

State discrimination with postmeasurement information and incompatibility of quantum measurements

Claudio Carmeli*

DIME, Università di Genova, Via Magliotto 2, I-17100 Savona, Italy

Teiko Heinosaari†

QTF Centre of Excellence, Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, FI-20014 Turku, Finland

Alessandro Toigo‡

Dipartimento di Matematica, Politecnico di Milano, Piazza Leonardo da Vinci 32, I-20133 Milano, Italy and INFN, Sezione di Milano, Via Celoria 16, I-20133 Milano, Italy



(Received 7 May 2018; published 19 July 2018)

We discuss the following variant of the standard minimum error state discrimination problem: Alice picks the state she sends to Bob among one of several disjoint state ensembles, and she communicates him the chosen ensemble only at a later time. Two different scenarios then arise: either Bob is allowed to arrange his measurement setup *after* Alice has announced him the chosen ensemble, or he is forced to perform the measurement *before* Alice's announcement. In the latter case, he can only postprocess his measurement outcome when Alice's extra information becomes available. We compare the optimal guessing probabilities in the two scenarios, and we prove that they are the same if and only if there exist compatible (i.e., jointly measurable) optimal measurements for all of Alice's state ensembles. When this is the case, postprocessing any of the corresponding joint measurements is Bob's optimal strategy in the postmeasurement information scenario. Furthermore, we establish a connection between discrimination with postmeasurement information and the standard state discrimination. By means of this connection and exploiting the presence of symmetries, we are able to compute the various guessing probabilities in many concrete examples.

DOI: [10.1103/PhysRevA.98.012126](https://doi.org/10.1103/PhysRevA.98.012126)

I. INTRODUCTION

Quantum state discrimination is one of the fundamental tasks in quantum information processing. In the setting of state discrimination, a quantum system is prepared in one out of a finite collection of possible states, chosen with a certain *a priori* probability. The aim is then to identify the correct state by making a single measurement, assuming that the possible states and their *a priori* probabilities are known before the measurement is chosen. This can be also seen as a task of retrieving classical information that has been encoded in quantum states. A collection of orthogonal pure states, or more generally mixed states with disjoint supports, can be perfectly discriminated, while in other cases one has to accept either error or inconclusive result. These alternatives lead to two main branches of discrimination problems, called *minimum error discrimination* and *unambiguous discrimination*, respectively, that have both been investigated extensively; thorough reviews are provided in [1–3].

Several types of variants of the state discrimination problem have been introduced and studied in the literature. A specific

variant of the minimum error state discrimination problem, called *state discrimination with postmeasurement information*, was elaborated in [4]. In this task, Alice encodes classical information in quantum states and Bob then performs a measurement to guess the correct state, but Alice announces some partial information on her encoding before Bob must make his guess. This task was further studied in [5], and it was suggested that the usefulness of postmeasurement information distinguishes the quantum from the classical world.

In this work we reveal a link between the task of state discrimination with postmeasurement information and the incompatibility of quantum measurements. We will first formalize discrimination tasks with premeasurement and postmeasurement information in a consistent way, allowing us to compare the optimal guessing probabilities in these two cases. (For clarification, we point out that our formulation slightly differs from the one presented in [4] and [5]. The formulations are compared in Sec. II C.) We then show that premeasurement information is strictly more favorable than postmeasurement information if and only if the optimal measurements for the subensembles are incompatible. Since incompatibility is a genuine nonclassical feature [6–8], this result uncovers a peculiarity that differentiates quantum from classical measurements.

As a technical method to calculate the optimal guessing probabilities and optimal measurements, we show that

*claudio.carmeli@gmail.com

†teiko.heinosaari@utu.fi

‡alessandro.toigo@polimi.it

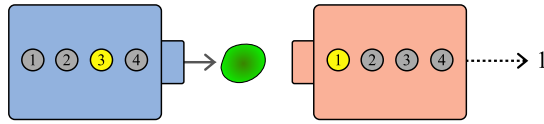


FIG. 1. In minimum error state discrimination, Alice prepares a quantum state ϱ_x from a given state ensemble which is known also to Bob. Bob aims to determine the label x by performing a measurement which maximizes his guessing probability. In the depicted event, Bob is making an incorrect guess.

it is always possible to transform the problem of state discrimination with postmeasurement information into a usual minimum error state discrimination problem; more precisely, any state discrimination problem with postmeasurement information is associated with standard state discrimination for a specific auxiliary state ensemble, in such a way that the two discrimination tasks have the same optimal measurements, and the respective success probabilities are related by a simple equation. In this way, the known results for the usual minimum error discrimination can be used for state discrimination with postmeasurement information.

Finally, we discuss the connection between state discrimination with postmeasurement information and approximate joint measurements in the cases when the optimal measurements for the subensemble discrimination problems are incompatible. We provide several examples, showing that the approximate joint measurement is sometimes optimal, although not always. In particular, we present an analytic solution for the problem of state discrimination with postmeasurement information of two Fourier conjugate mutually unbiased bases in arbitrary finite dimension.

Notations. We deal with quantum systems associated with a finite-dimensional Hilbert space \mathcal{H} . We denote by $\mathcal{L}(\mathcal{H})$ the set of all linear operators on \mathcal{H} , and $\mathbb{1} \in \mathcal{L}(\mathcal{H})$ is the identity operator of \mathcal{H} . The *states* of the system are all positive trace one operators in $\mathcal{L}(\mathcal{H})$. A *measurement* with outcomes in a finite set X is any positive-operator-valued measure based on X , i.e., any mapping $M : X \rightarrow \mathcal{L}(\mathcal{H})$ such that $M(x) \geq 0$ for all $x \in X$ and $\sum_{x \in X} M(x) = \mathbb{1}$.

II. STATE DISCRIMINATION WITH POSTMEASUREMENT INFORMATION

A. General scenario

A *state ensemble* \mathcal{E} is a sequence of states $(\varrho_x)_{x \in X}$, labeled with a finite set X , together with an assignment of some prior probability $p(x)$ to each label $x \in X$. It is convenient to regard \mathcal{E} as a map $X \rightarrow \mathcal{L}(\mathcal{H})$, given by $\mathcal{E}(x) = p(x)\varrho_x$. We say that a quantum system is prepared or chosen from the state ensemble \mathcal{E} when a label $x \in X$ is picked according to the probability distribution p , and the system is then set in the corresponding state ϱ_x .

In the standard minimum error state discrimination scenario (see Fig. 1), there is a state ensemble \mathcal{E} that is known to two parties, Alice and Bob. Alice prepares a quantum system from \mathcal{E} and the task of Bob is to guess the correct state. For a measurement M having the outcome set X , the guessing

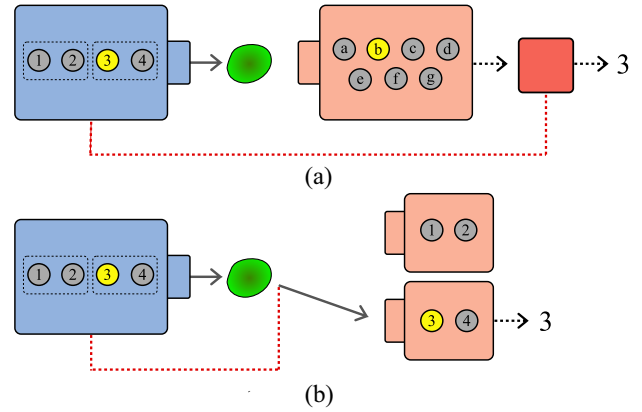


FIG. 2. Alice encodes a label x into a quantum state ϱ_x on which Bob performs a measurement. In the *postmeasurement* information scenario (a), Alice announces the subset from which she picked x after Bob has performed a measurement. After Alice's announcement, Bob can postprocess his measurement outcome accordingly, and finally he gives his guess. In the *premeasurement* information scenario (b), Alice announces the correct subset already before Bob arranges his measurement.

probability $P_{\text{guess}}(\mathcal{E}; M)$ is given as

$$P_{\text{guess}}(\mathcal{E}; M) = \sum_x \text{tr}[\mathcal{E}(x)M(x)] = \sum_x p(x)\text{tr}[\varrho_x M(x)].$$

The aim is to maximize the guessing probability, and we denote

$$P_{\text{guess}}(\mathcal{E}) := \max_M P_{\text{guess}}(\mathcal{E}; M), \quad (1)$$

where the optimization is over all measurements with outcome set X . This is called the *optimal guessing probability* for \mathcal{E} , and the minimum error discrimination problem is to find an optimizing measurement for a given state ensemble \mathcal{E} . The problem was introduced in [9–11]. The existence of optimal measurements, i.e., the fact that in (1) the maximum is actually attained, follows by a compactness argument ([9, Proposition 4.1], [10, Lemma 1]).

In the state discrimination with postmeasurement information, the standard scenario is modified by adding a middle step to it. The starting point, known both to Alice and Bob, is a state ensemble \mathcal{E} and a partition $\mathcal{P} = (X_\ell)_{\ell \in I}$ of the label set X into nonempty disjoint subsets. For each index $\ell \in I$, the probability of picking a label in X_ℓ is

$$q(\ell) := \sum_{x \in X_\ell} p(x). \quad (2)$$

We further assume that $q(\ell) \neq 0$ to avoid trivial cases. Then, conditioning the state ensemble \mathcal{E} to the occurrence of a label in X_ℓ , we obtain a new state ensemble \mathcal{E}_ℓ , which we call a *subensemble* of \mathcal{E} . The label set of \mathcal{E}_ℓ is X_ℓ , and

$$\mathcal{E}_\ell(x) := \frac{1}{q(\ell)}\mathcal{E}(x), \quad x \in X_\ell. \quad (3)$$

The steps in the scenario are the following [see Fig. 2(a)]:

(i) Alice picks a label x from the set X , according to the prior probability distribution p . She then prepares a state ϱ_x and delivers this state to Bob.

(ii) Bob performs a measurement \mathbf{M} , hence obtaining an outcome $y \in Y$ with probability $\text{tr}[\rho_x \mathbf{M}(y)]$. The outcome set Y of \mathbf{M} is freely chosen by Bob.

(iii) After the measurement is performed, Alice tells Bob the index ℓ of the correct subset X_ℓ where the label was picked from.

(iv) Based on the measurement outcome y and on the announced index ℓ , Bob must guess x . This means that Bob applies a function $f_\ell : Y \rightarrow X_\ell$ to the obtained measurement outcome y and his guess is $f_\ell(y)$.

Bob's guessing strategy is therefore determined by a measurement \mathbf{M} and postprocessing functions $(f_\ell)_{\ell \in I}$. We emphasize that the same measurement \mathbf{M} is used at every round, while the choice of the implemented relabeling function is determined by the announced label ℓ .

We denote by $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{M}, (f_\ell)_{\ell \in I})$ the guessing probability in the previously described scenario, and further, we denote by $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ the maximum of the guessing probability when \mathbf{M} and $(f_\ell)_{\ell \in I}$ vary over all suitable measurements and relabeling functions, respectively. Remarkably, optimal measurements and relabeling functions for the discrimination problem with postmeasurement information actually exist, as we will see in Sec. IV A. In the following we show that $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ is bounded below and above in a natural way by the guessing probabilities corresponding to scenarios with no information at all and with the partial information given before Bob has to choose his measurement.

To elaborate the expression of $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{M}, (f_\ell)_{\ell \in I})$, we denote by $f_{\ell*} \mathbf{M}$ the postprocessed measurement that Bob has effectively performed when he has applied f_ℓ after \mathbf{M} , i.e., the measurement that has outcomes X_ℓ and is defined as

$$f_{\ell*} \mathbf{M}(x) := \sum_{y \in f_\ell^{-1}(x)} \mathbf{M}(y), \quad x \in X_\ell, \quad (4)$$

where $f_\ell^{-1}(x)$ denotes the preimage of x , i.e., $f_\ell^{-1}(x) = \{y : f_\ell(y) = x\}$. We can then write the guessing probability as

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{M}, (f_\ell)_{\ell \in I}) = \sum_{\ell \in I} q(\ell) P_{\text{guess}}(\mathcal{E}_\ell; f_{\ell*} \mathbf{M}). \quad (5)$$

The use of postmeasurement information cannot decrease the guessing probability, that is,

$$P_{\text{guess}}(\mathcal{E}) \leq P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}). \quad (6)$$

Indeed, one possible strategy for Bob is to perform a measurement \mathbf{M} with outcomes in X that optimally discriminates \mathcal{E} . He thus obtains the correct outcome with the probability $P_{\text{guess}}(\mathcal{E})$, but he does not announce his guess yet. Then, after hearing the index ℓ of the correct subset X_ℓ , Bob does the following. If his obtained measurement outcome x belongs to X_ℓ , then Bob's guess is x . But if x is not in X_ℓ , then Bob infers that he got an incorrect result and chooses an arbitrary default label $x_\ell \in X_\ell$ as his guess. This means that the restrictions $f_\ell|_{X_\ell}$ of Bob's relabeling functions are the identity maps on X_ℓ , and $f_\ell(x) = x_\ell$ whenever $x \notin X_\ell$. In this way, the postmeasurement information allows Bob to sometimes neglect incorrect results, hence his guessing probability cannot be lower than $P_{\text{guess}}(\mathcal{E})$. Formally, $f_{\ell*} \mathbf{M}(x) \geq \mathbf{M}(x)$ for all

$x \in X_\ell$, implying

$$P_{\text{guess}}(\mathcal{E}_\ell; f_{\ell*} \mathbf{M}) \geq \frac{1}{q(\ell)} \sum_{x \in X_\ell} \text{tr}[\mathcal{E}(x) \mathbf{M}(x)]. \quad (7)$$

Using this inequality in (5), we get (6).

