Quantum Filtering and Discrimination between Sets of Boolean Functions

János A. Bergou,[1,2] Ulrike Herzog,[3] and Mark Hillery[1]

[1]*Department of Physics, Hunter College, City University of New York, 695 Park Avenue, New York, New York 10021, USA*

[2]*Institute of Physics, Janus Pannonius University, H-7624 Pécs, Ifjúság útja 6, Hungary*

[3]*Institut für Physik, Humboldt-Universität zu Berlin, Newtonstrasse 15, D-12489 Berlin, Germany*

(Received 23 September 2002; published 25 June 2003)

In quantum state filtering one wants to determine whether an unknown quantum state, which is chosen from a known set of states, $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$, is either a specific state, say $|\psi_1\rangle$, or one of the remaining states, $\{|\psi_2\rangle, \ldots, |\psi_N\rangle\}$. We present the optimal solution to this problem, in terms of generalized measurements, for the case that the filtering is required to be unambiguous. As an application, we propose an efficient, probabilistic quantum algorithm for distinguishing between sets of Boolean functions, which is a generalization of the Deutsch-Jozsa algorithm.

DOI: 10.1103/PhysRevLett.90.257901 PACS numbers: 03.67.Lx, 03.65.Ta, 03.65.Wj, 42.50.–p

Optimal discrimination among quantum states plays a central role in quantum information theory. Interest in this problem was prompted by the suggestion to use nonorthogonal quantum states for communication in certain secure quantum cryptographic protocols, most notably in the one based on the two-state procedure as developed by Bennett [1]. The reason why until recently the area has shown relatively slow progress within the rapidly evolving field of quantum information is that it poses quite formidable mathematical challenges. Except for a handful of very special cases, no general exact solution has been available involving more than two arbitrary states. In this Letter we present an exact solution to an optimum measurement problem involving an *arbitrary* number of quantum states, with *no restriction* on the states. The resulting method has the potential for widespread applications in quantum information processing. In particular, it lends itself quite naturally to a quantum generalization of probabilistic classical algorithms. Whenever it is possible to find a one-to-one mapping of classical alternatives onto quantum states, our method can discriminate among these quantum alternatives in a *single step* with optimum success probability.

We illustrate the strength of the method on the example of a probabilistic quantum algorithm to discriminate between sets of Boolean functions. A Boolean function on n bits is one that returns either 0 or 1 as output for every possible value of the input x, where $0 \leq x \leq 2^n - 1$. The function is uniform (or constant) if it returns the same output on all of its arguments, i.e., either all 0's or all 1's; it is balanced (or even) if it returns 0's on half of its arguments and 1's on the other half; and it is biased if it returns 0's on m_0 of its arguments and 1's on the remaining $m_1 = 2^n - m_0$ arguments ($m_0 \neq m_1 \neq 0$ or $2^n - 1$). Classically, if one is given an unknown function and told that it is either balanced or uniform, one needs $2^{(n-1)} + 1$ measurements to decide which. Deutsch and Jozsa [2] developed a quantum algorithm that can accomplish this task in one step. To discriminate a biased Boolean function from an unknown balanced one, $2^{(n-1)} + m_1 + 1$ measurements are needed classically, where, without loss of generality, we have assumed that $m_1 < m_0$. Here we propose a probabilistic quantum algorithm that can unambiguously discriminate a known biased Boolean function from a given set of balanced ones in one step.

The method is based on the optimum unambiguous quantum state filtering scenario which, in turn, is a special case of the following more general problem. We know that a given system is prepared in one of N known nonorthogonal quantum states, but we do not know which one. We want to assign the state of this system to one or the other of two complementary subsets of the set of the N given states where one subset has M elements and the other has $N - M$ ($M \leq N/2$). Since the subsets are not mutually orthogonal, the assignment cannot be done with a 100% probability of success. For the case that the assignment is required to be unambiguous, at the expense of allowing inconclusive results to occur the probability of which is minimized, the problem has recently been solved for $N = 3$ [3]. For the case that the assignment is to be performed with minimum error, the solution has been found for arbitrary M and N under the restriction that the Hilbert space spanned by the states is two dimensional [4]. We refer to either case as quantum state filtering when $M = 1$ and $N \geq 3$.

