework, it is reasonable to expect that a similar approach will pay dividends here.

For minimum error state discrimination, SDPs provide a route to produce necessary and sufficient conditions for a measurement to be optimal. Similarly, the SDP formalism can be applied to obtain such conditions for the task of minimum error state exclusion, and we derive these in this paper. By applying these requirements to exclusion problems, we have a method for proving whether a given measurement is optimal for a given ensemble of states.

From the SDP formalism, it is also possible to derive necessary conditions for m-state conclusive exclusion to be possible for a given set of states and lower bounds on the probability of error when it is not. A special case of this result is the fact that state discrimination cannot be achieved when the set of states under consideration are nonorthogonal. By regarding perfect state discrimination as $(k-1)$-state conclusive exclusion, we rederive this result.

As an application of our SDP and its properties, we consider a game, motivated by the argument, due to PBR [10], against a class of hidden variable theories. Assume that we have a physical theory, not necessarily that of quantum mechanics, such that, when we prepare a system, we describe it by a state, χ. If our theory were quantum mechanics, then χ would be identified with $|\psi\rangle$, the usual quantum state. Furthermore,

*Corresponding author: christopher.perry.12@ucl.ac.uk

suppose that χ does not give a complete description of the system. We assume that such a description exists, although it may always be unknown to us, and we denote it by λ. As χ is an incomplete description of the system, it will be compatible with many different complete states. We denote these states $\lambda \in \Lambda_\chi$. PBR investigate whether for distinct quantum descriptions, $|\psi_0\rangle$ and $|\psi_1\rangle$, it is possible that $\Lambda_{|\psi_0\rangle} \cap \Lambda_{|\psi_1\rangle} \neq \emptyset$. Models that satisfy this criterion are called ψ-epistemic; see [16] for a full description.

Consider now the following scenario. Alice gives Bob a system prepared according to one of two descriptions, χ_1 or χ_2, and Bob's task is to identify which preparation he has been given. Bob observes the system and will identify the wrong preparation with probability q. Note that $0 \leqslant q \leqslant 1/2$, as Bob will always have the option of randomly guessing the description without performing an observation. If $\Lambda_{\chi_1} \cap \Lambda_{\chi_2} \neq \emptyset$, then, even if Bob has access to the complete description of the system, λ, $q > 0$ as there will exist λ compatible with both χ_1 and χ_2.

Now suppose Bob is given n such systems prepared independently, and we represent the preparation as a string in $\{0,1\}^n$. Bob's task is to output such an n-bit string, and he wins if his is not identical to the string corresponding to Alice's preparation, i.e., he attempts to exclude one of the 2^n preparations. We refer to this as the "PBR game" and we will consider two scenarios for playing it. Under the first scenario, Bob can only perform measurements on each system individually. We refer to this as the separable version of the game. In the second scenario, we allow Bob to perform global measurements on the n systems he receives. We refer to this as the global version, and we are interested in how well quantum theory performs in this case. We shall make a key assumption of PBR, namely that the global complete state of n independent systems, Ω, is given by the tensor product of the individual systems' complete states. This second, quantum, task is related to the problem of "Hedging bets with correlated quantum strategies" as introduced in [17] and expanded upon in [18].

By calculating Bob's probability of success in the PBR game under each of these schemes, we gain a measure of how the predictions of quantum mechanics compare with the predictions of theories in which both $\Lambda_{\chi_1} \cap \Lambda_{\chi_2} \neq \emptyset$ and $\Omega = \otimes_{i=1}^n \lambda_i$ hold. As such, the result can be seen as similar in spirit to Tsirelson's bound [19] in describing how well quantum-mechanical strategies can perform at the CHSH game.

This paper is organized as follows. First, in Sec. II, we formulate the quantum state exclusion problem as an SDP, developing the structure we will need to analyze the task. Next, in Sec. III, we derive sufficient and necessary conditions for a measurement to be optimal in performing conclusive exclusion. It is these conditions that will assist us in investigating the entangled version of the PBR game. In Sec. IV, we derive a necessary condition on the set of possible states for single-state exclusion to be possible, and in Sec. V we give a lower bound on the probability of error when it is not. We apply the SDP formalism to the PBR game in Sec. VI and use it to quantify the discrepancy between the predictions of a class of hidden variable theories and those of quantum mechanics. Finally, in Sec. VII, we present alternative formulations of state exclusion and construct the relevant SDPs.

II. THE STATE EXCLUSION SDP

More formally, what does it mean to be able to perform conclusive exclusion? We first consider the case of single-state exclusion and then show how it generalizes to m-state exclusion. Let the set of possible preparations on a d-dimensional quantum system be $\mathcal{P} = \{\rho_i\}_{i=1}^k$ and let each preparation occur with probability p_i. For brevity of notation, we define $\tilde{\rho}_i = p_i \rho_i$. Call the prepared state σ. The aim is to perform a measurement on σ so that, from the outcome, we can state $j \in \{1,\ldots,k\}$ such that $\sigma \neq \rho_j$.

Such a measurement will consist of k measurement operators, one for attempting to exclude each element of $\mathcal{P}$. We want a measurement, described by $\mathcal{M} = \{M_i\}_{i=1}^k$, that never leads us to guess j when $\sigma = \rho_j$. We need

$$\mathrm{Tr}\,[\rho_i M_i] = 0, \quad \forall\, i, \tag{1}$$

or equivalently, since ρ_i and M_i are positive-semidefinite matrices and p_i is a positive number,

$$\alpha = \sum_{i=1}^{k} \mathrm{Tr}[\tilde{\rho}_i M_i] = 0. \tag{2}$$

There will be some instances of $\mathcal{P}$ for which an $\mathcal{M}$ cannot be found to satisfy Eq. (2). In these cases, our goal is to minimize α, which corresponds to the probability of failure of the strategy, "if outcome j occurs, say $\sigma \neq \rho_j$."

Therefore, to obtain the optimal strategy for single-state exclusion, our goal is to minimize α over all possible $\mathcal{M}$ subject to $\mathcal{M}$ forming a valid measurement. Such an optimization problem can be formulated as an SDP:

$$\begin{aligned} &\underset{\mathcal{M}}{\text{Minimize:}}\ \alpha = \sum_{i=1}^{k} \mathrm{Tr}\,[\tilde{\rho}_i M_i]\,. \\ &\text{Subject to: } \sum_{i=1}^{k} M_i = \mathbb{I}, \\ &M_i \geqslant 0, \quad \forall\, i. \end{aligned} \tag{3}$$

Here $\mathbb{I}$ is the d by d identity matrix and $A \geqslant 0$ implies that A is a positive-semidefinite matrix. The constraint $\sum_{i=1}^k M_i = \mathbb{I}$ corresponds to the fact that the M_i form a complete measurement and we do not allow inconclusive results.

Part of the power of the SDP formalism lies in constructing a "dual" problem to this "primal" problem given in Eq. (3). Details on the formation of the dual problem to the exclusion SDP can be found in Appendix A, and we state it here:

$$\begin{aligned} &\underset{N}{\text{Maximize:}}\ \beta = \mathrm{Tr}\,[N]\,, \\ &\text{Subject to: } N \leqslant \tilde{\rho}_i, \quad \forall\, i, \\ &N \in \text{Herm}. \end{aligned} \tag{4}$$

For single-state exclusion, the problem is essentially to maximize the trace of a Hermitian matrix N subject to $\tilde{\rho}_i - N$ being a positive-semidefinite matrix, $\forall\, i$.

What of m-state conclusive exclusion? Define $Y_{(k,m)}$ to be the set of all subsets of the integers $\{1,\ldots,k\}$ of size m. The aim is to perform a measurement on σ such that from the outcome we can state a set, $Y \in Y_{(k,m)}$, such that $\sigma \notin \{\rho_y\}_{y\in Y}$. Such a measurement, denoted $\mathcal{M}_m$, will consist of $\binom{k}{m}$ measurement operators and we require that, for each set Y,

$$\mathrm{Tr}[\tilde{\rho}_y M_Y] = 0, \quad \forall\, y \in Y. \tag{5}$$

If we define

$$\hat{\rho}_Y = \sum_{y\in Y} \tilde{\rho}_y, \tag{6}$$

then this can be reformulated as requiring

$$\mathrm{Tr}[\hat{\rho}_Y M_Y] = 0, \quad \forall\, Y \in Y_{(k,m)}. \tag{7}$$

Equation (7) is identical in form to Eq. (1). Hence we can view m-state exclusion as single-state exclusion on the set $\mathcal{P}_m = \{\hat{\rho}_Y\}_{Y\in Y_{(k,m)}}$. Furthermore, we can generalize this approach to an arbitrary collection of subsets that are not necessarily of the same size. With this in mind, we restrict ourselves to considering single-state exclusion in all that follows.

