Extraction of information from a single quantum

G. S. Paraoanu
Low Temperature Laboratory, Aalto University, P.O. Box 15100, FI-00076 Aalto, Finland
(Received 23 February 2011; published 18 April 2011)

We investigate the possibility of performing quantum tomography on a single qubit with generalized partial measurements and the technique of measurement reversal. Using concepts from statistical decision theory, we prove that, somewhat surprisingly, no information can be obtained using this scheme. It is shown that, irrespective of the measurement technique used, extraction of information from single quanta is at odds with other general principles of quantum physics.

DOI: 10.1103/PhysRevA.83.044101 PACS number(s): 03.65.Wj, 03.65.Ud, 03.67.−a, 42.50.Dv

In a paper published 75 years ago [1], Einstein, Podolsky, and Rosen (EPR) formulated their famous criterion for elements of reality as follows: "if, without in any way disturbing a system, we can predict with certainty [...] the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity." Is the wave function of a single quantum system an element of reality? A positive answer would entitle the wave function to an "ontological" status, much like Schrödinger believed to be the case, and in contradiction with the "epistemological" role reserved by the standard Copenhagen interpretation. Clearly, to think about the wave function as real, we would have to be able to measure it on a single quantum system. The question of whether this is possible was first raised in the context of the so-called "protective" (weakly disturbing) measurements in the early 1990s, where it was answered in the negative [2]. The Copenhagen-school view of the wave function as a mere mathematical tool for calculating probabilities was saved.

However, protective measurements are not the only possibility. A different idea for measuring the wave function is to employ reversible positive-operator valued measure (POVM) measurements [3]. With the recent demonstration of reversibility of the so-called "partial measurements" in systems of phase qubits [4,5], this idea looks theoretically attractive and experimentally feasible. Here we explore this strategy and consider generalized partial measurements [6], which have the property that they can be probabilistically reversed for both results of the measurement. We then consider a series of measurements followed by reversals and we address the question of whether in this way it is possible to extract (with a certain success probability) any information about the qubit. We show by employing concepts from statistical decision theory that this cannot be done — all the information we get from the measurements is nullified by the very process of undoing them. Therefore, we cannot measure the wave function of a single quanta, and as such we are not entitled to regard it as an element of reality. We further connect this result to more general physical principles by examining the consequences of being able to perform quantum tomography on a single qubit for experiments such as EPR, quantum teleportation, quantum cloning, and quantum key distribution.

For consistency, we first briefly review the properties of generalized partial measurements [6] for a qubit in a basis with states $|0\rangle$ and $|1\rangle$. We define two measurement operators, M_m and $M_{\bar{m}}$, corresponding to measurement results m and $\bar{m}$, and parameterized by two real numbers p and q, $0 \leqslant p, q \leqslant 1$:

$$M_m = \sqrt{1-q}|0\rangle\langle 0| + \sqrt{1-p}|1\rangle\langle 1|, \tag{1}$$

$$M_{\bar{m}} = \sqrt{q}|0\rangle\langle 0| + \sqrt{p}|1\rangle\langle 1|, \tag{2}$$

which implement a POVM measurement with effects (elements) $E_m = M_m^\dagger M_m$ and $E_{\bar{m}} = M_{\bar{m}}^\dagger M_{\bar{m}}$ [7]. If the qubit is in an unknown pure state $|\psi\rangle$, the probability of obtaining the result m is $P_m = \langle\psi|E_m|\psi\rangle$, and the probability of obtaining the result $\bar{m}$ is $P_{\bar{m}} = \langle\psi|E_{\bar{m}}|\psi\rangle$. The state after the measurement is $|\psi_m\rangle = (1/\sqrt{P_m})M_m|\psi\rangle$ in the first case, and $|\psi_{\bar{m}}\rangle = (1/\sqrt{P_{\bar{m}}})M_{\bar{m}}|\psi\rangle$ in the second. The physical meaning of the parameters p and q is that of probabilities for a qubit in the state $|1\rangle$ respectively $|0\rangle$ to yield the result $\bar{m}$; in the case of Josephson-junction qubits, these can be directly related to switching-current probabilities [6,8].

