Journal of Modern Optics
Vol. 00, No. 00, DD Month 200x, 1–8

Random qubit-states and how best to measure them

Stephen M. Barnett *

Department of Physics, SUPA, University of Strathclyde, Glasgow G4 0NG, UK

(February 2009)

We consider the problem of measuring a single qubit, known to have been prepared in either a randomly selected pure state or a randomly selected real pure state. We seek the measurements that provide either the best estimate of the state prepared or maximize the accessible information. Surprisingly, any sensible measurement turns out to be optimal.

1 Introduction

The state of a quantum system is not an observable. Given a large number of copies of the system of interest we can obtain a good estimation of the state [1], but it is not possible to determine the state given only a single copy.[1] Fundamentally, we can understand this limitation as a manifestation of complementarity, that is, the existence of incompatible observables. It is this limitation, moreover, that underlies the security of quantum key distribution [3–6] and gives quantum communications theory its distinctive character [3,6–8]. In a quantum communication system, we typically only have a single copy of each state and the receiving party is faced with the task of determining, as well as possible, the state originally prepared. This difficult task is usually made simpler by prior knowledge in the form of a set of possible states and associated probabilities for each of them. Quantum communications is, of course, is an important motivation for the study of quantum state discrimination [6, 9, 10].

The quality of the measurement strategy may be measured by reference to a variety of figures of merit. Amongst those most commonly employed are state discrimination with minimum probability of error or minimum Bayes cost [11, 12], unambiguous state discrimination [13–15], and maximizing the accessible information [16–18]. We may also be interested in the measurement that allows us to prepare a state most likely to pass as the original, which leads us to maximize the fidelity [19], or to maximize our confidence in the state identified by our measurement [20]. A number of these optimal detection strategies have been realized in experiments using optical polarization [21–26].

In this paper we consider the problem of measuring a single qubit, or a string of such qubits, about which we have only a bare minimum of information. We consider, in particular, how best to measure a qubit prepared in a pure state randomly selected either from all possible states or from all the real states. These sets of states correspond, respectively, to a uniform probability distribution of states over the whole surface of the Bloch sphere, and a uniform probability distribution on a single great circle on the Bloch sphere. The minimum-error figure of merit is not applicable in this case; the set of states is continuous and therefore the error probability is always unity. Similarly, the maximum confidence, that is the greatest probability for correctly identifying the state, is necessarily zero, and there is no strategy for unambiguous discrimination between the states. It is possible, however, to maximize the fidelity and the accessible information. In each case, we find that any sensible measurement strategy is optimal.

*Corresponding author. Email: steve@phys.strath.ac.uk

[1] It is possible, however, to obtain estimates of each of a number of properties, but this gives, at best only some indication of the state [2].

Journal of Modern Optics
ISSN 0950-0340 print/ISSN 1362-3044 online
http://www.tandf.co.uk/journals
DOI: 10.1080/0950034YYxxxxxxxx

2 Random states

A random state may be defined as a pure state about which we have no information [27]. For a single qubit, we can write any pure state in the form

$$|\theta,\phi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are a conveniently chosen pair of orthonomal states. With this parameterization, we can associate each of these states with the corresponding point on the surface of the Bloch sphere, with spherical polar coordinates θ, ϕ [6]. The a priori density operator for a random qubit-state is the maximally mixed state

$$\hat{\rho} = \frac{1}{2}\hat{\mathbb{I}}, \tag{2}$$

where $\hat{\mathbb{I}}$ is the identity operator. This operator allows us to make predictions for the results of any measurement we might perform, but it does not allow us to specify the ensemble of pure states prepared [3,28,29].

We specify, as random states, two possible ensembles; the set of all possible states, which we denote by the subscript A and the set of all real states, which we denote by the subscript R. The real states, (sometimes called 'rebits' [30]) are the states (1) for which $\phi = 0$ or π, so that they are real in the $|0\rangle$, $|1\rangle$ basis. Our ensembles may conveniently be expressed as a probability density on the surface of the Bloch sphere. For the random ensemble of all states we find the uniform probability density[1]

$$\mathcal{P}_A(\theta,\phi) = \frac{1}{4\pi}, \qquad 0 \le \theta < \pi \;\; 0 \le \phi < 2\pi, \tag{3}$$

so that the density operator is [33]

$$\hat{\rho}_A = \int_0^{2\pi} d\phi \int_0^{\pi} \sin\theta \, d\theta \, \frac{1}{4\pi} |\theta,\phi\rangle\langle\theta,\phi| = \frac{1}{2}\hat{\mathbb{I}}. \tag{4}$$

