Online identification of symmetric pure states

Gael Sentís, Esteban Martínez-Vargas, and Ramon Muñoz-Tapia

We consider online strategies for discriminating between symmetric pure states with zero error when \( n \) copies of the states are provided. Optimized online strategies involve local, possibly adaptive measurements on each copy and are optimal at each step, which makes them horizon independent, hence robust in front of particle losses or an abrupt termination of the discrimination process. We first review previous results on binary minimum and zero error discrimination with local measurements that achieve the maximum success probability set by optimizing over global measurements, highlighting their online features. We then extend these results to the case of zero error identification of three symmetric states with constant overlap. We provide optimal online schemes that attain global performance for any \( n \) if the state overlaps are positive, and for odd \( n \) if overlaps have a negative value. For arbitrary complex overlaps, we show compelling evidence that online schemes fail to reach optimal global performance. The online schemes that we describe only require to store the last outcome obtained in a classical memory, and adaptiveness of the measurements reduce to at most two changes, regardless of the value of \( n \).

1 Introduction

The task of discriminating among non-orthogonal quantum states \([1–4]\) underlies many prominent applications of quantum information sciences. A basic primitive in quantum communication \([5, 6]\), it also has fundamental implications in quantum key distribution \([7–10]\), in the design of quantum algorithms \([11]\), and in foundations of quantum theory \([12–15]\). Due to the no-cloning theorem \([16]\), it is not possible to perfectly and deterministically identify which is the state of a given quantum system out of a known finite set of possible ones, unless these are mutually orthogonal. If copies of identically prepared systems in the same unknown state are provided, we may extract more information and increase our chances of identifying it correctly. However, in order to take full advantage of these extra resources, one generally needs to apply a collective quantum measurement on all the provided systems, which requires performing entangling operations and keeping all systems to be measured in a coherent quantum memory. Such collective measurement, once optimized, is guaranteed to yield the best performance in the discrimination task allowed by quantum mechanics, but the necessary requirements to implement it are hardly met in practical situations.

More experimentally viable (albeit generally sub-optimal) schemes are those that only involve local measurements on each system, thus removing the need of quantum memories and quantum correlations in the measurement apparatus. Such schemes fall under the paradigm of \textit{local operations and classical communication} (LOCC). The question of when can LOCC schemes attain optimal (global) performance in a state discrimination task has been considered in the literature under different angles \([17–26]\).

The motivation behind this topic is not only practical, but also foundational: a performance gap between optimal local and global schemes
in discriminating separable states is a signature of the phenomenon called “quantum nonlocality without entanglement” [27], which has implications in the capacities of quantum channels [28], in the ability to hide information to classical observers [29], and in distinguishing quantum theory from other generalized probabilistic theories [30].

In this paper, we take a step further from LOCC and consider online strategies for state discrimination, that is, feed-forward local measurement schemes that do not depend on knowing beforehand the number of copies of the states available (the horizon), and are optimal at each step of the process. In contrast to horizon-dependent LOCC, online schemes do not loose optimality if some of the systems are lost or if the procedure stops at an earlier time than planned, thus making them the most desirable schemes for robust realistic implementations. This sort of data processing can be regarded as a self-learning process [31], and it is the natural procedure in sequential analysis algorithms [32, 33].

When trying to discriminate between two states, it is known that online strategies attain optimal global performance, regardless of whether one considers minimum error discrimination [22] or unambiguous identification [19, 21], the two usual approaches to state discrimination. Discriminating more than two hypotheses is a much harder problem: optimal protocols are only known for certain special cases [4, 34–39], and results on local distinguishability are even more scarce [24, 25, 40–42]. Here we tackle the problem of unambiguous (zero error) identification of three symmetric pure quantum states with constant (but arbitrary) overlap $c$ when $n$ copies are provided, characterizing for which parameter ranges do online schemes attain global performance. We first rederive the case of binary discrimination, highlighting the online features of the optimal local protocols, and then we extend our formalism to three hypotheses. Specifically, we show that online strategies based on Bayesian updating are globally optimal for any $n$ if $c \geq 0$, and for odd $n$ if $c < 0$. Our analysis straightforwardly extends to the case of tensor products of $n$ trines with constant but different overlaps. Importantly, the choice of each measurement in these strategies depends only on the last outcome obtained, thus greatly limiting the size of the classical memory required. For complex-valued overlaps, we provide strong evidence of a gap between online and global strategies.

The paper is organized as follows. In Sections 2 and 3 we review online binary minimum-error discrimination and unambiguous identification, respectively, and extend these results to non-identical copies of the states. This serves us to set notation and techniques that we use later. Section 4 contains our main results for three symmetric states, and we finish with some conclusions of our analysis.

2 Two-state minimum error discrimination

Here we briefly review binary discrimination for minimum error [22, 43] and its extension to the multi-hypothesis case.

Any two pure states can be written w.l.o.g. as

$$|\psi_{0/1}\rangle = \sqrt{\frac{1+c}{2}} |0\rangle \pm \sqrt{\frac{1-c}{2}} |1\rangle,$$

where $|0\rangle$ and $|1\rangle$ is a basis of the space spanned by $\{|\psi_0\rangle, |\psi_1\rangle\}$ and $c = \langle \psi_0 | \psi_1 \rangle$. For later reference it is convenient to view this parametrization as $|\psi_0\rangle = \xi_0 |0\rangle + \xi_1 |1\rangle$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of the unitary operation $U = |0\rangle \langle 0 | + e^{2\pi i} |1\rangle \langle 1 | = |0\rangle \langle 0 | - |1\rangle \langle 1 |$, $|\psi_1\rangle = U |\psi_0\rangle$, and $\xi_i = \sqrt{\lambda_i(G)} / 2$, $i = 0, 1$, where $\lambda_i(G)$ are the eigenvalues of the Gram matrix whose elements are $g_{ij} = \langle \psi_i | \psi_j \rangle$. With this parametrization the operator $\Omega = \sum_k |\psi_k\rangle \langle \psi_k |$, which plays a key role in the extension of larger sets of symmetric states (Sec 4), is diagonal, i.e., $\Omega = 2 \mathbf{diag}\{\xi_0^2, \xi_1^2\}$.