Generalized partial measurements can be probabilistically reversed no matter which result, m or $\bar{m}$, occurs under a measurement. The reversal is nondeterministic (probabilistic) in the sense that in both cases the reversal operation can also fail. More precisely, if p and q are neither 0 or 1, the operators M_m and $M_{\bar{m}}$ can be inverted,

$$M_m^{-1} = \frac{1}{\sqrt{(1-p)(1-q)}} X M_m X, \tag{3}$$

$$M_{\bar{m}}^{-1} = \frac{1}{\sqrt{pq}} X M_{\bar{m}} X, \tag{4}$$

where X is the Pauli-X matrix. The process of reversal is schematically represented in Fig. 1. Either m or $\bar{m}$ is obtained after a measurement on $|\psi\rangle$. In the first case we apply X, measure, and if we obtain m then we can put the system back to the initial state $|\psi\rangle$ by applying another X gate. In the case of the second occurrence $\bar{m}$, we have a successful reversal only if we again get $\bar{m}$ when applying X followed by a measurement; then we apply one more X gate and the system goes back to the initial state. The probability of success is independent of the initial state in both situations. In the case of the upper path, the probability of obtaining the result m is P_m; this has to be multiplied by the (conditional) probability $P(m|m)$ of again getting the result m after application of the gate X, which is

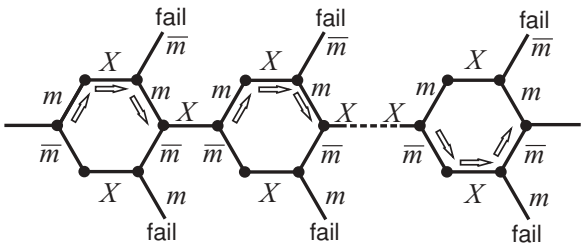

FIG. 1. Schematic of a series of generalized partial measurements and their reversal. The arrows indicate possible measurement-reversal paths actually occurring.

given by

$$\begin{aligned} P(m|m) &\overset{\text{def}}{=} \langle\psi_m|XM_m^\dagger M_m X|\psi_m\rangle \\ &= P_m^{-1}\langle\psi|M_m^\dagger X M_m^\dagger X X M_m X M_m|\psi\rangle \\ &= (1-p)(1-q)P_m^{-1}, \end{aligned} \tag{5}$$

where for the last equality we used Eq. (3). Therefore the total probability of success along the m path $|\psi\rangle \overset{m}{\to} |\psi\rangle$ is $P_{|\psi\rangle\overset{m}{\to}|\psi\rangle} = P(m|m)P_m = (1-p)(1-q)$. Similarly, for the $\bar{m}$ path $|\psi\rangle \overset{\bar{m}}{\to} |\psi\rangle$ we get

$$\begin{aligned} P(\bar{m}|\bar{m}) &\overset{\text{def}}{=} \langle\psi_m|XM_{\bar{m}}^\dagger M_{\bar{m}} X|\psi_{\bar{m}}\rangle \\ &= P_{\bar{m}}^{-1}\langle\psi|M_{\bar{m}}^\dagger X M_{\bar{m}}^\dagger X X M_{\bar{m}} X M_{\bar{m}}|\psi\rangle \\ &= pq\,P_{\bar{m}}^{-1}, \end{aligned} \tag{6}$$

where the last equality follows from Eq. (4). $P_{|\psi\rangle\overset{\bar{m}}{\to}|\psi\rangle} = P(\bar{m}|\bar{m})P_{\bar{m}} = pq$ is then the probability of success for the path $|\psi\rangle \overset{\bar{m}}{\to} |\psi\rangle$.

