PHYSICAL REVIEW A, VOLUME 64, 030303(R)

Minimum-error discrimination between multiply symmetric states

Stephen M. Barnett
Department of Physics and Applied Physics, University of Strathclyde, Glasgow G4 ONG, Scotland
(Received 17 May 2001; published 13 August 2001)

An optimum measurement strategy is presented for a new class of quantum states. This provides discrimination among the states with the minimum probability of error.

DOI: 10.1103/PhysRevA.64.030303 PACS number(s): 03.67.Hk

The communication of classical information by means of a quantum channel is a well-developed field of study [1–3]. The transmitting party (Alice) encodes her message as a string of quantum systems, each prepared in one of a set of agreed signal states $|\psi_j\rangle$. This set of states is known to the receiving party (Bob), who also knows the *a priori* probability p_j that Alice selected the state $|\psi_j\rangle$. Bob's problem is to find the best measurement strategy. The simplest requirement is to choose the strategy that minimizes the probability for error [1–5] although other criteria have also been studied [6–12].

The strategy realizing the minimum error probability will, in most cases, be a generalized measurement described in terms of the elements of a probability operator measure (POM) [1], also refered to as a positive operator-valued measure [13]. Each of the possible outcomes "k" of Bob's measurement is characterized by a corresponding POM element $\hat{\pi}_k$ [14]. The probability that Bob will observe the result k *given* that Alice selected the state $|\psi_j\rangle$ is

$$P(k|j)=\langle\psi_j|\hat{\pi}_k|\psi_j\rangle. \tag{1}$$

We label Bob's measurement results by the inference that he draws from them; he will associate the result k with the conclusion that Alice prepared the state $|\psi_k\rangle$. It follows that the probability for Bob to make an error in assigning the state is

$$P_{\mathrm{e}}=1-\sum_{j=1}^{M}\langle\psi_j|\hat{\pi}_j|\psi_j\rangle p_j, \tag{2}$$

where M is the number of possible signal states.

Necessary and sufficient conditions are known for minimizing P_{e} [1–5], although very few examples of the required POM elements have been given [15]. The measurement that leads to the minimum error probability will have POM elements $\hat{\pi}_k$ that satisfy the two conditions [1–5]

$$\hat{\pi}_j(p_j|\psi_j\rangle\langle\psi_j|-p_k|\psi_k\rangle\langle\psi_k|)\hat{\pi}_k=0, \tag{3}$$

$$\sum_{j=1}^{M}p_j|\psi_j\rangle\langle\psi_j|\hat{\pi}_j-p_k|\psi_k\rangle\langle\psi_k|\geqslant 0. \tag{4}$$

The first of these conditions is required to hold for all j and k. The second is a statement that the eigenvalues of the operator on the left-hand side must be greater than or equal to zero and it is required to hold for all k. The explicit form of the required POM elements has been found for some special cases. These include the cases of only two possible signal states [1] and of equiprobable states that are complete in the sense that a weighted sum of projectors onto the states equals the identity operator [4]. The required POM elements have also been given for the symmetric states [1,5]. These states can be written in the form

$$|\psi_j\rangle=\hat{V}^{j-1}|\psi\rangle \tag{5}$$

and are required to be *a priori* equally likely so that $p_j=1/M$. The operator $\hat{V}$ is unitary and satisfies the condition

$$\hat{V}^M=\hat{I}. \tag{6}$$

Note that we can also accommodate situations in which $\hat{V}^M=\hat{I}\,\mathrm{e}^{i\alpha}$, for some phase α, by replacing $\hat{V}$ with $\hat{V}'=\hat{V}\,\mathrm{e}^{i\alpha/M}$. This results only in changing the states (5) by an unobservable phase.