Unambiguous filtering is related to unambiguous quantum state discrimination: one is given a quantum system, prepared in a state that belongs to a known set of nonorthogonal states, and one wants to determine, without possibility of error, which state the system is in [5]. Since the states are not mutually orthogonal, at first glance the problem appears impossible. However, it becomes possible if we allow the procedure to fail a certain fraction of the time. That is, when we apply the procedure, we will either find out what the quantum state of the system is, or we will fail to do so, but we will never make an erroneous identification. The optimal method for discriminating between two states was found in Refs. [6–8]. No general

solution is known for more than two states but there are special cases that can be solved, and some features of the general solution have been extracted [9–13]. Chefles has shown [10] that the states have to be linearly independent for unambiguous state discrimination to succeed but orthogonality is not required.

We begin by presenting the solution to the unambiguous quantum state filtering problem. Suppose we are given a quantum system prepared in the state $|\psi\rangle$, which is guaranteed to be a member of the set of N nonorthogonal states $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$, but we do not know which one. We denote by η_i the *a priori* probability that the system was prepared in the state $|\psi_i\rangle$. We want to find a procedure that will unambiguously assign the state of the quantum system to one or the other of two complementary subsets of the set of the N given nonorthogonal quantum states, either $\{|\psi_1\rangle\}$ or $\{|\psi_2\rangle, \ldots, |\psi_N\rangle\}$. Quantum measurement theory tells us that nonorthogonal states cannot be discriminated perfectly. If we are given $|\psi_i\rangle$, we will have some probability p_i to correctly assign it to one of the subsets and, correspondingly, some failure probability, $q_i = 1 - p_i$, to obtain an inconclusive answer. The average probabilities of success and of failure are $P = \sum_{i=1}^{N} \eta_i p_i$, and

$$Q = \sum_{i=1}^{N} \eta_i q_i, \tag{1}$$

respectively. Our objective is to find the set of $\{q_i\}$ that minimizes the probability of failure, Q.

It is easy to see that a standard quantum measurement (SQM, a von Neumann projective measurement) can achieve error-free filtering. If we project on either of the two sets (state selective measurement, first strategy) a "no click" will indicate that we were given a state from the other set, assuming perfect detectors. A somewhat better approach is to project on a direction that is perpendicular to one of the sets (nonselective measurement, second strategy). Now, a detector "click" indicates that we were given a state from the other set and perfect detectors are not required. For example, if we measure the operator $F^{(1)} = I - |\psi_1\rangle\langle\psi_1|$, then a click (corresponding to the eigenvalue 1) shows that the vector is not $|\psi_1\rangle$ and the measurement has succeeded. If we do not obtain a click (eigenvalue 0), then the measurement has failed, and we do not know which vector we were given. The probability of failure, $Q^{(1)}_{\mathrm{SQM}}$, is given by

$$Q^{(1)}_{\mathrm{SQM}} = \eta_1 + S, \tag{2}$$

where $S = \sum_{i=2}^{N} \eta_i |\langle\psi_1|\psi_i\rangle|^2$ is the average overlap between the two subsets.

A second possibility is to split $|\psi_1\rangle$ into two components, $|\psi_1\rangle = |\psi_1^{\perp}\rangle + |\psi_1^{\parallel}\rangle$. Here $|\psi_1^{\perp}\rangle$ is orthogonal to the subspace, $\mathcal{H}_2$, that is spanned by the vectors $|\psi_2\rangle, \ldots, |\psi_N\rangle$, and $|\psi_1^{\parallel}\rangle$ lies in $\mathcal{H}_2$. Their normalized versions are $|\tilde{\psi}_1^{\perp}\rangle = |\psi_1^{\perp}\rangle / \| \psi_1^{\perp} \|$ and $|\tilde{\psi}_1^{\parallel}\rangle = |\psi_1^{\parallel}\rangle / \| \psi_1^{\parallel} \|$, respectively, where the norm is defined in the usual way, $\| \psi \|^2 = \langle\psi|\psi\rangle$. We then introduce the operator $F^{(2)} = |\tilde{\psi}_1^{\perp}\rangle\langle\tilde{\psi}_1^{\perp}| - (I - |\tilde{\psi}_1^{\perp}\rangle\langle\tilde{\psi}_1^{\perp}| - |\tilde{\psi}_1^{\parallel}\rangle\langle\tilde{\psi}_1^{\parallel}|)$, which has eigenvalues 1, 0, and -1. If we measure $F^{(2)}$ and obtain 1, then the vector was $|\psi_1\rangle$, if we obtain -1, then the vector was in the set $\{|\psi_2\rangle, \ldots, |\psi_N\rangle\}$, and if we obtain 0, the procedure failed. In this case the probability of failure, $Q^{(2)}_{\mathrm{SQM}}$, is given by