We are now ready to address the problem of information extraction from a single qubit. Let start by considering precisely such a process (see Fig. 1). At first sight it looks as if (with a certain probability of success) the unknown state of a single qubit can be determined by performing a series of measurements and reversing them. The probability of this happening is, admittedly, very small but still finite. Suppose we have a total of N successful reversals, out of which N_m occurred via the upper-half paths $|\psi\rangle \overset{m}{\to} |\psi\rangle$ of the hexagons in Fig. 1 and the other $N_{\bar{m}} = N - N_m$ occurred via the lower paths $|\psi\rangle \overset{\bar{m}}{\to} |\psi\rangle$. What we want is to estimate the state, that is, to find the two angles θ and φ parameterizing any state $|\psi\rangle = \cos(\theta/2)|0\rangle + \exp(i\varphi)\sin(\theta/2)|1\rangle$ of a two-level system. To do so we use the maximum-likelihood estimator technique from statistical decision theory [9]. We first notice that in the Bayesian sense, for both paths there exist conditional probabilities [$P(m|m)$ and $P(\bar{m}|\bar{m})$] and priors [P_m and $P_{\bar{m}}$]. Thus we have to define the so-called weighted likelihood,

$$L(N_m, N_{\bar{m}}) = [P_m]^{N_m}[P_{\bar{m}}]^{N_{\bar{m}}}[P(m|m)]^{N_m}[P(m|\bar{m})]^{N_{\bar{m}}}, \tag{7}$$

which is the total probability (obtained as a product of probabilities of each event) that the chain of nonfail events in Fig. 1 has occurred. As before, to simplify the notations we do not write explicitly the dependence on (θ,φ), but we keep in mind, as in standard decision theory, the likelihood that $L(N_m, N_{\bar{m}})$ is a probability density function on this two-parameter space. Then we should find the "maximum *a posteriori* (MAP) estimate" [9], which in our case is the pair (θ,φ) maximizing $L(N_m, N_{\bar{m}})$, or equivalently, $\ln L(N_m, N_{\bar{m}})$. The next step would be to study how sensitive our measurement method is to variations of (θ,φ) around their true value; this leads to the concept of Fisher information. But this standard procedure does not lead anywhere, and the reason is that $L(N_m, N_{\bar{m}})$ has in fact no dependence on (θ,φ). Indeed, this can be seen immediately by noticing that the exponent of both P_m and $P(m|m)$ [and $P_{\bar{m}}$ and $P(m|\bar{m})$, respectively] is the same. [We know that the reversing procedure has been successful each time the result m (respectively $\bar{m}$) has been obtained after a measurement, and by using Eqs. (5) and (6).] This means that it is not possible to get any information about the state by the chain of measurements depicted in Fig. 1.

How can this be? Where has the information about switching into m or $\bar{m}$ vanished? To understand what happens, let us take the logarithm of the weighted likelihood, which we call $-S = \ln L(N_m, N_{\bar{m}})$; we then obtain

$$S = S_{\text{meas}} + S_{\text{rev}} \tag{8}$$

where $S_{\text{meas}} = -N_m \ln P_m - N_{\bar{m}} \ln P_{\bar{m}}$ represents the Shannon information obtained from the measurements, and $S_{\text{rev}} = -N_m \ln P(m|m) - N_{\bar{m}} \ln P(m|\bar{m})$ is the Shannon information resulting from the reversals. But again, $P(m|m) = (1-p)(1-q)P_m^{-1}$ and $P(\bar{m}|\bar{m}) = pq\,P_{\bar{m}}^{-1}$, and in the asymptotic approximation of a large number of events, $N_m = (1-p)(1-q)N$ and $N_{\bar{m}} = pqN$; therefore we have $S = -N[pq\ln pq + (1-p)(1-q)\ln(1-p)(1-q)]$. What happens is that the information resulting from reversal cancels exactly the information obtained via measurement (up to a constant). The remaining part is independent of the parameters θ and φ, and thus, overall, the measurement procedure from Fig. 1 is completely insensitive to the state parameters. One recognizes also that S is the total conditional information (conditioned on the success of the reversal procedure) associated with the two paths, $S/N = -P_{|\psi\rangle\overset{m}{\to}|\psi\rangle} \ln P_{|\psi\rangle\overset{m}{\to}|\psi\rangle} - P_{|\psi\rangle\overset{\bar{m}}{\to}|\psi\rangle} \ln P_{|\psi\rangle\overset{\bar{m}}{\to}|\psi\rangle}$. At $p = q = 1/2$ this quantity reaches its maximum value of $\ln 2$. This entropy is all that remains after a chain of such events representing the physical records of a string of m's and $\bar{m}$'s (the information about which path the system actually took) that the experimentalist can write in the log notebook. The surprising fact is that although all the measurements have been performed on a qubit prepared in a certain state, there is no information left in the environment about this state. We also note that for the definition of standard estimation measures such as Fisher metric, all possible results need to be accessible. The sum of the corresponding probabilities is 1, and the information thus defined is positive. But here we eliminate by postselection the situations in which the scheme fails; therefore we have to use conditional information, which generally is not guaranteed to be positive. In our case, the part containing the (θ,φ) dependence is negative and exactly cancels S_{meas}. It simply has the meaning of an additional piece of information that logically contradicts some already-acquired knowledge. Finally, one can legitimately ask, what if we simply ignore the information coming from reversal? For example, in Eq. (7) what if we write only the first two terms? The answer is that it can be done but at one's own peril. Then the value of θ obtained has no connection with

