qitd181

Quantum Information Types

Robert B. Griffiths
Version of 6 February 2012

References:
R. B. Griffiths, *Types of Quantum Information*, Phys. Rev. A **76** (2007) 062320; arXiv:0707.3752

Contents

1 Introduction

★ Since the world (so far as we know) is quantum mechanical, "classical" information must be some sort of "quantum information."

• The precise sense in which this is so remains a subject of investigation at the present time. Despite (or because of?) an enormous number of publications on the subject, the community has not arrived at any consensus.

◦ E.g., the term "classical information" is widely used in the literature by authors who would be embarrassed if asked to actually define what they are talking about.

★ The purpose of these notes is to indicate a scheme based on *types* or *species* of quantum information which represents at least one way of seeing how quantum information theory is connected to classical information theory as developed by Shannon and his successors, and in what way new phenomena arise when quantum effects are taken into account.

• These new phenomena, which have no (direct, at least) classical analogs, include: teleportation, dense coding, quantum cryptography, quantum error correction, and, of course, quantum computing.

2 Information Types

2.1 Definition

★ Let $\{P_j\}$ represent a *decomposition of the identity* on the Hilbert space $\mathcal{H}$ we are interested in. I.e., each $P_j = P_j = P_j^2$ is a projector, and

$$I = \sum_j P_j, \quad P_j P_k = \delta_{jk} P_j. \tag{1}$$

◦ We assume that none of the P_j in such a decomposition is equal to the zero operator. The zero operator is, on the other hand, part of the corresponding event algebra defined below.

• Such a decomposition is the quantum counterpart of a *sample space* in ordinary probability theory: it represents a collection of mutually-exclusive properties or "events", one and only one of which is "true" or "occurs".

★ The corresponding *event algebra*, continuing the analogy with ordinary probability theory, is the collection of all projectors which can be written as sums of one or more of the P_j's in the decomposition, with the zero projector 0 and the identity itself included for good measure.

★ *Probabilities* $\{p_j\}$ can then be assigned to the elements of the sample space, and thereby to projectors in the event algebra in the usual way: $\Pr(P_1 + P_2 + P_7) = p_1 + p_2 + p_7$.

• Where do these probabilities come from? We leave that open for the moment, just noting that: (i) Probabilities can be generated from other probabilities, e.g., as conditional probabilities. (ii) In ordinary (classical) information theory one either proceeds on a formal level, assuming that probabilities are given, or else constructs a model to which probabilities are assigned as parameters, perhaps in light of experimental results. (iii) In quantum theory one can use the Born rule to generate probabilities provided one assumes that a ket or a density operator serves as a pre-probability.

★ The probability that a quantum "observable" (Hermitian operator) has a particular value is equal to the probability assigned to the projector onto the subspace of eigenkets associated with this eigenvalue.

• Thus the projector in question must be part of some decomposition of the identity to which one has (by some means or another) managed to assign probabilities.

◦ This is often referred to as the probability that this observable will have this particular value "if measured."

◦ Given a projector P the coarsest (fewest members) decomposition of the identity to which it belongs consists of the pair $P, I - P$.

2.2 Compatible and incompatible types

★ Two decompositions $\{P_j\}$ and $\{Q_k\}$ of the identity, two types of information, are *compatible* if $P_j Q_k = Q_k P_j$ for every j and k. When this is the case there is a third decomposition $\{R_l\}$ such that for each l $R_l = P_j Q_k$ for some choice of j and k. In fact, these R_l consists of all products of the form $P_j Q_k$, except when this product is 0 and one throws it away.

□ Exercise. Show that each R_l determines a unique pair P_j and Q_k such that $R_l = P_j Q_k$.

• All members of the event algebras associated with $\{P_j\}$ and $\{Q_k\}$ are also members of the event algebra associated with $\{R_l\}$, so for many purposes replacing the two coarser decompositions $\{P_j\}$ and $\{Q_k\}$ with the common refinement $\{R_l\}$, and thinking of this as the type of information entering a discussion, causes no problems.