The tasks of state exclusion and state discrimination share many similarities. Indeed, if we instead maximize α in Eq. (3) and minimize β in Eq. (4) together with inverting the inequality constraint to read $N \geqslant \tilde{\rho}_i$, we obtain the SDP associated with minimum error state discrimination. It is also possible to recast each problem as an instance of the other. First, state discrimination can be put in the form of an exclusion problem by taking $m = k - 1$ because if we exclude $k - 1$ of the possible states, then we can identify σ as the remaining state.

Following the observation of [20] regarding minimum Bayes cost problems, state exclusion can be converted into a discrimination task. To see this, from $\mathcal{P}$ define

$$\mathcal{R} = \left\{ \vartheta_i = \frac{1}{k-1} \sum_{j\neq i} \tilde{\rho}_j \right\}_{i=1}^{k}. \tag{8}$$

Writing $P_{\mathrm{error}}^{\mathrm{dis}}$ and $P_{\mathrm{error}}^{\mathrm{exc}}$ to distinguish between the probability of error in discrimination and exclusion, in state discrimination on $\mathcal{R}$ we would attempt to minimize

$$P_{\mathrm{error}}^{\mathrm{dis}}(\mathcal{R}) = 1 - \sum_{i=1}^{k} \mathrm{Tr}[\vartheta_i M_i], \tag{9}$$

which can be rearranged to give (see Appendix A 3)

$$P_{\mathrm{error}}^{\mathrm{dis}}(\mathcal{R}) = \frac{k-2}{k-1} + \frac{1}{k-1} P_{\mathrm{error}}^{\mathrm{exc}}(\mathcal{P}). \tag{10}$$

Hence, minimizing the error probability in discrimination on $\mathcal{R}$ is equivalent to minimizing the probability of error in state exclusion on $\mathcal{P}$, and the optimal measurement is the same for both. This interplay between the two tasks enables us to apply bounds on the error probability of state discrimination (see, for example, [21]) to the task of state exclusion.

Returning to the SDP, let us define the optimum solution to the primal problem to be α^* and the solution to the corresponding dual to be β^*. It is a property of all SDPs, known as weak duality, that $\beta \leqslant \alpha$. Furthermore, for SDPs satisfying certain conditions, $\alpha^* = \beta^*$, and this is known as strong duality. The exclusion SDP does fulfill these criteria, as shown in Appendix B 2. Using weak and strong duality allows us to derive properties of the optimal measurement for the problem, a necessary condition on $\mathcal{P}$ for conclusive exclusion to be possible and a bound on the probability of error in performing the task.

III. THE OPTIMAL EXCLUSION MEASUREMENT

Strong duality gives us a method for proving whether a feasible solution, satisfying the constraints of the primal problem, is an optimal solution. If $\mathcal{M}^*$ is an optimal measurement for the conclusive exclusion SDP, then, by strong duality, there must exist a Hermitian matrix N^*, satisfying the constraints of the dual problem, such that

$$\sum_{i=1}^{k} \mathrm{Tr}[\tilde{\rho}_i M_i^*] = \mathrm{Tr}[N^*]. \tag{11}$$

Furthermore, the following is true:

Theorem 1. Suppose a state σ is prepared at random using a preparation from the set $\mathcal{P}$ according to some probability distribution $\{p_i\}_{i=1}^k$. Applying the measurement $\mathcal{M}$ to σ is optimal for attempting to exclude a single element from the set of possible preparations if and only if

$$N = \sum_{i=1}^{k} [\tilde{\rho}_i M_i] \tag{12}$$

is Hermitian and satisfies $N \leqslant \tilde{\rho}_i, \forall\, i$.

The proof of Theorem 1 is given in Appendix B 3 and revolves around the application of strong duality together with a property called complementary slackness. It is similar in construction to Yuen *et al.*'s [7] derivation of necessary and sufficient conditions for showing that a quantum measurement is optimal for minimizing a given Bayesian cost function. This result provides us with a method for proving a measurement is optimal; we construct N according to Eq. (12) and show that it satisfies the constraints of the dual problem. It is this technique that will allow us to analyze the PBR game in the quantum setting.

IV. NECESSARY CONDITION FOR SINGLE-STATE CONCLUSIVE EXCLUSION

Through the application of weak duality, we can also gain insight into the SDP. As the optimal solution to the dual problem provides a lower bound on the solution of the primal problem, any feasible solution to the dual does too, although it may not necessarily be tight. This relation can be summarized as

$$\mathrm{Tr}[N^{\mathrm{feas}}] \leqslant \mathrm{Tr}[N^*] = \beta^* = \alpha^*. \tag{13}$$

In particular, if, for a given $\mathcal{P}$, we can construct a feasible N with $\mathrm{Tr}\,[N] > 0$, then we have $\alpha^* > 0$ and hence conclusive exclusion is not possible.

Constructing such an N gives rise to the following necessary condition on the set $\mathcal{P}$ for conclusive exclusion to be possible:

Theorem 2. Suppose a system is prepared in the state σ using a preparation chosen at random from the set $\mathcal{P} = \{\rho_i\}_{i=1}^k$.

Single-state conclusive exclusion is possible only if

$$\sum_{j\neq l=1}^{k} F(\rho_j,\rho_l) \leqslant k(k-2), \tag{14}$$

where $F(\rho_j,\rho_l)$ is the fidelity between states ρ_j and ρ_l.

The full proof of this theorem is given in Appendix C 1, but we sketch it here. Define N as follows:

$$N = -p\sum_{r=1}^{k}\rho_r + \frac{1-\epsilon}{k-2}p \times \sum_{1\leqslant j<l\leqslant k}(\sqrt{\rho_j}U_{jl}\sqrt{\rho_l} + \sqrt{\rho_l}U_{jl}^{*}\sqrt{\rho_j}), \tag{15}$$

where the U_{jl} are unitary matrices chosen such that

$$\mathrm{Tr}\,[N] = -kp + \frac{1-\epsilon}{k-2}p\sum_{j\neq l=1}^{k}F(\rho_j,\rho_l). \tag{16}$$

N is Hermitian, and for suitable p and ϵ it can be shown that $\rho_i - N \geqslant 0, \forall\, i$. Equation (14) follows by determining when $\mathrm{Tr}[N] > 0$ and letting $\epsilon \to 0$. Note that the probability with which states are prepared, $\{p_i\}_{i=1}^{k}$, has no impact on whether conclusive exclusion is possible or not.

This is only a necessary condition for single-state conclusive exclusion, and there exist sets of states that satisfy Eq. (14) for which it is not possible to perform conclusive exclusion. Nevertheless, there exist sets of states on the cusp of satisfying Eq. (14) for which conclusive exclusion is possible. For example, the set of states of the form

$$|\psi_i\rangle = \sum_{j\neq i}^{k}\frac{1}{\sqrt{k-1}}|j\rangle \tag{17}$$

for $i = 1$ to k can be conclusively excluded by the measurement in the orthonormal basis $\{|i\rangle\}_{i=1}^{k}$, and yet

$$\sum_{j\neq l=1}^{k}F(|\psi_j\rangle\langle\psi_j|,|\psi_l\rangle\langle\psi_l|) = \sum_{j\neq l=1}^{k}|\langle\psi_j|\psi_l\rangle| = k(k-2). \tag{18}$$

It can be shown that the necessary condition for conclusive state discrimination can be obtained from Theorem 2, and the interested reader can find this derivation in Appendix C 2.

