Optimal distinction between non-orthogonal quantum states

1998 J. Phys. A: Math. Gen. 31 7105

(http://iopscience.iop.org/0305-4470/31/34/013)

J. Phys. A: Math. Gen. **31** (1998) 7105–7111. Printed in the UK PII: S0305-4470(98)93511-9

Optimal distinction between non-orthogonal quantum states

Asher Peres† and Daniel R Terno‡

Department of Physics, Technion, Israel Institute of Technology, 32 000 Haifa, Israel

Received 20 April 1998

Abstract. Given a finite set of linearly independent quantum states, an observer who examines a single quantum system may sometimes identify its state with certainty. However, unless these quantum states are orthogonal, there is a finite probability of failure. A complete solution is given to the problem of optimal distinction of three states, having arbitrary prior probabilities and arbitrary detection values. A generalization to more than three states is outlined.

1. Non-orthogonal quantum signals

Quantum information theory is an emerging science, which combines two traditional disciplines: quantum mechanics and classical information theory. This subject has many fascinating potential applications for the transmission and processing of information, and yields results that cannot be achieved by classical means. A simple example is the use of quanta that have been prepared according to one of a finite set of states as signals for the transmission of information. The possibility of using non-orthogonal quantum states, which has no classical analogue, is especially interesting for its potential applications to cryptography (that is, for communication security) [1].

An observer, faced with such a set of signals whose prior probabilities are known, may follow various strategies. The approach favoured by information theorists is to maximize the mutual information that can be acquired in the detection process [2]: each event is analysed in a way from which it is possible to deduce definite posterior probabilities for the emission of the various signals, and the observer's aim is to reduce as much as possible the Shannon entropy of the ensemble of signals. On the other hand, communication engineers attempt to guess what the signal actually was and their aim is to miminize the number of errors [3]. Cryptographers, whose supply of signals is essentially unlimited but for whom security is paramount, do not want any error at all but on the other hand they are ready to lose some fraction of the signals. The latter strategy is the one that will be investigated in this article.

The case of just two non-orthogonal signals is quite simple and well known [4–6]. Recently, Chefles [7] investigated the case of N linearly independent signals, and obtained some partial results. In the following, we give a complete treatment of the case of three signals. Our method can readily be generalized to a larger number of signals (but explicit calculations become tedious).

† E-mail address: peres@photon.technion.ac.il
‡ E-mail address: terno@physics.technion.ac.il

0305-4470/98/347105+07$19.50

In the next section, we introduce a set of positive operator valued measures which describe generalized quantum measurements. (These are more general than the projection valued measures corresponding to the standard, von Neumann type of measurement.) An explicit algorithm is developed to ensure the positivity of the required matrices.

Optimization (namely, how to maximize the information gain) is discussed in section 3. We consider the possibility that the various signals may have different 'values'. The information gain is defined as the expected average of the values of detected signals (this includes the possibility that some types of signals are never identified). It is then shown in section 4 that even if a measurement fails to identify with certainty a signal, it is still usually possible to attribute to the various signals posterior probabilities, so that the observer acquires at least some mutual information on the emitted signals. Finally, section 5 briefly discusses an extension of this work to spaces with more than three dimensions.

2. Positive operator valued measures

Consider, in a three-dimensional complex vector space, three linearly independent normalized state vectors, $\boldsymbol{u}_1$, $\boldsymbol{u}_2$, and $\boldsymbol{u}_3$ (we are using here the standard notation for Euclidean vectors, so no confusion may arise). These vectors have the physical meaning of signals, and they are, in general, not orthogonal. They occur with probabilities p_1, p_2, and p_3, respectively. In each measurement the observer should either identify with certainty one of these signals or obtain an inconclusive answer (the latter will be labelled 0, meaning 'no answer'). The objective is to design a procedure that minimizes the probability of the inconclusive answer. More generally, we may attribute different values C_j to the various outcomes (for example, rare signals with small p_j may have larger values than frequent signals) and our aim is to maximize the expected gain of information.

