Extracting information from a qubit by multiple observers: Toward a theory of sequential state discrimination

Janos Bergou, Edgar Feldman, and Mark Hillery

1Department of Physics, Hunter College of the City University of New York, 695 Park Avenue, New York, NY 10065 USA and
2Department of Mathematics, Graduate Center of the City University of New York, 365 Fifth Avenue, New York, NY 10016 USA

We discuss sequential unambiguous state-discrimination measurements performed on the same qubit. Alice prepares a qubit in one of two possible states. The qubit is first sent to Bob, who measures it, and then on to Charlie, who also measures it. The object in both cases is to determine which state Alice sent. In an unambiguous state discrimination measurement, we never make a mistake, i.e., misidentify the state, but the measurement may fail, in which case we gain no information about which state was sent. We find that there is a nonzero probability for both Bob and Charlie to identify the state, and we maximize this probability. The probability that Charlie’s measurement succeeds depends on how much information about the state Alice sent is left in the qubit after Bob’s measurement, and this information can be quantified by the overlap between the two possible states in which Bob’s measurement leaves the qubit. This paper is a first step toward developing a theory of nondestructive sequential quantum measurements, which could be useful in quantum communication schemes.

PACS numbers: 03.67.-a

When an observer performs a standard projective quantum measurement on a system, the state of the system after the measurement, the so-called post-measurement state, \( |\phi\rangle \), is an eigenstate of the operator that we measured. The measurement is, thus, destructive, and it is generally assumed that any information about the initial state \( |\psi\rangle \) of the system is lost in this process. If, immediately after the first measurement, a second observer performs another measurement on the system the results are describable in terms of \( |\phi\rangle \), the post-measurement state of the first observer and not in terms of the initial state \( |\psi\rangle \). Therefore it is generally assumed that consecutive measurements on the same quantum system do not yield additional information on the initial preparation, every consecutive observation prepares the system in a new state.

The purpose of this paper is to show that this commonly accepted view of standard quantum measurements can be very significantly refined. We show that it is possible to perform consecutive observations on the same system by multiple observers in such a way that each observer in the chain obtains information about the initial state. In fact, and this is the most surprising of our findings, we show that it is possible that each observer obtains full information about the state in which the system was prepared initially. This paper is a first attempt toward developing a theory of nondestructive sequential quantum measurements.

We illustrate these ideas in the case in which there are two observers in the observation chain, and each of them performs an unambiguous state discrimination measurement. We emphasize that this is for illustrative purposes only, the same ideas work for more than two consecutive observers and other measurement scenarios.

In its simplest form unambiguous state discrimination (UD) is the following measurement task. Alice prepares a qubit in one of two known states, \( |\psi_1\rangle \) or \( |\psi_2\rangle \), and sends it to Bob. His task is to determine what the state of the qubit is, with no error permitted\(^1\). If \( |\psi_1\rangle \) and \( |\psi_2\rangle \) are not orthogonal, Bob cannot succeed all the time; the price to pay for no error is that the measurement that distinguishes the states will sometimes fail. That is, the measurement has three possible outcomes, 1, corresponding to \( |\psi_1\rangle \), 2, corresponding to \( |\psi_2\rangle \), and 0, corresponding to failure or inconclusive outcome. If the qubit is in the state \( |\psi_1\rangle \) Bob can obtain either 1 or 0 as a measurement result, but never 2. Similarly, if the qubit is in the state \( |\psi_2\rangle \) he can obtain the results 2 or 0, but never 1. The measurement is optimal if the probability of failure is a minimum and is given by \( |\langle \psi_1 | \psi_2 \rangle| \) in the case that the states are equally probable. UD is employed in, e.g., quantum key distribution, quantum secret sharing and quantum algorithms\(^5\)–\(^7\).