$$Q^{(2)}_{\mathrm{SQM}} = \eta_1 \| \psi_1^{\parallel} \|^2 + \frac{S}{\| \psi_1^{\parallel} \|^2}. \tag{3}$$

Which of these two particular strategies is better is determined by which of these two failure probabilities is smaller. In particular, $Q^{(1)}_{\mathrm{SQM}} > Q^{(2)}_{\mathrm{SQM}}$ if $\eta_1 \| \psi_1^{\parallel} \|^2 > S$, and vice versa.

Now, the question arises: Is this the best we can do? The answer is that under certain conditions a generalized measurement based on positive-operator valued measures (POVM, [14]) can do better in an intermediate range of parameters, and can achieve a higher probability of success than a standard von Neumann measurement. The POVM can be implemented by a unitary evolution on a larger space and a selective measurement. The larger space consists of two orthogonal subspaces, the original system space and a failure space. The unitary evolution transforms the input sets into orthogonal sets in the original system space and maps them onto the same vector in the failure space. A click in the detector measuring along this vector corresponds to failure of the procedure, since all inputs are mapped onto the same output. A no-click corresponds to success since now the nonorthogonal input sets are transformed into orthogonal output sets in the system space. The one-dimensionality of the failure space follows from the requirement that the filtering is optimum. Namely, suppose that $|\psi_1\rangle$ is mapped onto some vector in the failure space and the inputs from the other set are mapped onto vectors that have components perpendicular to this vector. Then a single von Neumann measurement along the orthogonal direction could identify the input as being from the second set, i.e., further filtering would be possible, lowering the failure probability and the original filtering could not have been optimum.

In particular, let $\mathcal{H}_S$ be the D-dimensional system space spanned by the vectors $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ where, obviously, $D \leq N$. We now embed this space in a space of $D + 1$ dimensions, $\mathcal{H}_{S+A} = \mathcal{H}_S \oplus \mathcal{H}_A$, where $\mathcal{H}_A$ is a one-dimensional auxiliary Hilbert space, the failure space or ancilla. The basis in this space is denoted by $|\phi^{(A)}\rangle$. Thus, the unitary evolution on $\mathcal{H}_{S+A}$ is specified by the requirement that for any input state $|\psi_i\rangle (= |\psi_i^{(S)}\rangle)$ $(i = 1, \ldots, N)$ the final state has the structure

$$|\psi_i\rangle_{\mathrm{out}} = U|\psi_i\rangle = \sqrt{p_i}|\psi_i'^{(S)}\rangle + \sqrt{q_i}e^{i\theta_i}|\phi^{(A)}\rangle. \tag{4}$$

From unitarity the relation, $p_i + q_i = 1$ follows. Furthermore, p_i is the probability that the transformation

$|\psi_i\rangle \rightarrow |\psi_i'\rangle$ succeeds and q_i is the probability that $|\psi_i\rangle$ is mapped onto the state $|\phi^{(A)}\rangle$. In order to identify p_i and q_i with the state-specific success and failure probability for quantum filtering we have to require that

$$\langle\psi_1'|\psi_i'\rangle = 0, \tag{5}$$

for $i = 2, \ldots, N$. We now introduce the operator $F^{(3)} = |\psi_1'\rangle\langle\psi_1'| - [I^{(S+A)} - |\psi_1'\rangle\langle\psi_1'| - |\phi^{(A)}\rangle\langle\phi^{(A)}|]$, which has eigenvalues 1, 0, and -1. If we measure $F^{(3)}$ and obtain 1, then the input was $|\psi_1\rangle$, if we obtain -1, then the input was from the other the set, and if we obtain 0, the procedure failed.