the real one, and the procedure is in no way better than just guessing.

Finally, we point out that all the results derived above can be immediately generalized for any number of effects (although a simple physical implementation of such a measurement is not obvious). Define the measurement operators as $M_k = \sqrt{q_k}|0\rangle\langle 0| + \sqrt{p_k}|0\rangle\langle 0|$ and the corresponding effects $E_k = M_k^\dagger M_k$, such that $\sum_k q_k = \sum_k p_k = 1$, therefore ensuring that $\sum_k E_k = I$. If none of the q_k's and p_k's are zero, then for each result k the measurement operator admits an inverse $M_k^{-1} = (p_k q_k)^{-1/2} X M_k X$. Then in Fig. 1 we can have more than two paths (each indexed by k). The weighted likelihood Eq. (7) can be immediately generalized to this situation, and the proof of information cancellation along each path k is similar.

We are now ready to address the following issue. Is the impossibility result above specific to the measurement scheme we have described, or do there exist more general physical principles from which it can be derived? In the following we discuss the relation between extraction of information from single quanta and the complementarity principle, the no-signaling principle, quantum teleportation, the no-cloning theorem, and quantum cryptography.

Take first the complementarity principle. Instead of using in Eqs. (1) and (2) the basis $\{|0\rangle, |1\rangle\}$ (the eigenvectors of the Pauli-Z operator) one can equally well use any other basis. For example, the elements of the basis $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are eigenvectors of the Pauli-X operator. It is perfectly possible to have a series of measurements and reversals along Z, followed by a similar series along X. Still, it is not possible to claim that this is a joint measurement of two complementary observables, so no obvious contradiction is obtained.

Let us turn now to the EPR experiment. Suppose we have a maximally entangled Bell state between Alice's and Bob's qubits, $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$. Applying M_m or $M_{\bar{m}}$ on Alice's qubit results in $(1/\sqrt{2-p-q})[\sqrt{1-q}|00\rangle + \sqrt{1-p}|11\rangle]$ or in $(1/\sqrt{p+q})[\sqrt{p}|00\rangle + \sqrt{q}|11\rangle]$, which have concurrence [10] $2\sqrt{(1-p)(1-q)}/(2-p-q)$ and $2\sqrt{pq}/(p+q)$, respectively. Both of these quantities are strictly smaller than 1 if $p \neq q$. Suppose now that we have obtained m for the measurement on Alice's qubit. If p is close enough to 1 and $q \neq 1$, to a satisfactory good approximation we can claim that the state of Bob's qubit is $|0\rangle$. Now we reverse the measurement (because p is large, the probability for succeeding is small but not zero). The interesting thing that happens in this case is that we have restored the state $|\Phi^+\rangle$, i.e., we managed to create a maximally entangled state from a state with almost zero entanglement. Thus partial measurements and their generalizations can be used to amplify entanglement! Furthermore, we can now perform a projective measurement in the $|\pm\rangle$ basis on Alice's qubit, which leaves Bob's qubit in the same state $|+\rangle$ if Alice got + or $|-\rangle$ if Alice got –. It seems now that Alice can predict the values of the two noncommuting observables Z and X (the first to a controllable degree of approximation, the second exactly) of Bob's qubit! Unlike in the original EPR argument where two sets of qubits are required for the argument, here this is achieved using only one pair.