From (5) we also conclude a simple upper bound,

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) \leq \sum_{\ell \in I} q(\ell) P_{\text{guess}}(\mathcal{E}_\ell). \quad (8)$$

The right-hand side of (8) is the optimal success probability if Alice would tell the used state ensemble to Bob *before* Bob performs a measurement, in which case Bob can choose the optimal measurement to discriminate the correct state ensemble [see Fig. 2(b)]. We will thereby denote

$$P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}) := \sum_{\ell \in I} q(\ell) P_{\text{guess}}(\mathcal{E}_\ell). \quad (9)$$

In summary, the optimal guessing probability with postmeasurement information is bounded in the interval

$$P_{\text{guess}}(\mathcal{E}) \leq P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) \leq P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}), \quad (10)$$

whose left and right extremes correspond to situations where Alice gives no information at all and Alice gives the partial information before Bob's choice of measurement, respectively.

B. Limiting to the standard form measurements

For simplicity, in the following we assume the index set $I = I_m := \{1, \dots, m\}$.

To maximize the guessing probability in the previously described postmeasurement information scenario, Bob must find the optimal measurement \mathbf{M} and relabeling functions $(f_\ell)_{\ell \in I_m}$. The outcome set of \mathbf{M} is, in principle, arbitrary and the role of relabeling functions is to adjust the obtained measurement outcome to give a meaningful guess. However, as we will next show, there is a fixed outcome set, determined by the separation of X into subsets $(X_\ell)_{\ell \in I_m}$, such that we can always restrict the optimization to measurements having that specific outcome set. This canonical choice of the outcome set is nothing else than the Cartesian product $X_1 \times \dots \times X_m$. Then, at each measurement round Bob obtains a measurement outcome (x_1, \dots, x_m) , and when Alice tells him the correct index ℓ , Bob just picks the outcome x_ℓ accordingly. The respective relabeling function f_ℓ is hence just the projection π_ℓ from $X_1 \times \dots \times X_m$ into X_ℓ .

When Bob's measurement has the Cartesian product $X_1 \times \dots \times X_m$ as its outcome set, we will use the shorthand notation

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C}) := P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C}, (\pi_\ell)_{\ell \in I_m}).$$

We thus have

$$\begin{aligned} P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C}) &= \sum_{\ell=1}^m q(\ell) P_{\text{guess}}(\mathcal{E}_\ell; \pi_{\ell*} \mathbf{C}) \\ &= \sum_{\ell=1}^m q(\ell) \sum_{x_\ell \in X_\ell} \text{tr}[\mathcal{E}_\ell(x_\ell) \pi_{\ell*} \mathbf{C}(x_\ell)], \end{aligned} \quad (11)$$

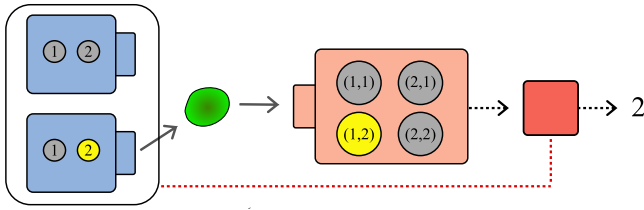


FIG. 3. In the approach described in [5], Alice encodes a classical string x into a quantum state $\varrho_{x,b}$, where b specifies one of the possible encodings Alice can choose from. Bob must determine the string x irrespectively of the encoding chosen by Alice. Alice announces the encoding after Bob has performed his measurement, but before he makes his guess.

where, according to (4),

$$\pi_{\ell_*} \mathbf{C}(x) = \sum_{\substack{x_1 \in X_1, \dots, x_m \in X_m \\ \text{such that } x_\ell = x}} \mathbf{C}(x_1, \dots, x_m). \quad (12)$$

The next result justifies the choice of the Cartesian product as the outcome set.

Proposition 1. For any choice of measurement \mathbf{M} and relabeling functions f_1, \dots, f_m , there is a measurement \mathbf{C} with product outcome set $X_1 \times \dots \times X_m$ such that

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{M}, (f_\ell)_{\ell \in I_m}) = P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C}).$$

Proof. We define \mathbf{C} as

$$\mathbf{C}(x_1, \dots, x_m) = \sum_{y \in f_1^{-1}(x_1) \cap \dots \cap f_m^{-1}(x_m)} \mathbf{M}(y).$$

Then, by (12),

$$\pi_{\ell_*} \mathbf{C}(x) = \sum_{y \in f_\ell^{-1}(x)} \mathbf{M}(y) = f_{\ell_*} \mathbf{M}(x),$$

hence, $\pi_{\ell_*} \mathbf{C} = f_{\ell_*} \mathbf{M}$. ■

C. Remarks on other formulations of the problem

The problem of state discrimination with postmeasurement information was first considered by Ballester *et al.* in [4]. According to their approach, before Alice announces the subensemble the state was picked from, Bob is allowed to store both classical and quantum information; his classical resources are unlimited (an unbounded amount of classical memory), and on the quantum side he can use a string of qubits with prescribed length. Later, Gopal and Wehner (GW) restricted to the case where only classical information is available for Bob [5]; for this reason, their approach more directly compares with ours.

In GW's problem, Alice encodes a string x of classical information in one of m possible quantum states $(\varrho_{x,b})_{b \in \mathcal{B}}$, with $\mathcal{B} = \{1, \dots, m\}$. The aim of Bob is to determine the string x , irrespectively of the encoding chosen by Alice (see Fig. 3). The set \mathcal{X} from which x is picked is the same for all encodings $b \in \mathcal{B}$, while the probability of selecting a specific encoding $b \in \mathcal{B}$ may depend on the chosen x . Thus, if $p(x, b)$ is the joint probability of picking the string x and using the encoding b , Bob's received state is the mixture $\sum_{x,b} p(x, b) \varrho_{x,b}$. On this state,

Bob performs a measurement \mathbf{C} with outcomes in the Cartesian product \mathcal{X}^m , thus obtaining the result (x_1, \dots, x_m) . Then, Alice declares him the selected encoding b , and, according to the announced b , Bob guesses the value x_b for the string x . Clearly, also in this scenario, Bob's maximum success probability with postmeasurement information p_{succ}^I cannot be smaller than the analogous probability without postmeasurement information p_{succ} . When $p_{\text{succ}}^I \equiv p_{\text{succ}}$, postmeasurement information is *useless* for the encoding at hand; in this case, if a measurement \mathbf{M} with outcomes in \mathcal{X} is optimal for the problem without postmeasurement information, then the diagonal measurement

$$\mathbf{C}(x_1, \dots, x_m) = \begin{cases} \mathbf{M}(x_0) & \text{if } x_1 = x_2 = \dots = x_m \equiv x_0 \\ 0 & \text{otherwise} \end{cases}$$

is optimal for the problem with postmeasurement information. Diagonal measurements correspond to the situation in which Bob guesses the same string x_0 independently of Alice's announced encoding, i.e., he completely ignores postmeasurement information.

To cast GW's approach into our framework, we choose as our label set X the disjoint union of m copies of \mathcal{X} , i.e., $X = \{(x, b) : x \in \mathcal{X}, b \in \mathcal{B}\}$, and we consider the state ensemble $\mathcal{E}(x, b) = p(x, b) \varrho_{x,b}$. For all $b \in \mathcal{B}$, we denote $X_b = \{(x, b) : x \in \mathcal{X}\}$, so that the sets $(X_b)_{b \in \mathcal{B}}$ constitute a partition \mathcal{P} of X . Then, Bob's task of identifying the string x with postmeasurement information b in GW's scenario is equivalent to the corresponding problem of detecting the label (x, b) within our approach; in particular, $p_{\text{succ}}^I = P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$. Note that GW actually do not consider Bob's possibility to arbitrarily enlarge his classical memory (i.e., his outcome set Y), as they directly set $Y = \mathcal{X}^m$; as we have proved in Proposition 1, this assumption is not restrictive.

However, it is important to stress that the success probabilities without postmeasurement information can differ in the two approaches; indeed, $p_{\text{succ}} \geq P_{\text{guess}}(\mathcal{E})$, with strict inequality in many concrete examples. This is due to the fact that in GW's setting Bob is required to guess only the string x , while with our definition of $P_{\text{guess}}(\mathcal{E})$ we require Bob to guess the whole label (x, b) , i.e., both the string x and the encoding b selected by Alice. For this reason, there are situations in which postmeasurement information is useless for GW's approach, although we have $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) > P_{\text{guess}}(\mathcal{E})$. For further discussion on this point, we defer to the examples in Sec. V.

III. POSTMEASUREMENT INFORMATION AND INCOMPATIBILITY OF MEASUREMENTS

A. Compatible measurements

As we see from (11), the guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ depends only on the relabeled measurements $\pi_{1_*} \mathbf{C}, \dots, \pi_{m_*} \mathbf{C}$, not on other details of \mathbf{C} . The measurement $\pi_{\ell_*} \mathbf{C}$, given by (12), is called the ℓ th *marginal* of \mathbf{C} . This way of writing reveals immediately the connection with the compatibility of measurements. Namely, we recall that measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$ are called *compatible* (also *jointly measurable*) if there exists a measurement \mathbf{M} on their Cartesian product outcome set such that each measurement \mathbf{N}_ℓ is the ℓ th marginal of \mathbf{M} . We remark that Proposition 1 can also be

extracted from the fact that the functional coexistence relation is equivalent to the compatibility relation [12]. We further note that, by applying the equivalent definition of compatibility in terms of the postprocessing preorder [6,13], we conclude that allowing nondeterministic postprocessing functions does not increase the optimal guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$.

Combining (11), (12), and Proposition 1 allows us to write the optimal guessing probability with postmeasurement information as follows:

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = \max \left\{ \sum_{\ell=1}^m q(\ell) P_{\text{guess}}(\mathcal{E}_\ell; \mathbf{N}_\ell) : \mathbf{N}_1, \dots, \mathbf{N}_m \text{ compatible} \right\}. \tag{13}$$

We now see that the difference between the guessing probabilities in premeasurement and postmeasurement information scenarios is that in the first one the optimization over measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$ has no restrictions, while in the second one the measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$ must be compatible. This leads to the following conclusion.

Theorem 1. There exist compatible optimal measurements for the discrimination problems of state ensembles $\mathcal{E}_1, \dots, \mathcal{E}_m$ if and only if the premeasurement and postmeasurement information discrimination problems have the same optimal guessing probability, i.e.,

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}). \tag{14}$$

Proof. It follows from the definition of $P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P})$ and (13) that, if there exists compatible optimal measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$, then (14) holds. Let us then assume that (14) holds. This means that there exist compatible measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$ such that $\sum_{\ell=1}^m q(\ell) P_{\text{guess}}(\mathcal{E}_\ell; \mathbf{N}_\ell) = \sum_{\ell=1}^m q(\ell) P_{\text{guess}}(\mathcal{E}_\ell)$. Since for any ℓ we have $P_{\text{guess}}(\mathcal{E}_\ell; \mathbf{N}_\ell) \leq P_{\text{guess}}(\mathcal{E}_\ell)$, the previous equality and $q(\ell) \neq 0$ for all ℓ imply $P_{\text{guess}}(\mathcal{E}_\ell; \mathbf{N}_\ell) = P_{\text{guess}}(\mathcal{E}_\ell)$. Therefore, each \mathbf{N}_ℓ is an optimal measurement for the discrimination problem of \mathcal{E}_ℓ . ■

We recall that a minimum error discrimination problem may not have a unique optimal measurement. For the statement of Theorem 1 it is enough that at least one collection of optimal measurements is made up of compatible measurements.

B. Incompatible measurements

We now turn to the case when optimal measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$ for the standard minimum error discrimination for the state ensembles $\mathcal{E}_1, \dots, \mathcal{E}_m$ are incompatible. From Theorem 1 we conclude that in this case $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ is strictly smaller than $P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P})$. However, we can still ask if the optimal solutions for the discrimination of subensembles \mathcal{E}_ℓ give some hint on the optimal solution for the postmeasurement information discrimination.

