Quantum Sequential Hypothesis Testing

Martínez Vargas, Esteban; Hirche, Christoph; Sentís, Gael; Skotiniotis, Michalis; Carrizo, Marta; Muñoz-Tapia, Ramon; Calsamiglia, John

Published in:
Physical Review Letters

DOI:
10.1103/PhysRevLett.126.180502

Publication date:
2021

Document version
Publisher's PDF, also known as Version of record

Document license:
Unspecified

Citation for published version (APA):
Quantum Sequential Hypothesis Testing

Esteban Martínez Vargas, Christoph Hirche, Gael Sentís, Michalis Skotiniotis, Marta Carrizo, Ramon Muñoz-Tapia, and John Calsamiglia

1Física Teòrica: Informació i Fenòmens Qu`antics, Departament de Física, Universitat Autònoma de Barcelona, 08193 Bellatera (Barcelona) Spain
2QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

(Received 23 November 2020; accepted 13 April 2021; published 6 May 2021)

We introduce sequential analysis in quantum information processing, by focusing on the fundamental task of quantum hypothesis testing. In particular, our goal is to discriminate between two arbitrary quantum states with a prescribed error threshold $\epsilon$ when copies of the states can be required on demand. We obtain ultimate lower bounds on the average number of copies needed to accomplish the task. We give a block-sampling strategy that allows us to achieve the lower bound for some classes of states. The bound is optimal in both the symmetric as well as the asymmetric setting in the sense that it requires the least mean number of copies out of all other procedures, including the ones that fix the number of copies ahead of time. For qubit states we derive explicit expressions for the minimum average number of copies and show that a sequential strategy based on fixed local measurements outperforms the best collective measurement on a predetermined number of copies. Whereas for general states the number of copies increases as $\log 1/\epsilon$, for pure states sequential strategies require a finite average number of samples even in the case of perfect discrimination, i.e., $\epsilon = 0$.

DOI: 10.1103/PhysRevLett.126.180502

Introduction.—Statistical inference permeates almost every human endeavor, from science and engineering all the way through to economics, finance, and medicine. The perennial dictum in such inference tasks has been to the way through to economics, finance, and medicine. The every human endeavor, from science and engineering all functions

$[1,2]$. This approach often entails the practical drawback that all $N$ resources need to be batch processed before a good inference can be made. Fixing the number of resources ahead of time does not reflect the situation that one encounters in many real-life applications that might require an online, early, inference—such as change-point detection $[3–6]$, or where additional data may be obtained on demand if the required performance thresholds are not met.

Sequential analysis $[7]$ is a statistical inference framework designed to address these shortcomings. Resources are processed on the fly, and with each new measured unit a decision to stop the experiment is made depending on whether prescribed tolerable error rates (or other cost functions) are met; the processing is continued otherwise. Since the decision to stop is solely based on previous measurement outcomes, the size $N$ of the experiment is not predetermined but is, instead, a random variable. A sequential protocol is deemed optimal if it requires the least average number of resources among all statistical tests that guarantee the same performance thresholds. For many classical statistical inference tasks it is known that sequential methods can attain the required thresholds with a substantially lower average number of samples than any statistical test based on a predetermined number of samples $[7]$. The ensuing savings in resources, and the ability to take actions in real time, have found applications in a wide range of fields $[3,8]$. Extending sequential analysis to the quantum setting is of fundamental interest, and with near-term quantum technologies on the verge of impacting the global market, the versatility and resource efficiency that sequential protocols provide for quantum information processing is highly desirable.