We assume that the two states can occur with arbitrary a priori probabilities $\eta_0$ and $\eta_1$, respectively. The aim is to minimize the average error probability $P_e = \eta_0 p(1|\psi_0) + \eta_1 p(0|\psi_1)$, or equivalently maximize the success probability $P_s = \eta_0 p(0|\psi_0) + \eta_1 p(1|\psi_1)$, where $p(r|\psi)$, $r = 0, 1$, is the probability of making the guess $|\psi_r\rangle$ when the state was $|\psi_i\rangle$. These conditional probabilities are determined by the measurement $\mathcal{M}$ performed on the system, which is
described mathematically as a positive operator-valued measure (POVM). Here the POVM has only two elements $\mathcal{M} = \{E_0, E_1\}$, with $E_r \geq 0$ and $E_0 + E_1 = 1$. The Born rule dictates that $p(r|\psi_i) = \text{tr} [E_r |\psi_i\rangle\langle\psi_i|]$. The optimal success probability has the well known expression [5]

$$P_s = \frac{1 + \sqrt{1 - 4\eta_0\eta_1 c^2}}{2}. \quad (2)$$

It is also well known that this success probability is attained with a POVM with elements that are the projectors on the positive and negative spectrum of the operator $\Gamma = \eta_0 |\psi_0\rangle\langle\psi_0| - \eta_1 |\psi_1\rangle\langle\psi_1|$, the so-called Helstrom measurement [5].

The generalization to the multi-copy case is straightforward. The optimal value of the success probability $P_s(n) = \eta_0 p(0|\psi^n) + \eta_1 p(1|\psi^n)$ is obtained by simply replacing $c \rightarrow c^n$ in Eq. (2), i.e.,

$$P_s^n(n) = \frac{1 + \sqrt{1 - 4\eta_0\eta_1 c^{2n}}}{2}, \quad (3)$$

where the superscript $G$ stands for global. The global measurement attaining this bound acts jointly on the $n$ copies, hence a quantum memory to store the systems is required. Note also that it may involve entangling operations between the systems.

Let us now succinctly show that there exists a scheme where each system is measured locally and still achieves the optimal success probability given by Eq. (3). It consists of a sequence of Helstrom measurements on each system where prior probabilities are updated at each step $k$ according to the Bayes rule

$$\eta_i^{(k)}(r_k) =: \eta_i^{(k)} = p(\psi_k|r_k) = \eta_i^{(k-1)} p(r_k|\psi_i) / \eta_i^{(k-1)} p(r_k|\psi_0) + \eta_i^{(k-1)} p(r_k|\psi_1). \quad (4)$$

Here $r_k = 0, 1$ is the outcome value of the $k$th measurement and we have streamlined the notation when no confusion arises.

The crucial property is that the Helstrom measurements yield the relation $\eta_i^{(k)}(k) = \eta_i^{(k-1)}(k-1) c^2$ for any value of the outcome $r_k$ (see [22]), and thus $\eta_i^{(k)}(k) = \eta_0\eta_1 c^{2k}$ that, once inserted in Eq. (2) for $k = n - 1$, precisely gives Eq. (3).

The Bayes rule (4) can be seen as a learning process that updates our belief on the occurrence of each state. Observe that the optimal value of the success probability is obtained at each step. This is an online procedure as the knowledge of the total number of systems that are available for measurement is not required, in contrast, e.g., to dynamic programming problems where the knowledge of the horizon is needed to carry out an optimization in reverse [44]. Furthermore, measurements in this local scheme only depend on the previous outcome (as opposed to the whole sequence of previous outcomes), thus the size of the required classical memory is minimal.

Interestingly, the same Bayesian updating local protocol turns out to be optimal in the non-i.i.d. case, i.e., for two arbitrary multiparty product states $|\Phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle$ and $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ with arbitrary priors $\eta_{\phi}$ and $\eta_{\psi}$, respectively [45]. The overlap in this case is $C = \langle |\Phi|\Psi\rangle = c_1 c_2 \cdots c_n$, with $c_k = |\langle \phi_k|\psi_k\rangle|$. We proceed as in the i.i.d. case, that is, we perform a series of local Helstrom measurements with sequentially updated priors and get $\eta_{\phi_k}^{(k)} = \eta_0\eta_1 c_1^2 c_2^2 \cdots c_k^2$. The success probability then reads

$$P_s = \frac{1 + \sqrt{1 - 4\eta_0\eta_1 c_1^2 c_2^2 \cdots c_n^2}}{2}, \quad (5)$$

i.e., the optimal success probability, Eq. (2) with $c \rightarrow C$.

Going beyond the binary case is much more involved as there are no closed expressions for the success probability for arbitrary priors. Optimal solutions (single or multi-copy) are known only in very few cases, that essentially correspond to symmetric instances (see e.g. [4]). Notice that in any local protocol, even with symmetric sources, the updating rule will necessarily bias the priors and hence render the problem intractable analytically. One can nevertheless carry out a numerical study. It has been recently shown numerically that local measurements supplemented with the Bayesian updating rule do not yield the optimal global success probability in the minimum error approach already in the case of three symmetric states [46] (see also [47] for an analysis with symmetric coherent states). However, it remains an
open question whether this feature also holds for zero-error protocols, which we discuss next.

3 Two-state zero-error identification

We now turn our attention to protocols that identify a state without errors at the expense of having inconclusive outcomes, a task also known as unambiguous discrimination [48, 49]. Here we show that in the binary case there is also a local online procedure that gives the maximum success probability provided by the most general global POVM acting on all systems.

