AAPT PHYSICS EDUCATION
AMERICAN JOURNAL of PHYSICS

Positive operator valued measure in quantum information processing

Howard E. Brandt

Citation: Am. J. Phys. **67**, 434 (1999); doi: 10.1119/1.19280

View online: http://dx.doi.org/10.1119/1.19280

View Table of Contents: http://ajp.aapt.org/resource/1/AJPIAS/v67/i5

Published by the American Association of Physics Teachers

CENGAGE Learning
WILEY
openstax COLLEGE
W. H. FREEMAN
Physics Curriculum & Instruction
Mc Graw Hill Higher Education
PEARSON

Positive operator valued measure in quantum information processing

Howard E. Brandt[a)]
U.S. Army Research Laboratory, Adelphi, Maryland 20783

(Received 18 May 1998; accepted 15 September 1998)

The positive operator valued measure (POVM), also known as the *probability* operator valued measure, is useful in quantum information processing. The POVM consists of a set of non-negative quantum-mechanical Hermitian operators that add up to the identity. The probability that a quantum system is in a particular state is given by the expectation value of the POVM operator corresponding to that state. Following a brief review of the mathematics and history of POVMs in quantum theory, and an expository discussion of the quantum mechanics of photonic qubits, a particular implementation of a POVM for use in the measurement of photonic qubits is reviewed.

I. INTRODUCTION

In quantum measurement theory, for a typical von Neumann-type projective measurement of a quantum system represented by a complete orthonormal set of states $|\mu\rangle$, the measurement operator corresponding to the measurement outcome μ is the projection operator $|\mu\rangle\langle\mu|$. This is also known as a projection valued measure or PV measure. Such orthogonal measurement operators are Hermitian and idempotent. Also, since orthogonal measurement operators commute, they correspond to simultaneous observables. The number of such operators is equal to the dimension of the Hilbert space of the quantum system. Measurement operators corresponding to nonorthogonal states do not commute and are therefore not simultaneously observable. A generalized type of measurement is represented by a positive operator valued measure (POVM). The corresponding measurement operators are not necessarily orthogonal or commutative. The main difference between a POVM and a PV measure is that the number of available outcomes may differ from the number of available preparations and the dimension of the Hilbert space. Also, POVMs allow the possibility of measurement outcomes associated with nonorthogonal states. It is also generally thought that a POVM belongs to the most general test to which a quantum system may be subjected.

Specifically, a positive operator valued measure (POVM) is a set of non-negative Hermitian operators A_μ that act in the Hilbert space of a quantum system and sum to the identity operator, namely,[1]

$$\sum_{\mu} A_\mu = 1. \tag{1}$$

The index μ labels the various possible outcomes of a measurement implementing the POVM. The probability P_μ of outcome μ, if the system is in a state described by the density matrix ρ, is given by

$$P_\mu = \mathrm{Tr}(A_\mu \rho). \tag{2}$$

The advantage of a POVM is that it may allow the extraction of more mutual information than can the usual von Neumann-type projective measurement.

Several decades ago, a POVM was used by Jauch and Piron in a generalized analysis of the localizability of quantum systems.[2] The formal mathematical theory of POVMs had already been clearly and usefully exposited by Berberian.[3] The representation of a POVM by a PV measure in an extended higher dimensional Hilbert space had decades earlier been demonstrated by Neumark.[4,5] The analysis of quantum observables in terms of POVMs was advanced by Davies and Lewis[6,7] and Holevo.[8–10] The use of the POVM in the mathematics of quantum measurement theory was further advanced by Benioff.[11–13] The application of the POVM in quantum detection and estimation theory was extensively exposited by Helstrom.[14] Helstrom also referred to a POVM as a *probability-operator measure*, which aptly designates the role of a POVM in directly determining the probability of a measurement outcome [Eq. (2)]. In work by Davies,[15] the POVM was used to investigate the mathematical characteristics of Shannon mutual information in quantum measurement theory. In recent work, Busch *et al.*[16,17] presented informative and useful expositions of the use of POVMs in exploring quantum measurement theory, resolving issues in the foundations of quantum mechanics, and analyzing numerous experiments.

In other recent work, the POVM has been applied to the analysis of key distribution in quantum cryptography.[1,18–27] Peres's book[1] presented the first widely accessible exposition of the mathematical characteristics of the POVM used in cryptographic key distribution.[28] Ekert *et al.*[18] applied the POVM in the quantitative analysis of various eavesdropping strategies. Their work was recently expanded upon by Brandt *et al.*,[19] for the particular case of entangled translucent eavesdropping. Fuchs and Peres[20,21] used a POVM in the analysis of optimal detection methods in quantum cryptography for specified tolerable disturbances. Lutkenhaus[22] provided a very extensive analysis, based on Shannon information and collision probability, of security against eavesdropping for a wide class of eavesdropping strategies described by a POVM. In other recent work, Fuchs[23] employed the POVM in an investigation of reliable information transfer rates using nonorthogonal input states in noisy channels. Also, Biham *et al.*[24] recently used the POVM in an analysis of the security of quantum key distribution against collective attacks.