• Compatibility extends in an obvious way to three or more decompositions of the identity. The rule is that every projector must project with every other projector.

★ If, on the other hand, it is the case that for some j and k, $P_j Q_k \neq Q_k P_j$, then $\{P_j\}$ and $\{Q_k\}$ are *incompatible* sample spaces, or types of information.

★ Example of a qubit. We refer to $\{[0], [1]\}$ as the "Z" type of information, because $Z = [0] - [1]$, i.e., this is the decomposition associated with, the one that diagonalizes, the Z or Pauli σ_z operator. Similarly, with $|+\rangle$ and $|-\rangle$ eigenstates of X (Pauli σ_x), the decomposition $\{[+], [-]\}$ is the "X" type of information. The Z and X types are incompatible.

• Similarly, one can use the Bloch sphere to define the W type of information as the one associated with the basis defined by points where a line in the direction w intersects with the sphere. Note that the

same decomposition results from w and the opposite direction, i.e., from (using polar coordinates) (θ, ϕ) and $(\pi - th, \phi + \pi)$. E.g., the X type of information, the Y type of information.

• Two distinct types of information for a single qubit are always incompatible with each other.

★ As long as one restricts attention to a *single* decomposition of the identity, a *single type* of information, or to a collection of *compatible* types of information, *all the results of classical (Shannon) information theory* can be immediately applied to the quantum domain.

◦ Which should not be very surprising. After all, classical information theory works very well in the classical world: in classical physics there is never any problem with noncommuting operators of the sort which arise all the time in quantum theory.

★ The *single framework rule* of consistent quantum reasoning prohibits *combining* incompatible types of information.

• This does not prohibit discussing different incompatible types of information. In fact quantum information theory, as a discipline that goes beyond classical or Shannon theory, necessarily involves discussions of incompatible types. But the probabilities employed for one type of quantum information cannot be combined with the probabilities employed for an incompatible type, and probabilistic inferences in incompatible frameworks must be kept separate.

◦ Failure to observe this rule leads to paradoxes.

3 Mutually-unbiased types

★ As noted previously, two distinct types of quantum information for a qubit are always incompatible. However, the degree of incompatibility may differ. The W type associated with a direction w on the Bloch sphere which is very close to the z axis will be almost compatible with the Z type: the failure of the projectors to commute will be small. Incompatibility is most evident for two w directions which are perpendicular to each other; e.g., the X and Y types of information are very incompatible. They are an example of mutually unbiased types of information.

★ Two orthonormal bases $\{|a_j\rangle\}$ and $\{|\bar{a}_j\rangle\}$ of a Hilbert space of dimension d are said to be *mutually unbiased* provided for every j and k (including $j = k$) it is the case that

$$|\langle a_j|\bar{a}_k\rangle| = 1/\sqrt{d}, \quad \text{or} \quad \mathrm{Tr}([a_j] \cdot [\bar{a}_k]) = 1/d. \tag{2}$$

We use the same term, "mutually unbiased," for the types of information associated with these two bases.

□ Exercise. Show that the two conditions in (2) are equivalent.

□ Exercise. Show that the X and Y types of information for a qubit are mutually unbiased.

• When two types of information are compatible one can combine them in a "classical" way. Two mutually unbiased types represent the other extreme, their relationship is as "quantum mechanical," in the sense of non-classical, as possible.

◦ So in trying to understand the oddities, relative to the classical case, of quantum information it is often helpful to consider mutually unbiased types.

★ Given any orthonormal basis in a Hilbert space $\mathcal{H}$ of dimension d it is always possible to find another basis which is mutually unbiased with respect to it. Indeed, one can always make the basis in question one member of a collection of three orthonormal bases, each of which is unbiased with respect to both of the other two.

◦ But could there be larger collections of orthonormal bases in which each member of the collection is mutually unbiased with respect to each of the others? This is an interesting mathematical question of the sort that quickly becomes entangled with issues of number theory. The answer depends on the dimension d of the Hilbert space, and has yet to be answered definitively for all d. We shall not discuss it further.