The zero-error POVM in principle has three elements: $F_0$, and $F_1$, that unambiguously detect $|\psi_0\rangle$ and $|\psi_1\rangle$, respectively, and $F_I$, which we associate to an inconclusive outcome. In order to achieve optimality the success probability $P_s = \eta_0 P(0|\psi_0) + \eta_1 P(1|\psi_1) =: \eta_0 p_0 + \eta_1 p_1$ is maximized or, equivalently, the inconclusive probability $Q = \eta_0 P(I|\psi_0) + \eta_1 P(I|\psi_1) =: \eta_0 q_0 + \eta_1 q_1$ is minimized while keeping the condition that no errors are committed, i.e. $P(1|\psi_0) = P(0|\psi_1) = 0$. Notice that necessarily $F_0 \propto |\psi_0^\perp\rangle\langle\psi_0^\perp|$ and $F_1 \propto |\psi_1^\perp\rangle\langle\psi_1^\perp|$, therefore the two proportionality constants are the only free parameters. It proves useful to cast the problem as a semidefinite program [50] and use the conditional success probabilities $p_0, p_1$ as the parameters to be optimized. The program reads [39, 51]

$$\max \quad \eta_0 p_0 + \eta_1 p_1$$

$$\text{s.t.} \quad G - \Gamma \geq 0$$

$$\Gamma \geq 0,$$

where recall that $G$ is the Gram matrix whose elements are given by the overlaps $g_{ij} = \langle \psi_i | \psi_j \rangle$, and $\Gamma$ is a diagonal matrix of the conditional success probabilities, $\Gamma = \text{diag}\{p_0, p_1\}$. The first constraint stems from the POVM condition $1 - F_0 - F_1 = F_I \geq 0$. We note that this condition does not depend on the priors, only on $G$. This is a general feature that applies to any number of hypotheses. In the binary case it yields the interesting uncertainty relation

$$q_0 q_1 \geq c^2,$$

from which the solution of the SDP (6) follows directly:

$$q_0 = c\sqrt{\frac{\eta_0}{\eta_1}}, \quad q_1 = c\sqrt{\frac{\eta_1}{\eta_0}}$$

if

$$c^2 \leq \frac{\eta_0}{\eta_1} \leq \frac{1}{c^2},$$

and either $q_0 = 1$ and $q_1 = c^2$ if $\eta_0/\eta_1 \leq c^2$, or $q_1 = 1$ and $q_0 = c^2$ if $\eta_0/\eta_1 \geq 1/c^2$. In these extremal cases the priors are so biased that the optimal measurement discards the state with the lowest prior and the POVM changes from having three to two elements. For instance, in the case $q_0 = 1$ we only have elements $F_1$ and $F_I$ with $F_1 + F_I = I$. The symmetric case $\eta_0 = \eta_1 = 1/2$ falls inside the range (9) for any value of the overlap and yields the well-known minimum inconclusive probability $Q = c$ (see, e.g., [3]).

The generalization to arbitrary $n$ amounts to do the change $c \rightarrow c^n$ in Eq. (8). Note that this replacement also widens the range of validity of the three outcome POVM

$$c^{2n} \leq \frac{\eta_0}{\eta_1} \leq \frac{1}{c^{2n}}.$$ (10)

This fact plays an important role when discussing local protocols. The minimum average success probability finally reads (here and thereof we assume w.l.o.g. that $\eta_0 \leq \eta_1$)

$$Q(n) = \begin{cases} 
2\sqrt{\eta_0 \eta_1} c^n & \text{if } \sqrt{\frac{\eta_0}{\eta_1}} \geq c^n \\
\eta_0 + \eta_1 c^{2n} & \text{if } \sqrt{\frac{\eta_0}{\eta_1}} \leq c^n
\end{cases}.$$ (11)

We next show that the optimal performance given by Eq. (11) can always be attained with local measurements. At first glance this result may seem a bit surprising because, for a given $n$ and the same pair of priors, the global optimal POVM has three outcomes [i.e., Eq. (10) is satisfied], while a local one has only two [i.e., Eq. (9) is not fulfilled]. This mismatch could lead us to think that a local strategy could not attain global optimal performance. However, we note that upon obtaining an inconclusive outcome in a two element local POVM, the priors get updated in such a way that they become more equilibrated. In fact, there is a step where the updated priors become sufficiently balanced as to satisfy Eq. (9).
From there on local POVMs also have three outcomes.

The proof of the agreement between the local and global procedures for any \( n \) and any initial value of the priors goes as follows. We have to consider the three different ranges of values where the ratio of the priors may lie:

\[
(i) \quad \frac{\eta_0}{\eta_1} \leq c^{2n}, \quad (ii) \quad c^{2n} \leq \frac{\eta_0}{\eta_1} \leq c^{2}, \quad (iii) \quad c^{2} \leq \frac{\eta_0}{\eta_1} \leq 1.
\]

We start addressing range (iii) (note that the symmetric case of equal priors falls in this range). Here both conditions (9) and (10) are satisfied for any \( n \), i.e., both global and local POVMs give a non-zero probability of detecting any of the states. The first local measurement is the optimal one yielding the inconclusive probabilities given by Eq. (8). After this measurement, if we have not been successful, it is straightforward to see that the priors are updated to \( \eta_0^i = \eta_1^i = 1/2 \).

The next measurement is hence optimized for equal priors, which gives an inconclusive outcome with probability \( c \) for both states. Upon failing we repeat the symmetric measurement in all subsequent copies. The overall inconclusive probability of this local strategy then reads

\[
Q^L(n) = \eta_0 \Pi_{k=1}^n q_k^0 + \eta_1 \Pi_{k=1}^n q_k^1
= \eta_0 c \sqrt{\frac{\eta_1}{\eta_0}} c^{n-1} + \eta_1 c \sqrt{\frac{\eta_0}{\eta_1}} c^{n-1}
= 2 \sqrt{\eta_0 \eta_1} c^n,
\]

i.e., the optimal value in the first case of Eq. (11).