A heuristic approach to the problem of state discrimination with postmeasurement information relies on (13) and goes as follows. We form a noisy version $\tilde{\mathbf{N}}_\ell$ of each optimal measurement \mathbf{N}_ℓ related to \mathcal{E}_ℓ , and we add enough noise to make the measurements $\tilde{\mathbf{N}}_1, \dots, \tilde{\mathbf{N}}_m$ compatible. Noisy versions can be, in principle, any measurements that are compatible but approximate the optimal measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$ reasonably

well. Bob then performs a joint measurement of $\tilde{\mathbf{N}}_1, \dots, \tilde{\mathbf{N}}_m$ and from here on out, he follows the same procedure as in the case of compatible measurements. One would expect the guessing probability to be relatively good if $\tilde{\mathbf{N}}_1, \dots, \tilde{\mathbf{N}}_m$ are good approximations of $\mathbf{N}_1, \dots, \mathbf{N}_m$.

One type of noisy version of a measurement \mathbf{N}_ℓ is given by the mixture

$$\tilde{\mathbf{N}}_\ell(x) = t_\ell \mathbf{N}_\ell(x) + (1 - t_\ell) v_\ell(x) \mathbb{1}, \tag{15}$$

where v_ℓ is a probability distribution and $t_\ell \in [0, 1]$ is a mixing parameter. We then have

$$P_{\text{guess}}(\mathcal{E}_\ell; \tilde{\mathbf{N}}_\ell) \geq t_\ell P_{\text{guess}}(\mathcal{E}_\ell). \tag{16}$$

One would aim to choose each mixing parameter t_ℓ as close to 1 as possible to make $\tilde{\mathbf{N}}_\ell$ a good approximation of \mathbf{N}_ℓ , but the requirement that $\tilde{\mathbf{N}}_1, \dots, \tilde{\mathbf{N}}_m$ must be compatible limits the region of the allowed tuples (t_1, \dots, t_m) . The set of all tuples (t_1, \dots, t_m) that make the mixtures (15) compatible for some choices of v_1, \dots, v_m is called the *joint measurability region* of $\mathbf{N}_1, \dots, \mathbf{N}_m$ [14], and we denote it as $J(\mathbf{N}_1, \dots, \mathbf{N}_m)$. Further, the greatest number t such that $(t, \dots, t) \in J(\mathbf{N}_1, \dots, \mathbf{N}_m)$ is called the *joint measurability degree* of $\mathbf{N}_1, \dots, \mathbf{N}_m$ [15], and we denote it as $j(\mathbf{N}_1, \dots, \mathbf{N}_m)$.

The choice of the most favorable tuple $(t_1, \dots, t_m) \in J(\mathbf{N}_1, \dots, \mathbf{N}_m)$ for the discrimination with postmeasurement information depends on the probability distribution q and the optimal guessing probabilities $P_{\text{guess}}(\mathcal{E}_\ell)$. Starting from (13) and using (16), we obtain a lower bound

$$\begin{aligned} P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) &\geq \max \left\{ \sum_{\ell=1}^m t_\ell q(\ell) P_{\text{guess}}(\mathcal{E}_\ell) : (t_1, \dots, t_m) \in J(\mathbf{N}_1, \dots, \mathbf{N}_m) \right\} \\ &\geq j(\mathbf{N}_1, \dots, \mathbf{N}_m) \cdot \sum_{\ell=1}^m q(\ell) P_{\text{guess}}(\mathcal{E}_\ell) \\ &= j(\mathbf{N}_1, \dots, \mathbf{N}_m) \cdot P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}). \end{aligned}$$

The joint measurability degree of a set of observables is 1 if and only if the observables are compatible, therefore the obtained inequality can be taken as a quantitative addition to Theorem 1.

To derive another related inequality, we consider noisy versions of the form

$$\tilde{\mathbf{N}}_\ell(x) = t_\ell \mathbf{N}_\ell(x) + (1 - t_\ell) \frac{1}{n_\ell} \mathbb{1}, \tag{17}$$

where n_ℓ is the number of elements of X_ℓ . Compared to the more general form (15), the added noise is here given by a uniform probability distribution. We denote by $J_u(\mathbf{N}_1, \dots, \mathbf{N}_m)$ and $j_u(\mathbf{N}_1, \dots, \mathbf{N}_m)$ the analogous objects as $J(\mathbf{N}_1, \dots, \mathbf{N}_m)$ and $j(\mathbf{N}_1, \dots, \mathbf{N}_m)$, but where all v_ℓ 's are given by uniform probability distributions. Clearly, $j_u(\mathbf{N}_1, \dots, \mathbf{N}_m) \leq j(\mathbf{N}_1, \dots, \mathbf{N}_m)$, but the benefit for the current task is that now we can calculate the exact relation between $P_{\text{guess}}(\mathcal{E}_\ell; \tilde{\mathbf{N}}_\ell)$ and $P_{\text{guess}}(\mathcal{E}_\ell)$. Namely, the bound (16) is replaced by

$$P_{\text{guess}}(\mathcal{E}_\ell; \tilde{\mathbf{N}}_\ell) = t_\ell P_{\text{guess}}(\mathcal{E}_\ell) + (1 - t_\ell) \frac{1}{n_\ell}, \tag{18}$$

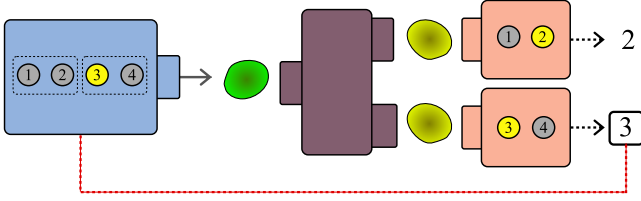


FIG. 4. Approximate cloning can be used to obtain lower bounds for the postmeasurement information guessing probability. Alice sends the state q_x from the subensemble \mathcal{E}_ℓ to Bob. He then makes an approximate cloning of q_x into as many copies as the number of subensembles and, on each approximate copy, he performs the measurement that optimally discriminates the corresponding subensemble. Finally, after Alice announces the index ℓ , Bob chooses his guess accordingly.

and the additional second term may improve the earlier bounds. For example, in the special case when $P_{\text{guess}}(\mathcal{E}_\ell) = 1$ and $n_\ell \equiv n$ for each $\ell = 1, \dots, m$, we get

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) \geq \frac{1}{n} + \frac{n-1}{n} j_u(\mathbf{N}_1, \dots, \mathbf{N}_m). \quad (19)$$

Similar lower bounds can be calculated in other cases.

C. Approximate cloning strategy

An approximate cloning device is, generally speaking, a physically realizable map that makes several approximate copies from an unknown quantum state. One such device is the Keyl-Werner cloning device [16,17], which takes an unknown state q as input and outputs m approximate copies \tilde{q} of the form

$$\tilde{q} = c_{m,d} q + (1 - c_{m,d}) \frac{1}{d} \mathbb{1}, \quad c_{m,d} = \frac{m+d}{m(1+d)}.$$

This device is known to be optimal if the quality of single clones is quantified as their fidelity with respect to the original state.

In the current scenario of state discrimination with post-measurement information, we can use an approximate cloning device in the following way (see Fig. 4). Bob, after receiving a quantum system from Alice, approximately copies the unknown state into m systems. For each copy, Bob performs the measurement \mathbf{N}_ℓ that optimally discriminates the subensemble \mathcal{E}_ℓ . Then, after Alice announces the index ℓ of the correct subset X_ℓ where the label was from, Bob chooses his guess accordingly.

This cloning strategy is rarely optimal (see examples in Sec. V), but it gives a nontrivial lower bound for the guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$. For instance, if the prior probability distribution p is uniform, the cloning strategy leads to the lower bound

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) \geq c_{m,d} P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}) + (1 - c_{m,d}) \frac{m}{N}, \quad (20)$$

where m is the number of blocks in the partition and $N = n_1 + \dots + n_m$ is the total size of the index set.

We can also think about approximate cloning in the Heisenberg picture; looking in that way the Keyl-Werner cloning

device transforms each measurement \mathbf{N}_ℓ into

$$\tilde{\mathbf{N}}_\ell(x) = c_{m,d} \mathbf{N}_\ell(x) + (1 - c_{m,d}) \text{tr}[\mathbf{N}_\ell(x)] \frac{1}{d} \mathbb{1}. \quad (21)$$

From this point of view, the approximate cloning strategy is just a particular instance of the noisy joint measurement strategy described in Sec. III B; the lower bound (20) then follows just by inserting (21) into the right-hand side of (13). The bound (20) is useful as it is universal, in the sense that it does not depend on any details of the optimal measurements $\mathbf{N}_1, \dots, \mathbf{N}_m$.

IV. METHODS TO CALCULATE THE OPTIMAL GUESSING PROBABILITY

A. Reduction to usual state discrimination problem

It was noted in [5] that the problem of state discrimination with postmeasurement information can be related to a suitable standard state discrimination problem. Here we provide a slightly different viewpoint on this connection.

As before, we consider a state ensemble \mathcal{E} with label set X , and a partition $\mathcal{P} = (X_\ell)_{\ell \in I_m}$ of X into m nonempty disjoint subsets. As shown in Sec. II B, in order to maximize the postinformation guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{M}, (f_\ell)_{\ell \in I_m})$ over all measurements \mathbf{M} and relabeling functions f_1, \dots, f_m , it is enough to consider all measurements \mathbf{C} with the Cartesian product outcome space and use the fixed postprocessings π_1, \dots, π_m . It turns out that, up to a constant factor, the guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ is the same as the guessing probability for a certain specific state ensemble in the standard state discrimination scenario using the same measurement \mathbf{C} . To explain the details of this claim, we define an auxiliary state ensemble \mathcal{F} having the Cartesian product $X_1 \times \dots \times X_m$ as its label set, and given by

$$\mathcal{F}(x_1, \dots, x_m) = \frac{1}{\Delta} \sum_{\ell=1}^m \mathcal{E}(x_\ell) = \frac{1}{\Delta} \sum_{\ell=1}^m q(\ell) \mathcal{E}_\ell(x_\ell), \quad (22)$$

where the probability q and the state ensembles \mathcal{E}_ℓ are defined in (2) and (3), and the numerical factor Δ is

$$\Delta \equiv \Delta(q; n_1, \dots, n_m) = n_1 \dots n_m \sum_{\ell=1}^m \frac{q(\ell)}{n_\ell}. \quad (23)$$

(We recall that n_ℓ denotes the number of labels in X_ℓ .) The state ensemble \mathcal{F} has $n_1 \dots n_m$ labels and its states are convex combinations of states from different subensembles \mathcal{E}_ℓ . Starting from (11), a direct calculation gives

$$\begin{aligned} P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C}) &= \sum_{\ell=1}^m q(\ell) \sum_{x_\ell \in X_\ell} \text{tr}[\mathcal{E}_\ell(x_\ell) \pi_{\ell*} \mathbf{C}(x_\ell)] \\ &= \sum_{\ell=1}^m q(\ell) \sum_{x_1 \in X_1, \dots, x_m \in X_m} \text{tr}[\mathcal{E}_\ell(x_\ell) \mathbf{C}(x_1, \dots, x_m)] \\ &= \sum_{x_1 \in X_1, \dots, x_m \in X_m} \text{tr} \left[\sum_{\ell=1}^m q(\ell) \mathcal{E}_\ell(x_\ell) \mathbf{C}(x_1, \dots, x_m) \right] \\ &= \Delta P_{\text{guess}}(\mathcal{F}; \mathbf{C}). \end{aligned}$$

The factor Δ is required as the state ensemble \mathcal{F} must be normalized, i.e.,

$$\sum_{x_1 \in X_1, \dots, x_m \in X_m} \text{tr}[\mathcal{F}(x_1, \dots, x_m)] = 1. \quad (24)$$

As mentioned in Sec. II A, it is known that the standard discrimination guessing probability $P_{\text{guess}}(\mathcal{F}; \mathbf{C})$ always attains the maximum. From the previous connection we can conclude that the same holds for the postmeasurement information problem.

The above discussion is summarized in the following result.

Theorem 2. The postmeasurement information guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ attains its maximum value when \mathbf{C} is the optimal measurement for the standard discrimination problem of the state ensemble \mathcal{F} in (22). The optimal guessing probabilities are related via the equation

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = \Delta(q; n_1, \dots, n_m) P_{\text{guess}}(\mathcal{F}).$$

As an illustration, suppose X has $2n$ elements and it is partitioned into X_1 and X_2 , both having n elements, and that the prior probability p is the uniform distribution on X . Then

$$\mathcal{F}(x_1, x_2) = \frac{1}{n^2} \frac{1}{2} (q_{x_1} + q_{x_2}).$$

We thus see that the state ensemble \mathcal{F} contains all possible equal mixtures of states from \mathcal{E}_1 and \mathcal{E}_2 .

