Choice of Measurement as the Signal

Amir Kalev

Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
Center for Quantum Information and Control, University of New Mexico, Albuquerque, New Mexico 87131-0001, USA

Ady Mann and Michael Revzen

Department of Physics, Technion—Israel Institute of Technology, Haifa 32000, Israel
(Received 5 April 2013; published 25 June 2013)

In classical mechanics, performing a measurement without reading the measurement outcome is equivalent to not exploiting the measurement at all. A nonselective measurement in the classical realm carries no information. Here we show that the situation is remarkably different when quantum mechanical systems are concerned. A nonselective measurement on one part of a maximally entangled pair can allow communication between two parties. In the proposed protocol, the signal is encoded in the *choice* of the measurement basis of one of the communicating parties, while the outcomes of the measurement are irrelevant for the communication and therefore may be discarded. Different choices for the (nonselective) measurement correspond to different signals. The implication of the study of measurements in quantum mechanics is considered. The scheme is studied in a Hilbert space of prime dimension.

DOI: 10.1103/PhysRevLett.110.260502 PACS numbers: 03.67.Hk, 03.65.Ta

An important distinction between classical and quantum measurement is that the latter implies an inevitable disturbance to the measured system. In the present work, we show that this disturbance is trackable to the extent that it may be used for communication. Thus we study nonselective measurements where the outcomes are not recorded. Such measurements within the classical theory do not carry information and hence cannot be used for communication [1,2]. Here we show how nonselective measurements on one part of a quantum system of a maximally entangled pair can be used to encode and eventually communicate information. In the proposed protocol the basis, i.e., the choice, of the (nonselective) measurement is the signal. The outcomes of the measurement are totally irrelevant. The trackable choice of measurement (rather than its outcome) analysis allows a novel interpretation of quantum measurements. Thus a quantum state does, in general [3–5], imply contextual values for measurable dynamical variables. Hence it is attractive to interpret our result as suggesting that quantum measurement is built up of two stages. The first stage, to be associated with the nonselective measurement, elevates a particular set of dynamical variables (those labeling the basis in our case) to reality (i.e., having a prescribed value). The state after this stage is, in general, mixed. The second stage involves the determination of the value of the dynamical variable. This stage has clear classical attributes.

Confining our study at the moment to a Hilbert space of odd prime dimension d, we consider as alternative choices for measurements the alternative mutual unbiased bases (MUB). For prime dimension there are $d+1$ MUB [6–12]. A possible set of $d+1$ MUB can be defined as follows. The first basis is the computational basis $\{|n\rangle\}_{n=0}^{d-1}$, composed of the d orthonormal eigenstates of the generalized Pauli operator $\hat{Z}$, $\hat{Z}|n\rangle = \omega^n|n\rangle$, $|n+d\rangle = |n\rangle$, $\omega = e^{i(2\pi/d)}$. The other d orthonormal bases are parametrized by $b = 0, 1, \ldots, d-1$. The kets that compose the d remaining bases are given in terms of the computational basis by [9]

$$|m;b\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle \omega^{bn^2-2nm}; \quad b, m = 0, 1, \ldots, d-1. \tag{1}$$

We shall designate the computational basis by $b = \ddot{0}$, and depending on the context we may also denote the kets of the computational basis $|m\rangle$ by $|m;\ddot{0}\rangle$. Thus, the $d+1$ bases are labeled by $b = \ddot{0}, 0, 1, \ldots, d-1$.

The proposed communication protocol is described in what follows. We assume that the two communicating parties, Alice and Bob, agree beforehand upon a code, associating messages with the parameters, b, specifying the MUB. There is no classical communication between Alice and Bob beyond this point. The protocol involves a two d-level system (qudit) entangled state prepared by Alice with one qudit available to Bob, who wishes to communicate a message, $b = \ddot{0}, 0, 1, \ldots, d-1$, to Alice. To this end, Bob measures the part of the system that is available to him in the basis parametrized with the b of his message. He must complete the measurement yet may ignore its outcome and then return the qudit to Alice. This step renders values to a class of dynamical variables: the complete set of commuting operators $(XZ^b)^n$; $n = 0, 1, \ldots, d-1$. Now Alice measures the two-qudit resultant state, deduces, almost always, the basis b used by Bob, and, hence, decodes the message. The procedure is quantal in that the signal corresponds to the basis of Bob's

measurement, that is, to the "alignment" of his instrument, and in that the measurement outcomes are irrelevant and may be unrecorded.