In the range (i) the priors are so biased that, even for a global measurement, it is not worth detecting the state \( |\psi_0\rangle \). The local procedure consists of a series of measurements \( \{ F_1 = |\psi_0^0\rangle \langle \psi_0^0|, F_2 = |\psi_0^1\rangle \langle \psi_0^1| \} \) that either detect unambiguously \( |\psi_1\rangle \) or fail. In this case we have

\[
Q^L(n) = \eta_0 \times (1)^n + \eta_1 (c^2)^n = \eta_0 + \eta_1 c^{2n},
\]

which coincides with the second line of Eq. (11). Note that, for large \( n \), the region (i) is increasingly small. We would like to stress that, while all the measurements are identical, the updated priors are not. Each time one gets an inconclusive result the belief that the state is \( |\psi_1\rangle \) diminishes and the belief in favor of \( |\psi_0\rangle \) increases. This balances the priors, however not enough to be worth testing the state \( |\psi_0\rangle \). Indeed, Bayesian updating gives that, for all \( k \leq n - 1 \),

\[
\frac{\eta_0^{(k)}}{\eta_1^{(k)}} = \frac{1}{c^2} \frac{\eta_0^{(k-1)}}{\eta_1^{(k-1)}} \to \frac{\eta_0^{(k)}}{\eta_1^{(k)}} = \frac{1}{c^{2k}} \frac{\eta_0}{\eta_1} \leq c^2,
\]

since \( \eta_0/\eta_1 \leq c^2 \) in this range.

The most interesting range is (ii). While the global strategy uses a three outcome POVM, the local strategy starts with a fully biased two outcome measurement (because \( \eta_0/\eta_1 \leq c^2 \)). Upon obtaining an inconclusive outcome, the priors are updated according to Eq. (15) and get more balanced, i.e., our belief that the state is \( |\psi_0\rangle \) increases. We keep doing the same measurement until a step \( k_0 \) that yields \( \eta_0^{(k_0)}/\eta_1^{(k_0)} \geq c^2 \). This step is guaranteed to be reached before \( n \), i.e., \( k_0 < n \). Simply observe that

\[
\frac{\eta_0^{(k_0)}}{\eta_1^{(k_0)}} = \frac{1}{c^{2k_0}} \frac{\eta_0}{\eta_1} \geq c^2 \to \frac{\eta_0}{\eta_1} \geq c^{2(k_0+1)},
\]

which is always compatible with the initial condition of beginning in range (ii) for some \( k_0 < n \) (the actual value of \( k_0 \) depends on the particular ratio \( \eta_0/\eta_1 \)). Therefore, the protocol consists in performing a sequence of fixed two-outcome measurements until the \( k_0 \) step, when we do a three-outcome measurement for biased priors \( \eta_0^{(k_0)} \) and \( \eta_1^{(k_0)} \), and continue with a sequence of three-outcome measurements for balanced priors as in region (iii) (of course, for as long as we keep on failing). The probability for \( n \) failures is

\[
Q^L(n) = \eta_0 \left[ (1)^{k_0} \times c \left( \frac{\eta_1^{(k_0)}}{\eta_0^{(k_0)}} \right) \times c^{n-k_0-1} \right]
+ \eta_1 \left[ (c^2)^{k_0} \times c \left( \frac{\eta_0^{(k_0)}}{\eta_1^{(k_0)}} \right) \times c^{n-k_0-1} \right],
\]

were we have explicitly displayed the terms corresponding to the three different stages of the procedure. Now, taking into account the expression of the updated priors ratio Eq. (15), we get

\[
Q^L(n) = \eta_0 \sqrt{\frac{\eta_1}{\eta_0}} c^n + \eta_1 \sqrt{\frac{\eta_0}{\eta_1}} c^n = 2 \sqrt{\eta_0 \eta_1} c^n,
\]

Accepted in Quantum 2022-01-28, click title to verify. Published under CC-BY 4.0.
which again coincides with the global bound, Eq. (11).

We can summarize the procedure in all three regions by the position \( k_0 \) of the first three-outcome local measurement in the sequence. In region (iii), \( k_0 = 0 \) and we already start with a three-outcome local measurement. In region (ii), \( k_0 \leq n - 1 \), i.e., the accumulated balance of the priors given by the inconclusive outcomes induces to start a three-outcome measurement at some point before reaching \( n \). Finally, in region (i), for very biased priors the number of copies is not enough to abandon the strategy that only detects one of the states.

As in the minimum error case, this local protocol works also in the non-i.i.d. case of product states. One just needs to take into account that at each step \( k \) we have a different overlap \( c_k \) and also a different validity range Eq. (9). The minimum failure probability is simply Eq. (11) with \( c^n \) replaced by \( C = c_1c_2\cdots c_n \).

It is worth emphasizing that the local procedure described yields the optimal success probability at each step, regardless of total number of systems that are finally available for measurement. Besides not requiring quantum memories, the local measurement at any given step depends only on the outcome of the previous measurement, hence the size of the classical memory required is minimal. Furthermore, the measurement setting at most changes two times.

4 Zero-error identification of symmetric multiple hypotheses

In this section we extend our results to multi-hypothesis scenarios. Rather surprisingly, the performance of online sequential strategies and their comparison with the global optimal values for zero-error identification have hardly been explored. Although even the simplest case of three symmetric states (TSS) is quite a big challenge, as discussed in [42], the constraints imposed by the zero-error requirement provide more chances to obtain analytical results. Here we will mainly focus our attention in the TSS case, and also address some straightforward generalizations.

The problem we address consists in doing a zero-error identification of a set of states that have equal prior probabilities \( \eta_i = 1/3 \), \( i = 0, 1, 2 \), and symmetric overlaps \( \langle \psi_0|\psi_1 \rangle = \langle \psi_1|\psi_2 \rangle = \langle \psi_2|\psi_0 \rangle = c \). We first analyze the case of positive values of \( c \) and then we address the negative range. We finally consider the sequential performance for complex values of \( c \).

