PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A
MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Quantum information via novel measurements

S. M. Barnett

Phil. Trans. R. Soc. Lond. A 1997 **355**, 2279-2290
doi: 10.1098/rsta.1997.0126

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Quantum information via novel measurements

By Stephen M. Barnett

Department of Physics and Applied Physics, University of Strathclyde, Glasgow G4 0NG, UK

The state projection associated with the familiar (von Neumann) measurement of an observable does not describe the most general means of interrogating a quantum system. Two problems requiring a more general description are the discrimination between non-orthogonal quantum states and the simultaneous measurement of incompatible observables. We discuss both of these problems within the context of measurements of optical polarization. We illustrate the technique of field measurement by projection synthesis by describing a possible means for determining the optical phase probability distribution.

1. Introduction

The emergence of quantum cryptography as a practical discipline (Phoenix & Townsend 1995; Barnett & Phoenix 1996; Townsend *et al.* 1996) and the first steps towards implementation of quantum computation (Cirac & Zoller 1995; Monroe *et al.* 1995; Ekert & Josza 1996) have provided both the motivation and the means to re-examine fundamental problems associated with quantum measurement. It has long been appreciated that the measurement paradigm of projection into the eigenstate of the measured observable corresponding to the experimental value found does not describe the full range of possible interactions providing information about a quantum system (Helstrom 1976). In this paper, we describe three problems of measurement in quantum optics and the ways in which a more general view of measurement can, at least partially, resolve them.

Our usual picture of a quantum measurement involves an observable u associated with a property of the observed system and represented by an Hermitian operator $\hat{u}$. A measurement of this observable will give one of the eigenvalues of $\hat{u}$ and (ideally) leave the system in the corresponding eigenstate (von Neumann 1955). This is the familiar, but mysterious, collapse of the wave function. The simplest example of a measurement of this type is the measurement of the projector $|v\rangle\langle v|$, where $|v\rangle$ is a possible state of the system. The question asked by such a measurement is 'is the system in the state $|v\rangle$?', with the eigenvalues 1 and 0 corresponding to the answers 'yes' and 'no', respectively. Measurements performed on a large ensemble of identically prepared states will give the probability that the system is in the state $|v\rangle$. Following the measurement, the original state $|\Psi\rangle$ becomes $|v\rangle$ if the result was 1 and $(1-|v\rangle\langle v|)|\Psi\rangle$ (multiplied by a normalization factor) if the result was 0. Most measurements are more destructive than this in that they do not leave the system in an eigenstate of the measured observable. For example, photodetection provides the means to measure the number of photons present, but in doing so it absorbs them, leaving the field in its vacuum state. We will, however, refer to all measurements which provide a precise measurement of the value of an observable associated with the system of interest alone as von Neumann measurements.

In this paper we discuss two problems for which it is helpful or even necessary to take a more general view of what constitutes a measurement. We will find that the task of determining in which of two non-orthogonal states a system is prepared with the minimum probability of error can be achieved by means of a von Neumann measurement (Helstrom 1976). The optimum error-free measurement, however, requires a more general type of measurement (Ivanovic 1987; Peres 1988). It is possible to perform a simultaneous measurement of two incompatible observables. This again is not described by a simple von Neumann measurement but requires introduction of observables associated with a second quantum system (Arthurs & Kelly 1965).

Even if a von Neumann measurement is required, its realization may be far from straightforward. We can, however, find the probability distribution associated with a given observable by synthesizing the projectors associated with its eigenvalues. We describe the method of projection synthesis as it might be applied to measuring the phase probability distribution of a electromagnetic field mode (Barnett & Pegg 1996).

2. Distinguishing between non-orthogonal states

The information that we gain on performing a measurement will depend, in part, on our prior knowledge of the system. If, for example, we know that the system under study has been prepared in one of two non-degenerate eigenstates of an Hermitian operator, then measuring the corresponding observable will tell us in which of the two states the system was prepared and there is no further information to be gained. A single measurement of the correctly chosen observable has provided the missing information with which to completely determine the state.

A more challenging situation occurs if we know that the system has been prepared in one of two non-orthogonal states. As the states are not orthogonal they are not the non-degenerate eigenstates of any Hermitian operator and cannot be distinguished from each other with certainty. Let us represent the two non-orthogonal states by the kets $|\boldsymbol{a}\rangle$ and $|\boldsymbol{b}\rangle$ and ask what is the best we can hope to do in distinguishing between the two states? The answer depends on what we mean by 'best'. We will present two answers to the question, each associated with a different criterion for best. In the first we require a definite answer in the form 'the system is in state $|\boldsymbol{a}\rangle$ (or $|\boldsymbol{b}\rangle$)' and ask that the probability of an error in the assignment of the state be as small as possible. It has been shown (Helstrom 1976) that the best that can be achieved is to arrive at an average error probability given by

$$P_{\text{error}} = \tfrac{1}{2}\{1 - [1 - 4\zeta_{\boldsymbol{a}}\zeta_{\boldsymbol{b}}|\langle\boldsymbol{a}|\boldsymbol{b}\rangle|^2]^{1/2}\}, \tag{2.1}$$

where $\zeta_{\boldsymbol{a}}$ and $\zeta_{\boldsymbol{b}} = 1 - \zeta_{\boldsymbol{a}}$ are the *a priori* probabilities that the system was prepared in the state $|\boldsymbol{a}\rangle$ or $|\boldsymbol{b}\rangle$, respectively. The Helstrom bound can be attained by means of a von Neumann measurement. It is convenient to represent the states $|\boldsymbol{a}\rangle$ and $|\boldsymbol{b}\rangle$ as column vectors in some suitable basis

$$|\boldsymbol{a}\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \quad |\boldsymbol{b}\rangle = \begin{pmatrix} \cos\theta \\ -\sin\theta \end{pmatrix}. \tag{2.2}$$