4 Quantum Channels

Figure 1: Channel transmitting x to y.

★ Consider a classical channel, Fig. 1 in which some symbol x chosen from a collection $\mathcal{X}$ is sent into the channel, and emerges as a symbol y which we shall think of as belonging to the same collection. It is characterized by a conditional probability $p(y|x)$ that y will emerge given the input is x.

• An *ideal* or *perfect* or *noise-free* classical channel is one for which whatever goes in at the entrance is exactly reproduced at the output: $p(y|x) = \delta_{xy}$.

★ In the quantum case imagine the channel as a tube into which a particle, one with various possible internal quantum states (e.g., spin-half) enters, and from which it emerges some time later. If nothing at all happens to the particle while it is inside the tube we expect that its internal state will be the same when it emerges. This is an instance of a *perfect quantum channel*.

• E.g., if it is a spin half particle and enters the channel with $S_z = +1/2$, it will emerge with $S_z = +1/2$. If it enters in the state $S_y = -1/2$, then it will exit with $S_y = -1/2$, and so forth.

◦ For a spin-half particle, such as a silver atom in its ground state, one would expect a tube from which all magnetic fields have been excluded to be a perfect channel.

★ We are only interested in the internal states, and therefore do not insist that the particle that comes out be exactly the same one that went in. The particle is, in this perspective, a carrier of information (in its internal state), and what interests us is what happens to the information, not what happens to the particle.

◦ Similarly, for a classical channel, Fig. 1, one is only concerned with how the signal that emerges from the channel is related to the one that enters, not on the details of what goes on inside, where there could be measurements, processing, etc.

• A channel in which the internal state of the particle that enters and the particle that emerges can be described using a two-dimensional Hilbert space is a *qubit* or *one qubit* channel; these terms can be employed both for a perfect channel and one that is noisy.

★ It may be that if the particle enters the channel in a state $|\psi\rangle$ (its internal quantum state), what emerges from the channel is not in the state $|\psi\rangle$ but in a state $U|\psi\rangle$, where U is a unitary operator that is fixed and independent of $|\psi\rangle$. In this case the channel is almost as good as a perfect channel, since we could potentially apply the unitary $U^\dagger$ to the output and turn it into a perfect channel. Let us refer to this as an *ideal* quantum channel.

• A spin-half particle passing at a fixed speed through a tube in which there is a static magnetic field would constitute an ideal quantum channel in this sense.

◦ Classical analogy: a one bit channel whose output is $1 - b$ if the input bit is $b = 0$ or 1.

◦ Example. For a qubit channel suppose that $U = H$ is the Hadamard gate. If at the input the particle is in the state $S_z = +1/2$ it will emerge in the state $S_x = +1/2$; if $S_y = -1/2$ at the input the output will be $S_y = +1/2$, and so forth.

★ How might we check if a quantum channel is perfect? Think of the analogous problem with a classical channel. One use of the channel is not sufficient; there must be repeated tests. What tests? Suppose we ask a competent experimentalist to repeatedly prepare particles either with $S_z = +1/2$ or $S_z = -1/2$, and measure what emerges from the channel in this same basis. If there is perfect agreement we say that the channel perfectly transmits the Z type of information. It is analogous to testing a classical channel by

sending in a series of 0's and 1's, and observing that the output always agrees with the input, $y = x$ in Fig. 1.

• But the test just mentioned does not show that one has a perfect *quantum* channel. It is quite possible (i.e., it violates no principles of quantum mechanics) to construct a channel which faithfully transmits the Z information associated S_z, but is completely noisy for X information: a particle with a given S_x sent into the channel emerges with a random value of this quantity, showing no correlation with what was sent in.

★ A quantum channel in which one type of quantum information, corresponding to a particular orthonormal basis, is perfectly transmitted, whereas all mutually unbiased types are turned into pure noise, no information transmitted, is a *perfect classical* channel or *perfectly decohering* channel. A perfect quantum channel, on the other hand, must perfectly transmit *all* types of quantum information.