Choice of measurement basis as signal.—To establish a communication channel, let Alice prepare one of the following d^3 two-qudit maximally entangled states [13,14]:

$$|c, r; s\rangle_{1,2} = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle_1 |c - n\rangle_2 \omega^{sn^2 - 2rn}, \tag{2}$$

with c, r, $s = 0, 1, \ldots, d-1$, and send one of the qudits, say, the one labeled by 1, to Bob. We note that, for a given s value, these states form an orthonormal, maximally entangled, basis for the Hilbert space of the two qudits. Thus, s labels the basis, and c and r label the d^2 orthonormal states within a basis. The reduced state for Bob's qudit is the completely mixed state.

To communicate a message to Alice, Bob measures his qudit in one of the MUB labeled by $b = \ddot{0}, 0, 1, \ldots, d-1$. The message is his choice of the basis used for the measurement. Bob may or may not record the measurement outcome. This is of no relevance to the protocol. After completing his nonselective measurement, Bob sends the qudit back to Alice. The two-qudit state is described now by

$$\rho_{1,2} = \sum_{m=0}^{d-1} |m; b\rangle_1 \langle m; b| c, r; s\rangle_{1,2} \langle c, r; s| m; b\rangle_1 \langle m; b|. \tag{3}$$

We note in passing that making a nonselective measurement in basis b is equivalent to performing a random unitary transformation which is diagonal in the b basis [1]. To retrieve the message, Alice now measures the two qudits in the basis of preparation, $\{|c', r'; s\rangle_{1,2}\}_{c',r'=0}^{d-1}$ of Eq. (2). The probability to obtain an outcome which corresponds to the basis state $|c', r'; s\rangle_{1,2}$ is

$$\langle c', r'; s|\rho_{1,2}|c', r'; s\rangle_{1,2} = \frac{1}{d} \begin{cases} \delta_{c,c'} & \text{for } b = \ddot{0}, \\ \delta_{(b-s)c+r,(b-s)c'+r'} & \text{for } b = 0, 1, 2, \ldots, d-1. \end{cases} \tag{4}$$

The arithmetics is modulo d. According to the above equation, based on the outcome of her measurement, Alice can decode the message sent from Bob, that is, the basis of his measurement. If the outcome corresponds to a state $|c', r'; s\rangle_{1,2}$ with $c \neq c'$, Alice infers that $b = s + (r' - r)/(c - c')$. Since she knows the values of c, r, c', r', and s, she can calculate the message b. If, on the other hand, $c = c'$ and $r \neq r'$, Alice infers that $b = \ddot{0}$. The case of $c = c'$ and $r = r'$ is inconclusive for Alice. The inconclusive outcome occurs with probability $1/d$. In that case, the preparation state and the detection state of the two qudits is the same, and she does not gain any information about Bob's message. Hence the decoding table is

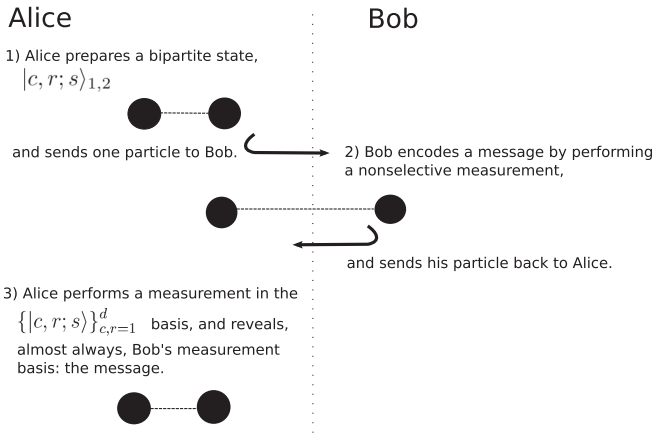

FIG. 1. The scheme of the communication protocol.