In this Letter, we consider the discrimination of two arbitrary finite dimensional quantum states $[9]$, $\rho$ (corresponding to the null hypothesis $H_0$) and $\sigma$ (corresponding to the alternative hypothesis $H_1$), in a setting where a large number of copies can be used in order to meet a desired error threshold $\epsilon$. A first step in this direction was taken in Ref. $[10]$, which considers the particular case where $\rho$ and $\sigma$ are pure states and restricts the analysis to specific local measurement strategies. Here, we address the problem in full generality, including arbitrary states, weak and collective measurements. For collective strategies involving a large fixed number of copies the relation between this number and the error $\epsilon$ is $N \sim -\frac{1}{\epsilon} \log \epsilon$ $[11]$, where the rate $\xi$ depends on the pair of hypotheses and on the precise setting as we explain shortly. We show that one can significantly reduce the expected number of copies ($N$) by considering sequential strategies where copies are

$\text{DOI: } 10.1103/PhysRevLett.126.180502$
provided on demand. We give the ultimate lower bounds as a single-letter expression of the form
\[ \langle N \rangle_0 \geq - \frac{\log \epsilon}{D(\rho||\sigma)} + O(1), \quad \langle N \rangle_1 \geq - \frac{\log \epsilon}{D(\sigma||\rho)} + O(1) \]  
\begin{equation} \tag{1} \end{equation}
for \( \epsilon \ll 1 \), where \( \langle N \rangle_\nu \) is the mean number of copies given the true hypothesis is \( \nu \in \{0, 1\} \) and \( D(\rho||\sigma) = \text{tr}\rho(\log \rho - \log \sigma) \) is the quantum relative entropy. In addition, we provide upper bounds which, for the worst-case \( N_{wc} = \max\{\langle N \rangle_0, \langle N \rangle_1\} \), are achievable for some families of states.

Specifically, we consider quantum hypothesis testing in a scenario where one can guarantee that for each realization of the test the conditional probability of correctly identifying each of the hypotheses is above a given threshold. This scenario, first introduced in [10], can be considered genuinely sequential since such strong error conditions cannot be generally met in a deterministic setting. The proof method can be easily extended to the more common symmetric and asymmetric scenarios involving the usual type I (or false positive) and type II (or false negative) errors. We give the optimal scaling of the mean number of copies when the thresholds for either one or both types of errors are asymptotically small.

Before proceeding, let us briefly review these fundamental hypothesis testing scenarios, which come about from the relative importance one places between type I error—the error of guessing the state to be \( \sigma \) when the true state is \( \rho \) whose probability we denote by \( \alpha = P(\hat{H}_1|\rho) \)—and type II error—the error of guessing \( \rho \) when the state is \( \sigma \) whose probability is \( \beta = P(\hat{H}_0|\sigma) \). Often, the two types of errors are put on equal footing (symmetric scenario) and one seeks to minimize the mean probability of error \( \bar{\epsilon} = \eta_0\alpha + \eta_1\beta \) with \( \eta_0, \eta_1 = 1 - \eta_0 \) the prior probabilities for each hypothesis. The mean error decays exponentially with the number of copies with an optimal rate given by the Chernoff distance [12,13], \( \xi_{Ch} = -\inf_{0 \leq \xi \leq 1} \log \text{tr}(\rho^{1-\xi\sigma}) \).

Yet, there are asymmetric instances, e.g., in medical trials, where the effect of approving an ineffective treatment (type II) is far worse than discarding a potentially good one (type I). In such cases it is imperative to minimize the type II error while maintaining a finite probability of successfully identifying the null hypothesis, i.e., \( P(\hat{H}_0|\rho) = 1 - \alpha \geq \rho > 0 \). The corresponding optimal error rate for quantum hypotheses is given by quantum Stein’s lemma [14,15], \( \bar{\epsilon} \sim e^{-\xi_{Ch}} \) where \( \xi_{Ch} = D(\rho||\sigma) \) is the quantum relative entropy. If, on the other hand, we require the type I error to decay exponentially, i.e., \( \alpha \leq e^{-\xi_{Ch}} \) for some rate \( r \), then the optimal rate is given by the quantum Hoeffding bound [16,17]. These optimal error rates for strategies with a fixed number of copies have found applications in quantum Shannon theory [18], quantum illumination [19], and provide operational meaning to abstract information measures [20–22].

What the above results also show is that for \( N \) fixed there is a trade-off between the probabilities of committing either error. The advantage of sequential analysis is that it provides strategies capable of minimizing the average number of copies when both errors are bounded, and yields higher asymptotic rates in each of the settings described above.

