Entanglement Manipulation

Steven T. Flammia[1]
[1]*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5 Canada*
(Dated: 22 March 2010)

These are notes for my RIT tutorial lecture at the University of Maryland math department.

I. INTRODUCTION

Entanglement serves as a resource which we can use to perform novel information processing tasks, in particular communication tasks. For example, superdense coding and teleportation are two such tasks which are impossible classically; they make essential use of entanglement. In this lecture I'm going to cover dense coding and teleportation and then show how we can manipulate entanglement into a standard "currency" which will allow us to quantify how useful different states are for these tasks. Based on an operational definition, we will define a way to measure the amount of entanglement in a quantum state.

We will consider the following scenario. We have two parties, Alice and Bob (labeled A and B), and they wish to communicate through a quantum or classical channel. In the literature, channel does have a technical meaning: it is a completely positive linear map, i.e. a linear map that takes density operators to density operators (and it is not necessarily surjective). We call these CP maps for short. We can consider that the channel is noisy, or we can consider a perfect channel (the identity map), but we have noisy quantum states. We will always assume that any classical channel is perfect.

A and B would like to communicate classical and quantum information in the most efficient way possible using the classical and quantum channels (respectively) that they share. In addition, we can consider that they share *prior entanglement* (which I'll define soon) and they would like to take advantage of these non-classical non-local correlations, if at all possible.

II. DEFINITION OF BIPARTITE ENTANGLEMENT

All the quantum states that we consider will live in finite-dimensional spaces like $\mathbb{C}^d$ of dimension d. Actually, we are working in $\mathrm{P}\mathbb{C}^d$, since we consider only normalized states that are equivalent up to an overall phase. Many physicists like to blur this distinction, for some reason.

Given a Hilbert space with a tensor product structure, $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, we can always write any state in this space into its (essentially unique) *Schmidt decomposition*,

$$|\psi\rangle = \sum_{j=1}^{r} \sqrt{p_j} |j_A\rangle |j_B\rangle \,. \tag{1}$$

This decomposition is just the singular value decomposition for the $d_A \times d_B$ matrix formed by "flipping" the second ket into a bra. It is unique up to some degeneracies. The positive integer r is called the *Schmidt rank* and satisfies

$$1 \leq r \leq \min\{d_A, d_B\} \,, \tag{2}$$

and the numbers p_j satisfy

$$p_j > 0 \,, \sum_{j}^{r} p_j = 1 \,. \tag{3}$$

They are just non-zero probabilities. (You could of course just complete the decomposition by adding zero a bunch of times and picking a basis for this degenerate space.)

A pure quantum state is called *entangled* if and only if the Schmidt rank $r > 1$. More specifically, I'm defining pure-state *bipartite* entanglement, meaning entanglement shared between two parties. The theory of multipartite entanglement is much more complicated is only very poorly understood, even for pure states. We will generalize this to mixed quantum states soon.

Being entangled means that there is no possible way to assign a local description of the state to just one party that captures all the correlations between the two halves. In the literature, we say there exists no *local hidden-variable*

theory for entangled states. In particular, for every entangled quantum state, there exists a type of inequality known as a Bell inequality that product states must satisfy but the entangled state violates. Thus, these Bell inequalities are like witnesses that prove a given state is entangled. I think that Jeff talked about these already, so I'm not going to talk more about Bell inequality violations.

A mixed quantum state, also called a density operator, is just a positive semi-definite matrix with unit trace. When we say that a state is mixed, we almost always mean that the state is not necessarily pure, but occasionally we mean that the state is not pure. A pure state is just a density operator that is rank 1. (Here I mean the standard matrix rank, not the Schmidt rank, of course.)