Note that the number of outcomes of the measuring process is larger than the dimensionality of the vector space. Therefore we need 'generalized measurements' that are represented by positive operator valued measures (POVM) [8]. Namely, we have to construct four positive semi-definite matrices $\boldsymbol{A}_j$, that satisfy

$$\sum_{j=0}^{3} \boldsymbol{A}_j = \mathbf{1} \tag{1}$$

where $\mathbf{1}$ is the unit matrix. Three of these matrices correspond to the three input signals, and the remaining one to an inconclusive answer. It is easily proved [2] that optimal $\boldsymbol{A}_j$ may be taken as matrices of rank 1. However, the optimal solution may not be unique, and higher rank matrices may also be optimal, as we shall see below.

By analogy with the well known solution for the case of two input vectors [4–6], let us define three auxiliary (unnormalized) vectors $\boldsymbol{v}_j$ as follows

$$\boldsymbol{v}_1 = (\boldsymbol{u}_2 \times \boldsymbol{u}_3)^* \tag{2}$$

and cyclic permutations. We thus have

$$\langle \boldsymbol{v}_i, \boldsymbol{u}_j \rangle = \delta_{ij}[\boldsymbol{u}_1 \boldsymbol{u}_2 \boldsymbol{u}_3] \tag{3}$$

where $[\boldsymbol{u}_1 \boldsymbol{u}_2 \boldsymbol{u}_3]$ stands for the triple product of the input vectors (that is, the determinant of their components, in any basis).

We then construct with the $\boldsymbol{v}_j$ three POVM matrices, which correspond to outcomes of experiments that give a definite identification of an input signal:

$$\boldsymbol{A}_j = k_j |\boldsymbol{v}_j\rangle\langle \boldsymbol{v}_j| \tag{4}$$

where the k_j are non-negative numbers that still have to be determined. Indeed, the probability that the jth outcome results from the ith input is

$$P_j = \langle \boldsymbol{u}_i, \boldsymbol{A}_j \boldsymbol{u}_i \rangle = k_j |\langle \boldsymbol{u}_i, \boldsymbol{v}_j \rangle|^2. \tag{5}$$

This vanishes if $j \neq i$. Therefore, observing the jth outcome implies that the input was $\boldsymbol{u}_j$. This result occurs with probability

$$P_j = k_j |[\boldsymbol{u}_1 \boldsymbol{u}_2 \boldsymbol{u}_3]|^2. \tag{6}$$

Note that the input states $\boldsymbol{u}_j$ must be linearly independent in order to unambiguously distinguish any one of them. It will be convenient for future use to introduce the notation

$$T = |[\boldsymbol{u}_1 \boldsymbol{u}_2 \boldsymbol{u}_3]|^2. \tag{7}$$

This can also be written as $T = [\boldsymbol{v}_1 \boldsymbol{v}_2 \boldsymbol{v}_3]$, or

$$T = 1 + s_{12}s_{23}s_{31} + s_{13}s_{32}s_{21} - |s_{12}|^2 - |s_{23}|^2 - |s_{31}|^2 \tag{8}$$

where $s_{ij} = \langle \boldsymbol{u}_i, \boldsymbol{u}_j \rangle$.

Finally, the remaining POVM matrix, which indicates an inconclusive answer, is given by

$$\boldsymbol{A}_0 = \mathbf{1} - \sum_{j=1}^{3} \boldsymbol{A}_j. \tag{9}$$

The probability of the inconclusive answer is

$$P_0 = \sum_{j=1}^{3} p_j \langle \boldsymbol{u}_j, \boldsymbol{A}_0 \boldsymbol{u}_j \rangle = 1 - T \sum_{j=1}^{3} k_j p_j. \tag{10}$$