B. Optimal guessing probability in the usual state discrimination problem

We have just seen that it is always possible to transform the problem of state discrimination with postmeasurement information to a usual minimum error state discrimination problem. For this reason, in this section we consider a class of cases where for a single state ensemble \mathcal{E} one can analytically calculate the optimal guessing probability $P_{\text{guess}}(\mathcal{E})$ as well as the optimal measurements. This covers the cases that we will present as examples in Secs. V and VI.

The main result is the following observation.

Proposition 2. Suppose \mathcal{E} is a state ensemble with label set X . For all $x \in X$, denote by $\lambda(x)$ the largest eigenvalue of $\mathcal{E}(x)$, and by $\Pi(x)$ the orthogonal projection onto the $\lambda(x)$ eigenspace of $\mathcal{E}(x)$. Define

$$\lambda_{\mathcal{E}} = \max_{x \in X} \lambda(x), \quad X_{\mathcal{E}} = \{x \in X : \lambda(x) = \lambda_{\mathcal{E}}\}.$$

Then, if there exists $\mu \in \mathbb{R}$ such that

$$\sum_{x \in X_{\mathcal{E}}} \Pi(x) = \mu \mathbb{1}, \quad (25)$$

we have the following consequences:

- (a) $\mu = \frac{1}{d} \sum_{x \in X_{\mathcal{E}}} \text{rank } \Pi(x)$;
- (b) $P_{\text{guess}}(\mathcal{E}) = d\lambda_{\mathcal{E}}$;
- (c) a measurement \mathbf{M}_0 attaining the maximum guessing probability $P_{\text{guess}}(\mathcal{E})$ is

$$\mathbf{M}_0(x) = \begin{cases} \mu^{-1} \Pi(x) & \text{if } x \in X_{\mathcal{E}} \\ 0 & \text{if } x \notin X_{\mathcal{E}}; \end{cases} \quad (26)$$

(d) a measurement \mathbf{M} attains the maximum guessing probability $P_{\text{guess}}(\mathcal{E})$ if and only if

- (i) $\mathbf{M}(x) \leq \Pi(x)$ for all $x \in X_{\mathcal{E}}$;
- (ii) $\mathbf{M}(x) = 0$ for all $x \notin X_{\mathcal{E}}$.

In the following we provide a simple proof of Proposition 2, relying on Lemma 1 given after that. We remark that an alternative longer proof can also be given by making use of the optimality conditions [10, Eq. (III.29)], [18, Theorem II.2.2], which follow from a semidefinite programming argument (see also [19] for a more recent account of these results).

Proof. We assume that (25) holds for some $\mu \in \mathbb{R}$. By taking the trace of both sides of (25), we get $\mu = \frac{1}{d} \sum_{x \in X_{\mathcal{E}}} \text{rank } \Pi(x)$. This proves (a).

For any measurement \mathbf{M} on X , we have

$$\begin{aligned} P_{\text{guess}}(\mathcal{E}; \mathbf{M}) &= \sum_{x \in X} \text{tr}[\mathcal{E}(x)\mathbf{M}(x)] \leq \sum_{x \in X} \lambda(x) \text{tr}[\mathbf{M}(x)] \\ &\leq \lambda_{\mathcal{E}} \sum_{x \in X} \text{tr}[\mathbf{M}(x)] = \lambda_{\mathcal{E}} \text{tr}[\mathbb{1}] = d\lambda_{\mathcal{E}}. \end{aligned}$$

The first inequality follows from Lemma 1 just below, which also implies that the equality is attained if and only if $\mathbf{M}(x) \leq \Pi(x)$ for all $x \in X$. The second inequality is trivial, and it becomes an equality if and only if $\mathbf{M}(x) = 0$ for all $x \notin X_{\mathcal{E}}$. In summary, $P_{\text{guess}}(\mathcal{E}; \mathbf{M}) \leq d\lambda_{\mathcal{E}}$, with equality if and only if the measurement \mathbf{M} satisfies conditions (i) and (ii) of (d).

Since $\Pi(x) \leq \mu \mathbb{1}$ for any $x \in X_{\mathcal{E}}$ by (25), we must have $\mu \geq 1$. Hence, $\mathbf{M}_0(x) \leq \Pi(x)$ for all $x \in X_{\mathcal{E}}$. Moreover, $\mathbf{M}_0(x) = 0$ for all $x \notin X_{\mathcal{E}}$ by the definition of \mathbf{M}_0 . By the discussion in the last paragraph, it follows that \mathbf{M}_0 is optimal, and $P_{\text{guess}}(\mathcal{E}) = P_{\text{guess}}(\mathcal{E}; \mathbf{M}_0) = d\lambda_{\mathcal{E}}$. This proves (b) and (c). Since any optimal measurement \mathbf{M} must then be such that $P_{\text{guess}}(\mathcal{E}; \mathbf{M}) = d\lambda_{\mathcal{E}}$, also (d) follows. ■

Lemma 1 (for Proposition 2). Let $A, B \in \mathcal{L}(\mathcal{H})$ with $A \geq 0$ and $0 \leq B \leq \mathbb{1}$. Let λ be the largest eigenvalue of A and Π the associated eigenprojection. Then,

$$\text{tr}[AB] \leq \lambda \text{tr}[B],$$

and the equality is attained if and only if $B \leq \Pi$.

Proof. Since $\lambda \mathbb{1} - A \geq 0$, we have $\lambda \text{tr}[B] - \text{tr}[AB] = \text{tr}[(\lambda \mathbb{1} - A)B] \geq 0$, where the inequality follows from [10, Lemma 2]. By the same result, the equality is attained if and only if $(\lambda \mathbb{1} - A)B = 0$, that is, $AB = \lambda B$. Note that $AB = \lambda B \Leftrightarrow \text{ran } B \subseteq \text{ran } \Pi$. The latter inclusion implies $\Pi B = B = B\Pi$ and then $B = \Pi B \Pi \leq \Pi \mathbb{1} \Pi = \Pi$. Conversely, if $B \leq \Pi$, then $\ker \Pi \subseteq \ker B$, so that $\text{ran } B \subseteq \text{ran } \Pi$. In conclusion, $AB = \lambda B$ if and only if $B \leq \Pi$, and this completes the proof. ■

Corollary 1. With the notations of Proposition 2, suppose (25) holds for some $\mu \in \mathbb{R}$ and $\text{rank } \Pi(x) = 1$ for all $x \in X_{\mathcal{E}}$. Then, the following facts are equivalent:

- (i) The operators $\{\Pi(x) : x \in X_{\mathcal{E}}\}$ are linearly independent.
- (ii) The measurement \mathbf{M}_0 given in (26) is the unique measurement giving the maximum guessing probability $P_{\text{guess}}(\mathcal{E})$.

Proof. Since $\Pi(x)$ is a rank-1 orthogonal projection, any positive operator A satisfying $A \leq \Pi(x)$ is a scalar multiple of $\Pi(x)$. Therefore, by (d) of Proposition 2, a measurement attains the maximum guessing probability $P_{\text{guess}}(\mathcal{E})$ if and only if it has the form

$$\mathbf{M}_{\alpha}(x) = \begin{cases} \alpha(x) \Pi(x) & \text{if } x \in X_{\mathcal{E}} \\ 0 & \text{if } x \notin X_{\mathcal{E}} \end{cases}$$

for some function $\alpha : X_{\mathcal{E}} \rightarrow [0, 1]$. Since

$$\mathbb{1} = \sum_{x \in X_{\mathcal{E}}} M_{\alpha}(x) = \sum_{x \in X_{\mathcal{E}}} \alpha(x) \Pi(x)$$

and

$$\mathbb{1} = \sum_{x \in X_{\mathcal{E}}} M_0(x) = \sum_{x \in X_{\mathcal{E}}} \mu^{-1} \Pi(x),$$

linear independence of the operators $\{\Pi(x) : x \in X_{\mathcal{E}}\}$ yields $\alpha(x) = \mu^{-1}$ for all $x \in X_{\mathcal{E}}$, hence $M_{\alpha} = M_0$. Conversely, if the operators $\{\Pi(x) : x \in X_{\mathcal{E}}\}$ are not linearly independent, then $\mu > 1$, as otherwise they would be an orthogonal resolution of the identity, which is a contradiction. Moreover, there exists some nonzero function $\beta : X_{\mathcal{E}} \rightarrow \mathbb{C}$ such that

$$0 = \sum_{x \in X_{\mathcal{E}}} \beta(x) \Pi(x) = \sum_{x \in X_{\mathcal{E}}} \overline{\beta(x)} \Pi(x).$$

By possibly replacing β with either $\beta + \bar{\beta}$ or $i(\beta - \bar{\beta})$, we can assume that $\beta : X_{\mathcal{E}} \rightarrow \mathbb{R}$. If $\epsilon \in \mathbb{R} \setminus \{0\}$ is such that $|\epsilon|$ is small enough, then $\alpha(x) = \mu^{-1} + \epsilon\beta(x) \in [0, 1]$ for all $x \in X_{\mathcal{E}}$; hence M_{α} is an optimal measurement with $M_{\alpha} \neq M_0$. ■

We remark that if the rank-1 condition in the statement of Corollary 1 is dropped, then the equivalence of items (i) and (ii) is no longer true; a simple example demonstrating this fact is provided in Appendix A.

Corollary 2. Suppose $\mathcal{P} = (X_{\ell})_{\ell \in I}$ is a partition of X into nonempty disjoint subsets, and define q and \mathcal{E}_{ℓ} as in (2) and (3). If each state ensemble \mathcal{E}_{ℓ} satisfies the hypothesis of Proposition 2 for all $\ell \in I$, then also \mathcal{E} does it, and

$$P_{\text{guess}}(\mathcal{E}) = \max_{\ell \in I} q(\ell) P_{\text{guess}}(\mathcal{E}_{\ell}).$$

Proof. Using the notations of Proposition 2 for the ensemble \mathcal{E} , and denoting by $\lambda_{\ell}(x)$ and $\Pi_{\ell}(x)$ the largest eigenvalue of $\mathcal{E}_{\ell}(x)$ and the corresponding eigenprojection, we have

$$\lambda(x) = q(\ell) \lambda_{\ell}(x) \quad \text{and} \quad \Pi(x) = \Pi_{\ell}(x) \quad \text{for all } x \in X_{\ell}.$$

Setting as usual

$$\lambda_{\mathcal{E}_{\ell}} = \max_{x \in X_{\ell}} \lambda_{\ell}(x), \quad X_{\mathcal{E}_{\ell}} = \{x \in X_{\ell} : \lambda_{\ell}(x) = \lambda_{\mathcal{E}_{\ell}}\},$$

the hypothesis is that

$$\sum_{x \in X_{\mathcal{E}_{\ell}}} \Pi_{\ell}(x) = \mu_{\ell} \mathbb{1} \quad \text{for some } \mu_{\ell} \in \mathbb{R} \text{ and all } \ell \in I.$$

Then,

$$\lambda_{\mathcal{E}} = \max_{\ell \in I} q(\ell) \lambda_{\mathcal{E}_{\ell}},$$

$$X_{\mathcal{E}} = \bigcup_{\ell \in I_0} X_{\mathcal{E}_{\ell}} \quad \text{where} \quad I_0 = \{\ell \in I : q(\ell) \lambda_{\mathcal{E}_{\ell}} = \lambda_{\mathcal{E}}\},$$

$$\sum_{x \in X_{\mathcal{E}}} \Pi(x) = \sum_{\ell \in I_0} \sum_{x \in X_{\mathcal{E}_{\ell}}} \Pi_{\ell}(x) = \sum_{\ell \in I_0} \mu_{\ell} \mathbb{1}.$$

Therefore, the state ensemble \mathcal{E} satisfies condition (25). In particular, by (b) of Proposition 2,

$$P_{\text{guess}}(\mathcal{E}) = d \lambda_{\mathcal{E}} = d \max_{\ell \in I} q(\ell) \lambda_{\mathcal{E}_{\ell}} = \max_{\ell \in I} q(\ell) P_{\text{guess}}(\mathcal{E}_{\ell}).$$

■

A situation where Proposition 2 is applicable occurs, for instance, when a state ensemble \mathcal{E} is invariant under an irreducible projective unitary representation of some symmetry group. More precisely, suppose G is a finite group, and let U be a projective unitary representation of G on \mathcal{H} . We say that a state ensemble \mathcal{E} is U -invariant if $U(g)\mathcal{E}(X)U(g)^* = \mathcal{E}(X)$ for all $g \in G$, where $\mathcal{E}(X) = \{\mathcal{E}(x) : x \in X\}$. The definition of U -invariance for a state ensemble was first given in [9], where an action of the group G on the index set X was also required (see also [20]). Further, we call a state ensemble \mathcal{E} injective if it is injective as a function, i.e., $\mathcal{E}(x) \neq \mathcal{E}(y)$ for $x \neq y$.