Recently, Eldar and Forney have generalized the symmetric states to produce the geometrically uniform states and have derived the detection strategy giving minimum error probability for these states [17]. In this paper, we will extend the idea of symmetric states in a different way by introducing the multiply symmetric states. The simplest example is the doubly symmetric states that have the form

$$|\psi_{j,k}\rangle=\hat{U}^{k-1}\hat{V}^{j-1}|\psi\rangle, \tag{7}$$

where $j=1,\ldots,M$ and $k=1,\ldots,N$, and $\hat{U}^N=\hat{I}=\hat{V}^M$. We will say that these states are doubly symmetric if they occur with equal *a priori* probabilities $p_{j,k}=(MN)^{-1}$ *and* if the two unitary operators $\hat{U}$ and $\hat{V}$ both commute with the operator

$$\hat{\Phi}=\sum_{j=1}^{M}\sum_{k=1}^{N}|\psi_{j,k}\rangle\langle\psi_{j,k}|=MN\hat{\rho}, \tag{8}$$

where $\hat{\rho}$ is the *a priori* density operator. It is clear from the form of the states that $\hat{U}$ will commute with $\hat{\Phi}$, but the requirement that $\hat{V}$ also commutes with $\hat{\Phi}$ is an additional condition. Note that there is *no* requirement that $\hat{U}$ and $\hat{V}$ should commute [18]. Given these conditions, the minimum error probability will be realized by a POM with the elements

$$\hat{\pi}_{j,k}=\hat{\Phi}^{-1/2}|\psi_{j,k}\rangle\langle\psi_{j,k}|\hat{\Phi}^{-1/2}. \tag{9}$$

These POM elements are an example of the so-called square-root measurement [19–21]. The associated minimum error probability is then

$$P_{\mathrm{e}}=1-\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\langle\psi_{j,k}|\hat{\pi}_{j,k}|\psi_{j,k}\rangle=1-|\langle\psi|\hat{\Phi}^{-1/2}|\psi\rangle|^{2}. \tag{10}$$

Our proof that the POM elements (9) give the minimum possible error probability follows closely one given for the symmetric states by Ban *et al.* [5] and consists of showing that the POM elements satisfy the conditions (3) and (4). Inserting our POM elements into (3) gives

$$\frac{1}{MN}\hat{\pi}_{j,k}(|\psi_{j,k}\rangle\langle\psi_{j,k}|-|\psi_{j',k'}\rangle\langle\psi_{j',k'}|)\hat{\pi}_{j',k'}$$
$$=\frac{1}{MN}\hat{\Phi}^{-1/2}|\psi_{j,k}\rangle F_{j,k;j',k'}\langle\psi_{j',k'}|\hat{\Phi}^{-1/2}, \tag{11}$$

where $F_{j,k;j',k'}$ is the c number

$$F_{j,k;j',k'}=\langle\psi|\hat{V}^{1-j}\hat{\Phi}^{-1/2}\hat{U}^{k'-k}\hat{V}^{j'-1}|\psi\rangle$$
$$\times(\langle\psi|\hat{V}^{1-j}\hat{\Phi}^{-1/2}\hat{V}^{j-1}|\psi\rangle$$
$$-\langle\psi|\hat{V}^{1-j'}\hat{\Phi}^{-1/2}\hat{V}^{j'-1}|\psi\rangle). \tag{12}$$

In obtaining Eq. (12) we have made use of the fact that $\hat{U}$ commutes with $\hat{\Phi}$. If we also enforce the condition $[\hat{V},\hat{\Phi}]=0$, then the term in parenthesis vanishes to give $F_{j,k;j',k'}=0$. It follows, therefore, that the first of our conditions (3) is satisfied.

The fact that Eq. (3) is satisfied means that the operator

$$\hat{\Gamma}=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}|\psi_{j,k}\rangle\langle\psi_{j,k}|\hat{\pi}_{j,k} \tag{13}$$

is Hermitian and therefore has real eigenvalues. This implies that it is meaningful to test the condition (4). We write the left-hand side of this inequality in the form

$$\hat{\Gamma}-\frac{1}{MN}|\psi_{j',k'}\rangle\langle\psi_{j',k'}|=\frac{1}{MN}\hat{U}^{k'-1}\hat{V}^{j'-1}\hat{G}\hat{V}^{1-j'}\hat{U}^{1-k'}, \tag{14}$$

where $\hat{G}$ is the Hermitian operator

$$\hat{G}=\langle\psi|\hat{\Phi}^{-1/2}|\psi\rangle\hat{\Phi}^{1/2}-|\psi\rangle\langle\psi|. \tag{15}$$

