# Quantum Entanglement as a resource for Quantum Communication

Murali Kota
*E15-430, 20 Ames Street*
*Massachusetts Institute Of Technology*
*Cambridge, MA 02139*

Over the past few years radically new ways of computing and communication have been found that exploit quantum mechanical phenomena of physical systems.. Quantum entanglement is one such phenomenon that happens to be the heart of quantum computation and communication. We review some of the very surprising consequences of entanglement for quantum communication.

Man has always been discovering and inventing things to make many of his tasks in life simpler. Computation is one such task that the human race has actively pursued over the past few years to solve many problems that occur in real life. Over the past few decades there has been a phenomenal progress in the power of computational devices using silicon based integrated circuits. This extraordinary technological progress based on the laws of classical physics cannot continue indefinitely as the size of the devices would reach atomic scales soon. At these extreme regimes of natures, the functioning of these devices would be governed by quantum mechanics. Physicists and computer scientists have come up with ideas that exploit quantum mechanical behaviour of these devices to show radically new forms of computing and communication with quantum mechanical states of physical systems. In this report we review quantum entanglement as applicable to quantum communications.

## I. QUANTUM ENTANGLEMENT

The simplest example of an entangled state is a two-qubit entangled state. This state can be mathematically represented as $\psi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ where $|0\rangle$ and $|1\rangle$ correspond to spin-up and spin-down states of nuclei or horizontal and vertical polarization of photons respectively. The state $\psi$ is entangled as the probability that the first bit is measured to be $|0\rangle$ is $1/2$ provided the second bit has not been measured. However, if the second bit had been measured, the probability that the first bit is measured as $|0\rangle$ is either 1 or 0, depending on whether the second bit was measured as $|0\rangle$ or $|1\rangle$ respectively. Thus the probable result of measuring the first bit is changed by a measurement of the second bit. Mathematically entangled states cannot be written as a tensor product of individual states.

### A The EPR Paradox

Einstein, Podolsky and Rosen proposed a gedanken experiment that uses entangled particles in a manner that seemed to violate fundamental principles relativity. Imagine a source that generates two maximally entangled particles $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, called an EPR pair, and sends one each to Alice and Bob.

Alice and Bob can be arbitrarily far apart. Suppose that Alice measures her particle and observes state $|0\rangle$. This means that the combined state will now be $|00\rangle$ and if now Bob measures his particle

he will also observe $|0\rangle$. Similarly, if Alice measures $|1\rangle$, so will Bob. Note that the change of the combined quantum state occurs instantaneously even though the two particles may be arbitrarily far apart. It appears that this would enable Alice and Bob to communicate faster than the speed of light. Further analysis, as we shall see, shows that even though there is a coupling between the two particles, there is no way for Alice or Bob to use this mechanism to communicate.

There are two standard ways that people use to describe entangled states and their measurement. Both have their positive aspects, but both are incorrect and can lead to misunderstandings. Let us examine both in turn.

Einstein, Podolsky and Rosen proposed that each particle has some internal state that completely determines what the result of any given measurement will be. This state is, for the moment, hidden from us, and therefore the best we can currently do is to give probabilistic predictions. Such a theory is known as a local hidden variable theory. The simplest hidden variable theory for an EPR pair is that the particles are either both in state $|0\rangle$ or both in state $|1\rangle$, we just don't happen to know which. In such a theory no communication between possibly distant particles is necessary to explain the correlated measurements. However, this point of view cannot explain the results of measurements with respect to a different basis. In fact, Bell showed that any local hidden variable theory predicts that certain measurements will satisfy an inequality, known as Bell's inequality. However, the result of actual experiments performing these measurements show that Bell's inequality is violated. Thus quantum mechanics cannot be explained by any local hidden variable theory.

The second standard description is in terms of cause and effect. For example, we said earlier that a measurement performed by Alice affects a measurement performed by Bob. However, this view is incorrect also, and results, as Einstein, Podolsky and Rosen recognized, in deep inconsistencies when combined with relativity theory. It is possible to set up the EPR scenario so that one observer sees Alice measure first, then Bob, while another observer sees Bob measure first, then Alice. According to relativity, physics must equally well explain the observations of the first observer as the second. While our terminology of cause and effect cannot be compatible with both observers, the actual experimental values are invariant under change of observer. The experimental results can be explained equally well by Bob's measuring first and causing a change in the state of Alice's particle, as the other way around. This symmetry shows that Alice and Bob cannot, in fact, use their EPR pair to communicate faster than the speed of light, and thus resolves the apparent paradox. All that can be said is that Alice and Bob will observe the same random behavior.

In the following sections on teleportation and dense coding, we show how EPR pairs can be used to aid communication.

## II. QUANTUM TELEPORTATION

Before we look into quantum teleportation, we review the No Cloning Theorem that states that an unknown quantum state can not be perfectly cloned.

### A The No Cloning Theorem

The unitary property implies that quantum states cannot be copied or cloned. The no cloning proof is a simple application of the linearity of unitary transformations.