For the random ensemble of real states we have the probability density

$$\mathcal{P}_R(\theta,\phi) = \frac{1}{2\pi}, \qquad 0 \le \theta < 2\pi. \tag{5}$$

Note that we have extended the range of θ to include a full rotation of 2π radians. The density operator associated with this probability density is

$$\hat{\rho}_R = \int_0^{2\pi} d\theta \, \frac{1}{2\pi} |\theta\rangle\langle\theta| = \frac{1}{2}\hat{\mathbb{I}}, \tag{6}$$

where $|\theta\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)|1\rangle$ are the real states. Note that we can identify our set of real states with those lying on any great circle on the Bloch sphere by suitably redefining our basis states $|0\rangle$ and $|1\rangle$.

The task that faces us is to determine, on the basis of a measurement, something about the state that was selected. This means either estimating the state by chosing values for θ and/or ϕ, or extracting as much information as possible. In order to find the optimum measurement, we need to consider all possible measurements and this means including the possibility of generalized measurements.

[1] It is interesting to note that we can derive this distribution using a Bayesian analysis [31]. The maximum entropy method naturally gives this isotropic distribution if we define the set of states as the isotropic limit of a suitable discrete set [32].

3 Generalized measurements

It is well-known that the measurements associated with the orthnormal eigenstates of Hermitian operators do not represent the most general possible measurement. Indeed, it is often the case that the best measurement in any given situation will be a generalized measurement. Such measurements are described, mathematically by a probability operator measure (POM) [6, 11] also called a positive operator valued measure (POVM) [34]. This associates a probability operator $\hat{\pi}_k$ with each possible measurement outcome k, in that the probability for this result to occur is the expectation value of $\hat{\pi}_k$. The probability operators are constrained only by the conditions that (i) they are Hermitian, (ii) they are positive and (iii) they sum to the identity [6]

$$\sum_k \hat{\pi}_k = \hat{\mathbb{I}}. \tag{7}$$

Any operators that satisify these conditions will correspond to a realizable measurement and any measurement can be described in this way.

It sufficies, for our purposes, to consider only probability operators that are proportional to pure-state projectors. Probability operators that are proportional to mixed-state density operators will not provide optimal measurements and so are not considered. This means that we can write our probability operators in the form

$$\hat{\pi}_k = |\pi_k\rangle\langle\pi_k|, \tag{8}$$

where the $|\pi_k\rangle$ are, in general, unnormalized states, which we write in the form

$$|\pi_k\rangle = a_k|0\rangle + b_k|1\rangle. \tag{9}$$

Writing the probability operators in this form guarantees the first two required properties (Hermiticity and positivity). The final condition (7) will be satified if we impose the conditions

$$\begin{aligned} \sum_k |a_k|^2 &= 1 = \sum_k |a_k|^2 \\ \sum_k a_k^* b_k &= 1 = \sum_k a_k b_k^*. \end{aligned} \tag{10}$$

We can find the optimum measurement in any given situtation by varying the probability operators subject to these constraints.

4 Fidelity and state estimation

Our first figure of merit determines how well our measurement allows us to approximate the state. To motivate the idea, let us suppose that we are given a qubit and, on the basis of a measurement, asked to prepare a second qubit in the same state. A quantitative measure of our success in performing this task is the fidelity [19].

4.1 *All states*

Let us start by considering the effect of a generalized measurement on a qubit from the random ensemble of all states. Our measurement will give an answer k associated with one of the probability operators $\hat{\pi}_k$. The isotropy of $\mathcal{P}_A(\theta, \phi)$ means that the only sensible and unbiased estimate for the premeasurement state

is the (normalized) state $|\tilde{\pi}_k\rangle = |\pi_k\rangle/\langle\pi_k|\pi_k\rangle^{1/2}$ and this must be our estimate of the single-qubit state. The probability that our estimated state will pass as the original, if the state prepared was $|\theta,\phi\rangle$, is

$$\begin{aligned} P(\text{pass}|\theta,\phi) &= \sum_k |\langle\tilde{\pi}_k|\theta,\phi\rangle|^2 |\langle\pi_k|\theta,\phi\rangle|^2 \\ &= \sum_k \frac{|\langle\pi_k|\theta,\phi\rangle|^4}{\langle\pi_k|\pi_k\rangle}. \end{aligned} \tag{11}$$