A bipartite mixed state is separable if and only if it can be written as a convex combination of separable states,

$$\rho = \sum_j p_j |j_A\rangle\langle j_A| \otimes |j_B\rangle\langle j_B| \,. \tag{4}$$

If ρ admits no such decomposition, then it is entangled. Understanding mixed state entanglement is much more difficult than pure state entanglement, even in the bipartite setting. Notice that we don't put an *a priori* upper bound on the number possible states in the decomposition. Also, we can use rank 1 states in the decomposition without loss of generality.

We represent the reduced state of a bipartite quantum system by labeling which party holds that half. So, for example, if Alice and Bob share the (potentially entangled) quantum state ρ, then Alice's reduced density operator (obtained by tracing over Bob's degree's of freedom) is denoted ρ_A. Note that this is just the quantum version of a marginal probability distribution. In fact, some people call these "quantum marginals" rather than reduced density operators.

III. QUANTIFYING ENTANGLEMENT

There are several ways in which one might want to quantify entanglement. We will take the following approach in this lecture. We are looking for an operational measure of entanglement that reflects its usefulness for some communication task. We will be specifically interested in pure-state bipartite entanglement, so the measure we will define is especially relevant for that case. (It can be extended to mixed states, but this will not concern us here.) To that end, we will introduce a particular measure of entanglement, the *entanglement entropy*. This is just the von Neumann entropy of the reduced density operator of one half of the bipartite pure state. It doesn't matter if we chose to use the reduced state ρ_A or ρ_B in the definition; it is symmetric. Note that for a general mixed state this symmetry is not manifest, but for an arbitrary pure state this is true. The entanglement entropy of the pure state $|\psi\rangle$ shared between systems A and B is then given by

$$E(\psi) = -\operatorname{Tr}[\rho_A \log(\rho_A)] = -\operatorname{Tr}[\rho_B \log(\rho_B)] \,. \tag{5}$$

We will choose to use a base 2 logarithm to fix the units with which we measure entanglement. This is just to normalize things properly. We will call a the unit of entanglement an "ebit".

Example 1 (Bell pairs)**.**

A maximally entangled state of two qubits has exactly one ebit of entanglement. Write out $|\phi_{00}\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$ and look at the reduced density operator. It is maximally mixed. Compute the entropy. □

As we will see, Bell pairs will form a sort of standard currency with which we can compare the entanglement of different states when assessing their usefulness for various communication tasks.

IV. LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

One of the characteristic features of entanglement is that it cannot increase when performing a restricted class of transformations called LOCC, which stands for Local Operations and Classical Communication. These are just the allowed transformations (CP maps) performed on each half of the system, together with classical communication between the parties. Therefore, we have that if σ is obtained from ρ by LOCC, then

$$E(\sigma) \leq E(\rho) \,. \tag{6}$$

When discussing entanglement manipulation for the purposes of communication tasks, we often allow the local operations free of charge, but we keep track of the classical communication by counting the number of "cbits" (classical bits) that we send down the perfect classical channel.

Example 2 (Local unitaries and the Bell basis)**.**

There is a basis for the space of two qubit states which consists entirely of maximally entangled states. Moreover, they are related to each other by local operations, specifically, by local unitary operations. If we define

$$|\phi_{00}\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}\,, \tag{7}$$

then the other three states are obtained by Alice rotating her local system about either the x-, y- or z-axis by 180°. This corresponds to applying the unitary operator X, Y, or Z respectively (the Pauli matrices). Notices that the entanglement did not increase with these operations. (Actually, it stayed the same in this case.) This basis is called the Bell basis.

More explicitly, we define the Bell basis by the following states labeled by two bits c_1 and c_2,

$$|\phi_{c_2 c_1}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0 \oplus c_1\rangle + (-1)^{c_2}|1\rangle|1 \oplus c_1\rangle\right) \tag{8}$$

where the symbol $\oplus$ denotes addition modulo 2. □

Let's discuss some examples where Alice and Bob share a prior entanglement and either a classical or quantum channel and see if they can do any surprising tasks that they couldn't have done otherwise.