We introduce the orthogonal states $|\boldsymbol{a}'\rangle$ and $|\boldsymbol{b}'\rangle$ which in the same basis are

$$|\boldsymbol{a}'\rangle = \begin{pmatrix} \cos\phi \\ \sin\phi \end{pmatrix}, \quad |\boldsymbol{b}'\rangle = \begin{pmatrix} -\sin\phi \\ \cos\phi \end{pmatrix}. \tag{2.3}$$

A von Neumann measurement of a suitable observable such as $|\boldsymbol{a}'\rangle\langle\boldsymbol{a}'| - |\boldsymbol{b}'\rangle\langle\boldsymbol{b}'|$ will, depending on the outcome of the observation, project the system into state $|\boldsymbol{a}'\rangle$ or $|\boldsymbol{b}'\rangle$. We associate the $+1$ result (corresponding to projection into $|\boldsymbol{a}'\rangle$) with the system being prepared in $|\boldsymbol{a}\rangle$, while the -1 result is associated with the system having been prepared in $|\boldsymbol{b}\rangle$. The average probability of error is then

$$P_{\text{error}} = \zeta_{\boldsymbol{a}}|\langle\boldsymbol{b}'|\boldsymbol{a}\rangle|^2 + \zeta_{\boldsymbol{b}}|\langle\boldsymbol{a}'|\boldsymbol{b}\rangle|^2, \tag{2.4}$$

which attains the Helstrom bound when we set $\tan 2\phi = (\tan 2\theta)/(\zeta_{\boldsymbol{a}} - \zeta_{\boldsymbol{b}})$.

Is it possible to distinguish between the two states without error? The answer again is yes, but only if we accept the possibility of an inconclusive outcome. We could, for example, make a measurement of the observable $|\boldsymbol{a}\rangle\langle\boldsymbol{a}|$. If we find the value zero then we know for certain that the system was prepared in the state $|\boldsymbol{b}\rangle$, but if we find the value unity then we do not know if the system was prepared in state $|\boldsymbol{a}\rangle$ or $|\boldsymbol{b}\rangle$ and our measurement has been inconclusive. Measurements of this type have been applied to the design of a quantum cryptographic protocol based on signals made up only of the two non-orthogonal states (Bennett 1992). The best error-free measurement will have a minimum probability for an inconclusive result $P(?)$ given by (Ivanovic 1987; Peres 1988)

$$P(?) = |\langle\boldsymbol{a}|\boldsymbol{b}\rangle|. \tag{2.5}$$

It follows therefore that the probability of correctly identifying the state, be it $|\boldsymbol{a}\rangle$ or $|\boldsymbol{b}\rangle$, is $1 - |\langle\boldsymbol{a}|\boldsymbol{b}\rangle|$. In order to present a strategy achieving this bound, represent our states as column vectors in a three-dimensional state-space (Huttner *et al.* 1996) in the form

$$|\boldsymbol{a}\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix}, \quad |\boldsymbol{b}\rangle = \begin{pmatrix} \cos\theta \\ -\sin\theta \\ 0 \end{pmatrix}. \tag{2.6}$$

We introduce the following three orthonormal vectors spanning this three-dimensional space:

$$\left.\begin{aligned} |\boldsymbol{\lambda}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} \tan\theta \\ 1 \\ \sqrt{1-\tan^2\theta} \end{pmatrix}, \quad |\boldsymbol{\mu}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} \tan\theta \\ -1 \\ \sqrt{1-\tan^2\theta} \end{pmatrix}, \\ |\boldsymbol{\nu}\rangle = \begin{pmatrix} -\sqrt{1-\tan^2\theta} \\ 0 \\ \tan\theta \end{pmatrix}. \end{aligned}\right\} \tag{2.7}$$

A suitable von Neumann measurement in this enlarged state space will determine which of these three states the system is in and we associate the results $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ with the conclusions that the system was prepared in $|\boldsymbol{a}\rangle$ or $|\boldsymbol{b}\rangle$, respectively. The result $\boldsymbol{\nu}$ gives us no information and is therefore associated with the inconclusive result. The states $|\boldsymbol{\lambda}\rangle$ and $|\boldsymbol{\mu}\rangle$ are orthogonal to the states $|\boldsymbol{b}\rangle$ and $|\boldsymbol{a}\rangle$, respectively, and

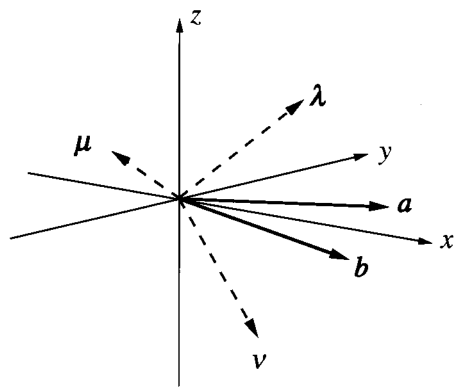

Figure 1. Geometrical interpretation of the Ivanovic–Peres bound. Vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ lie in the x–y plane. Vectors $\boldsymbol{\lambda}$, $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ are mutually orthogonal with non-zero z components and $\boldsymbol{\nu}$ lies in the x–z plane.