**Fixed local measurements.** We begin by considering the case when each quantum system is measured with the same measurement apparatus \( E \), giving rise to identically distributed samples of a classical probability distribution. This strategy has the advantage of being easily implementable, and that it lets us introduce the classical sequential analysis framework. Specifically, the optimal classical sequential test, for both the strong error as well as the symmetric and asymmetric setting, is known to be the sequential probability ratio test (SPRT) [23] which we now review.

After \( n \) measurements have been performed, we have a string of outcomes \( x_n = \{x_1, x_2, \ldots, x_n\} \), where each element has been sampled effectively from a probability distribution determined by the positive operator-valued measure (POVM) \( E = \{E_k\} \) and the true state of the system, i.e., either \( p(x) := \text{tr}(E_x \rho) \), or \( q(x) := \text{tr}(E_x \sigma) \). For given error thresholds \( \epsilon_0, \epsilon_1 \), the strong condition demands that for each conclusive sequence the conditional probabilities obey either
\[ P(\rho|x_n) = \frac{\eta_0p(x_n)}{\eta_0p(x_n) + \eta_1q(x_n)} \geq 1 - \epsilon_0, \quad \text{or} \quad (2) \]
\[ P(\sigma|x_n) = \frac{\eta_1q(x_n)}{\eta_0p(x_n) + \eta_1q(x_n)} \geq 1 - \epsilon_1, \quad \text{(3)} \]
where \( p(x_n) = \prod_{k=1}^{n} p(x_k) \) since the copies are identical and independent (the same holds for \( q \)). If neither condition is met, a new copy needs to be requested and we continue measuring. That is, starting at \( n = 1 \) at every step \( n \) we check whether (1) \( P(\rho|x_n) \geq 1 - \epsilon_0 \), then STOP and accept \( H_0 \), with guaranteed probability of success \( s_0 = 1 - \epsilon_0 \); (2) \( P(\sigma|x_n) \geq 1 - \epsilon_1 \), then STOP and accept \( H_1 \), with guaranteed probability of success \( s_1 = 1 - \epsilon_1 \); (3) if neither 1 nor 2 hold, continue sampling.

Using (2) and (3), the condition to continue sampling can be written in terms of a single sample statistic, the log-likelihood ratio
\[ Z_n = \log \frac{q(x_n)}{p(x_n)} = \sum_{k=1}^{n} z_k \quad \text{with} \quad z_k = \log \frac{q(x_k)}{p(x_k)} \quad \text{(4)} \]
as \( b := \log B \leq Z_n \leq \log A = a \), where \( A = (\eta_0/\eta_1)(1 - \epsilon_1/\epsilon_0) \), 
\[ B = (\eta_0/\eta_1)(\epsilon_0/1 - \epsilon_0). \]
It is convenient to interpret \( Z_n \) as a random walk (see Fig. 1) that at every instance performs a step of
length $z_k$ with probability $p(x_k)$, if $H_0$ holds, or with probability $q(x_k)$, if $H_1$ holds. Under $H_1$ the mean position of the walker at step $n$ is given by $\langle z_n \rangle_1 = \sum_{k=1}^{n} z_k = \sum_{k=1}^{n} D(q\|p)$, where $D(q\|p) = \sum_x q(x) \log (q(x)/p(x))$ is the relative entropy; while for $H_0$, $\langle z_n \rangle_0 = -\sum p(0) |q(0)| < 0$. That is, under $H_1$ the walker has a drift toward the positive axis, while under $H_0$ it drifts toward the negative axis. We define as the stopping time $N$ the first instance in which $\langle z \rangle_i = \sum_{k=1}^{n} z_k$ with probability $\alpha$ and $\beta$ is it minimizes both $\langle N \rangle_0$ and $\langle N \rangle_1$ among all tests (sequential or otherwise) with bounded type I and type II errors. This optimality result due to Wald and Wolfowitz [23] allows us to extend the above results to the asymmetric scenario. For the symmetric scenario, the SPRT has also been shown [28] to be optimal among all tests respecting a bounded mean error $\bar{\epsilon} \leq \bar{\epsilon}$. In the asymptotic limit of small error bounds, $\epsilon_0, \epsilon_1 \ll 1$, the threshold values are $a \sim -\log \epsilon_1$ and $b \sim \log \epsilon_0$, which correspond to $\alpha \sim \eta_1/\eta_0\epsilon_1$ and $\beta \sim \eta_0/\eta_1\epsilon_0$, yielding