Averaging this quantity over the initial random distribution of states (3) gives the fidelity for the measurement of the random states coverying all of the Bloch sphere [35, 36]:

$$\begin{aligned} F_A &= \int_0^{2\pi} d\phi \int_0^{\pi} \sin\theta \, d\theta \, \frac{1}{4\pi} \sum_k \frac{|\langle\pi_k|\theta,\phi\rangle|^4}{\langle\pi_k|\pi_k\rangle} \\ &= \frac{2}{3}, \end{aligned} \tag{12}$$

where we have used the conditions (10). This value is completely independent of the choice of measurement, as encoded in the coefficients a_k and b_k, and hence any measurement will provide an optimal estimation of the initial state. On average, and for any measurement we might perform, the state that we prepare will be twice as likely to pass as the orignal state as it is to fail to pass.

4.2 *Real states*

For the real states it is both reasonable and rigorously optimal to consider only those generalized measurements that correspond to states $|\pi_k\rangle$ that are themselves real. This means restricting ourselves to states of the form (8) for which the coefficients a_k and b_k are real. The conditions (10) remain in force, and it necessarily follows that these coeffcients will take both positive and negative values. The isotropy of the ensemble of real states (on the associated great circle) means that the only sensible estimate for the premeasurement state is is that associated with the measurement outcome. The probability that this estimated state will pass as the original, if the state prepared was $|\theta\rangle$, is

$$P(\text{pass}|\theta) = \sum_k \frac{|\langle\pi_k|\theta\rangle|^4}{\langle\pi_k|\pi_k\rangle}. \tag{13}$$

Averaging this quantity over the initial random distribution (5) gives the fidelity for the real states

$$\begin{aligned} F_R &= \int_0^{2\pi} d\theta \, \frac{1}{2\pi} \sum_k \frac{|\langle\pi_k|\theta,\phi\rangle|^4}{\langle\pi_k|\pi_k\rangle} \\ &= \frac{3}{4}. \end{aligned} \tag{14}$$

As with the random ensemble of all states, we find a result which is independent of the choice of measurement provided, of course, that we make the sensible choice and restrict ourselves to real measurement states $|\pi_k\rangle$. The fidelity is larger than F_A and corresponds to preparing a state that will pass as the orginal three times as often as it will fail to pass. That a higher fidelity is possible, in this case, is a consequence of the additional information contained in the statement that the state was real.

5 Accessible information

The maximum rate at which information can be transmitted through a communication channel is limited, through Shannon's noieless coding theory, by the mutual information, the maximum value of which is the channel capacity [37]. Let us consider communications based on a string of qubits in which each is independently selected either from our ensemble of all qubits states or all of the real qubit states. We note that the former has been suggested for use in quantum key distribution [38, 39]. The channel capacity is found by varying both the detection strategy and the preparation probabilities for each of the possible states. For us, the preparation probabilities are fixed to be those given in (3) or (5) and we seek to maximize the mutual information by varying only the choice of measurement. The resulting maximum value is the accessible information [18].

5.1 *All states*

The mutual information for our random ensemble of all qubit states is

$$\begin{aligned} I_A &= \sum_k \int_0^{2\pi} d\phi \int_0^{\pi} \sin\theta \, d\theta \, \frac{1}{4\pi} P(\pi_k|\theta,\phi) \log_2 \left(\frac{P(\pi_k|\theta,\phi)}{P(\pi_k)} \right) \\ &= \frac{1}{\ln 2} \sum_k \frac{1}{4\pi} \int_0^{2\pi} d\phi \int_0^{\pi} \sin\theta \, d\theta \, |\langle \pi_k|\theta,\phi\rangle|^2 \ln \left(\frac{|\langle \pi_k|\theta,\phi\rangle|^2}{\frac{1}{2}\langle \pi_k|\pi_k\rangle} \right). \end{aligned} \tag{15}$$

The integrals cover the entire surface of the Bloch sphere and therefore lead to values that depend on the measurement operators only through $\langle \pi_k|\pi_k\rangle$. The mutual information is

$$I_A = 1 - \frac{1}{2\ln 2} \approx 0.279 \, \text{bits}, \tag{16}$$

which is clearly independent of the choice of measurement (provided, of course, that each probability operator is proportional to a projector onto a pure state). This value has been noted before, albeit in a different context [40, 41].