Here we address the question whether more than one user can identify the initial state of the same qubit. In this scenario Alice prepares a qubit in either \( |\psi_1\rangle \) or \( |\psi_2\rangle \) and sends it to Bob. Bob performs an unambiguous discrimination measurement on the qubit, and sends it on to Charlie, who also performs an unambiguous discrimination measurement on the qubit. We want both Bob and Charlie to have a nonzero chance of identifying the state so that the probability of both of them succeeding is a maximum. The rules of the game are that any pre-measurement conspiracy is allowed among all parties but no classical communication can take place between Bob and Charlie after Bob performs his measurement, a scenario typical in secure quantum communication strategies. So, in particular, Charlie never knows
whether Bob’s measurement succeeded or failed. The key to making this procedure work is that the state discrimination Bob performs cannot be optimal, otherwise he would have extracted all of the quantum information carried by the qubit, and there would be none left for Charlie to measure.

Thus, the question of how much information about a state is left after it has been measured is more subtle that is commonly assumed, especially if the measurement is a generalized one, which is described by a POVM (Positive Operator Valued Measure). However, some information is left even in the case of projective measurements. Rapčan et al. [9] examined how a second observer could “scavenge” information about a quantum state that has previously been measured by a first observer. In their scenario, the second observer has no information about the measurement made by the first, and yet he is still able to gain information about the initial state of the system. In our scenario, Charlie knows exactly what type of measurement Bob will perform. Without this condition Charlie would not be able to perform unambiguous discrimination. It is, nonetheless somewhat surprising that after the disturbance of the quantum state of the qubit produced by Bob’s measurement, it is still possible for Charlie to perform an unambiguous discrimination measurement to determine which state was sent by Alice.

To begin we assume that Alice prepares qubits in |ψ₁⟩ or |ψ₂⟩ with equal probability. Without loss of generality, the overlap of the two possible states, s = ⟨ψ₁|ψ₂⟩ is taken to be real (0 ≤ s ≤ 1) and we choose the phase of |ψ₁⁺⟩, the vector orthogonal to |ψ₁⟩, so that

$$\begin{align*}
|ψ₁⟩ &= s|ψ₁⟩ + \sqrt{1 - s²}|ψ₁⁺⟩ \\
|ψ₂⟩ &= \sqrt{1 - s²}|ψ₁⟩ - s|ψ₁⁺⟩.
\end{align*}$$

Both Bob’s and Charlie’s measurements are described by POVM’s [9]. Each POVM has three elements, Π₁ corresponding to the detection of |ψ₁⟩, the second, Π₂ corresponding to the detection of |ψ₂⟩, and the third, Π₀, corresponding to the failure of the measurement. Each element is a positive operator on the two-dimensional qubit Hilbert space, and their sum is the identity operator. If one is measuring a qubit in the state |ψ₁⟩, the probability of obtaining the outcome j is ⟨ψ₁|Πⱼ|ψ₁⟩.

The requirement that errors are not allowed mandates that the POVM elements describing Bob’s measurement are of the form

$$\begin{align*}
Π₁^B &= c₁|ψ₁⁺⟩⟨ψ₁| \\
Π₂^B &= c₂|ψ₁⁺⟩⟨ψ₁| \\
Π₀^B &= I - Π₁^B - Π₂^B
\end{align*}$$

for the conclusive outcomes and

$$Π₀ = I - Π₁ - Π₂$$

for the inconclusive one, since the three elements add to the identity. Here c₁ and c₂ are positive constants yet to be determined, subject to the constraint Π₀ ≥ 0. Π₁ and Π₂ are positive by construction.

The probability that Bob unambiguously detects |ψ₁⟩ if it is sent is given by

$$p_i = \langle ψ₁|Π_i^B|ψ₁⟩,$$

for i = 1, 2 and the probability that the measurement fails if |ψᵢ⟩ is sent is given by

$$q_i = \langle ψᵢ|Π₀^B|ψᵢ⟩.$$ 

Note that the probability that |ψᵢ⟩ is detected if |ψ₁⟩ is sent is zero for i ≠ j, so pᵢ + qᵢ = 1. These relations allow us to express cᵢ in terms of the more physical success and failure probabilities,

$$c_i = \frac{p_i}{1 - s^2} = \frac{1 - q_i}{1 - s^2}.$$  

(3)