$$\langle N \rangle_0 \sim -\frac{\log \epsilon_0}{D(p\|q)}$$

and $\langle N \rangle_1 \sim -\frac{\log \epsilon_1}{D(q\|p)}$. The same expressions hold at leading order in the asymmetric scenario when the type I and II errors are vanishingly small, replacing $\log \epsilon_1$ and $\log \epsilon_0$ by $\log \alpha$ and $\log \beta$, respectively—and in the symmetric scenario replacing both quantities by $\log \bar{\epsilon}$. If one of the error thresholds, say $\alpha$, is kept finite while the second is made vanishingly small $\beta \ll 1$, $\langle N \rangle_1$ remains finite, while the other conditional mean scores as $\langle N \rangle_0 \sim -(1/\alpha) \log \beta / D(p\|q)$. In the Supplemental Material [29] we apply these results to the discrimination of qubit states using projective measurements and give closed expressions for the optimal Bayesian mean number of copies $N_{\text{opt}} \sim -\log \bar{\epsilon}/\bar{\epsilon}_\text{Ch}$ [12,21], and requires nontrivial collective measurements [35].
Ultimate quantum limit.—Quantum mechanics allows for much more sophisticated strategies. For a start, performing a nonprojective generalized measurement already gives important advantages (see below). One can also adapt the measurements depending on the previous measurement outcomes and, importantly, measurements may be weak so that each new measurement acts on a fresh copy but also on the preceding, already measured, copies. Without loss of generality we can assume that at every step \( k \) we perform a measurement with three outcomes \( x_k \in \{0, 1, 2\} \): the first two must fulfill conditions (2) and (3) and trigger the corresponding guess (\( H_0 \) or \( H_1 \), respectively), while the third outcome signals to continue measuring having an additional fresh copy available. The measurement at step \( k \) is characterized by a quantum instrument \( \mathcal{M} = \{ \mathcal{M}_0^k, \mathcal{M}_1^k, \mathcal{M}_2^k \} \), and the sequential strategy is given by a sequence of instruments \( \mathcal{M} = \{ \mathcal{M}_i^k \}_{i=1}^\infty \). With this, given hypothesis \( \nu = \{0, 1\} \), the probability of getting outcome \( x_k \) at step \( k \) can be written as

\[
P_\nu(x_k) = \text{tr}[\mathcal{M}_i^k \circ \mathcal{M}_{i-1}^k \cdots \circ \mathcal{M}_0^k (\rho^\otimes k)] = \text{tr}(E_{x_k}^k \rho^\otimes k),
\]

where we have used that in order to arrive to step \( k \) a “continue” outcome must be triggered in all previous steps, and in the last equality we have defined the effective POVM \( E^k = \{ E_i^k \}_{i=0}^\infty \). Making use of the indicator function \( \mathbb{1}_{\nu \leq N} \), the mean number of steps under hypothesis \( \nu \) can be computed as

\[
\langle N \rangle_\nu = \sum_{k=1}^N \mathbb{1}_{k \leq N} \nu = \sum_{k=1}^\infty \mathbb{1}_{\nu \leq k} \nu = \sum_{n=0}^\infty \mathbb{1}_{\nu < n+1} \nu = \sum_{n=0}^\infty T^\nu_n,
\]