V. LOWER BOUND ON THE PROBABILITY OF ERROR

Weak duality can also be used to obtain the following lower bound on α^*:

Theorem 3. For two Hermitian operators, A and B, define $\min(A,B)$ to be

$$\min(A,B) = \tfrac{1}{2}[A + B - |A - B|]. \tag{19}$$

Given a set of states $\mathcal{P} = \{\rho_i\}_{i=1}^{k}$ prepared according to some probability distribution $\{p_i\}_{i=1}^{k}$ and a permutation ε, acting on k objects, taken from the permutation group S_k, consider

$$N_\varepsilon = \min(\tilde{\rho}_{\varepsilon(k)}, \min(\tilde{\rho}_{\varepsilon(k-1)}, \min(\ldots, \min(\tilde{\rho}_{\varepsilon(2)}, \tilde{\rho}_{\varepsilon(1)})))). \tag{20}$$

Then

$$\alpha^* \geqslant \max_{\varepsilon\in S_k}: \mathrm{Tr}\,[N_\varepsilon]\,. \tag{21}$$

The proof of this result is given in Appendix C 3 and relies upon showing that $\min(A,B) \leqslant A$ and B, together with the iterative nature of the construction of N_ε. Note that by considering a suitably defined max function, analogous to the min used in Theorem 3, it is possible to derive a similar style of bound for the task of minimum error state discrimination. We omit it here, however, as it is beyond the scope of this paper.

VI. THE PBR GAME

We now turn our attention to the PBR game. Suppose Alice gives Bob n systems whose preparations are encoded by the string $\vec{x} \in \{0,1\}^n$. The state of system i is χ_{x_i}. Bob's goal is to produce a string $\vec{y} \in \{0,1\}^n$ such that $\vec{x} \neq \vec{y}$.

A. Separable version

In the first scenario, where Bob can only observe each system individually and we consider a general theory, we can represent his knowledge of the global system by

$$\Gamma = \gamma_1 \otimes \cdots \otimes \gamma_n, \tag{22}$$

with $\gamma_i \in \{\Gamma_0,\Gamma_1,\Gamma_?\}$, representing his three possible observation outcomes. If $\gamma_i \in \Gamma_0$, he is certain the system preparation is described by χ_0; if $\gamma_i \in \Gamma_1$, he is certain the system preparation is described by χ_1; and if $\gamma_i \in \Gamma_?$, he remains uncertain whether the system was prepared in state χ_0 or χ_1 and he may make an error in assigning a preparation to the system. We denote the probability that Bob, after performing his observation, assigns the wrong preparation description to the system as q. Provided that $\Gamma_? \neq \emptyset$, then $q > 0$.

Bob will win the game if for at least one individual system he assigns the correct preparation description. His strategy is to attempt to identify each value of x_i and choose y_i such that $y_i \neq x_i$. Bob's probability of outputting a winning string is hence

$$P_{\mathrm{win}}^{S} = 1 - q^n. \tag{23}$$

B. Global version

Now consider the second scenario. When the theory is quantum and global (i.e., entangled), measurements on the global system are allowed. We can write the global state that Alice gives Bob, labeled by $\vec{x}$, as

$$|\Psi_{\vec{x}}\rangle = \bigotimes_{i=1}^{n}|\psi_{x_i}\rangle. \tag{24}$$

Bob's task can now be regarded as attempting to perform single-state conclusive exclusion on the set of states $\mathcal{P} = \{|\Psi_{\vec{x}}\rangle\}_{\vec{x}\in\{0,1\}^n}$; he outputs the string associated with the state he has excluded to have the best possible chance of winning the game.

To calculate his probability of winning P_{win}^{G}, we need to construct and solve the associated SDP. Without loss of generality, we can take the states $|\psi_0\rangle$ and $|\psi_1\rangle$ to be defined as

$$|\psi_0\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle,$$
$$|\psi_1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle - \sin\left(\frac{\theta}{2}\right)|1\rangle, \quad (25)$$

where $0 \leqslant \theta \leqslant \pi/2$. The global states $|\Psi_{\vec{x}}\rangle$ are then given by

$$|\Psi_{\vec{x}}\rangle = \sum_{\vec{r}}(-1)^{\vec{x}\cdot\vec{r}}\left[\cos\left(\frac{\theta}{2}\right)\right]^{n-|\vec{r}|}\left[\sin\left(\frac{\theta}{2}\right)\right]^{|\vec{r}|}|\vec{r}\rangle, \quad (26)$$

where $\vec{r} \in \{0,1\}^n$ and $|\vec{r}| = \sum_{i=1}^n r_i$.

From [10], we know that single-state conclusive exclusion can be performed on this set of states provided θ and n satisfy the condition

$$2^{1/n} - 1 \leqslant \tan\left(\frac{\theta}{2}\right). \quad (27)$$

When this relation holds, $P_{\text{win}}^G = 1$. What, however, happens outside of this range? While strong numerical evidence is given in [10] that it will be the case that $P_{\text{win}}^G < 1$, can it be shown analytically?

Through analyzing numerical solutions to the SDP (performed using [22,23]), there is evidence to suggest that the optimum measurement to perform when Eq. (27) is not satisfied is given by the projectors

$$|\zeta_{\vec{x}}\rangle = \frac{1}{\sqrt{2^n}}\left(|\vec{0}\rangle - \sum_{\vec{r}\neq\vec{0}}(-1)^{\vec{x}\cdot\vec{r}}|\vec{r}\rangle\right), \quad (28)$$

which are independent of θ. That the set $\{|\zeta_{\vec{x}}\rangle\}_{\vec{x}\in\{0,1\}^n}$ is the optimal measurement for attempting to perform conclusive exclusion is shown in Appendix D.

If we construct N as per Eq. (12) and consider the trace, we can determine how successfully single-state exclusion can be performed. This is done in Appendix D, and we find

$$\text{Tr}[N] = \frac{1}{2^n}\left[\cos\left(\frac{\theta}{2}\right)\right]^{2n}\left\{2 - \left[1 + \tan\left(\frac{\theta}{2}\right)\right]^n\right\}^2. \quad (29)$$

This is strictly positive, and hence we have shown that Eq. (27) is a necessary condition for conclusive exclusion to be possible on the set $\mathcal{P}$.

In summary, we have the following:

If $2^{1/n} - 1 \leqslant \tan\left(\frac{\theta}{2}\right)$,

$P_{\text{win}}^G = 1.$

Otherwise

$$P_{\text{win}}^G = 1 - \frac{1}{2^n}\left[\cos\left(\frac{\theta}{2}\right)\right]^{2n}\left\{2 - \left[1 + \tan\left(\frac{\theta}{2}\right)\right]^n\right\}^2, \quad (30)$$

which characterizes the success probability of the quantum strategy.

C. Comparison

What is the relation between P_{win}^S and P_{win}^G? If, in the separable scenario, we take the physical theory as being quantum mechanics and Bob's error probability as arising from the fact that it is impossible to distinguish between nonorthogonal quantum states, we can write [5]

$$q = \left(\tfrac{1}{2}\right)\left(1 - \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}\right) = \left(\tfrac{1}{2}\right)[1 - \sin(\theta)]. \quad (31)$$

With this substitution, we find that $P_{\text{win}}^S \leqslant P_{\text{win}}^G$, $\forall\, n$. This is unsurprising as the first scenario is essentially the second but with a restricted set of allowable measurements.

Of more interest however, is if we view q as arising from some hidden variable completion of quantum mechanics. If $\Lambda_{|\psi_0\rangle} \cap \Lambda_{|\psi_1\rangle} = \emptyset$, then if an observation of each $|\psi_{x_i}\rangle$ were to allow us to deduce λ_{x_i}, then $q = 0$ and $P_{\text{win}}^S = 1 \geqslant P_{\text{win}}^G$. However, if $\Lambda_{|\psi_0\rangle} \cap \Lambda_{|\psi_1\rangle} \neq \emptyset$, then we have $q > 0$, and P_{win}^S will have the property that Bob wins with certainty only as $n \to \infty$. On the other hand, $P_{\text{win}}^G = 1$ if and only if Eq. (27) is satisfied and we have analytically proven the necessity of the bound obtained by PBR. Furthermore, we have defined a game that allows the quantification of the difference between the predictions of general physical theories, including those that attempt to provide a more complete description of quantum mechanics, and those of quantum mechanics.

VII. ALTERNATIVE MEASURES OF EXCLUSION

There exist multiple strategies and figures of merit when undertaking state discrimination. In addition to considering minimum error discrimination or unambiguous discrimination, further variants may try to minimize the maximum error probability [24] or allow only a certain probability of obtaining an inconclusive measurement result [25]. Similarly, alternative methods to that of minimum error can be defined for state exclusion, and in this section unambiguous exclusion and worst-case error exclusion are defined and the related SDPs given.