The first designs for all-optical implementations of a POVM in quantum cryptography were invented by Brandt and Myers,[25,26,19] and independently by Huttner *et al.*[27] In the latter, the implementation of a *loss-induced generalized quantum measurement* is also an implementation of a POVM. Based on Neumark's extension theorem,[4,5] analyses were also presented of the embedding of the two-dimensional Hilbert space of the POVM implementation in a three-dimensional Hilbert space of a PV measure.[26,27] Several aspects of this device implementation of a POVM are reviewed below in Sec. III.

Another recent all-optical implementation of the same POVM used in quantum cryptography was originated by Wootters and Grossman, influenced by work of Gisin.[29–31] This implementation is described qualitatively in Appendix A.

As background for the discussion of the all-optical POVM implementation, in Sec. II a general pedagogical discussion is presented of the quantum mechanics of photonic qubits for use in quantum information processing. In Sec. III, the Brandt–Myers implementation of a POVM is examined for use in the measurement of photonic qubits in quantum cryptography. The device serves as a real embodiment of a POVM in quantum information processing.

II. PHOTONIC QUBITS

A qubit is a quantum system with a two-dimensional Hilbert space, capable of existing in a superposition of Boolean states and of being entangled with the states of other qubits.[32] An example of a photonic qubit is that of two polarization states $|u\rangle$ and $|v\rangle$ of a photon, for which the two kets, respectively, correspond to u- and v-polarization states, respectively, of the photon. A general superposition state of the qubit is

$$|\psi\rangle=\alpha|u\rangle+\beta|v\rangle, \tag{3}$$

where α and β are complex numbers. The states $|u\rangle$ and $|v\rangle$ in Eq. (3) are not necessarily orthogonal. If the u- and v-polarization states encode binary digits 0 and 1, respectively, then the Boolean state corresponding to Eq. (3) is

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle. \tag{4}$$

This superposition state has a propensity to be a 0 or a 1.

The probability amplitude for finding a photon in a linear polarization state $|u\rangle$, as a result of a measurement performed on the photon previously selected to be in the linear polarization state $|v\rangle$, if the angle between the two corresponding polarization vectors is θ, is given by

$$\langle u|v\rangle=\langle u|e^{-i\theta J_z/\hbar}|u\rangle, \tag{5}$$

where J_z is the angular momentum operator about an axis perpendicular to the two polarization vectors, and $\hbar$ is Planck's constant divided by 2π. Equation (5) follows from the spin-one behavior of the photon under the rotation group, since one can obtain the polarization state $|v\rangle$ from the polarization state $|u\rangle$ by simply performing a rotation by angle θ about an axis perpendicular to the two polarization states. Denoting right- and left-circular polarization states about this axis by $|r\rangle$ and $|l\rangle$, respectively, and choosing the y axis along the u-polarization direction, one has

$$|u\rangle=2^{-1/2}(|l\rangle+|r\rangle), \tag{6}$$

$$J_z|r\rangle=\hbar|r\rangle, \tag{7}$$

$$J_z|l\rangle=-\hbar|l\rangle, \tag{8}$$

and

$$\langle l|l\rangle=1, \quad \langle r|r\rangle=1, \quad \langle l|r\rangle=0. \tag{9}$$

Substituting Eq. (6) in Eq. (5), and using Eqs. (7)–(9), one obtains

$$\begin{aligned}\langle u|v\rangle&=2^{-1/2}(\langle l|+\langle r|)e^{-i\theta J_z/\hbar}2^{-1/2}(|l\rangle+|r\rangle)\\&=2^{-1}(\langle l|+\langle r|)(e^{i\theta}|l\rangle+e^{-i\theta}|r\rangle)\\&=\tfrac{1}{2}(e^{i\theta}+e^{-i\theta}),\end{aligned} \tag{10}$$

or

$$\langle u|v\rangle=\cos\theta. \tag{11}$$

Equation (11) is, of course, simply the quantum basis for Malus's law, namely,

$$|\langle u|v\rangle|^2=\cos^2\theta, \tag{12}$$

giving the transmission probability for a photon of linear v polarization passing normally through a polarization analyzer with the polarizing direction oriented at an angle θ relative to the v-polarization direction. Equation (11) gives the Dirac bracket for two linear polarization states $|u\rangle$ and $|v\rangle$. For orthogonal polarization states it is vanishing, while for nonorthogonal polarization states it is nonvanishing.