In order to optimize the POVM, we have to determine those values of q_i in Eq. (4) that yield the smallest average failure probability Q. Taking the scalar product of $U|\psi_1\rangle$ and $U|\psi_i\rangle$ in Eq. (4), and using Eq. (5), gives

$$|\langle\psi_1|\psi_i\rangle|^2 = q_1 q_i, \tag{6}$$

for $i = 2, \ldots, N$, and Eq. (1) can be cast in the form $Q(q_1) = \eta_1 q_1 + S/q_1$. Unitarity of the transformation U delivers the necessary condition that q_1 must lie in the range $\| \psi_1^{\|} \|^2 \leq q_1 \leq 1$. Details of the derivation, along with a discussion of the sufficient conditions for the existence of U, will be presented in a future publication [15]. Provided that a POVM solution exists, the minimum of $Q(q_1)$ is reached for $q_1 = \sqrt{S/\eta_1}$ and is given by

$$Q_{\mathrm{POVM}} = 2\sqrt{\eta_1 S}. \tag{7}$$

Thus, the failure probability for optimal unambiguous quantum state filtering can be summarized as

$$Q = \begin{cases} 2\sqrt{\eta_1 S} & \text{if } \eta_1 \| \psi_1^{\|} \|^4 \leq S \leq \eta_1, \\ \eta_1 + S & \text{if } S > \eta_1, \\ \eta_1 \| \psi_1^{\|} \|^2 + \frac{S}{\| \psi_1^{\|} \|^2} & \text{if } S < \eta_1 \| \psi_1^{\|} \|^4 . \end{cases} \tag{8}$$

The first line represents the POVM result, Eq. (7), and it gives a smaller failure probability, in its range of validity, than the von Neumann measurements, Eqs. (2) and (3), cf. Fig. 1. Outside of the POVM range of validity we recover the von Neumann results. It should be noted that for these results to hold, unlike for unambiguous state discrimination, linear independence of all states is not required. Instead, the less stringent requirement of the linear independence of the sets is sufficient, in agreement with the findings in [16].

We can now apply this result to distinguishing between sets of Boolean functions. Let $f(x)$, where $0 \leq x \leq 2^n - 1$, be a Boolean function, i.e., $f(x)$ is either 0 or 1. One of the sets we want to consider is a set of balanced functions. In our example, the second set has only two members, and we shall call it $\mathcal{W}_k$. A function is in $\mathcal{W}_k$ if $f(x) = 0$ for $0 \leq x < [(2^k - 1)/2^k]2^n$ and $f(x) = 1$ for $[(2^k - 1)/2^k]2^n \leq x \leq 2^n - 1$, or if $f(x) = 1$ for $0 \leq x < [(2^k - 1)/2^k]2^n$ and $f(x) = 0$ for $[(2^k - 1)/2^k]2^n \leq x \leq 2^n - 1$. We now wish to distinguish between the given balanced functions and functions in $\mathcal{W}_k$, that is, we are given an unknown function that is in one of the two sets, and we want to find out which set it is in. We note that the two functions in $\mathcal{W}_k$ are biased functions, so that this is a special case of a more general problem of distinguishing a set of biased functions from balanced functions.