We naturally want the k_j to be as large as possible in order to increase the detection probabilities but their values are bounded above by the demand of positivity of $\boldsymbol{A}_0$. Recall that the necessary and sufficient conditions for the positivity of a matrix are the positivity of all the diagonal elements and diagonal subdeterminants, including the determinant of the entire matrix:

$$\det \boldsymbol{A}_0 \geqslant 0. \tag{11}$$

In the present case, this last condition is the decisive one that actually determines the domain of acceptable values of k_j. This is intuitively seen as follows: when all k_j vanish, $A_0 \equiv \mathbf{1}$, which has only positive eigenvalues. As we gradually increase the k_j, one of the eigenvalues of $\boldsymbol{A}_0$ will vanish and then become negative. When it vanishes, the determinant vanishes too (because it is equal to the product of eigenvalues) and this gives the boundary of the domain of legal k_j. The surface $\det(\boldsymbol{A}_0) = 0$ consists of several disjoint parts. The role of other positivity conditions is to eliminate (in practice, to confirm the elimination of) the irrelevant parts of that surface.

Explicitly, the condition $\det(\boldsymbol{A}_0) = 0$ can be written as

$$1 - \sum_{j=1}^{3} |\boldsymbol{v}_j|^2 k_j + T(k_1k_2 + k_2k_3 + k_3k_1) - T^2 k_1k_2k_3 = 0. \tag{12}$$

A simple way of obtaining equation (12) is to choose a basis in our vector space, such that the vector components are as simple as possible. Let the first basis vector be $\boldsymbol{u}_1$ itself, and the second one be a linear combination of $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$, with real coefficients. This

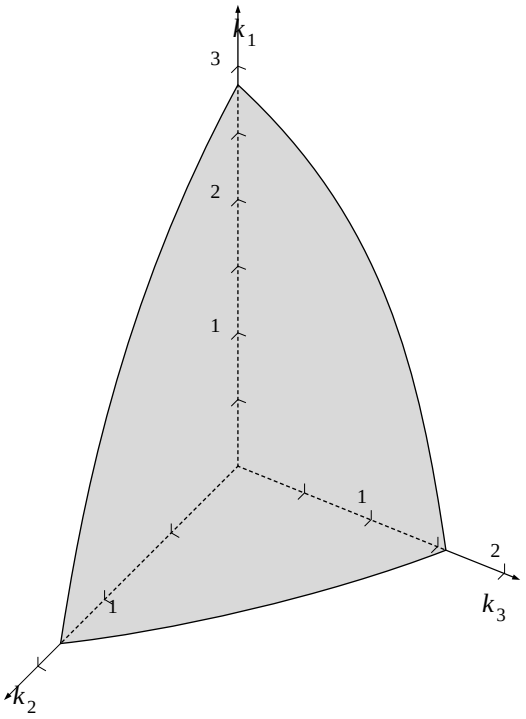

Figure 1. Domain of positivity of $\boldsymbol{A}_0$.

determines the third basis vector up to a phase. We can choose phases so that $\boldsymbol{u}_3$ has at most one complex coefficient. We thus obtain

$$\boldsymbol{u}_1 = (1, 0, 0) \qquad \boldsymbol{u}_2 = (a_2, b_2, 0) \qquad \boldsymbol{u}_3 = (a_3, b_3 \mathrm{e}^{\mathrm{i}\beta}, c_3). \tag{13}$$

Recall that all these vectors are normalized. It is now easy to write $\det(\boldsymbol{A}_0)$ explicitly in terms of the parameters in equation (13), and then to express these parameters in terms of the various vectors. The resulting surface, $\det(\boldsymbol{A}_0) = 0$, is sketched in figure 1, for the following choice of parameters:

$$\boldsymbol{u}_1 = (1, 0, 0) \qquad \boldsymbol{u}_2 = (0.6, 0.8, 0) \qquad \boldsymbol{u}_3 = (0.5, 0.5 + 0.5\mathrm{i}, 0.5). \tag{14}$$