Before concentrating on POVM methods for measuring photonic qubits, it is useful to consider, by means of Schwinger's algebra of measurement,[33–35] ordinary von Neumann-type projective measurements. The measurement operator $M(u,u)$, representing a selective measurement in which a photonic qubit is accepted in a state $|u\rangle$ and emerges also in the state $|u\rangle$, is given by

$$M(u,u)=|u\rangle\langle u|. \tag{13}$$

One can perform this measurement by using a polarization filter (in front of an ideal photodetector) with the polarization direction aligned along the u-polarization direction. It follows from Eqs. (11) and (13) that $M(u,u)$ is in fact a projection operator, namely it is idempotent:

$$M(u,u)M(u,u)=M(u,u). \tag{14}$$

Also, it is Hermitian:

$$M(u,u)^\dagger=M(u,u). \tag{15}$$

From Eqs. (11) and (13), it also follows that

$$M(u,u)|u\rangle=|u\rangle. \tag{16}$$

Thus the measurement operator $M(u,u)$ has eigenvalue 1 for the state $|u\rangle$; equivalently, the expectation value is

$$\langle u|M(u,u)|u\rangle=1. \tag{17}$$

However, using Eqs. (11) and (13), one also obtains

$$M(u,u)|v\rangle=\cos\theta|u\rangle, \tag{18}$$

so that the state $|v\rangle$ is not an eigenstate of $M(u,u)$, and the expectation value in the state $|v\rangle$ is

$$\langle v|M(u,u)|v\rangle=\cos^2\theta\leqslant 1. \tag{19}$$

Equation (19) is also an expression of Malus's law.

Consider two successive measurements,

$$M(u,u)M(v,v)=\cos\theta M(u,v). \tag{20}$$

Equation (20) follows from Eq. (11) and the definition,

$$M(u,v)\equiv|u\rangle\langle v|. \tag{21}$$

The operator $M(u,v)$ represents a selective measurement in which the qubit is accepted in the state $|v\rangle$ and emerges in the state $|u\rangle$. This can of course be accomplished with a polarization rotator following a polarization filter. The operator $M(u,v)$ is not a projection operator, since

$$M(u,v)M(u,v)=M(u,u)M(v,v)=\cos\theta M(u,v), \quad (22)$$

which follows from Eqs. (21), (11), and (18). It is noteworthy that the operator product, Eq. (22), can also be realized by a polarization analyzer with polarizing direction at an angle θ with respect to the v-polarization direction of a v-polarization filter. Equation (22) is of course consistent with Eq. (14). Also note that the operator $M(u,v)$ is not Hermitian,

$$M(u,v)^{\dagger}=M(v,u), \quad (23)$$

which follows directly from Eq. (21). However, to close the measurement algebra, one needs not only the projection operators $M(u,u)$ and $M(v,v)$, but also the non-Hermitian operators $M(u,v)$ and $M(v,u)$.

Next, consider the following commutator:

$$[M(u,u),M(v,v)]=\cos\theta(M(u,v)-M(u,v)^{\dagger}), \quad (24)$$

which follows from Eqs. (11), (20), and (23). Thus nonorthogonal photon polarization measurement operators do not commute. The corresponding uncertainty relation for such incompatible projective measurements of a qubit in some polarization state $|\psi\rangle$, such as that in Eq. (3), is[35]

$$\begin{aligned}&\langle\psi|(\Delta M(u,u))^2|\psi\rangle\langle\psi|(\Delta M(v,v))^2|\psi\rangle\\&\quad\geqslant\tfrac{1}{4}|\langle\psi|[M(u,u),M(v,v)]|\psi\rangle|^2\\&\qquad+\tfrac{1}{4}|\langle\psi|\{\Delta M(u,u),\Delta M(v,v)\}|\psi\rangle|^2, \quad (25)\end{aligned}$$

in which an anticommutator appears in the last term, and

$$\Delta M(u,u)=M(u,u)-\langle\psi|M(u,u)|\psi\rangle. \quad (26)$$

It is essential to retain the second term on the right-hand side of Eq. (25) (see Appendix B). For a state $|\psi\rangle$ with unit normalization, Eq. (25) reduces to

$$\begin{aligned}&(\langle\psi|(\Delta M(u,u))^2|\psi\rangle)^{1/2}(\langle\psi|(\Delta M(v,v))^2|\psi\rangle)^{1/2}\\&\quad\geqslant|\cos^2\theta|\mathrm{Im}(\langle\psi|M(u,v)|\psi\rangle)|^2\\&\qquad+|\cos\theta\,\mathrm{Re}(\langle\psi|M(u,v)|\psi\rangle)-\langle\psi|M(u,u)|\psi\rangle\\&\qquad\times\langle\psi|M(v,v)|\psi\rangle|^2|^{1/2}, \quad (27)\end{aligned}$$

which gives a generally nonvanishing product of the uncertainties in the measurement of nonorthogonal photon polarizations. In Appendix B, an example is given of the use of Eq. (27). Note, on the right-hand side of the inequality Eq. (27), the role of the operator $M(u,v)$ in determining the lower bound on the uncertainty product. It is this uncertainty, together with the nonclonability of unknown photon polarization states,[36,37] that makes quantum cryptography possible. It is next useful to analytically consider POVM-type measurements of photonic qubits.