Proposition 3. Suppose the projective unitary representation U is irreducible, and let \mathcal{E} be an injective and U -invariant state ensemble. Then, condition (25) holds for some $\mu \in \mathbb{R}$.

Proof. Since \mathcal{E} is injective and U -invariant, we can define an action of G on the index set X by setting $g \cdot x = \mathcal{E}^{-1}(U(g)\mathcal{E}(x)U(g)^*)$ for all $g \in G$ and $x \in X$. Then $\mathcal{E}(g \cdot x) = U(g)\mathcal{E}(x)U(g)^*$. Hence, with the notations of Proposition 2, we have $\lambda(g \cdot x) = \lambda(x)$ and $\Pi(g \cdot x) = U(g)\Pi(x)U(g)^*$. It follows that $g \cdot X_{\mathcal{E}} = X_{\mathcal{E}}$, and $U(g)[\sum_{x \in X_{\mathcal{E}}} \Pi(x)] = [\sum_{x \in X_{\mathcal{E}}} \Pi(x)]U(g)$. The irreducibility of U then implies $\sum_{x \in X_{\mathcal{E}}} \Pi(x) = \mu \mathbb{1}$ for some $\mu \in \mathbb{R}$ by Schur's lemma. ■

If $\mathcal{E}(X) = \{U(g)\mathcal{E}(x_0)U(g)^* : g \in G\}$ for some (hence for any) $x_0 \in X$, and $U(g)\mathcal{E}(x_0)U(g)^* \neq \mathcal{E}(x_0)$ for all $g \in G \setminus \{1\}$, Propositions 2 and 3 are [9, Theorem 4.2]. Under the additional constraint $\text{tr}[\mathcal{E}(x)] = \text{tr}[\mathcal{E}(y)]$ for all $x, y \in X$, U -invariant state ensembles are named *compound geometrically uniform state sets* in the terminology of [20].

V. QUBIT STATE ENSEMBLES WITH DIHEDRAL SYMMETRY

In this section we illustrate the previous general results with three examples of different qubit state ensembles. The first one (Sec. VB) has been already treated in [5] according to the approach explained in Sec. IIC. We provide the solution also for that example, since our method further allows one to establish when the problem has a unique optimal measurement.

A. Notation

The Hilbert space of the system is $\mathcal{H} = \mathbb{C}^2$. We denote by $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ the vector of three Pauli matrices, and

$$\vec{v} \cdot \vec{\sigma} = v_1 \sigma_1 + v_2 \sigma_2 + v_3 \sigma_3$$

for all $\vec{v} \in \mathbb{R}^3$. For any nonzero vector \vec{v} , we write $\hat{v} = \vec{v}/\|\vec{v}\|$. Further, we let \hat{e}_1, \hat{e}_2 , and \hat{e}_3 be the unit vectors along the three fixed coordinate axes.

All of the three examples to be presented share a common symmetry group, i.e., the dihedral group D_2 , consisting of the identity element 1, together with the three 180° rotations α, β , and γ along \hat{e}_1, \hat{e}_2 , and \hat{e}_3 , respectively. This group acts on \mathbb{C}^2 by means of the projective unitary representation

$$U(1) = \mathbb{1}, \quad U(\alpha) = \sigma_1, \quad U(\beta) = \sigma_2, \quad U(\gamma) = \sigma_3.$$

The representation U is irreducible as the operators $\{U(g) : g \in D_2\}$ span the whole space $\mathcal{L}(\mathbb{C}^2)$.

We will use the Bloch representation of qubit states; all states on \mathbb{C}^2 are parametrized by vectors $\vec{a} \in \mathbb{R}^3$ with $\|\vec{a}\| \leq 1$,

the state corresponding to \vec{a} being

$$\rho_{\vec{a}} = \frac{1}{2}(\mathbb{1} + \vec{a} \cdot \vec{\sigma}).$$

For any nonzero vector \vec{a} , the eigenvalues λ_+, λ_- of $\rho_{\vec{a}}$ and the corresponding eigenprojections Π_+, Π_- are

$$\lambda_{\pm} = \frac{1}{2}(1 \pm \|\vec{a}\|), \quad \Pi_{\pm} = \frac{1}{2}(\mathbb{1} \pm \hat{a} \cdot \vec{\sigma}).$$

B. Two equally probable qubit eigenbases

In the first example, the total state ensemble consists of four pure states $\rho_{\pm\hat{a}}$ and $\rho_{\pm\hat{b}}$, where

$$\hat{a} = \cos(\theta/2)\hat{e}_1 + \sin(\theta/2)\hat{e}_2,$$

$$\hat{b} = \cos(\theta/2)\hat{e}_1 - \sin(\theta/2)\hat{e}_2,$$

and θ is an angle in the interval $(0, \pi)$. The states $\rho_{\pm\hat{a}}$ and $\rho_{\pm\hat{b}}$ are the eigenstates of the operators $\hat{a} \cdot \vec{\sigma}$ and $\hat{b} \cdot \vec{\sigma}$, respectively. The label set is chosen to be $X = \{+\hat{a}, -\hat{a}, +\hat{b}, -\hat{b}\}$. We assume that all states are equally likely; thus the state ensemble \mathcal{E} is

$$\mathcal{E}(\hat{x}) = \frac{1}{8}(\mathbb{1} + \hat{x} \cdot \vec{\sigma}), \quad \hat{x} \in X.$$

We will then consider the partition $\mathcal{P} = (X_a, X_b)$, with $X_\ell = \{+\hat{\ell}, -\hat{\ell}\}$. As usual, the corresponding state subensembles are denoted by \mathcal{E}_a and \mathcal{E}_b , and $q(\ell) = 1/2$ is the probability that a label occurs in X_ℓ .

Since $\mathcal{E}_\ell(\pm\hat{\ell}) = \frac{1}{4}(\mathbb{1} \pm \hat{\ell} \cdot \vec{\sigma})$, we see that each state ensemble \mathcal{E}_ℓ corresponds to preparing one of the two orthogonal pure states $\rho_{+\hat{\ell}}, \rho_{-\hat{\ell}}$ with equal probability. So, the sharp measurements

$$\mathbf{N}_a(\pm\hat{a}) = \frac{1}{2}(\mathbb{1} \pm \hat{a} \cdot \vec{\sigma}), \quad \mathbf{N}_b(\pm\hat{b}) = \frac{1}{2}(\mathbb{1} \pm \hat{b} \cdot \vec{\sigma}),$$

perfectly discriminate \mathcal{E}_a and \mathcal{E}_b , respectively; in particular, $P_{\text{guess}}(\mathcal{E}_a) = P_{\text{guess}}(\mathcal{E}_b) = 1$, hence $P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}) = 1$. Moreover, Corollary 2 applies, and we conclude that $P_{\text{guess}}(\mathcal{E}) = 1/2$. The value of $P_{\text{guess}}(\mathcal{E})$ can be obtained in various different ways (see, e.g., [3]). Interestingly, $P_{\text{guess}}(\mathcal{E})$ does not depend on the angle θ .

To calculate the postinformation guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$, we apply Theorem 2 and calculate $P_{\text{guess}}(\mathcal{F})$, where the auxiliary state ensemble \mathcal{F} on $X_a \times X_b$ is given as

$$\begin{aligned} \mathcal{F}(h\hat{a}, k\hat{b}) &= \frac{1}{8} \left[\mathbb{1} + \frac{1}{2}(h\hat{a} + k\hat{b}) \cdot \vec{\sigma} \right], \quad h, k \in \{+, -\} \\ &= \begin{cases} \frac{1}{4}\rho_{h\cos(\theta/2)\hat{e}_1} & \text{if } h = k \\ \frac{1}{4}\rho_{h\sin(\theta/2)\hat{e}_2} & \text{otherwise,} \end{cases} \end{aligned}$$

and $\Delta = 2$. This state ensemble is clearly injective, and it is U -invariant as the set $\{h\hat{a} + k\hat{b} : h, k = \pm\} \subset \mathbb{R}^3$ is invariant under the action of the dihedral group D_2 . Hence, Proposition 2 is applicable by virtue of Proposition 3, and it thus leads us to find the largest eigenvalue of $\mathcal{F}(h\hat{a}, k\hat{b})$ and the corresponding eigenprojection. We obtain

$$\begin{aligned} \lambda(h\hat{a}, k\hat{b}) &= \begin{cases} \frac{1}{8} \left(1 + \sqrt{\frac{1+\cos\theta}{2}} \right) & \text{if } h = k \\ \frac{1}{8} \left(1 + \sqrt{\frac{1-\cos\theta}{2}} \right) & \text{otherwise,} \end{cases} \\ \Pi(h\hat{a}, k\hat{b}) &= \begin{cases} \frac{1}{2}(\mathbb{1} + h\sigma_1) & \text{if } h = k \\ \frac{1}{2}(\mathbb{1} + h\sigma_2) & \text{otherwise,} \end{cases} \end{aligned}$$

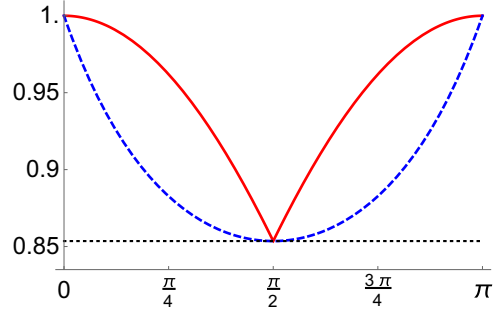


FIG. 5. The red solid curve is the optimal guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ as a function of the angle θ between \hat{a} and \hat{b} , while the blue dashed curve is the lower bound (28) coming from the optimal joint measurement of uniformly noisy versions of \mathbf{N}_a and \mathbf{N}_b .

and hence

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = \Delta d\lambda_{\mathcal{F}} = \frac{1}{2} \left(1 + \sqrt{\frac{1 + |\cos\theta|}{2}} \right). \quad (27)$$

As one could have expected, the unique minimum is in $\theta = \pi/2$ and the guessing probabilities are the same for θ_1 and θ_2 when $\theta_2 = \pi - \theta_1$ (see Fig. 5).

As shown in [21], we have $j(\mathbf{N}_a, \mathbf{N}_b) = j_u(\mathbf{N}_a, \mathbf{N}_b) = 1/\sqrt{1 + |\sin\theta|}$. Therefore, the lower bound for $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ given in (19) is

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) \geq \frac{1}{2} \left(1 + \frac{1}{\sqrt{1 + |\sin\theta|}} \right). \quad (28)$$

We see that the right-hand side agrees with $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ if and only if $\theta = \pi/2$ (see Fig. 5). In particular, this shows that the noisy versions of the form (17) are optimal only in the case $\theta = \pi/2$.

In order to find all optimal measurements, we distinguish the three cases $\theta \in (0, \pi/2)$, $\theta = \pi/2$, and $\theta \in (\pi/2, \pi)$.

1. Case $\theta \in (0, \pi/2)$

We have $(X_a \times X_b)_{\mathcal{F}} = \{(+\hat{a}, +\hat{b}), (-\hat{a}, -\hat{b})\}$, and the projections $\{\Pi(h\hat{a}, k\hat{b}) : (h\hat{a}, k\hat{b}) \in (X_a \times X_b)_{\mathcal{F}}\}$ are rank-1 linearly independent operators. From Corollary 1 we conclude that the measurement \mathbf{C}_+ , defined as

$$\mathbf{C}_+(h\hat{a}, k\hat{b}) = \begin{cases} \frac{1}{2}(\mathbb{1} + h\sigma_1) & \text{if } h = k \\ 0 & \text{otherwise} \end{cases}$$

is the unique measurement on $X_a \times X_b$ achieving $P_{\text{guess}}(\mathcal{F})$, and hence also $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$. The two marginals $\pi_{1*}\mathbf{C}_+$ and $\pi_{2*}\mathbf{C}_+$ of \mathbf{C}_+ are such that $\pi_{1*}\mathbf{C}_+(\pm\hat{a}) = \pi_{2*}\mathbf{C}_+(\pm\hat{b})$, and Bob therefore is not using the postmeasurement information to guess the spin value $+$ or $-$. Bob can, in fact, choose a measurement \mathbf{M} with outcomes $\{+, -\}$, $\mathbf{M}(h) = \frac{1}{2}(\mathbb{1} + h\sigma_1)$, and when Alice announces that her choice was from subset X_ℓ , Bob's guess is $h\hat{\ell}$, where h is the outcome of \mathbf{M} .