A. Unambiguous state exclusion

In unambiguous state exclusion on the set of preparations $\mathcal{P} = \{\tilde{\rho}_i\}_{i=1}^k$, we consider a measurement given by $\mathcal{M} = \{M_1, \ldots, M_k, M_?\}$. If we obtain measurement outcome i ($1 \leqslant i \leqslant k$), then we can exclude with certainty the state ρ_i. However, if we obtain the outcome labeled ?, we cannot infer which state to exclude. We wish to minimize the probability of obtaining this inconclusive measurement:

$$\alpha = \sum_{i=1}^k \text{Tr}[\tilde{\rho}_i M_?], \quad (32)$$

which can be rewritten as

$$\alpha = \text{Tr}\left[\sum_{j=1}^k \tilde{\rho}_j\left(\mathbb{I} - \sum_{i=1}^k M_i\right)\right]. \quad (33)$$

Defining $\tilde{\alpha} = 1 - \alpha$, the primal SDP associated with this task is given by

$$\begin{aligned} &\underset{\mathcal{M}}{\text{Maximize:}}\ \tilde{\alpha} = \text{Tr}\left[\sum_{j=1}^{k}\tilde{\rho}_j\sum_{i=1}^{k}M_i\right].\\ &\text{Subject to: } \sum_{i=1}^{k}M_i \leqslant \mathbb{I},\\ &\qquad \text{Tr}\,[\tilde{\rho}_i M_i] = 0, \quad 1 \leqslant i \leqslant k,\\ &\qquad M_i \geqslant 0, \quad 1 \leqslant i \leqslant k. \end{aligned} \tag{34}$$

Here, the first and third constraints ensure that $\mathcal{M}$ is a valid measurement, while the second, $\text{Tr}\,[\tilde{\rho}_i M_i] = 0,\ 1 \leqslant i \leqslant k$, encapsulates the fact that when measurement outcome i occurs, we should be able to exclude state ρ_i with certainty.

The dual problem can be shown to be (see Appendix E 1)

$$\begin{aligned} &\underset{N,\{a_i\}_{i=1}^k}{\text{Minimize:}}\ \beta = \text{Tr}\,[N].\\ &\text{Subject to: } a_i\tilde{\rho}_i + N \geqslant \sum_{j=1}^{k}\tilde{\rho}_j, \quad 1 \leqslant i \leqslant k,\\ &\qquad a_i \in \mathbb{R}, \quad \forall i,\\ &\qquad N \geqslant 0. \end{aligned} \tag{35}$$

Unambiguous state exclusion has recently found use in implementations of quantum digital signatures [26], enabling such schemes to be put into practice without the need for long-term quantum memory.

B. Worst-case error state exclusion

The goal of the SDP given in Eqs. (3) and (4) is to minimize the average probability of error, over all possible preparations, of the strategy, "if outcome j occurs, say $\sigma \neq \rho_j$." An alternative goal would be to minimize the worst-case probability of error that occurs:

$$\alpha = \max_i \text{Tr}\,[\tilde{\rho}_i M_i]. \tag{36}$$

The primal SDP associated with this task is

$$\begin{aligned} &\underset{\mathcal{M}}{\text{Minimize:}}\ \alpha = \lambda.\\ &\text{Subject to: } \lambda \geqslant \text{Tr}\,[\tilde{\rho}_i M_i], \quad \forall i,\\ &\qquad \sum_{i=1}^{k}M_i = \mathbb{I},\\ &\qquad \lambda \geqslant 0 \in \mathbb{R},\\ &\qquad M_i \geqslant 0, \quad 1 \leqslant i \leqslant k. \end{aligned} \tag{37}$$

These constraints again encode that $\mathcal{M}$ forms a valid measurement and ensure that α picks out the worst-case error probability across all possible preparations.

The associated dual problem is

$$\begin{aligned} &\underset{N,\{a_i\}_{i=1}^k}{\text{Maximize:}}\ \beta = \text{Tr}\,[N],\\ &\text{Subject to: } N \leqslant a_i\tilde{\rho}_i, \quad \forall i,\\ &\qquad \sum_{i=1}^{k}a_i \leqslant 1,\\ &\qquad a_i \geqslant 0 \in \mathbb{R}, \quad \forall i,\\ &\qquad N \in \text{Herm}. \end{aligned} \tag{38}$$

The derivation of this is given in Appendix E 2.

VIII. CONCLUSION

In this paper, we have introduced the task of state exclusion and shown how it can be formulated as an SDP. Using this, we have derived conditions for measurements to be optimal at minimum error state exclusion and a criterion for the task to be performed conclusively on a given set of states. We also gave a lower bound on the error probability. Furthermore, we have applied our SDP to a game which helps to quantify the differences between quantum mechanics and a class of hidden variable theories.

It is an open question, posed in [9], whether a POVM ever outperforms a projective measurement in conclusive exclusion of a single pure state. While it can be shown from the SDP formalism that this is not the case when the states are linearly independent and conclusive exclusion is not possible to the extent that $\text{Tr}\,[M_i\rho_i] > 0,\ \forall\, i$, further work is required to extend it and answer the above question. It would also be interesting to see whether it is possible to find further constraints and bounds, similar to Theorem 2 and Theorem 3, to characterize when conclusive exclusion is possible.

Finally, the main SDP, as given in Eq. (3), is just one method for analyzing state exclusion in which we attempt to minimize the average probability of error. Alternative formulations were presented in Sec. VII, and it would be interesting to study the relationships between them and that defined in Eq. (3).

ACKNOWLEDGMENTS

Part of this work was completed while S.B. and J.O. were visiting the Center for Quantum Technologies, Singapore and while R.J. was visiting the Bose Institute, Kolkata, India. S.B. thanks CQT for their support. The work of R.J. is supported by internal grants at CQT. J.O. is supported by the Royal Society and an EPSRC Established Career fellowship.

APPENDIX A: STATE EXCLUSION SDP FORMULATION

In this Appendix, we give the general definition of an SDP, derive the dual problem for the state exclusion SDP, and show the relation to state discrimination.

1. General SDPs

In this section, we state the general form of a semidefinite program as given in [12]. A semidefinite program is defined by three elements $\{A, B, \Phi\}$. A and B are Hermitian matrices,

$A \in \mathrm{Herm}(\mathcal{X})$ and $B \in \mathrm{Herm}(\mathcal{Y})$, where $\mathcal{X}$ and $\mathcal{Y}$ are complex Euclidean spaces. Φ is a Hermiticity preserving superoperator that takes elements in $\mathcal{X}$ to elements in $\mathcal{Y}$.

From these three elements, two optimization problems can be defined. The primal problem can be defined as

$$\begin{aligned} &\underset{X}{\text{Minimize:}}\ \alpha = \mathrm{Tr}[AX].\\ &\text{Subject to: } \Phi(X) = B,\\ &\qquad X \geqslant 0. \end{aligned} \tag{A1}$$

The dual problem can be defined as

$$\begin{aligned} &\underset{Y}{\text{Maximize:}}\ \beta = \mathrm{Tr}[BY].\\ &\text{Subject to: } \Phi^*(Y) \leqslant A,\\ &\qquad Y \in \mathrm{Herm}(\mathcal{Y}). \end{aligned} \tag{A2}$$

Here Φ^* is the dual map to Φ and is defined by

$$\mathrm{Tr}[Y\Phi(X)] = \mathrm{Tr}[X\Phi^*(Y)]. \tag{A3}$$

We define the optimal solutions to the primal and dual problems to be $\alpha^* = \inf_X \alpha$ and $\beta^* = \sup_Y \beta$, respectively.

2. State exclusion SDP

Looking at the state exclusion primal problem, Eq. (3), we see that for the exclusion SDP, the following holds true:

(i) A is a kd by kd block-diagonal matrix with each d by d block, labeled by i, given by $\tilde{\rho}_i$:

$$A = \begin{pmatrix} \tilde{\rho}_1 & & \\ & \ddots & \\ & & \tilde{\rho}_k \end{pmatrix}.$$

(ii) B is the d by d identity matrix.

(iii) X, the variable matrix, is a kd by kd block-diagonal matrix where we label each d by d block diagonal by M_i:

$$X = \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_k \end{pmatrix}.$$

(iv) Y is the d by d matrix we call N.