III. PHOTONIC IMPLEMENTATION OF A POVM

Because of the noncommutativity of nonorthogonal photon polarization projective measurement operators, a simple von Neumann-type projective measurement cannot conclusively distinguish the state of a photon having two possible nonorthogonal polarization states. If one wants to be able to distinguish conclusively between two nonorthogonal photon states $|u\rangle$ and $|v\rangle$ at least some of the time, it is useful to consider a POVM used in quantum cryptography.[1,18,19] This POVM consists of the following set of three non-negative Hermitian operators:

$$A_u=(1+\langle u|v\rangle)^{-1}[1-M(v,v)], \quad (28)$$

$$A_v=(1+\langle u|v\rangle)^{-1}[1-M(u,u)], \quad (29)$$

$$A_?=1-A_u-A_v, \quad (30)$$

in which kets $|u\rangle$ and $|v\rangle$ represent nonorthogonal single photon states, and the definition in Eq. (13) is employed. The POVM operators, Eqs. (28)–(30), clearly satisfy Eq. (1). Specifically in Ref. 19 and in the present work, the states $|u\rangle$ and $|v\rangle$ are taken to be linear-polarization states, as in Sec. II, with the Dirac bracket $\langle u|v\rangle$ given by Eq. (11). A general qubit state is given by Eq. (3). From Eqs. (28)–(30), (13), and (11), it follows that the operators (28)–(30) are all Hermitian; however, they are not projection operators, since the product of any one of them with itself does not yield itself. Also, for nonorthogonal states they do not commute:

$$\begin{aligned}[A_u,A_v]&=[A_?,A_u]\\&=[A_v,A_?]\\&=\tfrac{1}{4}\cos\theta\sec^4(\theta/2)[M(u,v)^{\dagger}-M(u,v)]. \quad (31)\end{aligned}$$

It then follows that minimum uncertainty products are associated with the measurement of these operators.

The probability that an arbitrary qubit $|\psi\rangle$ given by Eq. (3) is measured to be in the u-polarization state can be calculated with Eqs. (2), (3), (11), (13), and (28); the calculation yields

$$P_u=\langle\psi|A_u|\psi\rangle=|\alpha|^2(1-\cos\theta). \quad (32)$$

The first equality holds, since for a pure state $|\psi\rangle$, the trace of the operator A_μ with the density matrix $|\psi\rangle\langle\psi|$ reduces to the expectation value $\langle\psi|A_\mu|\psi\rangle$. One sees clearly that A_u is a positive operator, as it must be. This follows since $|\psi\rangle$ can represent any state in the two-dimensional Hilbert space of states, and the right-hand side of Eq. (32) is non-negative. This must be the case since P_u is a probability. Analogously, one obtains

$$P_v=\langle\psi|A_v|\psi\rangle=|\beta|^2(1-\cos\theta), \quad (33)$$

and

$$P_?=\langle\psi|A_?|\psi\rangle=|\alpha+\beta|^2\cos\theta, \quad (34)$$

both of which are also clearly non-negative. In Eq. (33), the qubit is measured to be in the state $|v\rangle$. In Eq. (34), $P_?$ is the probability of an inconclusive measurement, meaning that it is undecided whether the qubit is in state $|u\rangle$ or $|v\rangle$.[1,18,19] In the special case that the coefficients α and β are real, Eqs. (32)–(34) agree with Refs. 18 and 19. The present work addresses the more general case, in which α and β are complex, as in Ref. 26. If the state $|\psi\rangle$, Eq. (3), is normalized to unity, then

$$1=\langle\psi|\psi\rangle=|\alpha|^2+(\alpha^*\beta+\alpha\beta^*)\cos\theta+|\beta|^2, \quad (35)$$

and it then follows from Eqs. (32) to (35) that the probabilities sum to unity, as they must:

$$P_u+P_v+P_?=1. \quad (36)$$

When the incident photon is in the state $|u\rangle$, one has $(\alpha,\beta)=(1,0)$, and Eq. (33) becomes $\langle u|A_v|u\rangle=0$. When the incident photon is in the state $|v\rangle$, one has $(\alpha,\beta)=(0,1)$, and Eq. (32) becomes $\langle v|A_u|v\rangle=0$. Therefore, when an ideal detector representing the operator A_u responds positively, it

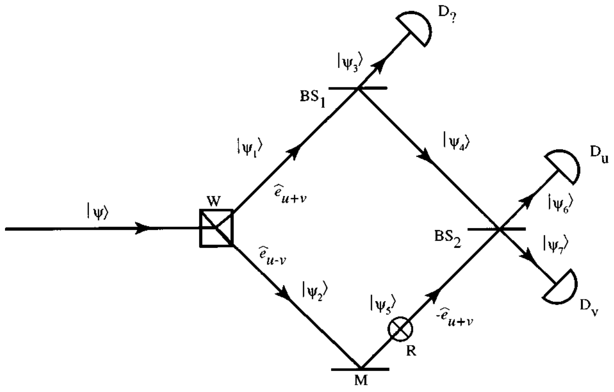

Fig. 1. POVM implementation.

follows that a photon with a v-polarization state cannot have been received. Likewise, when an ideal detector representing the operator A_v responds, a photon with a u-polarization state cannot have been received. The operator $A_?$ represents inconclusive responses, since Eq. (34) is nonvanishing for $(\alpha,\beta)=(0,1)$ or (1, 0). Thus a u-polarized photon can result in a nonzero expectation value (and the associated response) only for detectors representing the A_u or $A_?$ operators. A v-polarized photon excites only the A_v or $A_?$ detectors. It follows that the POVM of Eqs. (28)–(30) distinguishes conclusively between two nonorthogonal states $|u\rangle$ and $|v\rangle$ at least some of the time.