The positive range, \( 0 \leq c \leq 1 \), can actually be solved for any number \( r \) of hypotheses as we show below. Note that the anomaly identification problem [38] falls under this case. The Gram matrix, \( G \), together with the priors encapsulate all the discrimination properties of an ensemble, and no explicit form of the states is even needed, although the very existence of a valid Gram, i.e., \( G \geq 0 \), imposes some restrictions on the states that can give rise to \( G \). For instance, if \( 0 \leq c < 1 \) the states are necessarily linearly independent (a requisite to have zero-error discrimination [48]) and therefore the dimension \( d \) of the Hilbert space of the states must be at least \( d \geq r \). The Gram matrix of a set of three states with equal overlap \( c \) reads

\[
G = \begin{pmatrix}
1 & c & c \\
c & 1 & c \\
c & c & 1
\end{pmatrix}.
\]  

(19)

In this symmetric setting the optimal conditional success probabilities must be identical, \( p_i = p \), hence the SDP (6) reads

\[
\begin{align*}
\max & \quad p \\
\text{s.t.} & \quad G - pI \geq 0 \\
& \quad p \geq 0.
\end{align*}
\]

(20)

This optimization gives the minimum eigenvalue of \( G \),

\[
p = \lambda_{\min}(G) = 1 - c,
\]

(21)

i.e., \( q = c \). Note that this solution is the same for any number of symmetric hypotheses. Given \( n \) copies of the states, the minimum inconclusive probability for any set of symmetric states with constant positive overlaps is \( Q = c^n \).

Next we would like to know if the global performance can also be reached with an online protocol. This way, no quantum memory would be required and the identification process can be completed at much earlier times without compromising the probability of success [52]. The online
protocol consists simply in a local optimal unambiguous measurement at each step \( k \). One stops as soon as a conclusive outcome is obtained. This protocol can be regarded as a Bayesian updating procedure: if the identification is successful, the priors become 1 for the identified state and zero for the rest of states. If one fails, the updated priors are again symmetric. The proof follows directly from the fact that the inconclusive probability at each step is \( c \) and \( n \) consecutive failures have probability \( c^n \).

The particular form of the unambiguous POVM that we need depends on the specific source states at hand. We present the TSS case \( (r = 3) \) in detail, but the generalization to an arbitrary number of symmetric source states is straightforward. As already introduced in Section 2, the most convenient parametrization is to use the eigenbasis of the unitary \( U = |0\rangle\langle 0| + e^{2i\pi/3} |1\rangle\langle 1| + e^{4i\pi/3} |2\rangle\langle 2| \), and write the states as \( |\psi_0\rangle = \xi_0 |0\rangle + \xi_1 |1\rangle + \xi_2 |2\rangle \), \( |\psi_1\rangle = U |\psi_0\rangle \) and \( |\psi_2\rangle = U^2 |\psi_0\rangle \). Here the amplitudes \( \xi_i \) are related to the eigenvalues of \( G \), \( \lambda_i \), through

\[
\xi_i = \sqrt{\frac{\lambda_i}{3}}, \quad i = 0, 1, 2, \tag{22}
\]

which is the direct extension of Eq. (1). This parametrization can be regarded as the canonical form of symmetric states for any overlap \( c \) (real or complex), and generalizes trivially to any number of symmetric states. It is useful to note that the operator \( \Omega = \sum_{k=0}^{2} \sum_{m} |\psi_k\rangle\langle \psi_m| \) is diagonal in this basis:

\[
\Omega = 3 \begin{pmatrix} (\xi_0)^2 & 0 & 0 \\ 0 & (\xi_1)^2 & 0 \\ 0 & 0 & (\xi_2)^2 \end{pmatrix} \tag{23}
\]

(this property holds true for any set of three symmetric states, normalized or not). The specific values of \( \xi_i \) are

\[
\xi_0 = \sqrt{\frac{1 + 2c}{3}}, \quad \xi_1 = \sqrt{\frac{1-c}{3}}. \tag{24}
\]

The POVM has elements \( F_i = p_i |\tilde{\phi}_i\rangle\langle \tilde{\phi}_i|, \) \( i = 0, 1, 2 \), and \( F_1 = 1 - \sum_{i=0}^{2} F_i \), where \( p = 1 - c \), as given in Eq. (21). The unnormalized states \( |\tilde{\phi}_i\rangle \) satisfy the unambiguous condition \( \langle \tilde{\phi}_i | \psi_j \rangle = \delta_{ij} \) and are constructed from a state \( |\tilde{\phi}_0\rangle \) as \( |\tilde{\phi}_k\rangle = U^k |\tilde{\phi}_0\rangle \). With this parametrization the fiducial state simply reads

\[
|\tilde{\phi}_0\rangle = \sum_{i=0}^{2} \sqrt{\frac{1}{3\lambda_i}} |i\rangle. \tag{25}
\]

Let us next complete the analysis for negative values of the overlap. We note that \( G \geq 0 \) implies that \( c \geq -1/2 \). In the range \( c \in [-1/2, 0] \), the minimum eigenvalue of Eq. (20) changes to \( \lambda_{\min} = 1 - 2|c| \). For a given number of copies \( n \) the minimum eigenvalue alternates between \( 1 - 2|c|^n \) and \( 1 - |c|^n \) depending on whether \( n \) is odd or even, respectively. This means that the minimum inconclusive probability is

\[
Q(n) = \begin{cases} 2|c|^n & \text{if } n \text{ is odd} \\ |c|^n & \text{if } n \text{ is even} \end{cases}. \tag{26}
\]

Note that indeed \( Q(n) \) is a decreasing function of \( n \) since \( |c|^{2k} \geq 2|c|^{2k+1} \geq |c|^{2k+2} \) if \( |c| \leq 1/2 \).

A local protocol based on fixed unambiguous measurements gives a failure probability \( Q^L = 2^n |c|^n \), which is away from the optimal value by an exponential factor. Given such a large gap, one expects that there exist better local protocols. The analysis of the extremal value \( c = -1/2 \) gives us the clues on how to proceed. For this value one has \( \text{det} G = 0 \), i.e., the three states are linearly dependent. This means that zero-error identification is not possible [48] with only one copy. Of course, given \( n > 1 \) copies, the tensored states become linearly independent with a global Gram matrix \( G > 0 \). The global inconclusive probability is given by Eq. (26) with \( c = -1/2 \). It is remarkable that \( Q(n) \) is the same for \( 2k \) and \( 2k + 1 \) copies of the state, \( Q(2k) = Q(2k + 1) = 2^{-2k} \), i.e., having an additional copy is of no use (a result already noticed in [49]).