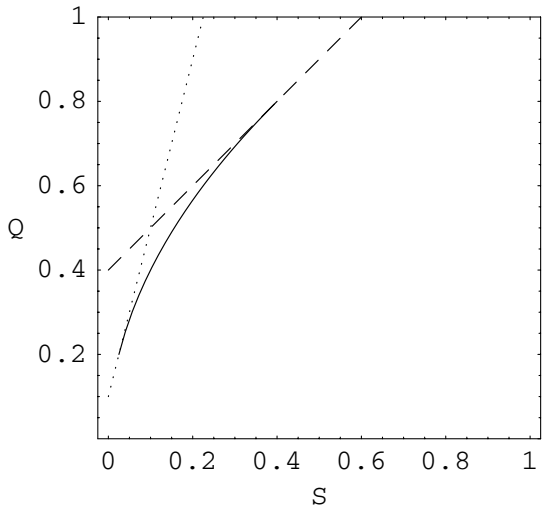

FIG. 1. Failure probability, Q, vs the average overlap, S. Dashed line: $Q_{\mathrm{SQM}}^{(1)}$, dotted line: $Q_{\mathrm{SQM}}^{(2)}$, solid line: Q_{POVM}. For the figure we used the following representative values: $\eta_1 = 0.4$ and $\| \psi_1^{\|} \|^2 = 0.25$. For these the optimal Q is given by $Q_{\mathrm{SQM}}^{(2)}$ for $0 < S < 0.025$, by Q_{POVM} for $0.025 \leq S \leq 0.4$, and by $Q_{\mathrm{SQM}}^{(1)}$ for $0.4 < S$.

This is by no means the only example the method can handle, but it is a particularly simple one and represents a generalization of the Deutsch-Jozsa problem [2]. In that case one is given an unknown function that is either balanced or constant, and one wants to determine which. Classically, in the worst case one would have to evaluate the function $D/2 + 1$ times, where we have set $D = 2^n$, but in the quantum case only one evaluation is necessary. The solution makes use of the unitary mapping

$$|x\rangle|y\rangle \rightarrow |x\rangle|y + f(x)\rangle, \tag{9}$$

where the first state, $|x\rangle$, is an n-qubit state, the second state, $|y\rangle$, is a single-qubit state, and the addition is modulo 2. The state $|x\rangle$, where x is an n-digit binary number, is a member of the computational basis for n qubits, and the state $|y\rangle$, where y is either 0 or 1, is a member of the computational basis for a single qubit. In solving the Deutsch-Jozsa problem, this mapping is employed in the following way:

$$\sum_{x=0}^{D-1} |x\rangle(|0\rangle - |1\rangle) \rightarrow \sum_{x=0}^{D-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle). \tag{10}$$

This has the effect of mapping Boolean functions to vectors in the D-dimensional Hilbert space, $\mathcal{H}_D$, and

we shall do the same. The final qubit is not entangled with the remaining n qubits and can be discarded. The vectors $\sum_{x=0}^{D-1}(-1)^{f(x)}|x\rangle$ that are produced by balanced functions are orthogonal to those produced by constant functions. This is why the Deutsch-Jozsa problem is easy to solve quantum mechanically. In our case, the vectors produced by functions in $\mathcal{W}_k$ are not orthogonal to those produced by balanced functions. However, unambiguous quantum state filtering provides an optimum probabilistic quantum algorithm for the solution of this problem.

In order to apply the filtering solution, we note that both functions in $\mathcal{W}_k$ are mapped, up to an overall sign, to the same vector in $\mathcal{H}_D$, which we shall call $|w_k\rangle$. The vectors that correspond to balanced functions are contained in the subspace, $\mathcal{H}_b$, of $\mathcal{H}_D$, where $\mathcal{H}_b = \{|v\rangle \in \mathcal{H}_D | \sum_{x=0}^{D-1} v_x = 0\}$, and $v_x = \langle x|v\rangle$. This subspace has dimension $2^n - 1 = D - 1$, and it is possible to choose an orthonormal basis, $\{|v_i\rangle | i = 2, \ldots, D\}$, for it in which each basis element corresponds to a particular balanced Boolean function [15].

Let us first see how the filtering procedure performs when applied to the problem of distinguishing $|w_k\rangle (= |\psi_1\rangle)$ from the set of the $D - 1$ orthonormal basis states, $|v_i\rangle (= |\psi_i\rangle)$, in $\mathcal{H}_b$. We assume their *a priori* probabilities to be equal, i.e., $\eta_i = \eta = (1 - \eta_1)/(D - 1)$ for $i = 2, \ldots, D$, where η_1 is the *a priori* probability for $|w_k\rangle$. For $\| \psi_1^{\|} \|^2 = \| w_k^{\|} \|^2 \equiv f_k$ we obtain $f_k = (2^k - 1)/2^{2k-2}$. Then the average overlap, S_k, between $|w_k\rangle$ and the set of balanced basis vectors can be written as