The recently proposed all-optical implementation of this POVM is shown schematically in Fig. 1.[19,25,26] The straight lines with arrows represent possible optical pathways for a photon to move through the device. The path labeled $|\psi\rangle$ is the incoming path for a photonic qubit represented by an arbitrary polarization state given by Eq. (3). Also in Fig. 1, D_u, D_v, and $\mathrm{D}_?$ designate photodetectors representing the measurement operators A_u, A_v, and $A_?$, respectively. Shown also is a Wollaston prism W, which is aligned so that an incident photon with polarization vector $\hat{e}_{u+v}$ takes the path labeled by the state $|\psi_1\rangle$ and $\hat{e}_{u+v}$, and not the path labeled by the polarization vector $\hat{e}_{u-v}$ and the state $|\psi_2\rangle$. Here $\hat{e}_{u+v}$ denotes a unit polarization vector corresponding to polarization state $|u+v\rangle=|u\rangle+|v\rangle$, and is perpendicular to the unit polarization vector $\hat{e}_{u-v}$ corresponding to the polarization state $|u-v\rangle=|u\rangle-|v\rangle$. It follows from Eq. (11) that the states $|u+v\rangle$ and $|u-v\rangle$ are orthogonal, namely,

$$\langle u+v|u-v\rangle=0. \tag{37}$$

Also, clearly

$$\hat{e}_{u+v}\cdot\hat{e}_{u-v}=0, \tag{38}$$

which is consistent with Eqs. (37) and (11). In accordance with the property of a Wollaston prism in separating orthogonal polarization states, an incident photon with polarization vector $\hat{e}_{u-v}$ takes the path labeled by the state $|\psi_2\rangle$. The device also has two beam splitters, designated by BS_1 and BS_2 in Fig. 1. Beam splitter BS_2 is a 50/50 beam splitter for a photon entering either of its entrance ports. Both paths from the Wollaston prism to the beam splitter BS_2 have equal optical path lengths. The transmission and reflection coefficients of beam splitter BS_1 are specified below. Also shown in Fig. 1 is a 90° polarization rotator designated by R, which transforms a photon with polarization vector $\hat{e}_{u-v}$ into one with polarization vector $-\hat{e}_{u+v}$. There is also a single mirror M, as shown in Fig. 1. All optical elements are here taken to be ideal.

The state of a photon taking the path designated by the state $|\psi_1\rangle$ in Fig. 1 is given by

$$|\psi_1\rangle=|\hat{e}_{u+v}\rangle\langle\hat{e}_{u+v}|\psi\rangle, \tag{39}$$

where $|\hat{e}_{u+v}\rangle$ represents a unit ket corresponding to polarization vector $\hat{e}_{u+v}$. Clearly,

$$|\hat{e}_{u+v}\rangle=\frac{|u\rangle+|v\rangle}{[(\langle u|+\langle v|)(|u\rangle+|v\rangle)]^{1/2}}. \tag{40}$$

Substituting Eq. (40) in Eq. (39), and using Eqs. (3) and (11), one obtains

$$|\psi_1\rangle=2^{-1/2}(\alpha+\beta)(1+\cos\theta)^{1/2}|\hat{e}_{u+v}\rangle. \tag{41}$$

One also has

$$|\psi_2\rangle=|\hat{e}_{u-v}\rangle\langle\hat{e}_{u-v}|\psi\rangle, \tag{42}$$

where

$$|\hat{e}_{u-v}\rangle=\frac{|u\rangle-|v\rangle}{[(\langle u|-\langle v|)(|u\rangle-|v\rangle)]^{1/2}} \tag{43}$$

is a unit ket corresponding to polarization vector $\hat{e}_{u-v}$. Next, using Eqs. (42), (43), (3), and (11), one obtains

$$|\psi_2\rangle=2^{-1/2}(\alpha-\beta)(1-\cos\theta)^{1/2}|\hat{e}_{u-v}\rangle. \tag{44}$$