Another important observation is that if it were possible to determine the state of a single quantum object, the EPR pair could be used to signal faster than light. Alice could encode information as a direction in space and perform a von Neumann measurement along it. Bob is then left with a qubit oriented along the same direction, and he can determine this state by using the measurement-and-reversal procedure. By *reductio ad absurdum*, extracting information from a single object is not possible.

Finally, let us consider the case of quantum teleportation. We show that if it were possible to extract information from a single quantum object, then this scheme would allow for remote cloning of a state using just two bits of information. This time, Alice has two qubits, the first in the unknown state $|\psi\rangle = \cos(\theta/2)|0\rangle + \exp(i\varphi)\sin(\theta/2)|1\rangle$, and the second entangled with Bob's only qubit, in a Bell state $|\Phi^+\rangle$. Then Alice performs a controlled-NOT (CNOT) gate (on her second qubit conditioned on the first) followed by a Hadamard gate on the first qubit [7]. The result of this is

$$|\psi\rangle|\Phi^+\rangle \to \tfrac{1}{2}[|00\rangle|\psi\rangle + |01\rangle X|\psi\rangle + |10\rangle Z|\psi\rangle + |11\rangle XZ|\psi\rangle]. \quad (9)$$

Suppose now that Alice is doing partial measurements on her qubits with strengths $q = 0$ and p close to 1, and the result of both measurements is m. Alice informs Bob about this, and Bob would be able to do a single-qubit partial-measurement tomography, which allows him to determine (within a certain degree of approximation and a lot of good luck) the state of his qubit. Note that a large amount of information can be encoded in the variables θ, φ (depending on the precision we want) and that it took 2 bits of classical communication for Bob to be able to "decode" it. Moreover, even if only one bit of information can be communicated (corresponding to a measurement by Alice of her second qubit), Bob could still determine with arbitrary precision the value of θ! From Eq. (9) it follows immediately that if Alice obtains 0, the resulting state is $\cos(\theta/2)|+\rangle|0\rangle + \exp(i\varphi)\sin(\theta/2)|-\rangle|1\rangle$, while if she gets 1 the resulting state is $\cos(\theta/2)|+\rangle|1\rangle + \exp(i\varphi)\sin(\theta/2)|-\rangle|0\rangle$. Bob now measures his probabilities of obtaining 0 and 1 and he uses the classically transmitted bit of information to decide which one of these probabilities to associate with the amplitudes $\cos(\theta/2)$ and $\exp(i\varphi)\sin(\theta/2)$. Moreover, Alice can also in principle recover her state exactly. As a result, Bob ends up again with a qubit maximally entangled with Alice's second qubit, but also with some classical information about the qubit which in principle could allow him to build another qubit in approximately the same state. Note that this procedure would not contradict directly the no-cloning theorem (which is proved using only unitary transformations), and it would allow us to build a relatively simple probabilistic cloning machine. However, it is still forbidden by quantum mechanics, as we have shown above; to get any true information, one needs to have an ensemble. Somehow, quantum physics does not like to provide all the information at once. Much like a hero in a treasure-hunting novel, Bob gets one little clue at a time (each time he measures an element of the ensemble).

Let us now examine the problem of quantum key distribution. We want to show that if extracting information from a single qubit were possible, this would provide a hacking strategy for quantum key distribution protocols. Take, for example, the Bennett 1992 protocol [7]. Alice generates a random string