therefore no errors of identification will occur. The state $|\boldsymbol{\nu}\rangle$ has the same minimum possible overlap with $|\boldsymbol{a}\rangle$ or $|\boldsymbol{b}\rangle$ consistent with the above constraints. It follows that the probability of an inconclusive result is the same in whichever state the system is prepared and attains the Ivanovic–Peres lower bound, $P(?) = |\langle\boldsymbol{\nu}|\boldsymbol{a}\rangle|^2 = |\langle\boldsymbol{\nu}|\boldsymbol{b}\rangle|^2 = |\langle\boldsymbol{a}|\boldsymbol{b}\rangle|$. Figure 1 illustrates a simple geometrical interpretation of this idea. The states $|\boldsymbol{a}\rangle$ and $|\boldsymbol{b}\rangle$ are represented by a pair of vectors in the x–y plane. The states $|\boldsymbol{\lambda}\rangle$, $|\boldsymbol{\mu}\rangle$ and $|\boldsymbol{\nu}\rangle$ are represented by three mutually orthogonal vectors chosen so that $|\boldsymbol{\lambda}\rangle$ and $|\boldsymbol{\mu}\rangle$ are orthogonal to $|\boldsymbol{b}\rangle$ and $|\boldsymbol{a}\rangle$, respectively.

Two simple optical examples of the problem arise if we attempt to distinguish between two non-orthogonal states of linear polarization given only a single photon and differentiating between two (non-orthogonal) coherent states of a field mode. Both of these problems arise in the study of secure communications by quantum cryptography (Ekert *et al.* 1994; Phoenix & Townsend 1995). The two linear polarization states (2.2) correspond to light polarized at θ and $-\theta$ relative to a chosen axis. A measurement achieving the Helstrom bound consists of determining whether the polarization is oriented at ϕ or $\phi - \frac{1}{2}\pi$ relative to this axis corresponding to the two basis states (2.3). Figure 2 shows the error rate for $\zeta_{\boldsymbol{a}} = \zeta_{\boldsymbol{b}}$ corresponding to equal *a priori* probabilities for the two states so that the Helstrom bound on the average error probability becomes $\frac{1}{2}[1 - \sin(2\theta)]$. The experimental data were recorded with highly attenuated laser pulses, each having a mean photon number of approximately 0.1 (Barnett & Riis 1997). An Ivanovic–Peres measurement of the polarization state is a little more difficult, but an ingenious scheme to achieve this has recently been demonstrated (Huttner *et al.* 1996).

The coherent states of a field mode, $|\alpha\rangle$, are labelled by a complex number (α) which may be thought of as the scaled complex amplitude of the corresponding electromagnetic field. The important properties for our purposes are that the photon number is not fixed but has the expectation value $\langle\hat{n}\rangle = |\alpha|^2$. The vacuum state $|0\rangle$ is the coherent state corresponding to zero amplitude and zero photons. The coherent states are not mutually orthogonal, so that

$$|\langle\alpha|\alpha'\rangle|^2 = \exp(-|\alpha - \alpha'|^2). \tag{2.8}$$

In simple interference experiments, the complex amplitude behaves like the amplitude of a classical field. (For a fuller discussion of these states see, for example,

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

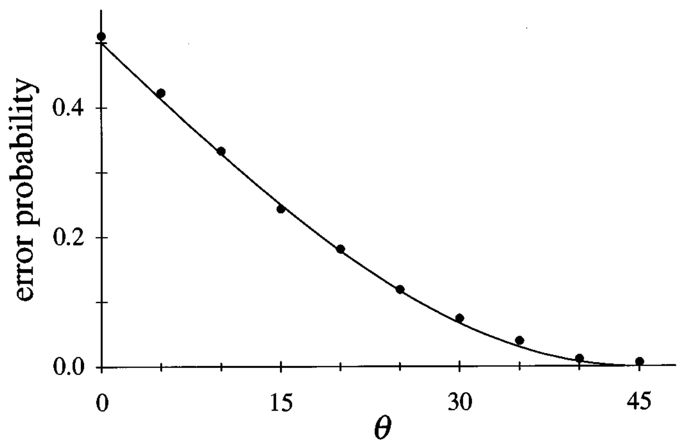

Figure 2. The Helstrom bound on the minimum average error probability for distinguishing between linear polarization states separated by angle 2θ.