V. DENSE CODING

We assume that Alice and Bob share one ebit of entanglement. That is, sometime ago, before Bob left for Baltimore, Alice in Annapolis gave him one half of a Bell state in the hope that it might come in handy some day.

Notice importantly that this changes the rules somewhat... there is a prior shared resource.

Alice and Bob also share a quantum channel. So Alice can send quantum states down this channel in the form of e.g. polarized photons. For now, we will assume that they have a *perfect* quantum channel, i.e. one that can faithfully transmit quantum systems without introducing any noise. Alice wants to send some classical information to Bob. She has to send him exactly two cbits, but she has already used all of her allowance for the month on her classical channel, and her service provider QT&T charges exorbitant overage charges. She still has a single qubit left on her quantum account though... can she succeed in transmitting *both* of the cbits to Bob by encoding them in a single qubit? Remember, she shares an ebit of entanglement with Bob, so this could be useful.

Fortunately for Alice, she and Bob both knew about dense coding, and they agreed beforehand on the following protocol which they could use in just this situation in case the need arose.

Depending on which two bits Alice wants to send, she performs a local unitary operation given by either I, X, Y, or Z on her half the the Bell pair $|\phi_{00}\rangle$. She then transmits her half of the Bell pair to Bob, thus transmitting one qubit of quantum information. Bob then performs a projective (von Neumann) measurement in the Bell basis. This measurement can perfectly distinguish which of the four possibilities Alice wished to transmit since the states in this basis are orthogonal to each other. Therefore, Bob has perfectly received two cbits of information by receiving only on qubit of quantum information!

Notice also that the reduced state of the half that Alice sends is completely mixed; it contains no information. So an eavesdropper that wanted to see what Alice was sending would learn nothing at all about the message. All of the information is encoded in the correlations. (Eve could still block the entire channel, of course, but this is always the true in the worst case.)

Let me quote from the book of Preskill, Chapter 4.

> From one point of view, Alice and Bob really did need to use the channel twice to exchange two bits of information. For example, we can imagine that Alice prepared the state $|\phi_{00}\rangle$ herself. Last year, she sent half of the state to Bob, and now she sends him the other half. So in effect, Alice has sent two qubits to Bob in one of four mutually orthogonal states, to convey two classical bits of information as the Holevo bound allows.
>
> Still, dense coding is rather weird, for several reasons. First, Alice sent the first qubit to Bob long before she knew what her message was going to be. Second, each qubit by itself carries no information at all;

all the information is encoded in the correlations between the qubits. Third, it would work just as well for Bob to prepare the entangled pair and send half to Alice; then two classical bits are transmitted from Alice to Bob by sending a single qubit from Bob to Alice and back again.

VI. QUANTUM TELEPORTATION

Teleportation is a converse of dense coding: it uses two cbits to transmit one qubit.

Now Alice's graduate student Carol has prepared a quantum state $|\psi\rangle$ of one qubit, and Alice wants to transmit this state to Bob so that Bob can use it in his experiment. Carol, like most grad students, isn't spending enough time in the lab and has left for the weekend. But Bob needs that state now to make a deadline! And wouldn't you know it, Alice forgot to pay the quantum part of her QT&T bill again, and now they cut her quantum channel to Bob. This is bad news.

How can Alice possibly transmit this qubit to Bob? At first it seems hopeless, since she can't measure the qubit and transmit a classical description of the state. If she could do that, it would violate the no cloning theorem because then Bob could just make repeated copies! The best she could hope to achieve with such a strategy would only transmit the qubit imperfectly.

But now again Alice remembers that she shares one ebit of entanglement with Bob. They have agreed beforehand on the following protocol. Alice takes the unknown state $|\psi\rangle$ that Carol gave her and places it next to her half of the Bell state $|\phi_{00}\rangle$. This is a state of two qubits, so Alice can perform a measurement on it in the Bell basis. Alice reads out the outcome of this measurement as a pair of bits, and then transmits these bit to Bob. This costs two cbits, of course. Bob then conditionally applies a local unitary operation to his half of the initial Bell pair, and remarkably, this enables him to recover the state $|\psi\rangle$. Let's see how this works.