(v) The map Φ is given by $\Phi(X) = \sum_i M_i$.

Using Eq. (A3), we see that Φ^* must satisfy

$$\mathrm{Tr}\left[N\sum_{i=1}^{k} M_i\right] = \mathrm{Tr}\left[\begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_k \end{pmatrix}\Phi^*(N)\right],$$

and hence $\Phi^*(N)$ produces a kd by kd block-diagonal matrix with N in each of the block diagonals:

$$\Phi^*(N) = \begin{pmatrix} N & & \\ & \ddots & \\ & & N \end{pmatrix}.$$

Substituting these elements into Eq. (A2), we obtain the dual SDP for state exclusion as stated in Eq. (4) .

3. The relation between state discrimination and state exclusion

Here we give the derivation of Eq. (10).

Given $\mathcal{P}$, we define

$$\mathcal{R} = \left\{\vartheta_i = \frac{1}{k-1}\sum_{j\neq i}\tilde{\rho}_j\right\}_{i=1}^{k}.$$

Then, in state discrimination on $\mathcal{R}$ we would attempt to minimize

$$\begin{aligned} P_{\text{error}}^{\text{dis}}(\mathcal{R}) &= 1 - \sum_{i=1}^{k}\mathrm{Tr}[\vartheta_i M_i],\\ &= 1 - \sum_{i=1}^{k}\sum_{j\neq i}\frac{1}{k-1}\mathrm{Tr}[\tilde{\rho}_j M_i],\\ &= 1 - \frac{1}{k-1}\sum_{i=1}^{k}\sum_{j=1}^{k}\mathrm{Tr}[\tilde{\rho}_j M_i] + \frac{1}{k-1}\sum_{i=1}^{k}\mathrm{Tr}[\tilde{\rho}_i M_i],\\ &= \frac{k-2}{k-1} + \frac{1}{k-1}P_{\text{error}}^{\text{exc}}(\mathcal{P}). \end{aligned}$$

APPENDIX B: STRONG DUALITY

In this appendix, we show that the SDP exhibits strong duality, and we give the proof of Theorem 1 from the main text.

1. Slater's theorem

Slater's theorem provides a means to test whether an SDP satisfies strong duality ($\alpha^* = \beta^*$).

Theorem 4 (Slater's theorem). The following implications hold for every SDP:

(i) If there exists a feasible solution to the primal problem and a Hermitian operator Y for which $\Phi^*(Y) < A$, then $\alpha^* = \beta^*$ and there exists a feasible X^* for which $\mathrm{Tr}[AX^*] = \alpha^*$.

(ii) If there exists a feasible solution to the dual problem and a positive semidefinite operator X for which $\Phi(X) = B$ and $X > 0$, then $\alpha^* = \beta^*$ and there exists a feasible Y^* for which $\mathrm{Tr}[BY^*] = \beta^*$.

2. Slater's theorem applied to the exclusion SDP

To see that the exclusion SDP satisfies the conditions of Slater's theorem, consider $X = \frac{1}{k}\mathbb{I}$ and $N = -\mathbb{I}$ (where the identity matrices are taken to have the correct dimension). X is strictly positive-definite and so it strictly satisfies the constraints of the primal problem. $N < 0$ and hence $N < \tilde{\rho}_i$, $\forall\, i$, so N strictly satisfies the constraints of the dual problem.

3. Necessary and sufficient conditions for a measurement to be optimal

To prove Theorem 1, we will need the following fact about SDPs:

Proposition 1 (complementary slackness). Suppose X and Y, which are feasible for the primal and dual problems, respectively, satisfy $\mathrm{Tr}[AX] = \mathrm{Tr}[BY]$. Then it holds that

$$\Phi^*(Y)X = AX \text{ and } \Phi(X)Y = BY.$$

We now give the proof for Theorem 1.

Proof. Suppose we are given a valid measurement, $\mathcal{M} = \{M_i\}_{i=1}^k$, and that N, defined by

$$N = \sum_{i=1}^{k} \tilde{\rho}_i M_i,$$

satisfies the constraints of the dual problem. Then

$$\begin{aligned}\beta &= \mathrm{Tr}[N],\\ &= \mathrm{Tr}\left[\sum_{i=1}^{k} \tilde{\rho}_i M_i\right],\\ &= \sum_{i=1}^{k} \mathrm{Tr}\left[\tilde{\rho}_i M_i\right],\\ &= \alpha.\end{aligned}$$

Hence, by strong duality, $\mathcal{M}$ is an optimal measurement.

Now suppose $\mathcal{M}$ is an optimal measurement. By Proposition 1, an optimal N satisfies

$$\Phi^*(N)\begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_k\end{pmatrix} = \begin{pmatrix} \tilde{\rho}_1 M_1 & & \\ & \ddots & \\ & & \tilde{\rho}_k M_k\end{pmatrix},$$

$$\Rightarrow \begin{pmatrix} NM_1 & & \\ & \ddots & \\ & & NM_k\end{pmatrix} = \begin{pmatrix} \tilde{\rho}_1 M_1 & & \\ & \ddots & \\ & & \tilde{\rho}_k M_k\end{pmatrix},$$

which implies that

$$NM_i = \tilde{\rho}_i M_i, \quad \forall\, i.$$

Taking the sum over i on both sides and using the fact that $\sum_i M_i = \mathbb{I}$, we obtain

$$N = \sum_{i=1}^{k} \tilde{\rho}_i M_i,$$

as required. ■

APPENDIX C: NECESSARY CONDITIONS AND BOUNDS

In this Appendix, we derive the necessary condition for conclusion exclusion to be possible that was given in Theorem 2 as well as an associated corollary regarding state discrimination. We also present the proof of the bound on the error probability of state exclusion, Theorem 3.

1. Necessary condition for conclusive exclusion

Here we derive the necessary condition for single-state conclusive exclusion to be possible that was given in Theorem 2.

Proof. Suppose that $\mathcal{P} = \{\rho_i\}_{i=1}^k$. A feasible solution to the dual SDP, N, must be Hermitian and satisfy $N \leqslant \rho_i, \forall\, i$. Our goal is to construct such an N with the property $\mathrm{Tr}[N] > 0$. If this is possible, conclusive exclusion is not possible.

First, we define U_{jl} to be a unitary such that $\mathrm{Tr}[\sqrt{\rho_l}\sqrt{\rho_j}U_{jl}] = F(\rho_j,\rho_l)$ and note that $U_{lj} = U_{jl}^*$. We construct N as follows [for $p,\epsilon \in (0,1)$]:

$$N = -p\sum_{r=1}^{k}\rho_r + \frac{1-\epsilon}{k-2}p\sum_{1\leqslant j<l\leqslant k}(\sqrt{\rho_j}U_{jl}\sqrt{\rho_l} + \sqrt{\rho_l}U_{jl}^*\sqrt{\rho_j}),$$

and note that N is Hermitian. Now consider

$$\begin{aligned}\rho_1 - N &= (1+p)\rho_1 + p\sum_{r=2}^{k}\rho_r - \frac{1-\epsilon}{k-2}p\sum_{1\leqslant j<l\leqslant k}(\sqrt{\rho_j}U_{jl}\sqrt{\rho_l} + \sqrt{\rho_l}U_{jl}^*\sqrt{\rho_j}),\\ &= \sum_{r=2}^{k}\left[\frac{1+p}{k-1}\rho_1 + \epsilon p\rho_r - \frac{1-\epsilon}{k-2}p(\sqrt{\rho_1}U_{1r}\sqrt{\rho_r} + \sqrt{\rho_r}U_{1r}^*\sqrt{\rho_1})\right]\\ &\quad + \frac{1-\epsilon}{k-2}p\sum_{2\leqslant j<l\leqslant k}[\rho_j + \rho_l - \sqrt{\rho_j}U_{jl}\sqrt{\rho_l} - \sqrt{\rho_l}U_{jl}^*\sqrt{\rho_j}],\\ &= \sum_{r=2}^{k}\left[\frac{1+p}{k-1}\rho_1 + \epsilon p\rho_r - \frac{1-\epsilon}{k-2}p(\sqrt{\rho_1}U_{1r}\sqrt{\rho_r} + \sqrt{\rho_r}U_{1r}^*\sqrt{\rho_1})\right]\\ &\quad + \frac{1-\epsilon}{k-2}p\sum_{2\leqslant j<l\leqslant k}(\sqrt{\rho_j}\sqrt{U_{jl}} - \sqrt{\rho_l}\sqrt{U_{jl}^*})(\sqrt{U_{jl}^*}\sqrt{\rho_j} - \sqrt{U_{jl}}\sqrt{\rho_l}).\end{aligned}$$