Loudon 1983; Barnett & Radmore 1997.) The coherent states we would like to distinguish are those associated with opposite signs of the field, that is $|\alpha\rangle$ and $|-\alpha\rangle$. An error-free Ivanovic–Peres measurement may be realized using a 50%:50% symmetric beam splitter (Huttner *et al.* 1995) for which the complex transmission and reflection coefficients are $1/\sqrt{2}$ and $\mathrm{i}/\sqrt{2}$, respectively (Fearn & Loudon 1987; Barnett & Radmore 1997). Figure 3 depicts an experimental arrangement designed to realize an Ivanovic–Peres measurement to distinguish between $|\alpha\rangle$ and $|-\alpha\rangle$. The unknown state, $|\alpha\rangle$ or $|-\alpha\rangle$, is introduced through port a and made to interfere at a beam splitter with the state $|\mathrm{i}\alpha\rangle$ introduced through port b. Interference transforms the input state $|\alpha\rangle_a \otimes |\mathrm{i}\alpha\rangle_b$ or $|-\alpha\rangle_a \otimes |\mathrm{i}\alpha\rangle_b$ into the output state $|0\rangle_c \otimes |\mathrm{i}\sqrt{2}\alpha\rangle_d$ or $|\sqrt{2}\alpha\rangle_c \otimes |0\rangle_d$, respectively. An unambiguous determination of the original state will occur when photocounts are registered in one of the detectors; counts in detector D or C determine the state to have been $|\alpha\rangle$ or $|-\alpha\rangle$, respectively. An inconclusive result occurs when no counts are registered in either detector. The probability for this to happen is simply the probability that the resulting coherent state has no photons and is

$$P(?) = |\langle \mathrm{i}\sqrt{2}\alpha|0\rangle|^2 = |\langle \sqrt{2}\alpha|0\rangle|^2 = \exp(-2|\alpha|^2) = |\langle\alpha|-\alpha\rangle|, \tag{2.9}$$

clearly satisfying the Ivanovic–Peres bound. Realising the Helstrom bound for two coherent states is more of a challenge, although progress in this direction has been reported recently (Sasaki & Hirota 1996*a*,*b*; Sasaki *et al.* 1996).

3. Simultaneous measurement of conjugate observables

It is not possible to prepare a state in which the precise values of a pair incompatible observables are known. This fundamental idea played an important role in the development of quantum theory and is encapsulated in the uncertainty (or indeterminacy) principle (Heisenberg 1930; Robertson 1929). For position $\boldsymbol{x}$ and momentum $\boldsymbol{p}$, this restricts our uncertainty in the two observables to

$$\Delta\boldsymbol{x}\Delta\boldsymbol{p} \geqslant \tfrac{1}{2}\hbar. \tag{3.1}$$

Measurement of two incompatible observables is restricted by a different bound so that for any given state a joint measurement of $\boldsymbol{x}$ and $\boldsymbol{p}$ leads to statistical uncer-

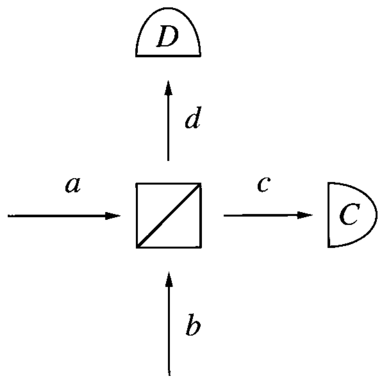

Figure 3. Schematic diagram of a 50%:50% beam splitter with input modes a and b and output modes c and d.

tainties bounded by the inequality

$$\Delta \boldsymbol{x} \Delta \boldsymbol{p} \geqslant \hbar, \tag{3.2}$$

so that the bound is twice that for state preparation (Arthurs & Kelly 1965; She & Heffner 1966; Busch 1985; Stenholm 1992). In order to understand the origin of the additional uncertainty, we recall that an unambiguous identification of the values of two observables can only be made if their corresponding operators commute. In order to achieve this for the position and momentum, we introduce a second (tilde) system characterized by position $\tilde{\boldsymbol{x}}$ and momentum $\tilde{\boldsymbol{p}}$. The total momentum $\boldsymbol{P} = \boldsymbol{p} + \tilde{\boldsymbol{p}}$ and relative position $\boldsymbol{X} = \boldsymbol{x} - \tilde{\boldsymbol{x}}$ are then compatible observables and can be determined simultaneously. The tilde system is a quantum system in its own right, bounded by the uncertainty relation (3.1). The origin of the increased bound seen in (3.2) is this additional uncertainty associated with specifying the position and momentum for the tilde system which was required in order to make the position and momentum simultaneously observable. In order to determine the values of the incompatible observables we have had to accept an additional statistical error not inherent to the system under scrutiny. We are, in effect, performing an *unsharp measurement* (Busch 1985). This doubling of the uncertainty is not restricted to position and momentum observables but is a general property of simultaneous measurements on any pair of incompatible observables (Arthurs & Goodman 1988).

A natural optical realization of a canonically conjugate pair of operators is given by the quadratures which are the quantized field observables associated with the real and imaginary parts of the classical complex electric field amplitude. The quadratures have risen to prominence in the study of squeezed states of light (Loudon & Knight 1987; Barnett & Radmore 1997). Measurement of a single quadrature can be performed by balanced homodyne detection using a large amplitude coherent field as a local oscillator (Loudon & Knight 1987). Measurement of both field quadratures can be achieved by coherently splitting the field to be measured into two parts, using a 50%:50% beam splitter, and then measuring a different quadrature on each of the two resulting (reduced amplitude) beams (Walker 1987). The enhanced uncertainty arises from the vacuum field entering the 50%:50% beam splitter through the unused port. Experimental realizations of the joint measurement demonstrate the expected enhanced uncertainty (Walker & Carroll 1984, 1986).