where \( T^\nu_n = P_\nu (n < N) \) is the probability that the sequence does not stop at step \( n \), which from (9) is given by \( T^\nu_n = P_\nu (X_n = 2) \). Optimizing \( \langle N \rangle_\nu \) over all quantum sequential strategies \( \mathcal{M} \) is daunting, as all terms \( T^\nu_n \) are strongly interrelated through the intricate structure of \( E^\nu \). However, a lower bound to each \( T^\nu_n \) can be found by relaxing such a structure and only imposing minimal requirements on the effective POVM; namely the error bounds (6), positivity and completeness:

\[
\begin{align*}
\min \text{tr}(E_i^n \rho^\otimes n) & \geq 0, \\
\sum_{i=0}^2 E_i^n & = 1, \\
\text{tr}[E_1^n (\sigma^\otimes n - A \rho^\otimes n)] & \geq 0, \\
\text{tr}[E_0^n (\rho^\otimes n - B^{-1} \sigma^\otimes n)] & \geq 0.
\end{align*}
\]

This semidefinite program, which can be considered a two-sided version of the quantum Neyman-Pearson test [20], is an interesting open problem in its own right. Our focus, however, is the asymptotic regime of small error bounds. In these asymptotic scenarios we are able to show, exploiting some recent strong converse results in hypothesis testing [33,36], that for all \( n < n^* = (\log \epsilon_0 / 1 - A^{-1}) / D(\rho | | \sigma) \), \( T^\nu_n \geq 1 - O(\epsilon_\nu^k) \) for some \( \nu \in \{0, 1\} \) [29], which leads to the desired bound:

\[
\langle N \rangle_0 \geq \sum_{n=0}^{n^*} T^\nu_n \geq - \frac{\log \epsilon_0 (1 - A^{-1})}{D(\rho | | \sigma)} + O(1).
\]

An analogous bound holds for \( \langle N \rangle_1 \). The bounds for asymmetric (symmetric) scenarios (see [29]) take the same form, replacing \( \log \epsilon_0 \) by \( \log \beta (\log \epsilon) \) and \( A^{-1} \) by \( \alpha (\epsilon) \). In the asymmetric scenario where \( \epsilon_1 \) or \( \alpha (\epsilon) \) is kept finite, it also holds that \( \langle N \rangle_1 = O(1) \) and \( \langle N \rangle_0 \) is given by the appropriate version of (12).

Attainability and upper bounds.—Consider a sequential strategy that involves a fixed, collective measurement \( K = \{ K_i \} \), acting on consecutive blocks of \( \ell \) copies, yielding two possible distributions \( p_{\ell, K}^\nu, q_{\ell, K}^\nu \). Using the classical SPRT we get that

\[
\langle N \rangle_0 \sim \ell \inf_{K} \inf_{\sigma} \frac{- \log \epsilon_0}{D(p_{\ell, K}^\nu q_{\ell, K}^\nu || \sigma || \sigma)} \sim \ell \inf_{K} \frac{- \log \epsilon_0}{D(\rho || \sigma)} (\epsilon),
\]

where \( \epsilon \) is the number of blocks used at the stopping time. In the last relation of (13) we have used the fact that we are in the asymptotic setting where \( \epsilon_0 \ll 1 \) and therefore we can take arbitrarily long block lengths \( \ell \gg 1 \). We also exploit the following property of the measured relative entropy [14,37]: \( \sup_{\sigma} D(p_{\ell, K}^\nu q_{\ell, K}^\nu || \sigma) \sim D(\rho || \sigma) \).

Notice, however, that for arbitrary states \( \rho \) and \( \sigma \) block sampling can attain either \( \langle N \rangle_0 \) or \( \langle N \rangle_1 \), but it is unknown whether one can attain in general both bounds simultaneously, i.e., whether a measurement achieving the
supremum of \( \lim_{\epsilon \to 0} 1/\epsilon D(q_K^\epsilon \| p_K^\epsilon) \) can also attain the supremum of \( \lim_{\epsilon \to 0} 1/\epsilon D(p_K^\epsilon \| q_K^\epsilon) \). For instance, if we wish to optimize the Bayesian mean number of copies \( \langle N \rangle \), we can use block sampling to attain

\[
\langle N \rangle_{\text{block}} \sim \liminf_{\epsilon \to 0} k \left( -\frac{\epsilon \eta_0 \log c_0 - \epsilon \eta_1 \log c_1}{D(p_K^\epsilon \| q_K^\epsilon) - D(q_K^\epsilon \| p_K^\epsilon)} \right).
\]  