For ideal photodetectors D_u, D_v, and $\mathrm{D}_?$, it is evident from Fig. 1 and Eq. (2) that one must require

$$P_u=|\psi_6|^2=\langle\psi_6|\psi_6\rangle=\langle\psi|A_u|\psi\rangle, \tag{45}$$

$$P_v=|\psi_7|^2=\langle\psi_7|\psi_7\rangle=\langle\psi|A_v|\psi\rangle, \tag{46}$$

and

$$P_?=|\psi_3|^2=\langle\psi_3|\psi_3\rangle=\langle\psi|A_?|\psi\rangle, \tag{47}$$

respectively, in order that the expectation values of A_u, A_v, and $A_?$, measured by detectors D_u, D_v, and $\mathrm{D}_?$, respectively, equal the probabilities P_u, P_v, and $P_?$, respectively, that a photon is incident. From Eqs. (34) and (47), it follows that, up to an irrelevant phase factor, one has

$$|\psi_3\rangle=(\alpha+\beta)(\cos\theta)^{1/2}|\hat{e}_{u+v}\rangle. \tag{48}$$

For a *single* photon incident on the beam splitter BS_1, one can effectively ignore the unused vacuum port of the beam splitter (see Ref. 26 and also p. 9 of Ref. 17). The transmission coefficient T_1 of beam splitter BS_1 must then be given by

$$T_1=\frac{\langle\psi_3|\psi_3\rangle}{\langle\psi_1|\psi_1\rangle}. \tag{49}$$

Therefore, substituting Eqs. (48) and (41) in Eq. (49), one obtains

$$T_1=1-\tan^2(\theta/2). \tag{50}$$

The corresponding reflection coefficient R_1 is

$$R_1=1-T_1=\tan^2(\theta/2). \tag{51}$$

From Fig. 1, it is also evident that

$$\langle\psi_4|\psi_4\rangle=R_1\langle\psi_1|\psi_1\rangle; \tag{52}$$

substituting Eqs. (41) and (51) in Eq. (52), one obtains

$$\langle \psi_4 | \psi_4 \rangle = \tfrac{1}{2} | \alpha + \beta |^2 (1 - \cos \theta). \tag{53}$$

Since the reflection at BS_1 results in a $\pi/2$-phase shift,[38–40] resulting in a factor of $\exp(i\pi/2) = i$, it follows from Eq. (53) that

$$| \psi_4 \rangle = i 2^{-1/2} (\alpha + \beta)(1 - \cos \theta)^{1/2} | \hat{e}_{u+v} \rangle. \tag{54}$$

Since polarization rotator R converts polarization in the direction $\hat{e}_{u-v}$ into that in the direction $-\hat{e}_{u+v}$, it follows from Eq. (44) that

$$| \psi_5 \rangle = -2^{-1/2} (\alpha - \beta)(1 - \cos \theta)^{1/2} | \hat{e}_{u+v} \rangle. \tag{55}$$

Since the beam splitter BS_2 is a 50/50 beam splitter, its reflection coefficient is

$$R_2 = \tfrac{1}{2} \tag{56}$$

and its transmission coefficient is

$$T_2 = \tfrac{1}{2}. \tag{57}$$

It then follows that

$$| \psi_6 \rangle = 2^{-1/2} | \psi_5 \rangle + i 2^{-1/2} | \psi_4 \rangle, \tag{58}$$

and

$$| \psi_7 \rangle = 2^{-1/2} | \psi_4 \rangle + i 2^{-1/2} | \psi_5 \rangle. \tag{59}$$

Therefore, substituting Eqs. (54) and (55) in Eqs. (58) and (59), one obtains

$$| \psi_6 \rangle = -\alpha (1 - \cos \theta)^{1/2} | \hat{e}_{u+v} \rangle, \tag{60}$$

and

$$| \psi_7 \rangle = i \beta (1 - \cos \theta)^{1/2} | \hat{e}_{u+v} \rangle. \tag{61}$$

For an ideal detector, Eq. (45) holds, and by substituting Eq. (60), one gets

$$\langle \psi | A_u | \psi \rangle = | \alpha |^2 (1 - \cos \theta), \tag{62}$$

consistent with Eq. (32). Similarly, from Eqs. (46) and (61), it follows that

$$\langle \psi | A_v | \psi \rangle = | \beta |^2 (1 - \cos \theta), \tag{63}$$

consistent with Eq. (33). Thus one can conclude that the device depicted in Fig. 1 satisfies all the appropriate statistics, Eqs. (45)–(47), and is a faithful all-optical implementation of the POVM given by Eqs. (28)–(30).

IV. SUMMARY

In this work, the mathematics and history of the use of the positive operator valued measure have been briefly reviewed. Also, a general discussion of the quantum mechanics of photonic qubits has been presented using Schwinger's algebra of measurement. The noncommutativity of nonorthogonal photon-polarization measurement operators was demonstrated explicitly, and the associated uncertainty was calculated. Finally, a review was given of the quantum statistics of a recently discovered all-optical implementation of a POVM for measuring photonic qubits, showing that the device faithfully represents the POVM.

ACKNOWLEDGMENTS

This work was supported by the U.S. Army Research Laboratory. Useful communications with J. M. Myers, J. D. Franson, W. K. Wootters, S. J. Lomonaco, J. D. Murley, and M. Kruger are gratefully acknowledged.