The surface given by equation (12) intersects each k_j axis at $k_j = |\boldsymbol{v}_j|^{-2}$. Note that, in the first octant, this surface is everywhere convex. This can be seen as follows. Let us cut it by one of the planes $k_j =$ constant. The intersection is a rectangular hyperbola with asymptotes parallel to the remaining axes. For example, if we cut the surface (12) by the plane $k_3 =$ constant, the asymptote $k_1 \to \infty$ is explicitly obtained by dividing equation (12) by k_1 and then setting $k_1 \to \infty$. This gives

$$-|\boldsymbol{v}_1|^2 + T\,(k_2 + k_3) - T^2 k_2 k_3 = 0. \tag{15}$$

It is then easily seen that for any fixed k_3 such that $0 < k_3 < |\boldsymbol{v}_3|^{-2}$, the resulting k_2 is positive. This means that, in the plane $k_3 =$ constant, the asymptote $k_1 \to \infty$ cuts the positive part of the k_2 axis. The same result holds for any other choice of section parallel to one of the coordinate planes. This proves the convexity of the surface in figure 1: all these sections are convex segments of rectangular hyperbolas.

3. Optimization

Finally, we are left with the problem of finding the set of k_j that maximize the information gain. The latter is

$$G = \sum_j C_j P_j = T \sum_j C_j p_j k_j \tag{16}$$

where C_j is the 'value' of signal $\boldsymbol{u}_j$ and use was made of equation (5). Define, for brevity,

$$B_j = C_j p_j. \tag{17}$$

All points of the plane

$$\sum_{j=1}^{3} B_j k_j = G/T \tag{18}$$

with $k_j \geqslant 0$, lead to the same information gain G, provided that these points belong to the domain of positivity of $\boldsymbol{A}_0$. The largest value of G can be obtained as follows.

Let us imagine that we start with a plane $\sum B_j k_j = X$, with large positive X, so that there is no contact between that plane and the relevant part of the surface (12). As we gradually decrease X, the plane will reach a point where it is tangent to that surface (thanks to its convexity). This happens at the point where the gradient of the left-hand side of (12) is parallel to the vector $\{B_j\}$. If the point of contact lies in the first octant, it gives the optimal solution. It may happen, however, that at this point of contact one of the k_j is negative, and therefore that point is not a valid solution. In that case, we further decrease X, until a contact point occurs on one of the coordinate planes (that is, one of the k_j vanishes), or even at one of the vertices (two of them vanish).

For example, when all $p_j = \frac{1}{3}$, and all $C_j = 1$, the optimal result is obtained when $k_1 = 2.4189$, $k_2 = 0$, and $k_3 = 0.6719$. This result means that we sacrifice the possibility of detecting signal $\boldsymbol{u}_2$ in order to get the lowest probability for the inconclusive answer, as may be seen from equation (10). In the present case, we obtain $P_0 = 0.8386$. On the other hand, if we give different values to the signals, such as $C_1 = 0.8$, $C_2 = 1.2$, and $C_3 = 1$, the optimal result is obtained with $k_1 = 2.083$, $k_2 = 0.2902$, and $k_3 = 0.2129$. The probability of obtaining an inconclusive answer then is slightly higher: $P_0 = 0.8626$.

4. Inconclusive answers still carry some information

An inconclusive answer is not completely useless (except in special, highly symmetric cases). For example, if $\boldsymbol{u}_1$ is orthogonal to $\boldsymbol{u}_2$ and $\boldsymbol{u}_3$, and these are not orthogonal to each other, then $\boldsymbol{v}_1$ is parallel to $\boldsymbol{u}_1$, and $\boldsymbol{v}_2$ and $\boldsymbol{v}_3$ lie in the $\boldsymbol{u}_2\boldsymbol{u}_3$ plane. The $\boldsymbol{A}_0$ matrix is of rank 1: $\boldsymbol{A}_0 = |\boldsymbol{w}\rangle\langle\boldsymbol{w}|$, with $\boldsymbol{w}$ in the $\boldsymbol{u}_2\boldsymbol{u}_3$ plane. In such a case, the signal $\boldsymbol{u}_1$ is always detected with certainty, while an inconclusive result means: either $\boldsymbol{u}_2$ or $\boldsymbol{u}_3$ (with known posterior probabilities, as explained below).