However, this strategy might be suboptimal and hence it only provides an upper bound to the optimal Bayesian mean \( \langle N \rangle \leq \langle N \rangle_{\text{block}} \). This notwithstanding, there are at least two cases when this upper bound coincides with the lower bound provided by (12): when \( \rho \) and \( \sigma \) commute, and when the two states do not have common support. If, say, \( \text{supp}(\sigma) \cap \ker(\rho) \neq 0 \), one can use block sampling to attain (12) for \( \langle N \rangle_0 \) and always detect \( \rho \) with a finite number of copies—note that since \( D(\sigma \| \rho) = \infty \), the lower bound \( \langle N \rangle_1 = O(1) \) is also attained.

We can also give achievable lower bounds for a worst-case type figure of merit \( N_{\text{wc}} \) and the Bayesian mean \( \langle N \rangle \). This shows that, for pure states, it suffices to perform local unambiguous measurements to attain the optimal (finite) average number of copies with zero error under hypothesis \( H_c \). Note that because of the tradeoff \( c_0 c_1 \geq tr(\rho \sigma) \), one cannot attain the minimal values of \( \langle N \rangle_{\text{local}} \) and \( \langle N \rangle_{\text{local}} \) for general states \( \rho, \sigma \), simultaneously. For instance, one can reach the minimal value \( c_0 = tr(\rho \sigma) \) for one hypothesis, but then having a maximal value \( c_1 = 1 \) for the second; or choose the optimal symmetric setting, \( c_0 = c_1 = \sqrt{tr(\rho \sigma)} \), that achieves the minimum value of both the worst-case \( N_{\text{wc}} \) and the Bayesian mean \( \langle N \rangle \) with equal priors (see [29]). This is in stark contrast with the behavior found in [10], where all strategies considered were based on two-outcome projective measurements, for which the average number of copies scaled as \( \langle N \rangle \propto -\log \epsilon \).

We acknowledge financial support from the Spanish Agencia Estatal de Investigación, project PID2019–107609 GB-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. C. H. acknowledges financial support from the European Research Council (ERC Grant Agreement No. 81876), VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059) and the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union Horizon 2020 Programme (QuantAlgo project) via Innovation Fund Denmark. J. C. acknowledges from the QuantERA grant C’MON-QSENS!, via Spanish MICINN PCI2019-111869-2, EMV thanks financial support from CONACYT. J. C. also acknowledges support from ICREA Academia award.

---

1. Esteban.Martinez@uab.cat
2. christoph.hirche@gmail.com
3. Gael.Sentis@uab.cat
4. michail.skoteiniotis@uab.cat
5. Ramon.Munoz@uab.cat
6. John.Calsamiglia@uab.cat

[11] By $f(\epsilon) \sim g(\epsilon)$ we mean asymptotic equivalence $\lim_{\epsilon \to 0} f(\epsilon)/g(\epsilon) = 1$.
[29] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.126.180502 where we provide the proof of the lower bound for the mean number of copies under each hypothesis, we apply our general results to the case of qubit states, we compute the exact optimal mean number of copies (worst-case and Bayesian) required for the perfect discrimination of pure states, and which includes [26,27,30–34].
[38] Note that the comparison with $N_{CH}$ is unfavorable to sequential strategies. Substituting $\epsilon_0$ and $\epsilon_1$ by $\bar{\epsilon}$ in Eq. (12) implies that each type of error is independently constrained, whereas $N_{CH}$ refers to a deterministic (symmetric) protocol where the mean error is $\bar{\epsilon}$ and thus to a weaker version of the problem. In spite of this, the sequential scenario displays a significant advantage.