We can apply the same reasoning as that outlined above to the measurement of other incompatible observables such as orthogonal components of spin associated with a spin-$\frac{1}{2}$ particle or other two-state system. The x and z components of the spin, σ_x and σ_z, are incompatible observables. In order to analyse a joint measurement of these observables, we introduce a second (tilde) two-state system with spin components $\tilde{\sigma}_x$ and $\tilde{\sigma}_z$. The collective observables $\sigma_x\tilde{\sigma}_x$ and $\sigma_z\tilde{\sigma}_z$ are compatible and so can be determined simultaneously. We can choose the state of the tilde system and therefore know the expectation values $\langle\tilde{\sigma}_x\rangle$ and $\langle\tilde{\sigma}_z\rangle$. The eigenvalues of $\sigma_x\tilde{\sigma}_x$ and $\sigma_z\tilde{\sigma}_z$ are ±1 and, as we know the expectation values of the tilde observables, we can interpret the results of the measurements of $\sigma_x\tilde{\sigma}_x$ and $\sigma_z\tilde{\sigma}_z$ as unsharp measurements of σ_x and σ_z. Consider, for example, a joint measurement of σ_x and σ_z if the system is prepared in the ±1 eigenstate of σ_z ($|\pm\rangle$) or of σ_x ($1/\sqrt{2}\{|+\rangle \pm |-\rangle\}$). We prepare the tilde spin in a superposition of the eigenstates of $\tilde{\sigma}_z$ so that the combined state of the two systems is

$$|\Psi\rangle = |\psi\rangle \otimes \{\cos(\tfrac{1}{2}\theta)|\tilde{+}\rangle + \sin(\tfrac{1}{2}\theta)|\tilde{-}\rangle\}, \tag{3.3}$$

where $|\psi\rangle$ is one of the eigenstates of σ_x or σ_z. The expectation values of $\tilde{\sigma}_x$ and $\tilde{\sigma}_z$ in this state are

$$\langle\tilde{\sigma}_x\rangle = \sin\theta, \quad \langle\tilde{\sigma}_z\rangle = \cos\theta, \tag{3.4}$$

which, for definiteness, we take to be positive. We then associate a measurement of $\sigma_x\tilde{\sigma}_x$ giving the result ±1 as an unsharp measurement of σ_x with the value ±1, respectively. Similarly, if we find the value of $\sigma_z\tilde{\sigma}_z$ to be ±1, then we associate ±1 with the value of σ_z. If the state is one of the eigenstates of σ_z, then this procedure will correctly identify the state with probability $\frac{1}{2}(1+\cos\theta)$. If, instead, we have one of the eigenstates of σ_x, then the probability of correctly identifying the state is $\frac{1}{2}(1+\sin\theta)$. Clearly, a more accurate or less 'unsharp' determination of σ_z or σ_x leads to a less accurate determination of σ_x or σ_z, respectively. In the symmetrical arrangement, for which $\theta = \frac{1}{4}\pi$, the probabilities of correctly identifying the spin components are approximately 85%.

In order to realize a measurement of both σ_x or σ_z we require an experimental arrangement with four possible outcomes corresponding to each spin component having the possible values ±1. As an explicit example, consider the problem of a single linearly polarized photon with either horizontal or vertical polarization (corresponding to an eigenstate of σ_z) or with polarization oriented at 45° to these axes (corresponding to an eigenstate of σ_x). Figure 4 illustrates a possible implementation of such a measurement (Busch 1987). A single photon is either transmitted or reflected at a 50%:50% beam splitter. The reflected beam is split at a polarizing beam splitter, oriented so that it transmits a polarization oriented at $\frac{1}{8}\pi$ to the vertical so as to be intermediate between the $+1$ eigenstates of σ_x and σ_z. The orthogonal polarization is reflected so that photodetectors placed at the outputs perform a measurement of $\{\sigma_z + \sigma_x\}/\sqrt{2}$. The beam transmitted through the first beam splitter is also split at a polarizing beam splitter, this time oriented so as to measure the polarization corresponding to the operator $\{\sigma_z - \sigma_x\}/\sqrt{2}$. For a single photon only, one of the detectors will register a photocount and we can then associate each of the possible outcomes with a different joint measurement of σ_x and σ_z. A photocount registered in detector A, B, C or D is interpreted as an unsharp measurement of σ_x and σ_z, corresponding to the values $(+1,+1)$, $(-1,-1)$, $(-1,+1)$ or $(+1,-1)$, respectively. For a polarization prepared in an eigenstate of σ_x or σ_z, the probability of correctly assigning the value of σ_x or σ_z is 85%. More generally, the statistics of the measurement are the same as those based on the measurement of $\sigma_x\tilde{\sigma}_x$ and $\sigma_z\tilde{\sigma}_z$ described above with the state (3.3) and $\theta = \frac{1}{4}\pi$.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