In general, for arbitrary $\boldsymbol{u}_j$, the optimal $\boldsymbol{A}_0$ is a matrix of rank 2 which can be written in terms of its eigenvalues and eigenvectors:

$$\boldsymbol{A}_0 = \lambda_m |\boldsymbol{m}\rangle\langle\boldsymbol{m}| + \lambda_n |\boldsymbol{n}\rangle\langle\boldsymbol{n}|. \tag{19}$$

Each one of the two terms on the right-hand side is by itself a legitimate POVM element, so that there can actually be two distinct inconclusive outcomes. Let us label them m and n.

Suppose that the outcome of a generalized measurement turns out to be m. The prior probability for that result, if the input was $\boldsymbol{u}_j$, is

$$P_{mj} = p_j \lambda_m |\langle \boldsymbol{m}, \boldsymbol{u}_j \rangle|^2. \tag{20}$$

By Bayes's theorem, the posterior probability for input $\boldsymbol{u}_j$ upon observing output m is [8]

$$Q_{jm} = P_{mj} \Big/ \sum_{i=1}^{3} P_{mi}. \tag{21}$$

The observer's final ignorance level, after receiving output m, is given by the Shannon entropy,

$$H_m = -\sum_{j=1}^{3} Q_{jm} \ln Q_{jm}. \tag{22}$$

This need not be, but often is, less than the initial entropy,

$$H_{\text{init}} = -\sum_{j=1}^{3} p_j \ln p_j \tag{23}$$

so that some information has been gained, even though the result is inconclusive.

5. Higher dimensional space

Finally, let us briefly outline how the above results can be generalized to N signals ($N > 3$). Consider the Nth order matrix formed by the components of all the input vectors, in any basis. Instead of the triple product $[\boldsymbol{u}_1 \boldsymbol{u}_2 \boldsymbol{u}_3]$, we now have the determinant of that matrix. Vector products $\boldsymbol{v}_j$ such as those in equation (2) become outer products of any $N - 1$ signal states. Their components, in any basis, are the appropriate cofactors in the above determinant. The argument leading to equation (12) remains essentially the same and we now obtain a $(N-1)$-dimensional hypersurface in the N-dimensional k-space. It is plausible that this hypersurface is convex in the first orthant (i.e. hyper-octant) in k-space. A formal proof of this conjecture is a straightforward but tedious exercise in differential geometry (perhaps a more clever proof can be found). Optimization then proceeds as in section 3, by considering a family of parallel hyperplanes $\sum B_j k_j = X$.

There are now many possibilities of partial answers. For example, if the signal states $\boldsymbol{u}_j$ can be divided into two (or more) mutually orthogonal subspaces, it is possible, in a first step, to determine unambiguously the subspace to which each signal belongs. Then, a second step is to try to identify individual non-orthogonal signals within a given subspace.

An interesting problem is how to utilize the resulting mixed information with some of the signals fully identified and others only partly identified. For example, if we have two mutually orthogonal subspaces and in each one two non-orthogonal states, an individual state encodes two bits but a subspace is still worth one bit, plus some amount of mutual (probabilistic) information. Further investigation is needed to clarify this issue.

Acknowledgments

DRT was supported by a grant from the Technion Graduate School. Work by AP was supported by the Gerard Swope Fund, and the Fund for Encouragement of Research.

References

[1] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[2] Davies E B 1978 *IEEE Trans. Inf. Theory* **IT-24** 239
[3] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic) ch 4
[4] Dieks D 1988 *Phys. Lett.* **126A** 303
[5] Peres A 1988 *Phys. Lett.* **128A** 19
[6] Jaeger G and Shimony A 1995 *Phys. Lett.* A **197** 83
[7] Chefles A 1998 *Phys. Lett.* A **239** 339
[8] Peres A 1993 *Quantum Theory: Concepts and Methods* (Dordrecht: Kluwer) pp 282–5