We will have to know the states after Bob’s measurement, since they will be the input states for Charlie’s measurement. They can be expressed in terms of the so-called detection operators Aⱼ that are related to the corresponding POVM elements by Πⱼ^B = Aⱼ^†Aⱼ for j = 0, 1, 2. If |ψᵢ⟩ is the state before the measurement, then if we obtain the result i for the measurement (i = 1, 2 success), the post-measurement state (success state) |φᵢ⟩ is given by

$$|φᵢ⟩ = \frac{A_i|ψᵢ⟩}{∥A_i|ψᵢ⟩∥},$$

(4)

and if we obtain the result 0 for the measurement, the post-measurement state (failure state) |χᵢ⟩ is given by

$$|χᵢ⟩ = \frac{A₀|ψᵢ⟩}{∥A₀|ψᵢ⟩∥}.$$  

(5)

The operators Aⱼ can be chosen in the form Aⱼ = Uⱼ(Πⱼ^B)½/2, where Uⱼ can be any unitary operator. Thus, we have quite a bit of freedom in choosing these operators and, consequently, Bob’s post-measurement states. In our case they can be expressed as

$$A₁ = \sqrt{a₁}|ψ₁⟩⟨ψ₁| + \sqrt{a₂}|ψ₂⟩⟨ψ₂|,$$

and

$$A₂ = \sqrt{a₂}|ψ₂⟩⟨ψ₂|.$$  

We can now see what happens after Bob’s measurement. If Alice sent |ψ₁⟩, then Bob will send Charlie the state |φ₁⟩ with probability p₁ or the state |χ₁⟩ with probability q₁. However, we know that for unambiguous discrimination to be possible, the states to be discriminated must be linearly independent [10], and since we are in a two-dimensional space, Charlie can only discriminate between two possible pure states. This mandates the choice |φ₁⟩ = |χ₁⟩ which, in turn, implies

$$A₀ = \sqrt{a₁}|ψ₁⟩⟨ψ₁| + \sqrt{a₂}|ψ₂⟩⟨ψ₂|,$$

(6)

where a₁ and a₂ are constants to be determined. Therefore, if Alice sent |ψ₁⟩, Bob will receive |φ₁⟩, whether Bob’s measurement succeeded or not, and if Alice sent |ψ₂⟩, Bob will receive |φ₂⟩, again whether Bob’s measurement succeeded or not. Charlie’s task, then, is to optimally discriminate between |φ₁⟩ and |φ₂⟩. Further, since ⟨ψ₁|A₀|ψ₁⟩ = q₁, we have that

$$a_i = q_i/(1 - s²).$$  

(7)

We now have two different expressions for Π₀, Eq. 2 and A₀, Eq. 6, so still have to check their compatibility. In the {⟨ψ₁⟩, |ψ₁⁺⟩} basis the operator Π₀^B, Eq. 2...
takes the form
\[ \Pi_0^B = \begin{pmatrix} 1 - c_1 + c_1 s^2 & c_1 s \sqrt{1 - s^2} \\ c_1 s \sqrt{1 - s^2} & 1 - c_1 s^2 - c_2 \end{pmatrix}. \] (8)

It is easy to obtain the eigenvalues and corresponding eigenvectors explicitly. For our purposes, however, the conditions of non-negativity of \( \Pi_0 \), \( \text{Tr}(\Pi_0) = 2 - c_1 - c_2 \geq 0 \) and \( \det \Pi_0 = 1 - c_1 - c_2 + c_1 c_2 (1 - s^2) \geq 0 \), are more useful. The second is the stronger of the two conditions. When it is satisfied the first one is always met. Using [3], the condition on the failure probabilities takes the form,
\[ 1 \geq q_1 q_2 \geq s^2. \] (9)

If we now calculate \( \Pi_0 = A_1^B A_0 \) from (6) with \( a_i \) from [7], we find that the two expressions agree if
\[ q_1 q_2 = \frac{s^2}{t^2} \] (10)

where we introduced \( \langle \phi_1 | \phi_2 \rangle \equiv t \), which we can assume is real and positive. The condition (10) is clearly compatible with (9) provided \( t = \langle \phi_1 | \phi_2 \rangle \geq s = \langle \psi_1 | \psi_2 \rangle \).