★ Suppose we have checked that a qubit channel transmits Z information perfectly and that it transmits X information perfectly. There is still Y information, and indeed, an infinity of other types of information which need to be checked. Checking all of these looks like a lot of work!

• Good news. The principles of quantum mechanics can be used to show that if a channel perfectly transmits two mutually-unbiased types of information, then it perfectly transmits all other types of information as well. [Proof: See Phys. Rev. a 75 (2007) 062320. The two types do not have to be mutually-unbiased, but this is the simplest thing to think about.]

5 Von Neumann Entropy

★ The Shannon entropy

$$H(p) = -\sum_j p_j \log p_j \tag{3}$$

is defined for any probability distribution $p = (p_1, p_2, \ldots)$, and so it can be used to quantify "missing information" for any specific type of quantum information once a probability distribution has been assigned to it.

• Similarly, given a physical variable (observable) V and the corresponding decomposition of the identity

$$V = \sum_j v_j P_j, \tag{4}$$

where we assume that $j \neq k$ means $v_j \neq v_k$, and a probability distribution $\{p_j\}$ associated with the $\{P_j\}$, one can assign a Shannon entropy $H(V)$ to V using (3).

★ Often, however, one is interested not in a single type of information, or a single observable, but in various different types of information to which probabilities can be assigned using a given density operator ρ, which could be a pure state $\rho = |\psi\rangle\langle\psi|$.

• For example, suppose that a qubit is prepared repeatedly a large number of times in exactly the same way. First it is measured a number of times in the S_x basis, then a number of times in the S_y basis, and so forth. For each basis the experiments will yield a probability distribution, one that depends on the basis employed for the measurement. Each basis defines a type of information, and (3) can be employed to calculate the Shannon entropy for this type. Is there anything systematic connecting these different entropies? This is a nontrivial question.

★ Experience suggests that a particularly useful entropy measure that applies directly to the preprobability, and is thus independent of the information type, is the *von Neumann entropy* defined by

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho). \tag{5}$$

• The logarithm of an operator looks a bit nasty. However, if one adopts an orthonormal basis $\{|j\rangle\}$ in which ρ is diagonal, with eigenvalues $\rho_j \geq 0$, things are not so bad:

$$\rho = \sum_j \rho_j \ [j], \quad \rho \log \rho = \sum_j \rho_j \log \rho_j \ [j], \tag{6}$$

where the ρ_j need not be different for different j. Then

$$S(\rho) = -\sum_j \rho_j \log \rho_j, \tag{7}$$

which is just the Shannon entropy for a collection of probabilities $p_j = \rho_j$, which means the Shannon entropy associated with the type of information corresponding to the basis that diagonalizes ρ. Since the trace of $\rho \log \rho$ in (5) is independent of the basis, the result in (7), expressed in terms of eigenvalues of ρ, is always valid.

– If $\rho_j = 0$, set $\rho_j \log \rho_j$ equal to 0.

◦ Just as with Shannon entropy, the von Neumann entropy depends upon the base used for the logarithm, which in quantum information theory is usually 2, so the numerical value of S is given in bits.

◦ In the case of a pure state, $\rho = |\psi\rangle\langle\psi|$. Thus exactly one of the ρ_j is equal to 1 and the rest are zero, and therefore $S(\rho) = 0$.

• If ρ as a pre-probability is used to calculate probabilities for some orthonormal basis other than the one in which it is diagonal, one can show that the Shannon entropy associated with this type of information is never less than the von Neumann entropy $S(\rho)$; the latter provides a lower bound for the former. Thus there is a sense in which the von Neumann entropy represents the *minimum* missing information associated with a pre-probability ρ.

□ Exercise. Show that for any density operator ρ in a Hilbert space of dimension d, used as a pre-probability, it is possible for find a type of information such that the Shannon entropy of the induced probability distribution is equal to $\log d$. [Hint. There is always a basis in which ρ is diagonal. How might one choose another basis in which the diagonal elements of ρ are equal?