$\{a\} = \{0,1\}$ of classical bits, and if $a = 0$ she sends the qubit $|0\rangle$ to Bob, while if $a = 1$ she sends $|+\rangle$. Bob generates his own random classical bits $\{a'\}$ and measures Z on the qubit sent by Alice if $a' = 0$ (in which case he obtains the result –1 only if $a = 1$) or X if $a' = 1$ (in which case he obtains the result –1 only if $a = 0$). After discussing over a classical channel, Alice and Bob keep only the qubits for which the result –1 has been obtained. The corresponding classical bits $\{a\}$ and $\{a'\}$ will be anticorrelated $a = 1 - a'$ and a shared secret key is obtained. If, however, Eve intercepts the qubit, she could perform an approximate partial-measurement quantum tomography. If she fails, she does nothing and Bob will interpret the result as the qubit being lost in the communication channel; if she succeeds, she learns approximately the state of the qubit (the value of a) and she can forward the qubit to Bob. Together with the value of Bob's result (which is publicly broadcasted), she could infer the value of a', that is, she would find the key shared by Alice and Bob without any of them noticing.

Finally, if there is no element of reality for *wave functions*, perhaps there could be one for *entanglement* [11]? Suppose we are interested in two-qubit systems and we use an ancilla as a probe. If instead of an ensemble we have just two qubits, can we measure their entanglement? The results above show that the answer is negative. One still has to erase all the classical information in order to reverse the measurements.

In conclusion, we proved that it is not possible to extract even probabilistically any information from a single qubit prepared in an unknown state by using a generalized version of partial measurements. We also examine how this result is connected to general principles such as no-signaling, no-cloning, complementarity, the possibility of quantum teleportation, and the security of quantum key distribution.

Financial support from the Academy of Finland is acknowledged (Grant No. 00857, and Projects No. 129896, No. 118122, and No. 135135).

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] Y. Aharonov and L. Vaidman, Phys. Lett. A **178**, 38 (1993); Y. Aharonov, J. S. Anandan, and L. Vaidman, Phys. Rev. A **47**, 4616 (1993); Found. Phys. **26**, 117 (1996); O. Alter and Y. Yamamoto, Phys. Rev. Lett. **74**, 4106 (1995); J. Aharonov, J. Anandan, and L. Vaidman, Found. Phys. **26**, 117 (1996); G. M. D'Ariano and H. P. Yuen, Phys. Rev. Lett. **76**, 2832 (1996); J. Uffink, Phys. Rev. A **60**, 3474 (1999).

[3] M. Ueda and M. Kitagawa, Phys. Rev. Lett. **68**, 3424 (1992); A. Imamoglu, Phys. Rev. A **47**, R4577 (1993); A. Royer, Phys. Rev. Lett. **73**, 913 (1994); **74**, 1040 (1995); M. Ueda, N. Imoto, and H. Nagaoka, Phys. Rev. A **53**, 3808 (1996); H. Mabuchi and P. Zoller, Phys. Rev. Lett. **76**, 3108 (1996); M. A. Nielsen and C. M. Caves, Phys. Rev. A **55**, 2547 (1997).

[4] G. S. Paraoanu, Phys. Rev. Lett. **97**, 180406 (2006); N. Katz *et al.*, Science **312**, 1498 (2006).

[5] A. N. Korotkov and A. N. Jordan, Phys. Rev. Lett. **97**, 166805 (2006); N. Katz *et al.*, *ibid.* **101**, 200401 (2008); A. N. Korotkov and A. N. Jordan, Contemp. Phys. **51**, 125 (2010); G. S. Paraoanu, *Partial Measurements and the Realization of Quantum-Mechanical Counterfactuals*, Found. Phys. advanced online publishing.

[6] G. S. Paraoanu, Europhys. Lett. **93**, 64002 (2011).

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[8] G. S. Paraoanu, Phys. Rev. B **72**, 134528 (2005); J. Low Temp. Phys. **146**, 263 (2007).

[9] M. DeGroot, *Optimal Statistical Decisions* (New York, McGraw-Hill, 1970); H. W. Sorenson, *Parameter Estimation: Principles and Problems* (New York, Marcel Dekker, 1980); B. R. Frieden, *Physics from Fisher Information: A Unification* (Cambridge University Press, 1998).

[10] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998); S. Hill and W. K. Wootters, *ibid.* **78**, 5022 (1997).

[11] G. Krenn and A. Zeilinger, Phys. Rev. A **54**, 1793 (1996).