The terms in the second summation on the last line are positive semidefinite. Consider, individually, the terms in the first summation:

$$\begin{aligned}&\frac{1+p}{k-1}\rho_1 + \epsilon p\rho_r - \frac{1-\epsilon}{k-2}p(\sqrt{\rho_1}U_{1r}\sqrt{\rho_r} + \sqrt{\rho_r}U_{1r}^*\sqrt{\rho_1}),\\ &\quad = \left[\frac{1+p}{k-1} - \left(\frac{(1-\epsilon)p}{k-2}\right)^2\frac{1}{\epsilon p}\right]\rho_1 + \left[\left(\frac{(1-\epsilon)p}{k-2}\right)^2\frac{1}{\epsilon p}\right]\rho_1 + \epsilon p\rho_r - \frac{1-\epsilon}{k-2}p(\sqrt{\rho_1}U_{1r}\sqrt{\rho_r} + \sqrt{\rho_r}U_{1r}^*\sqrt{\rho_1}),\end{aligned}$$

$$= \left[\frac{1+p}{k-1} - \left(\frac{(1-\epsilon)p}{k-2}\right)^2 \frac{1}{\epsilon p}\right]\rho_1 + \left(\frac{(1-\epsilon)p}{(k-2)\sqrt{\epsilon p}}\sqrt{\rho_1}\sqrt{U_{1r}} - \sqrt{\epsilon p}\sqrt{\rho_r}\sqrt{U_{1r}^*}\right)$$
$$\times \left(\frac{(1-\epsilon)p}{(k-2)\sqrt{\epsilon p}}\sqrt{U_{1r}^*}\sqrt{\rho_1} - \sqrt{\epsilon p}\sqrt{U_{1r}}\sqrt{\rho_r}\right).$$

Hence, for $\rho_1 - N$ to be positive-semidefinite, we need the first term in the last line to be positive:

$$\left[\frac{1+p}{k-1} - \left(\frac{(1-\epsilon)p}{k-2}\right)^2 \frac{1}{\epsilon p}\right] \geqslant 0,$$
$$\frac{\epsilon}{\frac{(k-1)(1-\epsilon)^2}{(k-2)^2} - \epsilon} \geqslant p. \tag{C1}$$

Therefore, provided p and ϵ satisfy Eq. (C1), $N \leqslant \rho_1$. Similarly, one can argue that $\rho_i \leqslant N$, $\forall\ i$, and hence N is a feasible solution to the dual problem.

We now wish to know under what conditions we have $\mathrm{Tr}[N] > 0$:

$$\mathrm{Tr}[N] > 0,$$
$$\Rightarrow -kp + \frac{1-\epsilon}{k-2}p \sum_{1\leqslant j<l\leqslant k} \mathrm{Tr}[\sqrt{\rho_j}U_{jl}\sqrt{\rho_l} + \sqrt{\rho_l}U_{jl}^*\sqrt{\rho_j}] > 0,$$
$$\Rightarrow \sum_{j\neq l=1}^{k} F(\rho_j,\rho_l) > \frac{k(k-2)}{1-\epsilon}.$$

Letting $\epsilon \to 0$ and using weak duality, we obtain our result. Conclusive exclusion is not possible if $\sum_{j\neq l=1}^{k} F(\rho_j,\rho_l) > k(k-2)$. ■

2. Necessary condition for conclusive state discrimination

Here we show how the necessary condition for perfect state discrimination to be possible can be derived from our necessary condition on conclusive state exclusion, Theorem 2.

Corollary 1. Conclusive state discrimination on the set $\mathcal{P} = \{\rho_i\}_{i=1}^k$ is possible only if $\mathcal{P}$ is an orthogonal set.

Proof. For $\mathcal{P} = \{\rho_i\}_{i=1}^k$, define

$$\hat{\rho}_j = \frac{1}{k-1}\sum_{i\neq j}\rho_i.$$

Let $j \neq l$ and consider

$$A = \frac{1}{k-1}\sum_{r\neq j,l}\rho_r.$$

We first show that $F(\hat{\rho}_j,\hat{\rho}_l) \geqslant F(\hat{\rho}_j,A)$. Consider

$$F(\hat{\rho}_j,A) = \mathrm{Tr}\Big[\sqrt{\sqrt{\hat{\rho}_j}A\sqrt{\hat{\rho}_j}}\Big],$$
$$\leqslant \mathrm{Tr}\Big[\sqrt{\sqrt{\hat{\rho}_j}\hat{\rho}_l\sqrt{\hat{\rho}_j}}\Big],$$
$$= F(\hat{\rho}_j,\hat{\rho}_l).$$

The inequality follows from the following facts:

(i) It can be easily seen from the definitions that $A \leqslant \hat{\rho}_l$.

(ii) If $B \geqslant C$, then $D^*BD \geqslant D^*CD$, $\forall\ D$. Hence

$$\sqrt{\hat{\rho}_j}A\sqrt{\hat{\rho}_j} \leqslant \sqrt{\hat{\rho}_j}\hat{\rho}_l\sqrt{\hat{\rho}_j}.$$

(iii) The square-root function is operator-monotone, so

$$\sqrt{\sqrt{\hat{\rho}_j}A\sqrt{\hat{\rho}_j}} \leqslant \sqrt{\sqrt{\hat{\rho}_j}\hat{\rho}_l\sqrt{\hat{\rho}_j}}.$$

(iv) The trace function is operator-monotone, and so finally

$$\mathrm{Tr}\Big[\sqrt{\sqrt{\hat{\rho}_j}A\sqrt{\hat{\rho}_j}}\Big] \leqslant \mathrm{Tr}\Big[\sqrt{\sqrt{\hat{\rho}_j}\hat{\rho}_l\sqrt{\hat{\rho}_j}}\Big].$$

Using a similar argument to the above, it is possible to show that

$$F(\hat{\rho}_j,A) \geqslant F(A,A) = \frac{k-2}{k-1}.$$

If ρ_j, ρ_l, and A are pairwise orthogonal, then $\hat{\rho}_j$ and $\hat{\rho}_l$ commute and are simultaneously diagonalizable. This means that

$$F(\hat{\rho}_j,\hat{\rho}_l) = ||\sqrt{\hat{\rho}_j}\sqrt{\hat{\rho}_l}||_{\mathrm{Tr}},$$
$$= ||A||_{\mathrm{Tr}},$$
$$= F(A,A),$$
$$= \frac{k-2}{k-1}.$$

Now suppose that ρ_j and A are not orthogonal. We take $\{a_r\}$ to be the eigenvalues and $\{|v_r\rangle\}$ to be the eigenvectors of $\sqrt{A}$, so

$$F(\hat{\rho}_l,A) \geqslant \mathrm{Tr}[\sqrt{\hat{\rho}_l}\sqrt{A}],$$
$$= \sum_r a_r\langle v_r|\sqrt{\hat{\rho}_l}|v_r\rangle.$$

We know that $\sqrt{\hat{\rho}_l} \geqslant \sqrt{A}$ and hence

$$\langle v_r|\sqrt{\hat{\rho}_l}|v_r\rangle \geqslant a_r, \quad \forall\ r.$$

As ρ_j and A are not orthogonal,

$$\sum_r \langle v_r|\sqrt{\hat{\rho}_l}|v_r\rangle > \sum_r a_r,$$

and there must exist some r such that

$$\langle v_r|\sqrt{\hat{\rho}_l}|v_r\rangle > a_r.$$

Hence

$$\begin{aligned} F(\hat{\rho}_l,A) &\geqslant \sum_r a_r \langle v_r|\sqrt{\hat{\rho}_l}|v_r\rangle,\\ &> \sum_r a_r^2,\\ &= \mathrm{Tr}\,[A],\\ &= \frac{k-2}{k-1}. \end{aligned}$$

So $F(\hat{\rho}_j,\hat{\rho}_l) = (k-2)/(k-1), \forall\, l \neq j$, if and only if $\mathcal{P}$ is an orthogonal set.