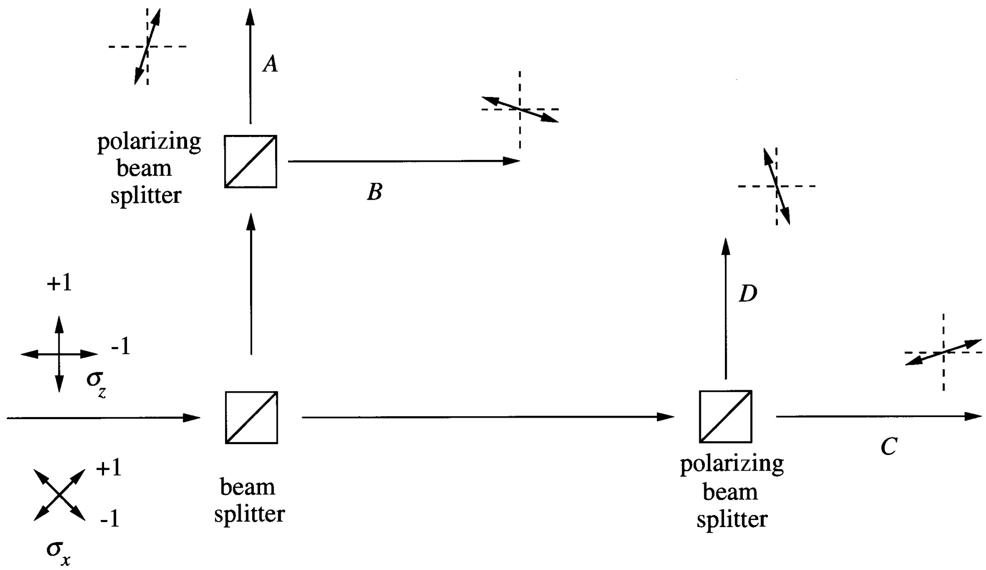

Figure 4. Representation of a possible simultaneous measurement of incompatible polarization observables. A 50%:50% beam splitter sends the photon to one of two polarizing beam splitters oriented so as to measure different polarization components.

We have seen that it is possible to measure incompatible polarization components for a single photon, but only at the expense of an increased uncertainty which manifests itself as a finite probability of error in assigning the polarization components. For this reason, simultaneous measurements of the observables corresponding to these polarizations will not provide a successful means of eavesdropping on a quantum cryptographic communication channel. Bell's theorem in the form it is usually expressed involves the choice of a pair of spin observables for each of two entangled two-state systems (Bell 1987). Under suitable conditions, the ensemble average over many measurements leads to a violation of the inequality. If we were to measure both of the single-particle observables appearing in the inequality simultaneously, then we would find that Bell's inequality is restored (Bédiat, unpublished research). This is because the additional uncertainty associated with the joint measurement reduces the level of correlation observed.

4. Measurement by projection synthesis

The simple von Neumann measurement described in the first section involves projection onto an eigenstate of the Hermitian operator corresponding to the observable being measured. The probability associated with a given result is simply the expectation value of the corresponding projector. If we can synthesize the projector corresponding to a given eigenstate then we can determine the corresponding probability distribution. The projection synthesis method described in this section provides quite a general method for measuring observables associated with an electromagnetic field mode. We will restrict our discussion to measurement of the phase probability density by projection synthesis (Barnett & Pegg 1996; Pegg *et al.* 1997).

For a quantized field mode, the photon number probability distribution can be determined by photodetection but other quantities, such as the phase probability distribution (Barnett & Pegg 1989; Pegg & Barnett 1989) are more difficult to measure, although this has been done (Beck *et al.* 1993). The probability density for pure state $|f\rangle = \sum c_n|n\rangle$ to have a phase θ is (Pegg & Barnett 1997)

$$P(\theta) = \frac{1}{2\pi}\left|\sum_{n=0}^{\infty} c_n \exp(-\mathrm{i}n\theta)\right|^2. \tag{4.1}$$

This is proportional to a quantity that can be approximated to within any required error by the square of the modulus of the projection of $|f\rangle$ onto the state

$$|\theta, N\rangle = \frac{1}{\sqrt{N+1}}\sum_{n=0}^{N} \exp(\mathrm{i}n\theta|n\rangle \tag{4.2}$$

by choosing N to be sufficiently large. That is, we can replace (4.1) for N suitably large by

$$P_N(\theta) = \frac{1}{2\pi k_N}\left|\sum_{n=0}^{N} c_N \exp(-\mathrm{i}n\theta)\right|^2, \tag{4.3}$$

where the normalization constant $k_N = \sum_{n=0}^{N}|c_n|^2 \approx 1$ is inserted to ensure that $P_N(\theta)$ is normalized over a 2π range. This normalization property allows us to find (4.3) by measuring a quantity proportional to it and later normalizing the results obtained for a large number of different values of θ. It is worth noting that (4.2) has the same mathematical form, with N in place of s, as the eigenstates of the Hermitian optical phase operator (Barnett & Pegg 1989; Pegg & Barnett 1989, 1997). Here, however, we are not taking the infinite N limit but rather choosing N to be large enough for (4.3) to serve as a good approximation to (4.1).

We seek an event, the amplitude for which is proportional to the projection of $|f\rangle$ onto $|\theta, N\rangle$, with a proportionality constant independent of θ. From this we can reconstruct the phase probability distribution by normalization. Consider a 50%:50% symmetric beam splitter with input modes a and b and output modes c and d (see figure 3). The photon annihilation operators for these four modes are a, b, c and d. We measure the probability that N photons are detected in mode c, while no photons are detected in mode d. For these events, we infer that the output state is

$$|N\rangle_n \otimes |0\rangle_d = \frac{c^{\dagger N}}{\sqrt{N!}}|0]\rangle_c \otimes |0\rangle_d, \tag{4.4}$$