$$\begin{aligned} c \neq c' &\rightarrow b = s + \frac{r - r'}{c' - c}, \\ r \neq r',\ c = c' &\rightarrow b = \ddot{0}, \\ r = r',\ c = c' &\rightarrow \text{inconclusive.} \end{aligned} \tag{5}$$

For the even prime dimension $d = 2$, by plugging the imaginary unit i instead of ω in all of the above equations, one retrieves the same decoding table (5). The protocol is schematically drawn in Fig. 1.

Conclusions and remarks.—In conclusion, we showed how nonselective measurements in MUB on one part of an entangled pair could be used to encode information. The scheme uniquely utilizes quantum features of the system, since performing nonselective measurements on classical systems (no matter how correlated they are) cannot carry or manipulate information [1,2]. Alternatively, the trackability of the nonselective measurement allows a novel view of quantum measurement. Thus we may view a quantum measurement as a two-stage process. The first, to be associated with the nonselective part, involves the promotion of a set of dynamical variables (labeled, in our case, by the basis b) to reality (i.e., [5] having a definite value). After this stage, in general, the state is a mixed state. The second stage involves the determination of the outcome among these values. This stage allows a classical interpretation: The experiment determines a possible preassigned value. Dealing, as we do in this work, with an entangled state renders the stages separable: Bob's measurement (unknown to Alice) consummates a first stage *for the two-particle system*. The sequential measurement, by Alice, selects possible values of the two-particle system allowed by the (mixed) state that resulted from Bob's measurement.

In the considered protocol, by sending a qudit, Bob is able to transfer, on average, more than $\log_2 d$ bits of information to Alice. This is, in some respect, a form of dense coding. We note for comparison that superdense coding [15] achieves $2\log_2 d$ bits per qudit sent from Bob to Alice. However, in the superdense coding scheme specific unitary transformations are used for the encoding, while here nonselective measurements, or, equivalently, random unitary transformations, are utilized. Though, in its present form, the protocol cannot be used for secure communication, we leave it as an open question whether one could consider variations of the present protocol that would render it suitable for cryptography tasks. Preliminary study indicates that the proposed scheme can be generalized to encompass prime-powers dimensions. Finally, this protocol exemplifies how tasks which seem impossible by classical reasoning are realized in quantum systems.

A. K. thanks Professor B.-G. Englert for fruitful discussions and for his insightful comments. The Centre for Quantum Technologies is a Research Centre of Excellence funded by the Ministry of Education and by the National Research Foundation of Singapore. This research was supported in part by NSF Grant No. PHY-1212445.

[1] J. Schwinger, *Quantum Mechanics: Symbolism of Atomic Measurements*, edited by B.-G. Englert (Springer, Berlin, 2001).
[2] L. Diósi, *A Short Course in Quantum Information Theory*, Lecture Notes in Physics Vol. 827 (Springer, Berlin, 2011), 2nd ed.
[3] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).
[4] J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966).
[5] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990); Rev. Mod. Phys. **65**, 803 (1993).
[6] I. D. Ivanovic, J. Phys. A: Math. Gen. **14**, 3241 (1981).
[7] A. Vourdas, Rep. Math. Phys. **40**, 367 (1997).
[8] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[9] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[10] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, Phys. Rev. A **70**, 062101 (2004).
[11] A. Vourdas, Rep. Prog. Phys. **67**, 267 (2004).
[12] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, Int. J. Quantum. Inform. **08**, 535 (2010).
[13] M. Revzen, Phys. Rev. A **81**, 012113 (2010).
[14] M. Revzen, J. Phys. A: Math. Theor. **46**, 075303 (2013).
[15] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).