By Theorem 2, for conclusive $(m-1)$-state exclusion (and hence conclusive state discrimination) to be possible, we require that

$$\sum_{j\neq l=1}^{k} F(\hat{\rho}_j,\hat{\rho}_l) = k(k-2),$$

which implies that $\mathcal{P}$ must be an orthogonal set. ■

3. Bound on success probability

In this section, we give the proof of Theorem 3.

Proof. The goal is to show that $N_\varepsilon \leqslant \tilde{\rho}_i, \forall\, i$, where N_ε is defined in Eq. (20). Recall that given two Hermitian operators, A and B, $\min{(A,B)}$ is defined by

$$\min(A,B) = \tfrac{1}{2}[A+B-|A-B|].$$

Note that $\min(A,B) \leqslant A$ and $\min(A,B) \leqslant B$ as

$$\begin{aligned} A - \min(A,B) &= \frac{1}{2}\left[A - B + |A-B|\right],\\ &= \frac{1}{2}\left[\sum_{i=1}^{d} \lambda_i |u_i\rangle\langle u_i| + \sum_{i=1}^{d} |\lambda_i|\, |u_i\rangle\langle u_i|\right],\\ &\geqslant 0, \end{aligned}$$

and similarly $B - \min(A,B) \geqslant 0$. Here $\sum_{i=1}^{d} \lambda_i |u_i\rangle\langle u_i|$ is the spectral decomposition of $A - B$.

The bound is obtained by constructing N_ε iteratively as follows:

$$\begin{aligned} N_\varepsilon^{(2)} &= \min(\tilde{\rho}_{\varepsilon(2)},\tilde{\rho}_{\varepsilon(1)}),\\ N_\varepsilon^{(3)} &= \min\left(\tilde{\rho}_{\varepsilon(3)},N_\varepsilon^{(2)}\right),\\ \vdots &= \vdots\\ N_\varepsilon = N_\varepsilon^{(k)} &= \min\left(\tilde{\rho}_{\varepsilon(k)},N_\varepsilon^{(k-1)}\right). \end{aligned}$$

Using the fact that $\min(A,B) \leqslant A$ and $\min(A,B) \leqslant B$, by construction we have $N_\varepsilon \leqslant \tilde{\rho}_i, \forall\, i$.

APPENDIX D: PBR GAME

In this appendix, we analyze the PBR game.

1. Proof that $\mathcal{M}$ is a measurement

To see that $\mathcal{M} = \{|\zeta_{\vec{x}}\rangle\}_{\vec{x}\in\{0,1\}^n}$, where

$$|\zeta_{\vec{x}}\rangle = \frac{1}{\sqrt{2^n}}\left(|\vec{0}\rangle - \sum_{\vec{r}\neq\vec{0}} (-1)^{\vec{x}\cdot\vec{r}}\, |\vec{r}\rangle\right),$$

forms a valid measurement, we shall show that it is a set of orthogonal vectors. Consider

$$\begin{aligned} \langle\zeta_{\vec{s}}|\zeta_{\vec{t}}\rangle &= \frac{1}{2^n}\left(\langle\vec{0}| - \sum_{\vec{r}\neq\vec{0}} (-1)^{\vec{s}\cdot\vec{r}}\, \langle\vec{r}|\right)\left(|\vec{0}\rangle - \sum_{\vec{q}\neq\vec{0}} (-1)^{\vec{t}\cdot\vec{q}}\, |\vec{q}\rangle\right),\\ &= \frac{1}{2^n}\left(1 + \sum_{\vec{r},\vec{q}\neq\vec{0}} (-1)^{\vec{s}\cdot\vec{r}}\, (-1)^{\vec{t}\cdot\vec{q}}\, \langle\vec{r}|\vec{q}\rangle\right),\\ &= \frac{1}{2^n}\sum_{\vec{r}} (-1)^{(\vec{s}+\vec{t})\cdot\vec{r}},\\ &= \delta_{\vec{s}\vec{t}}. \end{aligned}$$

Hence $\mathcal{M}$ is a set of orthogonal vectors and therefore a valid measurement basis.

2. Derivation of conditions under which $\mathcal{M}$ is an optimal measurement

To show that this measurement, $\mathcal{M}$, is optimal for certain pairs of n and θ, we need to construct an N as per Eq. (12) and show that it satisfies the constraints of the dual problem. Writing $\tilde{\rho}_{\vec{x}} = \frac{1}{2^n}|\Psi_{\vec{x}}\rangle\langle\Psi_{\vec{x}}|$ and $M_{\vec{x}} = |\zeta_{\vec{x}}\rangle\langle\zeta_{\vec{x}}|$, we have

$$N = \frac{1}{2^n}\sum_{\vec{x}} |\Psi_{\vec{x}}\rangle\langle\Psi_{\vec{x}}|\zeta_{\vec{x}}\rangle\langle\zeta_{\vec{x}}|.$$

Note that

$$\begin{aligned} \langle\Psi_{\vec{x}}|\zeta_{\vec{x}}\rangle &= \frac{1}{\sqrt{2^n}}\left\{\left[\cos\left(\frac{\theta}{2}\right)\right]^n - \sum_{i=1}^{n}\binom{n}{i}\left[\cos\left(\frac{\theta}{2}\right)\right]^{n-i}\right.\\ &\quad\left.\times\left[\sin\left(\frac{\theta}{2}\right)\right]^i\right\},\\ &= \frac{1}{\sqrt{2^n}}\left[\cos\left(\frac{\theta}{2}\right)\right]^n\left\{2 - \left[1 + \tan\left(\frac{\theta}{2}\right)\right]^n\right\}. \end{aligned}$$

So we have

$$N = C\,(\theta)\left[|\vec{0}\rangle\langle\vec{0}| - \sum_{\vec{r}\neq\vec{0}}\left[\tan\left(\frac{\theta}{2}\right)\right]^{|\vec{r}|}|\vec{r}\rangle\langle\vec{r}|\right], \tag{D1}$$

where $C(\theta)$ is given by

$$C\,(\theta) = \frac{1}{2^n}\left[\cos\left(\frac{\theta}{2}\right)\right]^{2n}\left\{2 - \left[1 + \tan\left(\frac{\theta}{2}\right)\right]^n\right\}.$$

Note also that N is a real, diagonal matrix and hence is Hermitian, so it remains to determine under what conditions $\rho_i - N$ is a positive-semidefinite matrix for all i.

Let us define the matrices A_i by

$$A_i = -N + \rho_i .$$

The goal is to prove that none of the A_i have a negative eigenvalue. Say A_i has eigenvalues $\{a_i^r\}$, where $a_i^1 \geqslant a_i^2 \geqslant \cdots a_i^{2^n}$. The matrix $-N$ has eigenvalues $\{v^r\}$ where for $1 \leqslant r \leqslant 2^n - 1$,

$$v^r = C(\theta)\left[\tan\left(\frac{\theta}{2}\right)\right]^{|\vec{r}|},$$

and for $r = 2^n$,

$$v^{2^n} = -C(\theta).$$

Each ρ_i is a rank-1 density matrix and hence has eigenvalues $u_i^1 = 1$ and $u_i^r = 0$ for $2 \leqslant r \leqslant 2^n$.

By Weyl's inequality,

$$v^r + u_i^{2^n} \leqslant a_i^r .$$

So, provided $C(\theta) > 0$, we have $a_i^r > 0$ for $1 \leqslant r \leqslant 2^n - 1$. Hence at most one eigenvalue of A_i is nonpositive. Investigating this nonpositive eigenvalue further, consider A_i acting on the state $|\zeta_i\rangle$:

$$A_i|\zeta_i\rangle = \rho_i|\zeta_i\rangle - \sum_{j=1}^{2^n} \rho_j|\zeta_j\rangle\langle\zeta_j|\zeta_i\rangle = 0.$$

Hence the nonpositive eigenvalue of A_i is 0 implying that $A_i \geqslant 0, \forall\, i$, which in turn implies that $N \leqslant \rho_i, \forall\, i$, provided $C(\theta) > 0$. As $[\cos(\theta/2)]^{2n} \geqslant 0$, we have shown that $\{|\zeta_{\vec{x}}\rangle\}_{\vec{x}\in\{0,1\}^n}$, as defined in Eq. (28), is the optimal measurement for exclusion provided

$$\left\{2 - \left[1 + \tan\left(\frac{\theta}{2}\right)\right]^n\right\} > 0. \tag{D2}$$

This region is the complement of that given in Eq. (27), so we know the optimal measurement to perform for all values of n and θ.