In GW's approach, this is a situation in which postmeasurement information is useless [5, Sec. III C], as the diagonal measurement $\mathbf{C}'_+(h, k) = \delta_{h, k}\mathbf{C}_+(h\hat{a}, k\hat{b})$ is optimal for the task of discriminating a string in $\mathcal{X} = \{+, -\}$ even if Alice announces her encoding a or b after the measurement (see Sec. II C). In spite of this fact, $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$ is strictly larger than

$P_{\text{guess}}(\mathcal{E})$. The reason is that with postmeasurement information Bob gets the correct index $\ell \in \{a, b\}$ for free, so he can optimize his measurement to distinguish between one of the two alternatives $\pm \hat{\ell}$, instead of four alternatives $\pm \hat{a}, \pm \hat{b}$.

2. Case $\theta \in (\pi/2, \pi)$

Now $(X_a \times X_b)_{\mathcal{F}} = \{(+\hat{a}, -\hat{b}), (-\hat{a}, +\hat{b})\}$; hence, proceeding as in the previous case, we find that the unique optimal measurement is

$$\mathbf{C}_-(h\hat{a}, k\hat{b}) = \begin{cases} 0 & \text{if } h = k \\ \frac{1}{2}(\mathbb{1} + h\sigma_2) & \text{otherwise.} \end{cases}$$

In this case, we have $\pi_{1*}\mathbf{C}_-(\pm\hat{a}) \neq \pi_{2*}\mathbf{C}_-(\pm\hat{b})$, therefore Bob is actually using postmeasurement information (see [5, Sec. III C]).

3. Case $\theta = \pi/2$

In this case, $(X_a \times X_b)_{\mathcal{F}} = X_a \times X_b$, and the projections $\{\Pi(h\hat{a}, k\hat{b}) : (h\hat{a}, k\hat{b}) \in (X_a \times X_b)_{\mathcal{F}}\}$ are not linearly independent. However, they are still rank-1, hence, by (d) of Proposition 2, any measurement maximizing $P_{\text{guess}}(\mathcal{F}; \mathbf{C})$ is of the form $\mathbf{C}(h\hat{a}, k\hat{b}) = \alpha(h, k)\Pi(h\hat{a}, k\hat{b})$ for some function $\alpha : \{+, -\}^2 \rightarrow [0, 1]$. The normalization condition $\sum_{h, k} \mathbf{C}(h\hat{a}, k\hat{b}) = \mathbb{1}$ imposes

$$\begin{aligned} \alpha(+, +) &= \alpha(-, -) = t, \\ \alpha(+, -) &= \alpha(-, +) = 1 - t \end{aligned}$$

for some $t \in [0, 1]$. Therefore, an optimal measurement is any convex combination of the two measurements \mathbf{C}_+ and \mathbf{C}_- found earlier. The convex combination $\mathbf{C}_0 = \frac{1}{2}\mathbf{C}_+ + \frac{1}{2}\mathbf{C}_-$ is the optimal measurement given in (26), which in this case reads

$$\mathbf{C}_0(h\hat{a}, k\hat{b}) = \frac{1}{4} \left(\mathbb{1} + \frac{h+k}{2} \sigma_1 + \frac{h-k}{2} \sigma_2 \right).$$

Its marginals are

$$\begin{aligned} \pi_{1*}\mathbf{C}_0(h\hat{a}) &= \frac{1}{\sqrt{2}} \mathbf{N}_a(h\hat{a}) + \left(1 - \frac{1}{\sqrt{2}}\right) \frac{1}{2} \mathbb{1}, \\ \pi_{2*}\mathbf{C}_0(k\hat{b}) &= \frac{1}{\sqrt{2}} \mathbf{N}_b(k\hat{b}) + \left(1 - \frac{1}{\sqrt{2}}\right) \frac{1}{2} \mathbb{1}. \end{aligned}$$

These are noisy versions of the optimal measurements \mathbf{N}_a and \mathbf{N}_b for the maximization problems $\max_{\mathbf{M}} P_{\text{guess}}(\mathcal{E}_a; \mathbf{M})$ and $\max_{\mathbf{M}} P_{\text{guess}}(\mathcal{E}_b; \mathbf{M})$, respectively. In this case, as we already observed, one implementation of the optimal strategy is hence to make an approximate joint measurement of \mathbf{N}_a and \mathbf{N}_b .

C. Two qubit state ensembles with dihedral D_{2n} -symmetry

Let us consider a state ensemble \mathcal{E} , labeled by the $2n + 2$ labels $X = \{+, -, 0, 1, \dots, 2n - 1\}$, and defined as

$$\begin{aligned} \mathcal{E}(\pm) &= \frac{q_1}{4} (\mathbb{1} \pm \sigma_1), \\ \mathcal{E}(k) &= \frac{q_2}{4n} (\mathbb{1} + \hat{a}_k \cdot \vec{\sigma}), \quad k = 0, \dots, 2n - 1, \end{aligned}$$

where

$$\hat{a}_k = \cos(\pi k/n) \hat{e}_2 + \sin(\pi k/n) \hat{e}_3$$

and $q_1, q_2 > 0, q_1 + q_2 = 1$.

We consider the partition $\mathcal{P} = (X_\ell)_{\ell \in \{1, 2\}}$ of X , with $X_1 = \{+, -\}$ and $X_2 = \{0, 1, \dots, 2n - 1\}$. The corresponding subensembles are $\mathcal{E}_1(\pm) = \frac{1}{4}(\mathbb{1} \pm \sigma_1)$ and $\mathcal{E}_2(k) = \frac{1}{4n}(\mathbb{1} + \hat{a}_k \cdot \vec{\sigma})$, and the probability q is $q(\ell) = q_\ell$.

Each of the two state ensembles $\mathcal{E}_1, \mathcal{E}_2$ is injective and D_2 -invariant. By Proposition 3 (or even by direct inspection), it follows that \mathcal{E}_1 and \mathcal{E}_2 satisfy the hypothesis of Proposition 2. Then, by Corollary 2 we have

$$P_{\text{guess}}(\mathcal{E}) = \max\{q_1 P_{\text{guess}}(\mathcal{E}_1), q_2 P_{\text{guess}}(\mathcal{E}_2)\}.$$

The subensemble \mathcal{E}_1 consists of two orthogonal pure states, hence it can be perfectly discriminated with the measurement $\mathbf{N}_1(\pm) = \frac{1}{2}(\mathbb{1} \pm \sigma_1)$. On the other hand, an optimal measurement to discriminate the states in \mathcal{E}_2 is $\mathbf{N}_2(k) = \frac{1}{2n}(\mathbb{1} + \hat{a}_k \cdot \vec{\sigma})$ by (c) of Proposition 2, and $P_{\text{guess}}(\mathcal{E}_2) = 1/n$ by (b) of the same proposition. It follows that

$$P_{\text{guess}}(\mathcal{E}) = \max\left\{q_1, \frac{q_2}{n}\right\} = \begin{cases} q_1 & \text{if } q_1 > \frac{1}{n+1} \\ \frac{1-q_1}{n} & \text{if } q_1 \leq \frac{1}{n+1} \end{cases}$$

and

$$P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}) = q_1 + \frac{q_2}{n} = \frac{(n-1)q_1 + 1}{n}.$$

To calculate $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$, we first form the auxiliary state ensemble \mathcal{F} of Theorem 2. Its label set is the Cartesian product $\{+, -\} \times \{0, 1, \dots, 2n - 1\}$, it has $\Delta = 2(nq_1 + q_2)$, and it is given by

$$\mathcal{F}(h, k) = \frac{1}{8n} \left(\mathbb{1} + \frac{nq_1 h \hat{e}_1 + q_2 \hat{a}_k}{nq_1 + q_2} \cdot \vec{\sigma} \right).$$

The state ensemble \mathcal{F} is injective and U -invariant. Although the symmetry group of \mathcal{F} can be extended to the order $4n$ dihedral group $D_{2n} \supset D_2$, Proposition 3 yields that D_2 -symmetry is already enough to ensure the applicability of Proposition 2. The largest eigenvalue of $\mathcal{F}(h, k)$ and the corresponding eigenprojection are found to be

$$\begin{aligned} \lambda(h, k) &= \frac{1}{8n} \left(1 + \frac{\sqrt{n^2 q_1^2 + q_2^2}}{nq_1 + q_2} \right), \\ \Pi(h, k) &= \frac{1}{2} \left(\mathbb{1} + \frac{nq_1 h \hat{e}_1 + q_2 \hat{a}_k}{\sqrt{n^2 q_1^2 + q_2^2}} \cdot \vec{\sigma} \right). \end{aligned}$$

It follows that $(X_1 \times X_2)_{\mathcal{F}} = X_1 \times X_2$. The operators $\{\Pi(h, k) : (h, k) \in (X_1 \times X_2)_{\mathcal{F}}\}$ are rank-1 but they are not linearly independent. Thus, we do not have uniqueness of optimal measurements. By Theorem 2 and Proposition 2,

$$\begin{aligned} P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) &= \Delta d \lambda_{\mathcal{F}} \\ &= \frac{1}{2n} \left(nq_1 + q_2 + \sqrt{n^2 q_1^2 + q_2^2} \right) \\ &= \frac{1}{2n} \left[(n-1)q_1 + 1 + \sqrt{(n^2 + 1)q_1^2 - 2q_1 + 1} \right]. \end{aligned}$$

This maximum is attained by $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ if and only if \mathbf{C} is a measurement of the form

$$\mathbf{C}(h, k) = \frac{\alpha(h, k)}{2} \left(\mathbb{1} + \frac{nq_1 h \hat{e}_1 + q_2 \hat{a}_k}{\sqrt{n^2 q_1^2 + q_2^2}} \cdot \vec{\sigma} \right),$$

where $\alpha : X_1 \times X_2 \rightarrow [0, 1]$ is such that

$$\begin{aligned} \sum_k \alpha(+, k) &= \sum_k \alpha(-, k) = 1, \\ \sum_k [\alpha(+, k) + \alpha(-, k)] \hat{a}_k &= 0 \end{aligned}$$

by the normalization condition for \mathbf{C} .

By choosing the constant function $\alpha(h, k) = \frac{1}{2n}$, we recover the optimal measurement of (26). The marginals of that measurement are the uniformly noisy versions of the measurements $\mathbf{N}_1(\pm) = \frac{1}{2}(\mathbb{1} \pm \sigma_1)$ and $\mathbf{N}_2(k) = \frac{1}{2n}(\mathbb{1} + \hat{a}_k \cdot \vec{\sigma})$ optimally discriminating the subensembles \mathcal{E}_1 and \mathcal{E}_2 .

D. Three orthogonal qubit eigenbases

Next we consider a state ensemble \mathcal{E} with six elements, having the index set $X = \{+\hat{e}_1, -\hat{e}_1, +\hat{e}_2, -\hat{e}_2, +\hat{e}_3, -\hat{e}_3\}$ and defined as

$$\mathcal{E}(\pm \hat{e}_\ell) = \frac{q_\ell}{4} (\mathbb{1} \pm \sigma_\ell), \quad \ell \in \{1, 2, 3\},$$

where $q_1, q_2, q_3 > 0$ and $q_1 + q_2 + q_3 = 1$. As the partition of X , we fix $\mathcal{P} = (X_\ell)_{\ell \in \{1, 2, 3\}}$ with $X_\ell = \{+\hat{e}_\ell, -\hat{e}_\ell\}$. The corresponding subensembles are $\mathcal{E}_\ell(\pm \hat{e}_\ell) = \frac{1}{4}(\mathbb{1} \pm \sigma_\ell)$, and $q(\ell) = q_\ell$.

Each subensemble \mathcal{E}_ℓ consists of orthogonal pure states and hence can be discriminated with probability 1, the optimal measurement being $\mathbf{N}_\ell(\pm \hat{e}_\ell) = \frac{1}{2}(\mathbb{1} \pm \sigma_\ell)$. We thus have $P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}) = 1$, and from Corollary 2 it follows that $P_{\text{guess}}(\mathcal{E}) = \max\{q_1, q_2, q_3\}$.

To calculate $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P})$, we again form the auxiliary state ensemble \mathcal{F} , which in this case is

$$\mathcal{F}(k_1 \hat{e}_1, k_2 \hat{e}_2, k_3 \hat{e}_3) = \frac{1}{16} \left(\mathbb{1} + \sum_{\ell=1}^3 q_\ell k_\ell \sigma_\ell \right).$$

In the above formula, $k_\ell \in \{+, -\}$; moreover, we have $\Delta = 4$. As in the previous cases, the state ensemble \mathcal{F} is injective and U -invariant, and Proposition 2 then applies. We obtain

$$\begin{aligned} \lambda(k_1 \hat{e}_1, k_2 \hat{e}_2, k_3 \hat{e}_3) &= \frac{1}{16} (1 + \|\vec{q}\|), \\ \Pi(k_1 \hat{e}_1, k_2 \hat{e}_2, k_3 \hat{e}_3) &= \frac{1}{2} \left(\mathbb{1} + \frac{1}{\|\vec{q}\|} \sum_{\ell=1}^3 q_\ell k_\ell \sigma_\ell \right), \end{aligned}$$

where we set $\vec{q} = \sum_{\ell=1}^3 q_\ell \hat{e}_\ell$. Therefore,

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = \Delta d \lambda_{\mathcal{F}} = \frac{1}{2} \left(1 + \sqrt{q_1^2 + q_2^2 + q_3^2} \right).$$

In the case $q_1 = q_2 = q_3 = 1/3$, we have $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = (1 + 1/\sqrt{3})/2$. As explained in Appendix B, $j(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3) = j_u(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3) = 1/\sqrt{3}$. Therefore, the guessing probability with postmeasurement information equals with the lower

bound given in (19), and we conclude that one way to implement the optimal measurement is to make a joint measurement of uniformly noisy versions of $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3$.