APPENDIX A

An alternative all-optical implementation of the POVM of Eqs. (28)–(30) is briefly described here. It is conceptually simpler than the one emphasized in the present work, though it may be less practical. This implementation was originated by Wootters and Grossman.[29,30] In the Wootters–Grossman implementation, an incident linearly polarized photon in polarization state $|u\rangle$ or $|v\rangle$ is incident at Brewster's angle on the planar surface of a transparent dielectric material. The surface is oriented so that the plane of incidence of the incident photon bisects the angle between the two polarization vectors corresponding to states $|u\rangle$ and $|v\rangle$, respectively, so that the components of the polarization vectors in the plane of incidence are smaller than the perpendicular components. Then, according to Brewster's law, the polarization vector of a reflected photon must be perpendicular to the plane of incidence. Therefore the polarization vectors of state $|u'\rangle$ or $|v'\rangle$ of a refracted photon must have smaller components perpendicular to the plane of incidence, than did the incident photon. The index of refraction of the dielectric is chosen so that the polarization vectors of states $|u'\rangle$ and $|v'\rangle$ are orthogonal, and the two states can therefore be distinguished by a Wollaston prism. Ideal photodetectors located at the two output ports of the Wollaston prism measure the POVM operators A_u and A_v, and another ideal photodetector receiving a reflected photon measures the operator $A_?$.[29]

APPENDIX B

As an example of the use of Eq. (27), consider the product of the uncertainties in the measurement of nonorthogonal photon polarizations u and v for the following polarization state:

$$| \psi \rangle = \frac{|u\rangle + |v\rangle}{\left| |u\rangle + |v\rangle \right|}. \tag{B1}$$

This state has linear-polarization direction oriented symmetrically between the u and v polarization directions, since from Eqs. (11) and (B1), it follows that

$$\langle \psi | u \rangle = \langle \psi | v \rangle = \cos(\theta/2). \tag{B2}$$

Substituting Eqs. (13), (21), and (B2) in the right-hand side of Eq. (27), and simplifying by means of trigonometric identities, one obtains

$$(\langle \psi | (\Delta M(u,u))^2 | \psi \rangle)^{1/2} (\langle \psi | (\Delta M(v,v))^2 | \psi \rangle)^{1/2} \geqslant \tfrac{1}{4} \sin^2 \theta. \tag{B3}$$

Also, if one calculates the left-hand side of Eq. (27) directly, using Eqs. (B2), (13), and (26), one gets

$$(\langle \psi | (\Delta M(u,u))^2 | \psi \rangle)^{1/2} (\langle \psi | (\Delta M(v,v))^2 | \psi \rangle)^{1/2} = \tfrac{1}{4} \sin^2 \theta. \tag{B4}$$

Comparing Eqs. (27), (B3), and (B4), one concludes that the symmetrically oriented state, Eq. (B1), is a minimum uncertainty state, as might be expected. The uncertainty product, Eq. (B4), is seen to be greatest for $\theta = \pi/2$, and vanishing for

$\theta = 0$, as one might intuitively expect. It is also to be noted that in this example, the first term on the right-hand side of Eq. (27) is vanishing, since $\langle \psi | M(u,v) | \psi \rangle$ has no imaginary part. This term arises from the commutator in Eq. (25), so if one ignores the anticommutator and includes only the first term on the right-hand side of Eq. (25), as is frequently and erroneously done in the literature, one would not obtain the correct minimum uncertainty product.