First let's decompose $|\psi\rangle = a|0\rangle + b|1\rangle$. Then the joint quantum state is given by

$$|\psi\rangle|\phi_{00}\rangle = (a|0\rangle + b|1\rangle)\left(\tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)\right) \tag{9}$$

$$= \frac{1}{2}|\phi_{00}\rangle(Z^0X^0|\psi\rangle) + \frac{1}{2}|\phi_{01}\rangle(Z^0X^1|\psi\rangle) + \frac{1}{2}|\phi_{10}\rangle(Z^1X^0|\psi\rangle) + \frac{1}{2}|\phi_{11}\rangle(Z^1X^1|\psi\rangle)\,. \tag{10}$$

Thus, if Alice measures and obtains the two bit outcome c_2c_1, then when she sends these two bits to Bob all he has to do is perform the local unitary operation

$$Z^{c_2}X^{c_1} \tag{11}$$

to his local state and he will transform it back into the state $|\psi\rangle$. We've succeeded in transmitting one qubit by sending two cbits by consuming a single ebit of entanglement at the same time.

VII. ENTANGLEMENT CONCENTRATION AND DISTILLATION

For the remainder, we denote $|\phi_{00}\rangle$ by simply $|\phi\rangle$.

The previous sections have established that entanglement can be used as a resource. In practice, we don't have perfect Bell pairs between Alice and Bob, because our quantum channel is noisy; sending one half of the state $|\phi\rangle$ down the channel degrades the joint state into some other state ρ (which is hopefully still at least a little entangled).

Entanglement distillation addresses this by transforming n copies of ρ into approximately $nE(\rho)$ Bell pairs using only LOCC. Thus, distillation is an asymptotic result. Remember that $E(\rho)$ is an entropy, so this is reminiscent of Shannon's noisy channel coding theorem. These perfect Bell pairs then serve as a noiseless resource for dense coding, teleportation, or other protocols.

Entanglement concentration is the special case when the state shared by Alice and Bob is a pure state. We don't have time in just one lecture to cover distillation, so we will content ourselves with just entanglement concentration.

Imagine that Alice and Bob share the state $\rho^{\otimes n}$, which they obtained from n uses of their noisy quantum channel. How many Bell pairs is this worth, and how can they convert this state into those Bell pairs through LOCC alone? That is, we want an LOCC protocol whose output is a new state $\sigma \approx |\phi\rangle\langle\phi|^{\otimes m}$ for some $m \leq n$, with fidelity $F \to 1$ in the large n limit. We define the fidelity of the state ρ with a given pure state $|\psi\rangle$ to be simply $F = F(\rho) = \langle\psi|\rho|\psi\rangle$.

Of course, m will depend on n. We want the best possible asymptotic rate of conversion from our LOCC protocol, too, ignoring the asymptotically vanishing corrections.

The first thing to notice is that since the protocol is LOCC, we must have

$$E(\phi^{\otimes m}) = mE(\phi) = m \leq nE(\rho) = E(\rho^{\otimes n})\,, \tag{12}$$

for any admissible m. In particular, the important part is that

$$\frac{m}{n} \leq E(\rho)\,, \tag{13}$$

which tells us that the best possible rate we could hope to achieve is upper bounded by $E(\rho)$.

The *distillable entanglement* is a measure of entanglement that tells us the asymptotic rate of the best entanglement distillation protocol. It is defined as

$$E_D(\rho) = \sup \lim_{n\to\infty} \frac{m}{n}\,, \tag{14}$$

where the sup is taken over all possible protocols.

We see from above that

$$E_D(\rho) \leq E(\rho)\,. \tag{15}$$

The amazing thing is that for pure states, this rate is achievable. That is, if ρ is a pure quantum state, then

$$E_D(\rho) = E(\rho) \quad (\text{if } \rho \text{ is pure}). \tag{16}$$

The protocol which achieves this is called entanglement concentration, which I will outline in the next section.