5.2 *Real states*

Calculation of the mutual information for the random ensemble of real states follows the same line as that for the ensemble of all states. The mutual information in this case is

$$\begin{aligned} I_R &= \sum_k \int_0^{2\pi} d\theta \, \frac{1}{2\pi} P(\pi_k|\theta) \log_2 \left(\frac{P(\pi_k|\theta)}{P(\pi_k)} \right) \\ &= \frac{1}{\ln 2} \sum_k \frac{1}{2\pi} \int_0^{2\pi} d\theta \, |\langle \pi_k|\theta\rangle|^2 \ln \left(\frac{|\langle \pi_k|\theta\rangle|^2}{\frac{1}{2}\langle \pi_k|\pi_k\rangle} \right), \end{aligned} \tag{17}$$

where, in this case, the $|\pi_k\rangle$ are restricted to be real states. The result is again independent of the choice of measurement and takes the value

$$I_R = \frac{1}{\ln 2} - 1 \approx 0.443 \, \text{bits}. \tag{18}$$

The fact that I_R is greater that I_A is a consequence of the additional prior information available in the statement that the states are real.

We see that, as with the fidelity, the mutual information is (largely) independent of the choice of measurement and hence finding the accessible information is, in this sense, a trivial exercise.

5.3 *Comparison with known results*

Calculating the accessible information is, in most cases, a difficult problem and only a few results are known. We start with sets of equiprobable states symmetrically arranged around a great circle on the Bloch sphere. For M such states we can write these as real states in the form

$$|M, m\rangle = \cos\left(\frac{m\pi}{M}\right)|0\rangle + \sin\left(\frac{m\pi}{M}\right)|1\rangle \qquad 0 \leq m \leq M-1. \tag{19}$$

For $M = 2$ the states are simply $|0\rangle$ and $|1\rangle$ and we can extract 1 bit of information by performing a convenional measurement in this basis. For $M = 3$, 5 and 7, we have the trine, quinary and septenary ensembles [18, 24, 25]. The accessible information in each of these cases is given in Table 1 [42]. As the number of states increases, we rapidly converge to the result for the random ensemble of real states, which we can associate with the limit as M tends to infinity.

Real states	Accessible Information
$M = 2$: $\|0\rangle$ and $\|1\rangle$	1 bit
$M = 3$: Trine ensemble	0.585 bits
$M = 5$: Quinary ensemble	0.472 bits
$M = 7$: Septenary ensemble	0.453 bits
$M \to \infty$: Random real ensemble	0.443 bits

Table 1 The accessible information for real symmetric states.

The accessible information is also known for the tetrad ensemble of states. This is a set of four equiprobable states chosen so as to form a regular tetrahedron on the Bloch sphere. One such set is comprised of the four states [24]

$$\begin{aligned}
|\psi_1\rangle &= |0\rangle \\
|\psi_2\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle - \sqrt{2}|1\rangle\right) \\
|\psi_3\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle - \sqrt{2}e^{2\pi i/3}|1\rangle\right) \\
|\psi_4\rangle &= \frac{1}{\sqrt{3}}\left(|0\rangle - \sqrt{2}e^{-2\pi i/3}|1\rangle\right).
\end{aligned} \tag{20}$$

Clearly this set of states does not lie on a single great circle of the Bloch sphere and, for whichever basis is used to write them, at least two of the probability amplitudes will be complex. We can view the two-state ensemble, the trine ensemble and the tetrad ensemble as the first members of a sequence leading to our random ensemble of all possible states. The accessible information for this sequence is given in Table 2 [42].

States	Accessible Information
$\|0\rangle$ and $\|1\rangle$	1 bit
Trine ensemble	0.585 bits
Tetrad ensemble	0.415 bits
Random ensemble	0.279 bits

Table 2 The accessible information for a sequence of states culminating in the random ensemble.

6 Conclusion

We have addressed the problem of how best to measure a qubit prepared in an unknown pure state. It is something of a surprise to have found that almost any measurement is optimal. It is a surprise for two reasons: firstly we might have expected to need a generalized measurement that told us something about each of the x-, y- and z- directions of spin, and secondly, it has proven to be a difficult problem to find optimal measurements for all but the simplest ensembles of states.

For both the fidelity measure (or state estimation) and the accessible information we found higher values for the random real ensemble than for the random ensemble of all states. These differences are quantitative measures of the difference between the statements either that the state is any unknown pure state or that it is any real pure state. The fact that the state is known to be real means that we can perform an optimal measurement with probability operators corresponding only to directions associated with the corresponding great circle on the Bloch sphere. For state estimation this allows an increase in the fidelity form $\frac{2}{3}$ to $\frac{3}{4}$. For the accessible information we find an increase from 0.279 bits to 0.443 bits. We can view the difference between these two, that is 0.164 bits or about one sixth of a bit, as the information associated with specifying that the unknown qubit state is real.