The emerging picture is now the following. Bob extracts some information about the two possible inputs, |\( \psi_1 \rangle \) and |\( \psi_2 \rangle \). By doing so he produces states with a greater overlap, \( t > s \). Charlie’s task, then, is to optimally discriminate between |\( \phi_1 \rangle \) and |\( \phi_2 \rangle \). Since an optimized measurement extracts all of the remaining information, Charlie’s post-measurement states can carry no further information about the initial preparation so for all inputs and outcomes they are collapsed to the same common state. The failure probabilities for Bob’s measurement must satisfy the constraint given by Eq. (10). Charlie’s failure probabilities must satisfy an entirely similar constraint that we can most easily obtain by replacing \( s \) with \( t \) and \( t \) with \( 1 \) in (10), since we notice that for his measurement \( t \) is the overlap of the input states and the overlap of the post-measurement states is 1. The two constraints are given together as [upper index B (C): Bob (Charlie)]
\[ q_1 q_2 = \frac{s^2}{t^2}, \quad q_1^C q_2^C = t^2. \] (11)

The corresponding measurement tree is shown in Fig. 1.

Let us now examine the probability of both measurements succeeding. Clearly, for the upper branch of the measurement tree in Fig. 1 the joint probability of success is \( P_1 = p_1^B p_1^C = (1 - q_1^B)(1 - q_1^C) \) and for the lower branch \( P_2 = p_2^B p_2^C = (1 - q_2^B)(1 - q_2^C) \), so the average joint success probability is
\[ P_S = \frac{1}{2} [(1 - q_1^B)(1 - q_1^C) + (1 - q_2^B)(1 - q_2^C)]. \] (12)

This is the quantity we want to optimize under the two constraints given in (11). The optimization is straightforward and can be done by, e.g., using the method of Lagrange multipliers, with the result \( q_1^B = q_2^B = q_1^C = q_2^C = \sqrt{s} \) and \( t = \sqrt{s} \). That the result must be fully symmetric under the exchange of the states could have been guessed from the full exchange symmetry of the problem for equal priors.

Using the optimal values in (12), we finally obtain
\[ P_S^{(\text{opt})} = (1 - \sqrt{s})^2. \] (13)

This equation constitutes the central result of our paper. It clearly shows that there is a finite probability that both of the consecutive observers succeed in extracting the full information about the states. We also note that the probability of at least one of Bob’s or Charlie’s measurements succeeding is just \( 1 - s \), which is just the probability of a single optimal unambiguous discrimination measurement of |\( \psi_1 \rangle \) and |\( \psi_2 \rangle \) succeeding.

If we do not allow Bob and Charlie to communicate classically, this is the best we can do. Let us compare this result to some strategies that do allow Bob and Charlie to communicate. The strategies to be discussed, like the one discussed above, will not produce any errors.

One possibility would be for Bob to perform an optimal unambiguous discrimination measurement on the qubit he receives from Alice. If he succeeds he tells Charlie the
results, while if he fails he informs Charlie that his measurement failed, and that is the end of the procedure. In this case, if Bob fails, they both fail and if Bob succeeds they both succeed. The probability of Bob succeeding is

\[ P_S^{(1)} = 1 - s \]

which is also the probability of both of them succeeding. This strategy, allowing full classical communication after Bob’s measurement, is expected to have the highest probability of both of them succeeding.

One other possibility would be for Bob to perform an optimal unambiguous discrimination measurement on the qubit he receives from Alice. If he succeeds he sends a qubit in the state he found to Charlie, while if he fails he informs Charlie that his measurement failed, and that is the end of the procedure. In this case, if Bob fails, they both fail. The probability of at least one of them succeeding is the same as that of Bob succeeding, \(1 - s\), while the probability of both of them succeeding is

\[ P_S^{(2)} = (1 - s)^2 \]  

This strategy has the same probability of at least one of the parties succeeding, but a smaller probability of joint success than the previous one because there is less classical communication.