3. Derivation of how well $\mathcal{M}$ performs at the exclusion task

Is conclusive exclusion possible in the region defined by Eq. (D2)? To answer this, we must consider the trace of the N given in Eq. (D1):

$$\mathrm{Tr}[N] = \frac{1}{2^n}\left[\cos\left(\frac{\theta}{2}\right)\right]^{2n}\left\{2 - \left[1 + \tan\left(\frac{\theta}{2}\right)\right]^n\right\}^2 .$$

This is strictly positive and hence conclusive exclusion is not possible. The value of $\mathrm{Tr}[N]$ does, however, tell us how accurately we can perform state exclusion when we cannot do it conclusively.

APPENDIX E: ALTERNATIVE STATE EXCLUSION SDPS

In this appendix, we derive alternative state exclusion SDPs.

1. Unambiguous state exclusion SDP

In this section, the dual problem for the primal SDP for unambiguous state exclusion as given in Eq. (34) is derived.

Comparing Eq. (34) with Eq. (A1), we see that here the following holds true:

(i) A is a kd by kd block-diagonal matrix with each d by d block containing $\sum_{j=1}^k \tilde{\rho}_j$:

$$A = \begin{pmatrix} \sum_{j=1}^k \tilde{\rho}_j & & \\ & \ddots & \\ & & \sum_{j=1}^k \tilde{\rho}_j \end{pmatrix}.$$

(ii) B is a $(d+k)$ by $(d+k)$ matrix with the top left d by d block being an identity matrix and all other elements being 0:

$$B = \begin{pmatrix} \mathbb{I} & 0 \\ 0 & 0 \end{pmatrix}.$$

(iii) X, the variable matrix, is a kd by kd block-diagonal matrix where we label each d by d block diagonal by M_i:

$$X = \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_k \end{pmatrix}.$$

(iv) Y is a $(d+k)$ by $(d+k)$ matrix whose top left d by d block we call N and the remaining k diagonal elements we label by a_i.

$$Y = \begin{pmatrix} N & & & \\ & a_1 & & \\ & & \ddots & \\ & & & a_k \end{pmatrix}.$$

(v) The map Φ is given by

$$\Phi(X) = \begin{pmatrix} \sum_{i=1}^k M_i & & & \\ & \mathrm{Tr}[\tilde{\rho}_1 M_1] & & \\ & & \ddots & \\ & & & \mathrm{Tr}[\tilde{\rho}_k M_k] \end{pmatrix}.$$

Using Eq. (A3), we see that Φ^* must satisfy

$$\mathrm{Tr}\left[N\sum_{i=1}^k M_i\right] + \sum_{i=1}^k a_i \mathrm{Tr}[\tilde{\rho}_i M_i]$$
$$= \mathrm{Tr}\left\{\begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_k \end{pmatrix} \Phi^*\left[\begin{pmatrix} N & & & \\ & a_1 & & \\ & & \ddots & \\ & & & a_k \end{pmatrix}\right]\right\},$$

and hence $\Phi^*(Y)$ produces a kd by kd block-diagonal matrix:

$$\Phi^*(Y) = \begin{pmatrix} N + a_1\tilde{\rho}_1 & & \\ & \ddots & \\ & & N + a_k\tilde{\rho}_k \end{pmatrix}.$$

Substituting these elements into Eq. (A2) and taking into account the fact that we are maximizing rather than minimizing in the primal problem, we obtain the dual SDP as stated in Eq. (35).

2. Worst-case error state exclusion SDP

In this section, the dual problem for the primal SDP for worst-case error state exclusion as given in Eq. (37) is derived.

Comparing Eq. (37) with Eq. (A1), we see that here the following holds true:

(i) A is a $(kd+1)$ by $(kd+1)$ matrix with $A_{11}=1$ being the only nonzero element:

$$A=\begin{pmatrix}1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0\end{pmatrix}.$$

(ii) B is a $(d+k)$ by $(d+k)$ where the bottom right d by d block is the identity matrix. All other elements are zero:

$$B=\begin{pmatrix}0 & 0\\ 0 & \mathbb{I}\end{pmatrix}.$$

(iii) X, the variable matrix, is a $kd+1$ by $kd+1$ block-diagonal matrix where $X_{11}=\lambda$ and we label each subsequent d by d block diagonal by M_i:

$$X=\begin{pmatrix}\lambda & & & \\ & M_1 & & \\ & & \ddots & \\ & & & M_k\end{pmatrix}.$$

(iv) Y is a $(d+k)$ by $(d+k)$ matrix whose bottom right d by d block we call N and the remaining k diagonal elements we label by a_i,

$$Y=\begin{pmatrix}a_1 & & & \\ & \ddots & & \\ & & a_k & \\ & & & N\end{pmatrix}.$$

(v) The map Φ is given by

$$\Phi(X)=\begin{pmatrix}\lambda-\mathrm{Tr}\,[\tilde{\rho}_1 M_1] & & & \\ & \ddots & & \\ & & \lambda-\mathrm{Tr}\,[\tilde{\rho}_k M_k] & \\ & & & \sum_{i=1}^{k} M_i\end{pmatrix}.$$

Using Eq. (A3), we see that Φ^* must satisfy

$$\lambda\sum_{i=1}^{k} a_i-\sum_{i=1}^{k} a_i \mathrm{Tr}\,[\tilde{\rho}_i M_i]=\mathrm{Tr}\left\{\begin{pmatrix}\lambda & & & \\ & M_1 & & \\ & & \ddots & \\ & & & M_k\end{pmatrix}\Phi^*\left[\begin{pmatrix}a_1 & & & \\ & \ddots & & \\ & & a_k & \\ & & & N\end{pmatrix}\right]\right\},$$

and hence $\Phi^*(Y)$ produces a kd by kd block-diagonal matrix:

$$\Phi^*(Y)=\begin{pmatrix}\sum_{i=1}^{k} a_i & & & \\ & N-a_1\tilde{\rho}_1 & & \\ & & \ddots & \\ & & & N-a_k\tilde{\rho}_k\end{pmatrix}.$$

Substituting these elements into Eq. (A2), we obtain the dual SDP as stated in Eq. (38).

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2010).

[2] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[3] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[4] A. Peres, Phys. Lett. A **128**, 19 (1988).

[5] C. W. Helstrom *et al.*, *Quantum Detection and Estimation Theory* (Academic, New York, 1976), Vol. 84.

[6] A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973).

[7] H. Yuen, R. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **21**, 125 (1975).

[8] S. M. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238 (2009).

[9] C. M. Caves, C. A. Fuchs, and R. Schack, Phys. Rev. A **66**, 062111 (2002).

[10] M. F. Pusey, J. Barrett, and T. Rudolph, Nat. Phys. **8**, 475 (2012).

[11] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[12] J. Watrous, https://cs.uwaterloo.ca/∼watrous/LectureNotes.html.

[13] M. Ježek, J. Řeháček, and J. Fiurášek, Phys. Rev. A **65**, 060301(R) (2002)..

[14] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. Inf. Theory **49**, 1007 (2003).

[15] Y. C. Eldar, IEEE Trans. Inf. Theory **49**, 446 (2003).

[16] N. Harrigan and R. W. Spekkens, Found. Phys. **40**, 125 (2010).
[17] A. Molina and J. Watrous, Proc. R. Soc. A **468**, 2614 (2012).
[18] S. Arunachalam, A. Molina, and V. Russo, arXiv:1310.7954.
[19] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[20] K. Nakahira and T. S. Usuda, Phys. Rev. A **86**, 062305 (2012).
[21] D. Qiu and L. Li, Phys. Rev. A **81**, 042329 (2010).
[22] J. Löfberg, in *IEEE International Symposium on Computer Aided Control Systems Design* (IEEE, Piscataway, NJ, 2004), pp. 284–289.
[23] J. F. Sturm, Opt. Methods Software **11**, 625 (1999).
[24] R. L. Kosut, I. Walmsley, Y. Eldar, and H. Rabitz, arXiv:quant-ph/0403150.
[25] J. Fiurášek and M. Ježek, Phys. Rev. A **67**, 012321 (2003).
[26] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, arXiv:1311.5760.