Because $E_D(\psi) = E(\psi)$ for any bipartite pure state ψ, the entanglement entropy defines an *achievable rate*, so we have a nice operational meaning for this quantity, as promised. It turns out that E is unique as such an asymptotic entanglement measure in this setting. Also note that this LOCC transformation taking n copies of the pure state ψ to $m = E(\psi)n$ copies of ϕ is an asymptotically reversible process.

A. Entanglement Concentration

The entanglement concentration protocol is very straightforward if you are familiar with the notion of typical sequences, which we now define. Let x be a random variable which takes the values 0 or 1 with probabilities p_0 and $p_1 = 1 - p_0$ respectively. If we sample from this distribution independently n times, we get a string $\mathbf{x} = x_1 x_2 \dots x_n$ with probability $p_{\mathbf{x}} = p_{x_1} p_{x_2} \dots p_{x_n}$. We call a sequence ϵ-typical if

$$2^{-n(H(x)+\epsilon)} \leq p_{\mathbf{x}} \leq 2^{-n(H(x)-\epsilon)}\,, \tag{17}$$

where the function H is the entropy of x, namely

$$H(x) = -p_0 \log p_0 - p_1 \log p_1\,. \tag{18}$$

Let $A_{\epsilon,n}$ be the set of typical sequences of length n. If n is sufficiently large, then one can always take ϵ to be arbitrarily small such that

$$(1-\epsilon)2^{n(H(x)-\epsilon)} \leq |A_{\epsilon,n}| \leq 2^{n(H(x)+\epsilon)}\,, \tag{19}$$

and the probability that a given string lies in $A_{\epsilon,n}$ is at least $1 - \epsilon$.

The protocol for entanglement concentration is now as follows. The initial state $|\psi\rangle$ written in its Schmidt basis looks like

$$|\psi\rangle = \sqrt{p_0}|0\rangle_A|0\rangle_B + \sqrt{p_1}|1\rangle_A|1\rangle_B\,, \tag{20}$$

so the n-fold tensor product is

$$|\psi\rangle^{\otimes n} = \sum_{\mathbf{x}} \sqrt{p_{\mathbf{x}}}|\mathbf{x}\rangle_A|\mathbf{x}\rangle_B\,. \tag{21}$$

We can split this into a sum over the typical and the atypical sequences,

$$|\psi\rangle^{\otimes n} = \sum_{\mathbf{x}\in A_{\epsilon,n}} \sqrt{p_{\mathbf{x}}}|\mathbf{x}\rangle_A|\mathbf{x}\rangle_B + \sum_{\mathbf{x}\notin A_{\epsilon,n}} \sqrt{p_{\mathbf{x}}}|\mathbf{x}\rangle_A|\mathbf{x}\rangle_B\,. \tag{22}$$

Now we can do a projective measurement onto the typical subspace, which will successfully project the state onto that subspace with probability at least $1 - \epsilon$, and then renormalize the state, giving us

$$|\psi\rangle^{\otimes n} \to c \sum_{\mathbf{x}\in A_{\epsilon,n}} \sqrt{p_{\mathbf{x}}}|\mathbf{x}\rangle_A|\mathbf{x}\rangle_B\,. \tag{23}$$

Here c is the normalization factor after the projective measurement. But this factor is at most $1/\sqrt{1-\epsilon}$. A simple computation verifies that this state has large overlap with the state of m Bell pairs.

VIII. FURTHER READING

All of the material covered here is discussed in detail in the excellent book by Nielsen and Chuang. The Bell states are discussed in section 1.3.6. Teleportation is discussed in section 1.3.7 and dense coding in section 2.3. Properties of the quantum entropy are discussed in section 11.3 and entanglement concentration and distillation are discussed in section 12.5.2.