[a] Electronic mail: hbrandt@lamp0.arl.army.mil

[1] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[2] J. M. Jauch and C. Piron, ''Generalized Localizability,'' Helv. Phys. Acta **40**, 559–570 (1967).
[3] S. K. Berberian, *Notes on Spectral Theory* (Van Nostrand, Princeton, 1966).
[4] M. A. Neumark, ''On a Representation of Additive Operator Set Functions,'' Dokl. Acad. Sci. URSS **41**, 359–361 (1943).
[5] B. Sz. Nagy, ''Extensions of Linear Transformations in Hilbert Space which Extend Beyond this Space,'' Appendix in F. Riesz and B. Sz. Nagy, *Functional Analysis* (Dover, New York, 1990).
[6] E. B. Davies and J. T. Lewis, ''An Operational Approach to Quantum Probability,'' Commun. Math. Phys. **17**, 239–260 (1970).
[7] E. B. Davies, *Quantum Theory of Open Systems* (Academic, New York, 1976).
[8] A. S. Holevo, ''An Analogue of the Theory of Statistical Decisions in Noncommutative Probability Theory,'' Trans. Moscow Math. Soc. **26**, 133–149 (1972).
[9] A. S. Holevo, ''Statistical Decision Theory for Quantum Systems,'' J. Multivariate Anal. **3**, 337–394 (1973).
[10] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[11] P. A. Benioff, ''Operator Valued Measures in Quantum Mechanics: Finite and Infinite Processes,'' J. Math. Phys. **13**, 231–242 (1972).
[12] P. A. Benioff, ''Decision Procedures in Quantum Mechanics,'' J. Math. Phys. **13**, 908–915 (1972).
[13] P. A. Benioff, ''Procedures in Quantum Mechanics without von Neumann's Projection Axiom,'' J. Math. Phys. **13**, 1347–1355 (1972).
[14] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[15] E. B. Davies, ''Information and Quantum Measurement,'' IEEE Trans. Inf. Theory **IT-24**, 596–599 (1978).
[16] P. Busch, P. J. Lathi, and P. Mittelstaedt, *The Quantum Theory of Measurement* (Springer, Berlin, 1996), 2nd ed.
[17] P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics* (Springer, Berlin, 1995).
[18] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, ''Eavesdropping on Quantum-Cryptographical Systems,'' Phys. Rev. A **50**, 1047–1056 (1994).
[19] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., ''Aspects of Entangled Translucent Eavesdropping in Quantum Cryptography,'' Phys. Rev. A **56**, 4456–4465 (1997); Erratum, **58**, 2617 (1998).
[20] C. A. Fuchs and A. Peres, ''Quantum-State Disturbance Versus Information Gain: Uncertainty Relations for Quantum Information,'' Phys. Rev. A **53**, 2038–2045 (1996).
[21] C. A. Fuchs, ''Information Gain vs State Disturbance in Quantum Theory,'' lanl e-print quant-ph/9611010 (1996).
[22] N. Lutkenhaus, ''Security Against Eavesdropping in Quantum Cryptography,'' Phys. Rev. A **54**, 97–111 (1996).
[23] C. A. Fuchs, ''Nonorthogonal Quantum States Maximize Classical Information Capacity,'' Phys. Rev. Lett. **79**, 1162–1165 (1997).
[24] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, ''Security of Quantum Key Distribution Against All Collective Attacks,'' lanl e-print quant-ph/9801022 (1998).
[25] H. E. Brandt and J. M. Myers, *Invention Disclosure: POVM Receiver for Quantum Cryptography* (U.S. Army Research Laboratory, Adelphi, MD, 1996).
[26] J. M. Myers and H. E. Brandt, ''Converting a Positive Operator-Valued Measure to a Design for a Measuring Instrument on the Laboratory Bench,'' Meas. Sci. Technol. **8**, 1222–1227 (1997).
[27] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, ''Unambiguous Quantum Measurement of Nonorthogonal States,'' Phys. Rev. A **54**, 3783–3789 (1996).
[28] C. H. Bennett, ''Quantum Cryptography Using Any Two Nonorthogonal States,'' Phys. Rev. Lett. **68**, 3121–3124 (1992).
[29] W. K. Wootters (private communication).
[30] J. Grossman, ''Realizing Generalized Quantum Measurements on the Polarization of Photons,'' Williams College senior thesis, 1996.
[31] N. Gisin, ''Hidden Quantum Nonlocality Revealed by Local Filters,'' Phys. Lett. A **210**, 151–156 (1996).
[32] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, ''Elementary Gates for Quantum Computation,'' Phys. Rev. A **52**, 3457–3467 (1995).
[33] J. Schwinger, *Quantum Kinematics and Dynamics* (Addison–Wesley, Redwood City, CA, 1991).
[34] J. Schwinger, ''Hermann Weyl and Quantum Kinematics,'' in *Exact Sciences and Their Philosophical Foundations* (Peter Lang, Frankfurt am Main, 1988), pp. 107–129.
[35] K. Gottfried, *Quantum Mechanics* (Benjamin, New York, 1966).
[36] W. K. Wootters, and W. H. Zurek, ''A Single Quantum Cannot be Cloned,'' Nature (London) **299**, 802–803 (1982).
[37] D. Dieks, ''Communication by EPR Devices,'' Phys. Lett. **92A**, 271–272 (1982).
[38] V. Degiorgio, ''Phase Shift Between the Transmitted and the Reflected Optical Fields of a Semireflecting Lossless Mirror is $\pi/2$,'' Am. J. Phys. **48**, 81–82 (1980).
[39] A. Zeilinger, ''General Properties of Lossless Beam Splitters in Interferometry,'' Am. J. Phys. **49**, 882–883 (1981).
[40] Z. Y. Ou and L. Mandel, ''Derivation of Reciprocity Relations for a Beam Splitter from Energy Balance,'' Am. J. Phys. **57**, 66–67 (1989).

NOT A NEUTRAL OR INNOCENT COMMODITY

Science is not a neutral or innocent commodity which can be employed as a convenience by people wishing to partake only of the West's material power. Rather it is spiritually corrosive, burning away ancient authorities and traditions. It cannot really co-exist with anything. Scientists inevitably take on the mantle of the wizards, sorcerers and witch-doctors. Their miracle cures are our spells, their experiments our rituals.

Bryan Appleyard, *Understanding the Present—Science and the Soul of Modern Man* (Pan Books, London, 1992), p. 9.