The operator (14) is unitarily equivalent to $\hat{G}$ and therefore has the same eigenvalues. It is sufficient, therefore, to show that $\hat{G}$ is a positive semidefinite operator and this will be true if $\langle u|\hat{G}|u\rangle\geqslant 0$ for all states $|u\rangle$. From the definition of $\hat{G}$ we have

$$\langle u|\hat{G}|u\rangle=\langle\psi|\hat{\Phi}^{-1/2}|\psi\rangle\langle u|\hat{\Phi}^{1/2}|u\rangle-|\langle u|\psi\rangle|^{2}$$
$$\geqslant|\langle\psi|\hat{\Phi}^{-1/4}\hat{\Phi}^{1/4}|u\rangle|^{2}-|\langle u|\psi\rangle|^{2}=0, \tag{16}$$

where we have used the Cauchy-Schwarz inequality. It follows that our POM satisfies the necessary and sufficient conditions (3) and (4) and therefore gives the minimum probabilty for error in assigning the state selected by Alice.

As an example, consider the multiply symmetric states generated from an entangled two-qubit state of the form

$$|\psi\rangle=a|+_{1},-_{2}\rangle+b|-_{1},+_{2}\rangle, \tag{17}$$

where a and b are complex coefficients, by the action of two unitary operators

$$\hat{U}=\cos\theta(|+_{1}\rangle\langle-_{1}|+|-_{1}\rangle\langle+_{1}|)$$
$$+\sin\theta(|+_{1}\rangle\langle+_{1}|-|-_{1}\rangle\langle-_{1}|), \tag{18}$$

$$\hat{V}=\cos\theta(|+_{1}\rangle\langle+_{1}|-|-_{1}\rangle\langle-_{1}|)$$
$$-\sin\theta(|+_{1}\rangle\langle-_{1}|+|-_{1}\rangle\langle+_{1}|). \tag{19}$$

The set of four multiply symmetric states produced in this way is

$$|\psi_{1,1}\rangle=a|+_{1},-_{2}\rangle+b|-_{1},+_{2}\rangle, \tag{20}$$

$$|\psi_{1,2}\rangle=a[\cos\theta|-_{1}\rangle+\sin\theta|+_{1}\rangle]|-_{2}\rangle+b[\cos\theta|+_{1}\rangle$$
$$-\sin\theta|-_{1}\rangle]|+_{2}\rangle, \tag{21}$$

$$|\psi_{2,1}\rangle=a[-\sin\theta|-_{1}\rangle+\cos\theta|+_{1}\rangle]|-_{2}\rangle-b[\sin\theta|+_{1}\rangle$$
$$+\cos\theta|-_{1}\rangle]|+_{2}\rangle, \tag{22}$$

$$|\psi_{2,2}\rangle=a|-_{1},-_{2}\rangle-b|+_{1},+_{2}\rangle. \tag{23}$$

The operator $\hat{\Phi}$ for these states is

$$\hat{\Phi}=2\hat{I}_{1}\otimes(|a|^{2}|-_{2}\rangle\langle-_{2}|+|b|^{2}|+_{2}\rangle\langle+_{2}|), \tag{24}$$

which clearly commutes with both $\hat{U}$ and $\hat{V}$. The corresponding minimum error probability is found by use of Eq. (10) to be

$$P_{\mathrm{e}}=\frac{1}{2}-|ab|. \tag{25}$$

This error probability is zero if $|a|=|b|$ corresponding to four mutually orthogonal states. It takes its maximum value of 1/2 if either $|a|$ or $|b|$ is zero, in which case the problem becomes one of discriminating between four multiply symmetric states of qubit 1.