Since $(X_1 \times X_2 \times X_3)_{\mathcal{F}} = X_1 \times X_2 \times X_3$ and all operators $\Pi(k_1 \hat{e}_1, k_2 \hat{e}_2, k_3 \hat{e}_3)$'s are rank-1, any optimal measurement is of the form

$$\mathbf{C}(k_1 \hat{e}_1, k_2 \hat{e}_2, k_3 \hat{e}_3) = \frac{\alpha(k_1, k_2, k_3)}{2} \left(\mathbb{1} + \frac{1}{\|\vec{q}\|} \sum_{\ell=1}^3 q_\ell k_\ell \sigma_\ell \right)$$

for some function $\alpha : \{+, -\}^3 \rightarrow [0, 1]$. The normalization of \mathbf{C} implies that, for every $k_1, k_2, k_3 \in \{+, -\}$,

$$\sum_{i, j} \alpha(k_1, i, j) = \sum_{i, j} \alpha(i, k_2, j) = \sum_{i, j} \alpha(i, j, k_3) = 1.$$

One solution is to take the constant function $\alpha \equiv 1/4$, and that choice gives the optimal measurement of (26). The marginals of this measurement are uniformly noisy versions of \mathbf{N}_1 , \mathbf{N}_2 , and \mathbf{N}_3 . Another possibility is

$$\alpha(k_1, k_2, k_3) = \begin{cases} 1 & \text{if } k_1 = k_2 = k_3 \\ 0 & \text{otherwise.} \end{cases}$$

In GW's approach of Sec. IIC, the latter choice corresponds to the diagonal optimal measurement

$$\mathbf{C}'(k_1, k_2, k_3) = \begin{cases} \frac{1}{2} (\mathbb{1} + k \hat{q} \cdot \vec{\sigma}) & \text{if } k_1 = k_2 = k_3 \equiv k \\ 0 & \text{otherwise.} \end{cases}$$

In particular, we see that from the point of view of GW's approach, postmeasurement information is useless in this example.

VI. TWO FOURIER CONJUGATE MUTUALLY UNBIASED BASES

In this section, we consider the discrimination problem with postmeasurement information for two mutually unbiased bases (MUB) in arbitrary finite dimension d . We restrict to the case in which the two bases are conjugated by the Fourier transform of the cyclic group $\mathbb{Z}_d = \{0, \dots, d-1\}$, endowed with the composition law given by addition mod d . Moreover, we assume that all elements of each basis have equal *a priori* probabilities. However, we allow the occurrence probability of a basis to differ from that of the other one.

In formulas, we fix two orthonormal bases $(\varphi_h)_{h \in \mathbb{Z}_d}$ and $(\psi_k)_{k \in \mathbb{Z}_d}$ of \mathcal{H} , such that

$$\psi_k = \frac{1}{\sqrt{d}} \sum_{h \in \mathbb{Z}_d} \omega^{hk} \varphi_h \quad \text{where} \quad \omega = e^{2\pi i/d}.$$

They satisfy the mutual unbiasedness condition

$$|\langle \varphi_h | \psi_k \rangle| = \frac{1}{\sqrt{d}} \quad \forall h, k \in \mathbb{Z}_d.$$

We label the two bases by means of the symbols $X_\varphi = \{0\varphi, \dots, (d-1)\varphi\}$ and $X_\psi = \{0\psi, \dots, (d-1)\psi\}$, respectively, and we let $X = X_\varphi \cup X_\psi$ be the overall label set. Notice that, consistently with the previous examples, the elements of X are denoted by juxtaposing the index of the vector with the symbol of the basis which the vector belongs to [for example, the symbol 0φ labels the first vector in the basis $(\varphi_h)_{h \in \mathbb{Z}_d}$].

Then, we partition X and use it to construct a state ensemble \mathcal{E} as follows:

$$\mathcal{P} = (X_\ell)_{\ell \in \{\varphi, \psi\}}, \quad (29)$$

$$\mathcal{E}(h\ell) = \frac{q_\ell}{d} |\ell_h\rangle \langle \ell_h|, \quad h\ell \in X, \quad (30)$$

where $q_\varphi, q_\psi > 0$ with $q_\varphi + q_\psi = 1$. The partition \mathcal{P} yields the two subensembles

$$\mathcal{E}_\ell(h\ell) = \frac{1}{d} |\ell_h\rangle \langle \ell_h|, \quad h \in \mathbb{Z}_d,$$

with $\ell \in \{\varphi, \psi\}$; the probability that a label occurs in the subset X_ℓ is $q(\ell) = q_\ell$.

Note that in Sec. VB, the two equally probable qubit eigenbases with angle $\theta = \pi/2$ constitute two MUB that are conjugated by the Fourier transform of the cyclic group \mathbb{Z}_2 . Indeed, this follows by setting

$$\varphi_0 = \frac{1}{\sqrt{2}}(e^{-i(\pi/8)}\eta_1 + e^{i(\pi/8)}\eta_2)$$

$$\varphi_1 = \frac{i}{\sqrt{2}}(e^{-i(\pi/8)}\eta_1 - e^{i(\pi/8)}\eta_2),$$

where (η_1, η_2) is the canonical (computational) basis of \mathbb{C}^2 , choosing $q_\varphi = q_\psi = 1/2$, and relabeling

$$0\varphi \rightarrow +\hat{a}, \quad 1\varphi \rightarrow -\hat{a}, \quad 0\psi \rightarrow +\hat{b}, \quad 1\psi \rightarrow -\hat{b}.$$

We define two measurements \mathbf{N}_φ and \mathbf{N}_ψ with outcomes in X_φ and X_ψ , respectively, as

$$\mathbf{N}_\ell(h\ell) = |\ell_h\rangle \langle \ell_h|, \quad h \in \mathbb{Z}_d.$$

Each of these measurements perfectly discriminates the corresponding subensemble \mathcal{E}_ℓ . Moreover, once again Corollary 2 can be applied, thus leading to

$$P_{\text{guess}}(\mathcal{E}) = \max\{q_\varphi, q_\psi\} = |q_\varphi - \frac{1}{2}| + \frac{1}{2}.$$

$$P_{\text{guess}}^{\text{prior}}(\mathcal{E}; \mathcal{P}) = 1.$$

By Theorem 2, optimizing the postinformation guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ over all measurements \mathbf{C} on $X_\varphi \times X_\psi$ amounts to the same optimization problem for $P_{\text{guess}}(\mathcal{F}; \mathbf{C})$, where \mathcal{F} is the auxiliary state ensemble

$$\mathcal{F}(h\varphi, k\psi) = \frac{1}{d^2}(q_\varphi |\varphi_h\rangle \langle \varphi_h| + q_\psi |\psi_k\rangle \langle \psi_k|).$$

The state ensemble \mathcal{F} has the direct product Abelian group $G = \mathbb{Z}_d \times \mathbb{Z}_d$ as its natural symmetry group. Indeed, by defining the generalized Pauli operators

$$W(r, s) = \sum_{z \in \mathbb{Z}_d} \omega^{sz} |\varphi_{r+z}\rangle \langle \varphi_z|,$$

we obtain a projective unitary representation of $\mathbb{Z}_d \times \mathbb{Z}_d$, such that

$$W(r_1, s_1)W(r_2, s_2) = \omega^{s_1 r_2} W(r_1 + r_2, s_1 + s_2),$$

$$W(r, s)\varphi_h = \omega^{sh}\varphi_{r+h}, \quad W(r, s)\psi_k = \omega^{-r(s+k)}\psi_{s+k}$$

(see, e.g., [22,23]; here, $W(r, s) = U_r V_s$ in terms of the discrete position and momentum displacement operators U_r and V_s

defined in [23, Sec. IV A]). Then, the state ensemble \mathcal{F} is W -invariant, as

$$W(r, s)\mathcal{F}(h\varphi, k\psi)W(r, s)^* = \mathcal{F}((h+r)\varphi, (k+s)\psi) \quad (31)$$

for all $h, k, r, s \in \mathbb{Z}_d$. Since the representation W is irreducible [22] and the state ensemble \mathcal{F} is clearly injective, Proposition 2 can be applied to \mathcal{F} by Proposition 3. In order to proceed as usual, we need the next lemma.

Lemma 2. For all $h, k \in \mathbb{Z}_d$, the largest eigenvalue and the corresponding eigenprojection of $\mathcal{F}(h\varphi, k\psi)$ are

$$\lambda(h\varphi, k\psi) = \frac{1}{2d^2} \left[1 + \sqrt{(q_\varphi - q_\psi)^2 + \frac{4}{d} q_\varphi q_\psi} \right], \quad (32a)$$

$$\begin{aligned} \Pi(h\varphi, k\psi) &= |\alpha\varphi_h + \beta\omega^{-hk}\psi_k\rangle \langle \alpha\varphi_h + \beta\omega^{-hk}\psi_k| \\ &= W(h, k)|\alpha\varphi_0 + \beta\psi_0\rangle \langle \alpha\varphi_0 + \beta\psi_0| W(h, k)^*, \end{aligned} \quad (32b)$$

where the couple (α, β) is the unique solution to the following system of equations:

$$\alpha > 0, \quad \beta > 0, \quad (33a)$$

$$\alpha^2 + \beta^2 + \frac{2}{\sqrt{d}}\alpha\beta = 1, \quad (33b)$$

$$\frac{\alpha}{\beta} = \frac{\sqrt{d}}{2q_\psi} \left[q_\varphi - q_\psi + \sqrt{(q_\varphi - q_\psi)^2 + \frac{4}{d} q_\varphi q_\psi} \right]. \quad (33c)$$

Equation (33b) describes an ellipse in the $\alpha\beta$ plane centered at $(0,0)$ and having the minor axis along the $\alpha = \beta$ direction. The solution of (33) is where this ellipse intersects the half-line originating at $(0,0)$, lying in the first quadrant (33a) and having the positive slope given by (33c).

Proof. By means of the covariance condition (31) for \mathcal{F} , it is enough to prove (32) only for $h = k = 0$. In order to do it, we preliminarily observe that the operator $\mathcal{F}(0\varphi, 0\psi)$ leaves the linear subspace $\mathcal{H}_0 = \text{span}(\varphi_0, \psi_0)$ invariant, and it is null on \mathcal{H}_0^\perp . Moreover, with respect to the linear (nonorthogonal) basis (φ_0, ψ_0) of \mathcal{H}_0 , the restriction of $\mathcal{F}(0\varphi, 0\psi)$ to \mathcal{H}_0 has the matrix form

$$\mathcal{F}(0\varphi, 0\psi)|_{\mathcal{H}_0} = \frac{1}{d^2} \begin{pmatrix} q_\varphi & \frac{1}{\sqrt{d}}q_\varphi \\ \frac{1}{\sqrt{d}}q_\psi & q_\psi \end{pmatrix}.$$

The roots of the characteristic polynomial of the above matrix are

$$\lambda_\pm = \frac{1}{2d^2} \left[1 \pm \sqrt{(q_\varphi - q_\psi)^2 + \frac{4}{d} q_\varphi q_\psi} \right]$$

(recall $q_\varphi + q_\psi = 1$), and they are clearly different. This gives (32). By direct inspection of the previous matrix, the vector $\chi = \alpha\varphi_0 + \beta\psi_0$ is a nonzero λ_+ eigenvector of $\mathcal{F}(0\varphi, 0\psi)$ if and only if the ratio α/β is given by (33c). Normalization of χ gives (33b). Since the ratio α/β is real and positive, (33b) and (33c) have a unique common solution satisfying (33a). ■

Proposition 4. For the state ensemble \mathcal{E} of (30) and the partition \mathcal{P} of (29), we have

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = \frac{1}{2} \left[1 + \sqrt{(q_\varphi - q_\psi)^2 + \frac{4}{d} q_\varphi q_\psi} \right]. \quad (34)$$

Moreover, a measurement on $X_\varphi \times X_\psi$ maximizing the guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ is

$$\begin{aligned} \mathbf{C}_0(h\varphi, k\psi) &= \frac{1}{d} |\alpha\varphi_h + \beta\omega^{-hk}\psi_k\rangle\langle\alpha\varphi_h + \beta\omega^{-hk}\psi_k| \\ &= \frac{1}{d} W(h, k) |\alpha\varphi_0 + \beta\psi_0\rangle\langle\alpha\varphi_0 + \beta\psi_0| W(h, k)^*, \end{aligned} \quad (35)$$

where (α, β) is the solution to the system of equations (33). The measurement \mathbf{C}_0 is the unique measurement maximizing the guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ if and only if the dimension d of \mathcal{H} is odd.