Although with only one copy it is impossible to unambiguously identify the state, one can still gather useful information to be used in the following measurements. In particular, it is possible to perform a measurement that is able to exclude one of the states [53] with 100% probability. It is easy to see that a POVM with elements \( E_k = \frac{1}{2} |\tilde{\psi}_k\rangle\langle \tilde{\psi}_k|, k = 0, 1, 2 \), does the job, as indeed it constitutes a POVM: \( \sum_{k=0}^{2} E_k = 1 \). Then, from the second step onwards, one can proceed with two-state discrimination measurements.
as in Section 3 with equal priors. The failure probability then reads

$$Q^L(n) = \left( \frac{1}{2} \right)^{n-1},$$  

(27)

which coincides with the optimal value for odd $n$, Eq. (26). Hence, this protocol is optimal for any odd number of states. For even $n$ it does not reach global optimality, but we conjecture that also in this case no local protocol can do better than this one.

We can now tackle the whole negative range $-1/2 < c < 0$ with local protocols. The idea is to combine unambiguous identification with the state-excluding measurement that has been the key idea to solve the extremal point $c = -1/2$. The unambiguous POVM elements are

$$F_k = (1 - 2|c|)|\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|, \quad k = 0, 1, 2,$$

where $|\tilde{\psi}_0\rangle = |0\rangle - |1\rangle$, and $|\tilde{\psi}_1\rangle = |0\rangle$, $|\tilde{\psi}_2\rangle = |1\rangle$. They give an optimal inconclusive symmetric which give an optimal inconclusive probability $|c|$, Eq. (8) with $\eta_0/\eta_1 = 1$. Therefore, after $n$ measurements the overall inconclusive probability reads

$$Q^L(n) = 2|c|^n,$$

(31)

which again coincides with the optimal value Eq. (26) for odd $n$. This result also proves that, for negative values of $c$, this protocol is the optimal one among all local procedures when the number of states measured is odd. For even numbers of states, although we do no have a rigorous proof, there are strong evidences that this is also the case. A measurement can provide three types of information: (i) exclude two states (unambiguous identification), (ii) exclude one of the states (exclusion) or (iii) update our belief over the different states (learning). Naturally (i) is the most valuable information. In a convex combination of POVM elements that achieve (ii) and (iii), note that the overall failure probability with two copies decreases if one puts the maximum weight in the elements leading to (ii). The POVM $\{F_0, F_1, F_2\}$ maximizes the contribution to the success probabilities of (i) and (ii) by construction, hence it is presumably the optimal local measurement for any $n$.

Finally, for complex overlaps $c = se^{i\theta}$, the eigenvalues of the Gram matrix read

$$\lambda_k = 1 + 2s \cos \left[ \frac{2k\pi}{3} \right], \quad k = 0, 1, 2.$$  

(32)

The minimum eigenvalue is $\lambda_1$ for $0 \leq \theta \leq 2\pi/3$, $\lambda_0$ for $2\pi/3 \leq \theta \leq 4\pi/3$, and $\lambda_2$ for $4\pi/3 \leq \theta \leq 2\pi$. The positivity of the Gram matrix imposes some restrictions on the phase $\theta$ for $s > 1/2$. The region allowed by the physical restriction $G \geq 0$ is the triangle depicted in Fig. 1. Note that, by symmetry, values of the overlap $c$ differing in a phase of $2\pi/3$ are equivalent. In particular this holds true for the three lines with $\theta = 0, 2\pi/3, 4\pi/3$ and the dashed lines with $\theta = \pi/3, \pi, 5\pi/3$. That is, for values of $c$ lying in the “Mercedes-Benz” lines of Fig. 1 a protocol of repeated unambiguous local measurements provide the same success probability as gathering all the copies and performing an optimal global measurement, for any $n$. For values in the dashed lines of Fig. 1 this is only true for odd $n$.

For complex values of the overlap and for $n = 2$ copies, it is possible to find a region with a
“Mitsubishi-logo” shape where a sequence of two local measurements yields the same success probability as the global measurement [42]. However, the strategy proposed in [42] is not online, since it requires knowing the horizon. Indeed, it sacrifices optimality in the first step (by not putting the maximum possible weight on the POVM elements $F_{0,1,2}$) in order to match global performance at the second step. We have carried out numerical checks by optimizing over online strategies with local POVMs of the form \( \{F_{0,1,2}, E_{0,1,2,1} - F - E\} \). Our results indicate that there is no online protocol yielding the global optimal success probability outside the dark blue and magenta lines of Fig. 1.

![Figure 1: Complex plane of the overlap values.](image)

Our results naturally extend to the case of product states that are not necessarily identical, but where each local state comes from a different symmetric trine \( \{|\psi_0^{(k)}\rangle, |\psi_1^{(k)}\rangle, |\psi_2^{(k)}\rangle\} \) with overlap \( c_k \), \( k = 1, \ldots, n \). This case corresponds to a non-i.i.d. source that produces three possible global hypotheses of the form \( |\psi_i^{(1)}\rangle|\psi_i^{(2)}\rangle|\cdots|\psi_i^{(n)}\rangle \), \( i = 0, 1, 2 \). For instance, as in the case of identical copies, our online scheme yields the optimal global success probability if \( c_k \geq 0 \), \( \forall k \). Also, if the local trines have positive and negative values of the overlap, the online scheme matches optimal performance if \( \Pi_{k=1}^n c_k < 0 \). Notice that in this case there must be a first trine with negative overlap, say at step \( k \). Recall that the local measurement for this trine either identifies the state with probability \( 1 - 2|c_k| \) or excludes one of the possibilities with probability \( 2|c_k| \) and thereafter one has a symmetric binary problem. Thus, the total inconclusive probability reads \( Q = c_1c_2\cdots 2|c_k| |c_{k+1}| \cdots |c_n| \) which coincides with the global optimum \( 2|c_1c_2\cdots c_n| \) since \( c_i > 0 \) for \( i < k \).