$$S_k = \frac{1 - \eta_1}{D - 1} f_k, \tag{11}$$

in terms of f_k [15]. The failure probabilities are given by Eq. (8), using $S = S_k$ and, to good approximation, the POVM result holds when $1/2^{k-2} \leq D\eta_1 \leq 2^{k-2}$. For example, in the case in which all of the *a priori* probabilities are equal, i.e., $\eta_1 = 1/D$, we find that $Q_{\mathrm{SQM}}^{(1)} = Q_{\mathrm{SQM}}^{(2)} = Q_{\mathrm{SQM}} = (1 + f_k)/D$. From Fig. 1 the difference between the POVM and the von Neumann measurement is at its largest. To good approximation, $Q_{\mathrm{POVM}}/Q_{\mathrm{SQM}} = 4/2^{k/2}$, which, for $k \gg 1$, shows that the POVM can perform significantly better than the von Neumann measurements.

Now that we know how this procedure performs on the basis vectors in $\mathcal{H}_b$, we shall examine its performance on any balanced function, i.e., we apply it to the problem of distingushing $|w_k\rangle$ from the set of all states in $\mathcal{H}_b$ that correspond to balanced functions. The number of such states is $N = D!/(D/2)!^2$ and we again assume their *a priori* probabilities to be equal, $\eta = (1 - \eta_1)/N$. It can be shown [15] that the average overlap between $|w_k\rangle$ and the set $\{|v\rangle\}$ is given by the same expression, Eq. (11), as in the previous case. Therefore, much of what was said in the previous paragraph remains valid for this case, as well, with one notable difference. The case $\eta_1 = 1/D$ now does not correspond to equal *a priori* probability for the states but, rather, to *a priori* weight of the sets that is proportional to their dimensionality. In this case it is the POVM that performs best. In the case of equal *a priori* probability for all states, $\eta_1 = 1/(N + 1)$, we are outside of the POVM range of validity and it is the first standard quantum measurement (SQM1) that performs best. Both the POVM and the SQM1 are good methods for distinguishing functions in $\mathcal{W}_k$ from balanced functions. Which one is better would depend on the *a priori* probabilities of the functions.

Classically, in the worst case, one would have to evaluate a function $2^n[(1/2) + (1/2^k)] + 1$ times to determine if it is in $\mathcal{W}_k$ or if it is an even function. Using quantum information processing methods, one has a very good chance of determining this with only one function evaluation. This shows that Deutsch-Jozsa-type algorithms need not be limited to constant functions; certain kinds of biased functions can be discriminated as well.

Unambiguous state discrimination is a procedure that is of fundamental interest in quantum information theory. Its only application so far has been to quantum cryptography. The results presented here suggest that related methods can also serve as a tool in the development of quantum algorithms.

This research was supported by the Office of Naval Research (Grant No. N00014-92-J-1233), the National Science Foundation (Grant No. PHY-0139692), the Hungarian Science Research Fund (Grant No. T 03061), a PSC-CUNY grant, and a CUNY collaborative grant.

[1] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[2] D. Deutsch and R. Jozsa, Proc. R. Soc. London A **439**, 553 (1992).
[3] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A **66**, 032315 (2002).
[4] U. Herzog and J. A. Bergou, Phys. Rev. A **65**, 050305(R) (2002).
[5] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[6] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[7] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[8] A. Peres, Phys. Lett. A **128**, 19 (1988).
[9] A. Peres and D. Terno, J. Phys. A **31**, 7105 (1998).
[10] A. Chefles, Phys. Lett. A **239**, 339 (1998).
[11] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
[12] L-M. Duan and G-C. Guo, Phys. Lett. A **261**, 25 (1999).
[13] Y. Sun, M. Hillery, and J. A. Bergou, Phys. Rev. A **64**, 022311 (2001).
[14] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).
[15] J. A. Bergou, U. Herzog, and M. Hillery (to be published).
[16] Sh. Zhang and M. Ying, Phys. Rev. A **65**, 062322 (2002).