Proof. We have already seen that Proposition 2 can be applied to the state ensemble \mathcal{F} . With the notations of that proposition, we have

$$\lambda_{\mathcal{F}} = \frac{1}{2d^2} \left[1 + \sqrt{(q_\varphi - q_\psi)^2 + \frac{4}{d} q_\varphi q_\psi} \right],$$

$$(X_\varphi \times X_\psi)_{\mathcal{F}} = X_\varphi \times X_\psi$$

by Lemma 2. In particular, the value of $\lambda_{\mathcal{F}}$ and Theorem 2 with $\Delta = d$ imply (34). Moreover, still by Lemma 2, the measurement \mathbf{C}_0 in (35) is the optimal measurement (26) for the guessing probability $P_{\text{guess}}(\mathcal{F}; \mathbf{C})$, hence also for $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$. By Corollary 1, there is no other measurement maximizing the guessing probability $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ if and only if the operators $\{\Pi(h\varphi, k\psi) : h, k \in \mathbb{Z}_d\}$ are linearly independent. The argument used in the proof of [23, Proposition 9] shows that this is equivalent to the dimension d of \mathcal{H} being odd. ■

In the particular case $q_\varphi = q_\psi = \frac{1}{2}$, formulas (34) and (35) simplify as follows:

$$P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{d}} \right),$$

$$\mathbf{C}_0(h\varphi, k\psi) = \frac{1}{2(\sqrt{d} + d)} W(h, k) |\varphi_0 + \psi_0\rangle\langle\varphi_0 + \psi_0| W(h, k)^*,$$

which, for $d = 2$, are easily seen to be consistent with the results of Sec. VB.

For general q_φ, q_ψ , the first marginal of \mathbf{C}_0 is

$$\begin{aligned} \pi_{1*}\mathbf{C}_0(h\varphi) &= \frac{1}{d} \sum_{k \in \mathbb{Z}_d} [\alpha^2 |\varphi_h\rangle\langle\varphi_h| + \beta^2 |\psi_k\rangle\langle\psi_k| \\ &\quad + \alpha\beta (|\omega^{-hk}\psi_k\rangle\langle\varphi_h| + |\varphi_h\rangle\langle\omega^{-hk}\psi_k|)] \\ &= \alpha^2 |\varphi_h\rangle\langle\varphi_h| + \frac{\beta^2}{d} \mathbb{1} + \frac{2\alpha\beta}{\sqrt{d}} |\varphi_h\rangle\langle\varphi_h| \\ &= t_\varphi \mathbf{N}_\varphi(h\varphi) + (1 - t_\varphi) \frac{1}{d} \mathbb{1}, \end{aligned} \quad (36)$$

where $t_\varphi = \alpha^2 + \frac{2\alpha\beta}{\sqrt{d}}$. Here, we have used the fact that

$$\sum_{k \in \mathbb{Z}_d} \omega^{-hk} \psi_k = \sqrt{d} \varphi_h, \quad \forall h \in \mathbb{Z}_d.$$

With a similar calculation,

$$\pi_{2*}\mathbf{C}_0(k\psi) = t_\psi \mathbf{N}_\psi(h\psi) + (1 - t_\psi) \frac{1}{d} \mathbb{1}, \quad (37)$$

where $t_\psi = \beta^2 + \frac{2\alpha\beta}{\sqrt{d}}$. We conclude that the marginals of \mathbf{C}_0 are uniformly noisy versions of \mathbf{N}_φ and \mathbf{N}_ψ .

We remark that approximate joint measurements of \mathbf{N}_φ and \mathbf{N}_ψ were studied in [23]. In particular, by [23, Propositions 5 and 6], noisy measurements of the form (36) and (37) are jointly measurable if and only if

$$t_\varphi + t_\psi \leq 1 \quad (38a)$$

$$\text{or } t_\varphi^2 + t_\psi^2 + \frac{2(d-2)}{d} (1-t_\varphi)(1-t_\psi) \leq 1. \quad (38b)$$

Moreover, regardless of the dimension d of \mathcal{H} , there is a unique joint measurement when the equality is attained in (38b). One can confirm that t_φ and t_ψ with α and β given by (33b) lead to equality in (38b), hence \mathbf{C}_0 can be identified as that unique joint measurement. It also follows by Proposition 4 that for even dimensions d there are measurements maximizing $P_{\text{guess}}^{\text{post}}(\mathcal{E}; \mathcal{P}; \mathbf{C})$ whose marginals $\pi_{1*}\mathbf{C}$ and $\pi_{2*}\mathbf{C}$ are not uniformly noisy versions of \mathbf{N}_φ and \mathbf{N}_ψ .

ACKNOWLEDGMENT

This work was performed as part of the Academy of Finland Centre of Excellence program (Project 312058).

APPENDIX A: NECESSITY OF THE RANK-1 CONDITION IN COROLLARY 1

The following state ensemble $\mathcal{E} : \{1, 2, 3\} \rightarrow \mathcal{L}(\mathbb{C}^2)$

$$\begin{aligned} \mathcal{E}(1) &= \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & \mathcal{E}(2) &= \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}, \\ \mathcal{E}(3) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/2 \end{pmatrix} \end{aligned}$$

satisfies (25) and item (i) of Corollary 1. However, it does not fulfill item (ii) of the same corollary, as both the following measurements

$$\mathbf{M}_0(x) = \mathcal{E}(x), \quad x \in \{1, 2, 3\},$$

and

$$\mathbf{M}_1(1) = \mathcal{E}(1) + \mathcal{E}(2) - \mathcal{E}(3),$$

$$\mathbf{M}_1(2) = \mathcal{E}(1) - \mathcal{E}(2) + \mathcal{E}(3),$$

$$\mathbf{M}_1(3) = -\mathcal{E}(1) + \mathcal{E}(2) + \mathcal{E}(3),$$

attain the maximum guessing probability $P_{\text{guess}}(\mathcal{E}; \mathbf{M}_i) = P_{\text{guess}}(\mathcal{E}) = 3/2$.

APPENDIX B: JOINT MEASURABILITY DEGREE OF THREE ORTHOGONAL QUBIT MEASUREMENTS

Let $\mathbf{N}_\ell(\pm\hat{e}_\ell) = \frac{1}{2}(\mathbb{1} \pm \sigma_\ell)$ for $\ell = 1, 2, 3$. We aim to show that $j(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3) = 1/\sqrt{3}$, which means that we need to find the largest t such that the noisy versions

$$\tilde{\mathbf{N}}_\ell(\pm\hat{e}_\ell) = t\mathbf{N}_\ell(\pm\hat{e}_\ell) + (1-t)v_\ell(\pm\hat{e}_\ell)\mathbb{1} \quad (B1)$$

are compatible. The probability distributions ν_1 , ν_2 , and ν_3 can be chosen freely, meaning that we optimize among all their possible choices. It has been shown in [24] that $j_u(\mathbf{N}_1, \dots, \mathbf{N}_m) = 1/\sqrt{3}$. Therefore, the remaining point in order to conclude that $j(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3) = 1/\sqrt{3}$ is provided by the following result.

Proposition 5. If $\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \tilde{\mathbf{N}}_3$ given by (B1) are compatible, then the observables

$$\tilde{\mathbf{N}}'_\ell(\pm\hat{e}_\ell) = t\mathbf{N}_\ell(\pm\hat{e}_\ell) + (1-t)\frac{1}{2}\mathbb{1}, \quad \ell = 1, 2, 3,$$

are also compatible.

Proof. We assume that $\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \tilde{\mathbf{N}}_3$ defined in (B1) are compatible, and we let \mathbf{C} be any measurement having marginals $\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \tilde{\mathbf{N}}_3$. We denote by $A : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ the antiunitary operator satisfying $A\sigma_\ell A^* = -\sigma_\ell$ for $\ell = 1, 2, 3$. Explicitly, $A = \sigma_2 J$, where J denotes complex conjugation with respect to the canonical basis of \mathbb{C}^2 . We then define \mathbf{C}' as

$$\begin{aligned} \mathbf{C}'(k_1\hat{e}_1, k_2\hat{e}_2, k_3\hat{e}_3) &= \frac{1}{2}[\mathbf{C}(k_1\hat{e}_1, k_2\hat{e}_2, k_3\hat{e}_3) \\ &+ A\mathbf{C}(-k_1\hat{e}_1, -k_2\hat{e}_2, -k_3\hat{e}_3)A^*]. \end{aligned}$$

A direct calculation shows that the marginals of \mathbf{C}' are $\tilde{\mathbf{N}}'_1, \tilde{\mathbf{N}}'_2, \tilde{\mathbf{N}}'_3$. ■

-
- [1] M. Sedláč, Quantum theory of unambiguous measurements, *Acta Phys. Slovaca* **59**, 653 (2009).
- [2] J. A. Bergou, Discrimination of quantum states, *J. Mod. Opt.* **57**, 160 (2010).
- [3] J. Bae, Structure of minimum-error quantum state discrimination, *New J. Phys.* **15**, 073037 (2013).
- [4] M. A. Ballester, S. Wehner, and A. Winter, State discrimination with postmeasurement information, *IEEE Trans. Inf. Theory* **54**, 4183 (2008).
- [5] D. Gopal and S. Wehner, Using postmeasurement information in state discrimination, *Phys. Rev. A* **82**, 022326 (2010).
- [6] T. Heinosaari, T. Miyadera, and M. Ziman, An invitation to quantum incompatibility, *J. Phys. A: Math. Theor.* **49**, 123001 (2016).
- [7] M. Plávala, All measurements in a probabilistic theory are compatible if and only if the state space is a simplex, *Phys. Rev. A* **94**, 042108 (2016).
- [8] A. Jenčová, Incompatible measurements in a class of general probabilistic theories, [arXiv:1705.08008](https://arxiv.org/abs/1705.08008).
- [9] A. S. Holevo, Statistical decision theory for quantum systems, *J. Multivariate Anal.* **3**, 337 (1973).
- [10] H. P. Yuen, R. S. Kennedy, and M. Lax, Optimum testing of multiple hypotheses in quantum detection theory, *IEEE Trans. Inf. Theory* **IT-21**, 125 (1975).
- [11] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
- [12] P. Lahti and S. Pulmannová, Coexistent observables and effects in quantum mechanics, *Rep. Math. Phys.* **39**, 339 (1997).
- [13] S. T. Ali, C. Carmeli, T. Heinosaari, and A. Toigo, Commutative POVMs and fuzzy observables, *Found. Phys.* **39**, 593 (2009).
- [14] P. Busch, T. Heinosaari, J. Schultz, and N. Stevens, Comparing the degrees of incompatibility inherent in probabilistic physical theories, *Europhys. Lett.* **103**, 10002 (2013).
- [15] T. Heinosaari, J. Schultz, A. Toigo, and M. Ziman, Maximally incompatible quantum observables, *Phys. Lett. A* **378**, 1695 (2014).
- [16] R. F. Werner, Optimal cloning of pure states, *Phys. Rev. A* **58**, 1827 (1998).
- [17] M. Keyl and R. F. Werner, Optimal cloning of pure states, testing single clones, *J. Math. Phys.* **40**, 3283 (1999).
- [18] A. S. Holevo, *Investigations in the General Theory of Statistical Decisions* (American Mathematical Society, Providence, 1978), translated from Russian by Lisa Rosenblatt, *Proc. Steklov Inst. Math.* **1978**, 3.
- [19] Y. C. Eldar, A. Megretski, and G. C. Verghese, Designing optimal quantum detectors via semidefinite programming, *IEEE Trans. Inf. Theory* **49**, 1007 (2003).
- [20] Y. C. Eldar, A. Megretski, and G. C. Verghese, Optimal detection of symmetric mixed quantum states, *IEEE Trans. Inf. Theory* **50**, 1198 (2004).
- [21] P. Busch and T. Heinosaari, Approximate joint measurements of qubit observables, *Quant. Inf. Comput.* **8**, 0797 (2008).
- [22] J. Schwinger, Unitary operator bases, *Proc. Natl. Acad. Sci. USA* **46**, 570 (1960).
- [23] C. Carmeli, T. Heinosaari, and A. Toigo, Informationally complete joint measurements on finite quantum systems, *Phys. Rev. A* **85**, 012109 (2012).
- [24] Y.-C. Liang, R. W. Spekkens, and H. M. Wiseman, Specker's parable of the overprotective seer: A road to contextuality, nonlocality and complementarity, *Phys. Rep.* **506**, 1 (2011).