A third possibility is for Bob to probabilistically clone the qubit he receives from Alice. A probabilistic cloner can produce perfect clones of an input qubit if the state of that qubit is chosen from a limited set [11]. In addition, it does not always succeed, but we do know when it has succeeded. If the input qubit can only be in either \(|\psi_1\rangle\) or \(|\psi_2\rangle\), then the probability of successfully producing two clones at the output is \(1/(1 + s)\). The cloning strategy consists of Bob cloning the qubit he gets from Alice, and if the cloning is successful, he keeps one qubit and sends the other to Charlie. If the cloning fails, he tells Charlie, and that is the end of the procedure. Both Bob and Charlie perform optimal unambiguous discrimination measurements on their qubits. The probability that at least one of the parties learns which state Alice sent, is the probability that the cloning succeeds and that at least one of the measurements succeeds is \(1 - s\). This is the same as in the two previous strategies. The probability that both parties determine which state Alice sent, which is the probability that the cloning succeeds and both measurements succeed, is

\[ P_S^{(3)} = (1 - s)^2/(1 + s) \]

which is greater than \((1 - \sqrt{3})^2\), but less than \((1 - s)^2\) since there is some classical communication but less than in the previous cases.

Therefore, none of the strategies that allow Bob and Charlie to communicate classically does better than the strategy that does not allow them to communicate when we only consider the probability of one or both of the parties identifying the state. However, they all do better when we consider the probability of both parties identifying the state. Note that all of the protocols described in the last three paragraphs use more than one qubit, while the sequential unambiguous discrimination protocol uses only one. Their performance is compared in Fig. [2].

FIG. 2: Joint success probability \(P_s\) vs. \(s\) for the four strategies discussed in the paper. Solid line: \(P_S^{(opt,n)}\) vs. \(s\), Eq. (13). Dotted line: \(P_S^{(1)}\) vs. \(s\), Eq. (14). Dot dashed line: \(P_S^{(2)}\) vs. \(s\), Eq. (15). Dashed line: \(P_S^{(3)}\) vs. \(s\), Eq. (16).

Increasing the amount of classical communication clearly increases the probability of joint success. However, classical communication also decreases the secrecy of the shared bits. Alice sending out one qubit can establish a secret key with Bob and Charlie separately but there will be also a three way key on the instances when both recipients succeed.

The sequential scheme we propose can be generalized in several directions. One obvious generalization is for general prior probabilities. Another one could be the extension to more than two consecutive observers. Instead of just Bob and Charlie one could have \(B_1, B_2, \ldots, B_n\) and there will be a finite probability that each one successfully identifies the initial state of the qubit. The optimal joint probability of success is given by

\[ P_S^{(opt,n)} = (1 - s^{1/n})^n \]

which is a straightforward generalization of [13]. Finally, the theory of sequential measurements is not at all restricted to POVMs and can be extended to other measurement scenarios including, in particular, standard projective measurements. These and other generalizations are left, however, for a separate publication [12].

In summary, the scheme we have proposed, successive unambiguous discrimination measurements on the same qubit, could be useful in quantum communication schemes. The B92 quantum cryptography protocol is based on communication using nonorthogonal states [5]. An eavesdropper, Eve, is not able to perfectly identify
which state has been sent, and will, consequently, introduce errors, which will reveal her presence. The measurement scheme presented here could allow this protocol to be extended to more than two parties without increasing the number of qubits involved. Once the measurements are complete, Bob and Charlie announce whether their measurements succeeded or failed, and, in the case of success, one or both of them will share a secret bit with Alice and with each other.

Acknowledgments. This research was partially supported by the Institute for Quantum Optics and Quantum Information, University of Vienna (JB).

[1] I. D. Ivanovic, Phys. Lett. A 123, 257 (1987).
[2] D. Dieks, Phys. Lett. A 126, 303 (1988).
[3] A. Peres, Phys. Lett. A 128, 19 (1988).
[4] For a review of state discrimination see Discrimination of Quantum States by J. A. Bergou, U. Herzog, and M. Hillery in Quantum State Estimation, edited by M. G. A. Paris and J. Rehacek (Springer Verlag, Berlin, 2004).
[5] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).
[6] M. Hillery and J. Mimih, Phys. Rev. A 67, 042304 (2003).
[7] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. Lett 90, 257901 (2003).
[8] P. Rapčan, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, and V. Bužek, Phys. Rev. A 84, 032326 (2012).
[9] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge, England, 2000).
[10] A. Chefles, Phys. Lett. A 239, 339 (1998).
[11] L-M. Duan and G.-C. Guo, Phys. Rev. Lett. 80, 4999 (1998).
[12] J. A. Bergou, E. Feldman, and M. Hillery, in preparation.