It is straightforward to demonstrate that our example does not correspond to any of the previously mentioned cases for which the required POM has been constructed [1,4,5,17]. The reduced density operator for qubit 2 has the same form for each of the four states, and hence, it is not possible to construct the identity operator $\hat{I}_{1}\otimes\hat{I}_{2}$ from projectors onto the four states. The simplest way to see that the states are not simply a symmetric set is to consider the case in which $b=0$. For a symmetric set of states it is necessary to find a single unitary operator $\hat{V}$, the action of which generates all the states in the form (5). This is clearly not possible unless $\theta = n\pi/4$. Futhermore, the operators $\hat{U}$ and $\hat{V}$ do not commute and so our states are not a geometrically uniform set.

It is straightforward to show that the square-root measurement also provides the minimum error probability for multiply symmetric states. These are equiprobable states generated by the action of multiple unitary operators, $|\psi_{j_1 \cdots j_n}\rangle = \hat{V}_n^{j_n - 1} \cdots \hat{V}_1^{j_1 - 1}|\psi\rangle$, where the *a priori* density operator commutes with all of the unitary operators $\hat{V}_l$. The proof is a natural generalization of that presented above for doubly symmetric states.

The multiply symmetric states form a new class of states for which state discrimination with minimum error probability can be demonstrated. Recent experimental progress [16] means that it is possible to implement such optimal strategies in the laboratory. The states also provide a tool with which to test ideas in quantum communication and measurement including studies of quantum channel capacities and quantum key distribution.

I am grateful to C. R. Gilson, M. Sasaki, and O. Hirota for helpful and encouraging comments and to E. Andersson and A. Chefles for their careful reading of the manuscript. This work was supported by the Royal Society of Edinburgh, the Scottish Executive Education and Lifelong Learning Department, and by the British Council.

[1] C.W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[2] A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[3] O. Hirota, *Optical Communication Theory* (Morikita, Tokyo, 1985) (in Japanese).
[4] H.P. Yuen, R.S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory **IT-21**, 125 (1975).
[5] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[6] E.B. Davies, IEEE Trans. Info. Theory **IT-24**, 596 (1978).
[7] C.A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[8] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
[9] M. Ban, Y. Kamazaki, and O. Hirota, Phys. Rev. A **55**, 22 (1997).
[10] M. Osaki, M. Ban, and O. Hirota, J. Mod. Opt. **45**, 269 (1998).
[11] M. Sasaki, S.M. Barnett, R. Jozsa, M. Osaki, and O. Hirota, Phys. Rev. A **59**, 3325 (1999).
[12] S.M. Barnett, C.R. Gilson, and M. Sasaki, J. Phys. A: Math. Gen. (to be published).
[13] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, 1993).
[14] These operators are required to be Hermitian, non-negative definite and resolve the identity operator in the form $\Sigma_k \hat{\pi}_k = \hat{I}$.
[15] Some of these have recently been realized in experiments with optical polarization [16].
[16] B. Huttner, A. Muller, J.D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996); S.M. Barnett and E. Riis, J. Mod. Opt. **45**, 1295 (1997); R.B.M. Clarke, V.M. Kendon, A. Chefles, S.M. Barnett, E. Riis, and M. Sasaki, Phys. Rev. A **64**, 012303 (2001); J. Mizuno, M. Fujiwara, M. Akiba, T. Kawanishi, S. M. Barnett, and M. Sasaki, e-print quant-ph/0106164.
[17] Y.C. Eldar and G.D. Forney, Jr., IEEE Trans. Inf. Theory **IT-47**, 858 (2001); the geometrically uniform states are equiprobable states $|\phi_i\rangle = \hat{U}_i|\phi\rangle$, where the unitary operators $\hat{U}_i$ form a finite Abelian (commutative) group and $|\phi\rangle$ is any state.
[18] Our states become an example of the geometrically uniform states [17] *only* if $\hat{U}$ and $\hat{V}$ commute.
[19] A.S. Holevo, Theor. Probab. Appl. **23**, 411 (1978).
[20] P. Hausladen and W.K. Wootters, J. Mod. Opt. **41**, 2385 (1994).
[21] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, Phys. Rev. A **54**, 1869 (1996).