We can then use the beam splitter relations (Fearn & Loudon 1987; Barnett & Radmore 1997) to rewrite (4.4) as an entangled state of the input modes in the form

$$\begin{aligned} |M\rangle &= \frac{2^{-N/2}}{\sqrt{N!}}\sum_{l=0}^{N}\begin{pmatrix} N \\ l \end{pmatrix} a^{\dagger(N-l)}(-\mathrm{i}b^\dagger)^l|0\rangle_a \otimes |0\rangle_b \\ &= 2^{-N/2}\sum_{l=0}^{N}\begin{pmatrix} N \\ l \end{pmatrix}^{1/2}(-\mathrm{i})^l|N-l\rangle_a \otimes |l\rangle_b. \end{aligned} \tag{4.5}$$

The amplitude for the output to be $|N\rangle_c \otimes |0\rangle_d$ is just the projection of the input state $|F\rangle = |f\rangle_a \otimes |\boldsymbol{b}\rangle_b$ onto the state $|M\rangle$, where $|\boldsymbol{b}\rangle_b = \sum b_n|n\rangle_b$ is the input state into mode b. The amplitude for this is simply

$$\langle F|M\rangle = 2^{-N/2}\sum_{l=0}^{N}(-\mathrm{i})\begin{pmatrix} N \\ l \end{pmatrix}^{1/2} b_l^* c_{N-l}^*. \tag{4.6}$$

For the modulus of this amplitude to be proportional to the modulus of the projection of $|f\rangle$ onto $|\theta, N\rangle$, we require

$$b_n^* \propto \begin{pmatrix} N \\ n \end{pmatrix}^{-1/2} \exp[-\mathrm{i}n(\theta - \tfrac{1}{2}\pi)] \tag{4.7}$$

for $0 \leqslant n \leqslant N$. Ideally, we require a reciprocal binomial state for which only the first $N + 1$ photon numbers are non-zero (Barnett & Pegg 1996). However, if N is not required to exceed one or two, then coherent or squeezed states may be used (Pegg *et al.* 1997). If such states can be prepared (Pegg *et al.* 1997), then the phase probability distribution can be found by determining the proportion of events in which N photocounts are registered in detector C and none in detector D. The full phase probability distribution may be found by measuring this proportion for a sufficient range of values of θ in (4.7) and then normalizing the resulting distribution to give (4.3).

State projection synthesis provides the means to obtain the probabilities associated with states other than the phase states. The ability to prepare any chosen reference state for mode b would, in principle, allow the experimental determination of the expectation value of any chosen projector formed from the first $N+1$ number states.

5. Conclusions

We have presented three extensions of conventional (von Neumann) measurements and described possible quantum optical implementations of these. It is not possible to discriminate with certainty between two non-orthogonal states of a single system, such as non-orthogonal polarization states of a single photon. The best we can do is to minimize the error rate to the Helstrom bound (Helstrom 1976) or provide error-free discrimination but with a bounded probability for an inconclusive result (Ivanovic 1987; Peres 1988). Both of these measurement bounds have been achieved in measurements of optical polarization (Barnett & Riis 1997; Huttner *et al.* 1996).

It is not possible to measure two incompatible observables, such as the position and momentum of a particle, with unlimited accuracy. Such measurements necessarily involve additional uncertainty over and above that inherent in the uncertainty principle (Arthurs & Kelly 1965; Arthurs & Goodman 1988). A quantum optical implementation in which values for the canonically conjugate field quadratures are determined has been demonstrated (Walker & Carroll 1984, 1986). We have described a rather simple arrangement by which unsharp values for different polarization components can be determined. This is only one of a number of such possible realizations for simultaneous measurement of polarization (Busch 1987).

It would be useful to have a general technique for measuring the probability distribution associated with any chosen field observable. One way of achieving this is to perform enough measurements in order to reconstruct the state (Smithey *et al.* 1993) and then calculate the required probability distribution from the reconstructed state. A more direct and practical method in some cases might be to use projection synthesis (Barnett & Pegg 1996). We have shown how the phase probability distribution can be found by this method if we have access to suitable reference states.

The examples presented in this paper by no means exhaust the possibilities for generalized measurements in quantum optics. Exotic schemes involving entanglement between the system to be measured and an ancilla have been proposed. The rapid

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

advance in ion trap techniques, aimed at developing quantum computing (Monroe *et al.* 1995), offer an excellent opportunity to put some of these into practice.

The material in this paper was developed in collaboration with Nathalie Bédiat, Norbet Lütkenhaus, Lee Phillips, David Pegg, Simon Phoenix and Erling Riis. I am grateful to them and also to Claire Gilson, Osamu Hirota, Geoff New and Masahide Sasaki for helpful comments and suggestions.

References

Arthurs, E. & Goodman, M. S. 1988 Quantum correlations: a generalized Heisenberg uncertainty relation. *Phys. Rev. Lett.* **60**, 2447–2449.

Arthurs, E. & Kelly, J. L. 1965 On the simultaneous measurement of a pair of conjugate observables. *Bell Syst. Tech. J.* **44**, 725–729.

Barnett, S. M. & Pegg, D. T. 1989 On the Hermitian optical phase operator. *J. Mod. Opt.* **36**, 7–19.

Barnett, S. M. & Pegg, D. T. 1996 Phase measurement by projection synthesis. *Phys. Rev. Lett.* **76**, 4148–4150.

Barnett, S. M. & Phoenix, S. J. D. 1996 The principles of quantum cryptography. *Phil. Trans. R. Soc. Lond.* A **354**, 793–803.

Barnett, S. M. & Radmore, P. M. 1997 *Methods in theoretical quantum optics.* Oxford University Press.