5 Conclusions

The tasks of binary pure state identification for minimum and zero error can be carried out in an online fashion with optimal performance. The scheme has no horizon, i.e., the information about the number of states available does not affect the measurement scheme. Optimality is attained at each step regardless of whether systems are lost or one has to stop at an earlier time than planned.

Extending the analysis beyond the binary case is a much more challenging task. Already the minimum extension of three symmetric states is a highly non-trivial case. For minimum error the direct application of local measurements with Bayesian updating for two copies of the states does not give the optimal global performance [46, 47]. As far as we are aware, there is no proof that this is the case for more general one-way local protocols.

The zero-error identification task, still being quite involved, offers more possibilities to be tackled as most of the structure of the POVM is already fixed by the zero-error constraints. We have formulated the problem as a semidefinite program that greatly simplifies the optimization task and also provides a very useful tool, not only for numerical calculations but, as we exploit here, also for obtaining analytical results. It also opens the path for addressing more complex instances as, e.g., non-symmetric overlaps or different priors. We have given a canonical way of writing \( r \) symmetric states in terms of the eigenvalues of their Gram matrix. For \( r = 3 \), we have obtained the optimal online protocol for arbitrary positive values of the overlap and any \( n \), and for negative values for odd \( n \). We have proven that these
protocols attain the optimal global performance. These results directly extend to symmetric complex values of the overlap with phases $2\pi/3$. Our findings for positive overlaps also hold for any number of hypotheses $r$. Unlike [42], we are not restricted to sources of linearly independent states. We are able to find, e.g., online optimal protocols for trines of symmetric qubits.

For arbitrary complex values of the overlap, our results also suggest that there is no online protocol achieving the same performance as global protocols outside the three symmetric lines of Fig. 1. The existence of this gap could be exploited in several ways. For instance, one could consider an extension of the B92 protocol [7] with trine states to produce keys of trits. If Alice were to use multiple copies of a trine state for which such gap exists with the objective of increasing the key rate, Bob would take advantage by measuring collectively, while Eve would be forced to measure in an online manner (thus suboptimally) to keep the rate of communication. Another direct application of our results is probabilistic cloning of states from a finite set [54] in the asymptotic limit of producing many clones: if the set is a trine where there is no gap between online and global strategies, the task could be optimally performed by an online measure and prepare strategy, thus saving resources with respect to measuring several copies collectively.

Acknowledgments

We acknowledge discussions with E. Bagan and K. Nakahira. We acknowledge financial support from the Spanish Agencia Estatal de Investigación, project PID2019-107609GB-I00, from Secretaría d’Universitats i Recerca del Departament d’Empresa i Coneixement de la Generalitat de Catalunya, co-funded by the European Union Regional Development Fund within the ERDF Operational Program of Catalonia (project QuantumCat, ref. 001-P-001644), and Generalitat de Catalunya CIRIT 2017-SGR-1127. EMV thanks financial support from CONACYT.

References

[1] A. Chefles, *Quantum state discrimination*, Contemporary Physics 41, 401 (2000), DOI: 10.1080/00107510010002599.

[2] S. M. Barnett and S. Croke, *Quantum state discrimination*, Advances in Optics and Photonics 1, 238 (2009), DOI: 10.1364/AOP.1.000238.

[3] J. A. Bergou, *Discrimination of quantum states*, Journal of Modern Optics 57, 160 (2010), DOI: 10.1080/09500340903477756.

[4] J. Bae and L.-C. Kwek, *Quantum state discrimination and its applications*, Journal of Physics A: Mathematical and Theoretical 48, 083001 (2015), DOI: 10.1088/1751-8113/48/8/083001.

[5] C. W. Helstrom, *Quantum detection and estimation theory* (Academic press) (1976).

[6] N. Gisin and R. Thew, *Quantum communication*, Nature Photonics 1, 165 (2007), DOI: 10.1038/nphoton.2007.22.

[7] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Physical Review Letters 68, 3121 (1992), DOI: 10.1103/PhysRevLett.68.3121.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics 74, 145 (2002), DOI: 10.1103/RevModPhys.74.145.

[9] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia, *Secrecy properties of quantum channels*, Physical Review A 73, 012327 (2006), DOI: 10.1103/PhysRevA.73.012327.

[10] R. Renner, *Security of quantum key distribution*, International Journal of Quantum Information 6, 1 (2008), DOI: 10.1142/S0219749908003256.

[11] D. Bacon, A. Childs, and W. van Dam, *From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups*, in 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS’05), vol. 2005, 469–478 (IEEE) (2005), ISBN 0-7695-2498-0, DOI: 10.1109/SFCS.2005.38.

[12] J. Bae, W.-Y. Hwang, and Y.-D. Han, *No-Signaling Principle Can Determine Optimal Quantum State Discrimination*, Physical Review Letters 107, 170403 (2011), DOI: 10.1103/PhysRevLett.107.170403.
[13] R. Takagi and B. Regula, General Resource Theories in Quantum Mechanics and Beyond: Operational Characterization via Discrimination Tasks, Physical Review X 9, 031053 (2019), DOI: 10.1103/PhysRevX.9.031053.

[14] M. Oszmaniec and T. Biswas, Operational relevance of resource theories of quantum measurements, Quantum 3, 133 (2019), DOI: 10.22331/q-2019-04-26-133.

[15] R. Uola, T. Kraft, J. Shang, X.-D. Yu, and O. Gühne, Quantifying Quantum Resources with Conic Programming, Physical Review Letters 122, 130404 (2019), DOI: 10.1103/PhysRevLett.122.130404.

[16] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature 299, 802 (1982), DOI: 10.1038/299802a0.