Acknowledgements

I thank Daniel Oi, Sarah Croke and Adrian Kent for helpful comments and suggestions. I gratefully acknowledge the support of the Royal Society and the Wolfson Foundation.

References

[1] V. Bužek and R. Derka in *Coherence and Statistics of Photons and Atoms* J. Peřina ed. (Wiley, New York, 2001).
[2] O. Alter and Y. Yamamoto *Quantum Measurement of a Single System* (Wiley, New York, 2001) and references therein.
[3] M. A. Nielsen and I. L. Chuang *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, (2000).
[4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[5] S. Loepp and W. K. Wootters *Protecting Information: from Classical Error Correction to Quantum Cryptography* (Cambridge University Press, Cambridge, 2006).
[6] S. M. Barnett *Quantum Information* (Oxford University Press, Oxford, in press).
[7] S. Stenholm and K.-A. Suominen *Quantum Approach to Informatics* (Wiley, New Jersey, 2005).
[8] V. Vedral *Introduction to Quantum Information Science* (Oxford University Press, Oxford, 2006).
[9] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[10] S. M. Barnett and S. Croke, Advances in Optics and Photonics (in press).
[11] C. W. Helstrom *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[12] A. S. Holevo *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[13] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[14] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[15] A. Peres, Phys. Lett. A **128**, 19 (1988).
[16] E. B. Davies, IEEE Trans. Inf. Theory **IT-24**, 596 (1978).
[17] L. B. Levitin in *Quantum Communications and Measurement* V. P. Belavkin, O. Hirota and R. L. Hudson eds. (Plenum Press, New York, 1995).
[18] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki and O. Hirota, Phys. Rev. A **59**, 3325 (1999).
[19] S. M. Barnett, C. R. Gilson and M. Sasaki, J. Phys. A: Math. Gen. **34**, 6755 (2001).
[20] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson and J. Jeffers, Phys. Rev. Lett. **96**, 070401 (2006).
[21] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden and N. Gisin, Phys. Rev. A **54**, 3783 (1996).
[22] S. M. Barnett and E. Riis, J. Mod. Opt. **44**, 1061 (1997).
[23] R. B. M. Clarke, A. Chefles, S. M. Barnett and E. Riis, Phys. Rev. A **63**, 040305 (2001).
[24] R. B. M. Clarke, V. M. Kendon, A. Chefles, S. M. Barnett, E. Riis and M. Sasaki, Phys. Rev. A **64**, 012303 (2001).
[25] J. Mizuno, M. Fujiwara, M. Akiba, T. Kawanishi, S. M. Barnett and M. Sasaki, Phys. Rev. A **65**, 012315 (2001).
[26] P. J. Moseley, S. Croke, I. A. Walmsley and S. M. Barnett, Phys. Rev. Lett. **97**, 193601 (2006).
[27] W. K. Wootters, Found. Phys. **20**, 1365 (1990).
[28] E. T. Jaynes, Phys. Rev. **106**, 620 (1957).
[29] L. P. Hughston, R. Jozsa and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
[30] C. M. Caves, C. A. Fuchs and P. Rungta, Found. Phys. Lett. **14**, 199 (2001).
[31] S. Sýkora, J. Stat. Phys., **11**, 17 (1974).
[32] E. T. Jaynes *Probability Theory the Logic of Science* (Cambridge University Press, Cambridge, 2003).
[33] J. M. Radcliffe, J. Phys. A: Math. Gen. **4**, 313 (1971).
[34] A. Peres *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[35] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[36] V. Bužek, M. Hillery and R. Bednik, Acta Physica Slavonica **48**, 177 (1988).
[37] C. E. Shannon and W. Weaver *The Mathematical Theory of Communication* (University of Illinois Press, Urbana, 1963).

[38] A. P. Kent, W. J. Munro, T. Spiller and R. G. Beausoleil *Quantum Cryptography with Quantum Channel Check* International Patent Publication Number WO 2005/013549.
[39] D. V. Sych, B. A. Grishanin and V. N. Zadov, Proc. SPIE **5833**, 229 (2005).
[40] C. M. Caves and C. A. Fuchs in *The Dilemma of Einstein, Podolsky and Rosen - 60 Years Later* A. Mann and M. Revzen eds. (Institute of Physics Publishing, Bristol, 1996).
[41] B. A. Grishanin and V. N. Zadkov, Journal of Communications Technology and Electronics **47**, 933 (2002).
[42] S. M. Barnett, Quantum Information and Computation **4**, 450 (2004).