Barnett, S. M. & Riis, E. 1997 Experimental demonstration of polarization discrimination at the Helstrom bound. *J. Mod. Opt.* **44**, 1061–1064.

Beck, M., Smithey, D. T., Cooper, J. & Raymer, M. G. 1993 Experimental determination of number-phase uncertainty relations. *Opt. Lett.* **18**, 1259–1261.

Bell, J. S. 1987 *Speakable and unspeakable in quantum mechanics.* Cambridge University Press.

Bennett, C. H. 1992 Quantum cryptography using any two non-orthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124.

Busch, P. 1985 Indeterminacy relations and simultaneous measurements in quantum theory. *Int. J. Theor. Phys.* **24**, 63–92.

Busch, P. 1987 Some realizable joint measurements of complementary observables. *Found. Phys.* **17**, 905–937.

Cirac, J. I. & Zoller, P. 1995 Quantum computations with cold traped ions. *Phys. Rev. Lett.* **74**, 4091–4094.

Ekert, A. K. & Josza, R. 1996 Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.* **68**, 733–753.

Ekert, A. K., Huttner, B., Palma, G. M. & Peres, A. 1994 Eavesdropping on quantum-cryptographical systems. *Phys. Rev.* A **50**, 1047–1056.

Fearn, H. & Loudon, R. 1987 Quantum theory of the lossless beam splitter. *Opt. Commun.* **64**, 485–490.

Heisenberg, W. 1930 *The physical principles of the quantum theory.* University of Chicago Press. (Reprinted 1949 New York: Dover).

Helstrom, C. W. 1976 *Quantum detection and estimation theory.* New York: Academic.

Huttner B., Imoto, N., Gisin, N. & Mor, T. 1995 Quantum cryptography with coherent states. *Phys. Rev.* A **51**, 1863–1869.

Huttner, B., Muller, A., Gautier, J. D., Zbinden, H. & Gisin, N. 1996 Unambiguous quantum measurement of nonorthogonal states. *Phys. Rev.* A **54**, 3783–3789.

Ivanovic, I. D. 1987 How to differentiate between non-orthogonal states. *Phys. Lett.* A **123**, 257–259.

Loudon, R. 1983 *The quantum theory of light.* Oxford University Press.

Loudon, R. & Knight, P. L. 1987 Squeezed light. *J. Mod. Opt.* **34**, 709–759.

Monroe, C., Meekhof, D., King, B. E., Itano, W. M. & Wineland, D. J. 1995 Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.* **75**, 4714–4717.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Pegg, D. T. & Barnett, S. M. 1989 Phase properties of the quantized single-mode field. *Phys. Rev.* A **39**, 1665–1675.

Pegg, D. T. & Barnett, S. M. 1997 Tutorial review: quantum optical phase. *J. Mod. Opt.* **44**, 225–264.

Pegg, D. T., Barnett, S. M. & Phillips, L. S. 1997 Quantum phase distribution by projection synthesis. *J. Mod. Opt.* (In the press.)

Peres, A. 1988 How to differentiate between non-orthogonal states. *Phys. Lett.* A **128**, 19.

Phoenix, S. J. D. & Townsend, P. D. 1995 Quantum cryptography—how to beat the codebreakers. *Contemp. Phys.* **36**, 165–195.

Robertson, H. P. 1929 The uncertainty principle. *Phys. Rev.* **34**, 163–164.

Sasaki, M. & Hirota, O. 1996a Two examples of measurement processes illustrating Helstrom's optimum decision bound. *Phys. Lett.* A **210**, 21–25.

Sasaki, M. & Hirota, O. 1996b Optimum decision scheme with a unitary control process for binary quantum state control. *Phys. Rev.* A **54**, 2728–2736.

Sasaki, M., Usuda, T. S., Hirota, O. & Holevo, A. S. 1996 Applications of the Jaynes–Cummings model for the detection of nonorthogonal quantum states. *Phys. Rev.* A **53**, 1273–1279.

She, C. Y. & Heffner, H. 1966 Simultaneous measurement of non-commuting observables. *Phys. Rev.* **152**, 1103–1110.

Smithey, D. T., Beck, M., Cooper, J., Raymer, M. G. & Faridani, A. 1993 Complete experimental characterization of the quantum state of a light mode via the Wigner function and the density matrix: application to quantum phase distributions of vacuum and squeezed-vacuum states. *Phys. Scripta* T **48**, 35–44.

Stenholm, S. 1992 Simultaneous measurement of conjugate variables. *Ann. Phys. (NY)* **218**, 233–254.

Townsend, P. D., Marand, C., Phoenix, S. J. D., Blow, K. J. & Barnett, S. M. 1996 Secure optical communications systems using quantum cryptography. *Phil. Trans. R. Soc. Lond.* A **354**, 805–817.

von Neumann, J. 1955 *Mathematical foundations of quantum mechanics*. Princeton University Press.

Walker, N. G. 1987 Quantum theory of multiport optical homodyning. *J. Mod. Opt.* **34**, 15–60.

Walker, N. G. & Carroll, J. E. 1984 Simultaneous phase and amplitude measurements on optical signals using a multiport junction. *Elect. Lett.* **20**, 981–983.

Walker, N. G. & Carroll, J. E. 1986 Multiport homodyne detection near the quantum noise limit. *Opt. Quant. Electr.* **18**, 355–363.