[17] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multiparty Orthogonal Quantum States, Physical Review Letters 85, 4972 (2000), DOI: 10.1103/PhysRevLett.85.4972.

[18] S. Virmani, M. Sacchi, M. Plenio, and D. Markham, Optimal local discrimination of two multipartite pure states, Physics Letters A 288, 62 (2001), DOI: 10.1016/S0375-9601(01)00484-4.

[19] Y.-X. Chen and D. Yang, Optimal conclusive discrimination of two nonorthogonal pure product multipartite states through local operations, Physical Review A 64, 064303 (2001), DOI: 10.1103/PhysRevA.64.064303.

[20] Y.-X. Chen and D. Yang, Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communications, Physical Review A 65, 022320 (2002), DOI: 10.1103/PhysRevA.65.022320.

[21] Z. Ji, H. Cao, and M. Ying, Optimal conclusive discrimination of two states can be achieved locally, Physical Review A 71, 032323 (2005), DOI: 10.1103/PhysRevA.71.032323.

[22] A. Acín, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia, Multiple-copy two-state discrimination with individual measurements, Physical Review A 71, 032338 (2005), DOI: 10.1103/PhysRevA.71.032338.

[23] S. Croke, S. M. Barnett, and G. Weir, Optimal sequential measurements for bipartite state discrimination, Physical Review A 95, 052308 (2017), DOI: 10.1103/PhysRevA.95.052308.

[24] A. Peres and W. K. Wootters, Optimal detection of quantum information, Physical Review Letters 66, 1119 (1991), DOI: 10.1103/PhysRevLett.66.1119.

[25] E. Chitambar and M.-H. Hsieh, Revisiting the optimal detection of quantum information, Physical Review A 88, 020302 (2013), DOI: 10.1103/PhysRevA.88.020302.

[26] H.-C. Cheng, A. Winter, and N. Yu, Discrimination of quantum states under locality constraints in the many-copy setting, in 2021 IEEE International Symposium on Information Theory (ISIT), 1188–1193 (IEEE) (2021), DOI: 10.1109/ISIT45174.2021.9518100.

[27] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Physical Review A 59, 1070 (1999), DOI: 10.1103/PhysRevA.59.1070.

[28] C. A. Fuchs, Just two nonorthogonal quantum states, in P. Kumar, G. M. D’Ariano, and O. Hirota (eds.), Quantum Communication, Computing, and Measurement 2, 11–16 (Springer) (2002), DOI: 10.1007/0-306-47907-7·2.

[29] T. Eggeling and R. F. Werner, Hiding classical data in multipartite quantum states, Physical Review Letters 89, 097905 (2002), DOI: 10.1103/PhysRevLett.89.097905.

[30] S. S. Bhattacharya, S. Saha, T. Guha, and M. Banik, Nonlocality without entanglement: Quantum theory and beyond, Physical Review Research 2, 012068 (2020), DOI: 10.1103/PhysRevResearch.2.012068.

[31] D. G. Fischer, S. H. Kienle, and M. Freyberger, Quantum-state estimation by self-learning measurements, Physical Review A 61, 032306 (2000), DOI: 10.1103/PhysRevA.61.032306.

[32] A. Wald, Sequential Analysis, Dover books on advanced mathematics (Dover Publications) (1973), ISBN 9780486615790.

[33] E. Martínez Vargas, C. Hirche, G. Sentís, M. Skotiniotis, M. Carrizo, R. Muñoz-Tapia, and J. Calsamiglia, Quantum Sequential Hypothesis Testing, Physical Review Letters...
[34] S. M. Barnett, Minimum-error discrimination between multiply symmetric states, Physical Review A 64, 030303 (2001), DOI: 10.1103/PhysRevA.64.030303.

[35] J. A. Bergou, U. Futschik, and E. Feldman, Optimal unambiguous discrimination of pure quantum states, Physical Review Letters 108, 250502 (2012), DOI: 10.1103/PhysRevLett.108.250502.

[36] N. Dalla Pozza and G. Pierobon, Optimality of square-root measurements in quantum state discrimination, Physical Review A 91, 042334 (2015), DOI: 10.1103/PhysRevA.91.042334.

[37] H. Krovi, S. Guha, Z. Dutton, and M. P. da Silva, Optimal measurements for symmetric quantum states with applications to optical communication, Physical Review A 92, 062333 (2015), DOI: 10.1103/PhysRevA.92.062333.

[38] M. Skotiniotis, R. Hotz, J. Calsamiglia, and R. Muñoz Tapia, Identification of malfunctioning quantum devices, arXiv:1808.02729 (2018).

[39] G. Sentís, J. Calsamiglia, and R. Muñoz Tapia, Exact identification of a quantum change point, Physical Review Letters 119, 140506 (2017), DOI: 10.1103/PhysRevLett.119.140506.

[40] E. Chitambar, R. Duan, and M.-H. Hsieh, When Do Local Operations and Classical Communication Suffice for Two-Qubit State Discrimination?, IEEE Transactions on Information Theory 60, 1549 (2014), DOI: 10.1109/TIT.2013.2295356.

[41] G. Sentís, E. Martínez-Vargas, and R. Muñoz Tapia, Online strategies for exactly identifying a quantum change point, Physical Review A 98, 052305 (2018), DOI: 10.1103/PhysRevA.98.052305.

[42] K. Nakahira, K. Kato, and T. S. Usuda, Local unambiguous discrimination of symmetric ternary states, Physical Review A 99, 022316 (2019), DOI: 10.1103/PhysRevA.99.022316.

[43] D. Brody and B. Meister, Minimum decision cost for quantum ensembles, Physical Review Letters 76, 1 (1996), DOI: 10.1103/PhysRevLett.76.1.
66, 062111 (2002), DOI: 10.1103/PhysRevA.66.062111.

[54] L.-M. Duan and G.-C. Guo, Probabilistic cloning and identification of linearly independent quantum states, Physical Review Letters 80, 4999 (1998), DOI: 10.1103/PhysRevLett.80.4999.