Assume that $U$ is a unitary transformation that clones, in that $U(|a0\rangle) = |aa\rangle$ for all quantum states $|a\rangle$. Let $|a\rangle$ and $|b\rangle$ be two orthogonal quantum states. Say $U(|a0\rangle) = |aa\rangle$ and $U(|b0\rangle) = |bb\rangle$. Consider $|c\rangle = (1/\sqrt{2})(|a\rangle + |b\rangle)$. By linearity,

$$\begin{aligned} U(|c0\rangle) &= \tfrac{1}{\sqrt{2}}(U(|a0\rangle) + U(|b0\rangle)) \\ &= \tfrac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle). \end{aligned}$$

But if $U$ is a cloning transformation then

$$U(|c0\rangle) = |cc\rangle = 1/2(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle),$$

which is not equal to $(1/\sqrt{2})(|aa\rangle + |bb\rangle)$. Thus there is no unitary operation that can reliably clone unknown quantum states. It is clear that cloning is not possible by using measurement since measurement is both probabalistic and destructive of states not in the measuring device's associated subspaces.

It is important to understand what sort of cloning is and isn't allowed. It is possible to clone a known quantum state. What the no cloning principle tells us is that it is impossible to reliably clone an unknown quantum state. Also, it is possible to obtain $n$ particles in an entangled state $a|0000\ldots0\rangle + b|1111\ldots1\rangle$ from an unknown state $a|0\rangle + b|1\rangle$. Each of these particles will behave in exactly the same way when measured with respect to the standard basis for quantum computation $\{|00\ldots0\rangle, |00\ldots01\rangle, \ldots, |11\ldots1\rangle\}$, but not when measured with respect to other bases. It is therefore impossible to create the $n$ particle state $(a|0\rangle + b|1\rangle) \otimes \ldots \otimes (a|0\rangle + b|1\rangle)$ from an unknown state $a|0\rangle + b|1\rangle$.

## B Telportation

Teleportation is a process of reproducing an unknown quantum state by the use classical communication and EPR pairs. The objective is to transmit the quantum state of a particle using classical bits and reconstruct the exact quantum state at the receiver. Since quantum state cannot be copied, the quantum state of the given particle will necessarily be destroyed. Here is the protocol for teleporting a quantum state.

*Alice* Alice has a qubit whose state she doesn't know. She wants to send the state of ths qubit

$$\phi = a|0\rangle + b|1\rangle$$

to Bob through classical channels. Alice and Bob each possess one qubit of an entangled pair

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The starting quantum state is written as

$$\begin{aligned}\phi \otimes \psi_0 &= \frac{1}{\sqrt{2}}(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)) \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle),\end{aligned}$$

of which Alice controls the first two bits and Bob controls the last one. Alice now applies $C_{not} \otimes I$ and $H \otimes I \otimes I$ to this state:

$$\begin{aligned}&(H \otimes I \otimes I)(C_{not} \otimes I)(\phi \otimes \psi_0) \\ &= (H \otimes I \otimes I)(C_{not} \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\ &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\ &= \frac{1}{2}(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\ &= \frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle))\end{aligned}$$

where $C_{not}$ is the Controlled-NOT operator, $I$ the identity operator and $H$ is the Hadamard Tranform. Alice measures the first two qubits to get one of $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with equal probability. Depending on the result of the measurement, the quantum state of Bob's qubit is projected to $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$, or $a|1\rangle - b|0\rangle$ respectively. Alice sends the result of her measurement as two classical bits to Bob.

Note that when she measured it, Alice irretrievably altered the state of her original qubit $\phi$, whose state she is in the process of sending to Bob. This loss of the original state is the reason teleportation does not violate the no cloning principle.

*Bob* When Bob receives the two classical bits from Alice he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit.

| bits received | state | decoding |
|---|---|---|
| 00 | $a\|0\rangle + b\|1\rangle$ | $I$ |
| 01 | $a\|1\rangle + b\|0\rangle$ | $X$ |
| 10 | $a\|0\rangle - b\|1\rangle$ | $Z$ |
| 11 | $a\|1\rangle - b\|0\rangle$ | $Y$ |

Here $X$,$Y$, and $Z$ are the Pauli operators. Bob can reconstruct the original state of Alice's qubit, $\phi$, by applying the appropriate decoding transformation to his part of the entangled pair. Note that this is the encoding step of dense coding.

## III. SUPERDENSE CODING

Superdense coding uses one quantum bit together with an EPR pair to encode and transmit two classical bits. Since EPR pairs can be distributed ahead of time, only one qubit (for example a photon) needs to be physically transmitted to communicate two bits of information. This result is surprising as only one classical bit's worth of information can be extracted from a qubit. Superdense Coding is the opposite of teleportation, in that it uses two classical bits to transmit a single qubit.

The key to both dense coding and teleportation is the use of entangled particles. The initial set up is the same for both processes. Alice and Bob wish to communicate. Each is sent one of the entangled particles making up an EPR pair,

$$\psi_0 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Say Alice is sent the first particle, and Bob the second. So until a particle is transmitted, only Alice can perform transformations on her particle, and only Bob can perform transformations on his.

### A The Superdense Coding Protocol

*Alice* Alice receives two classical bits, encoding the numbers 0 through 3. Depending on this number Alice performs one of the transformations $\{I, X, Y, Z\}$ on her qubit of the entangled pair $\psi_0$. Transforming just one bit of an entangled pair means performing the identity transformation on the other bit. The resulting state is shown in the table.

| Value | Transformation | New state |
|---|---|---|
| 0 | $\psi_0 = (I \otimes I)\psi_0$ | $\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$ |
| 1 | $\psi_1 = (X \otimes I)\psi_0$ | $\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$ |
| 2 | $\psi_2 = (Y \otimes I)\psi_0$ | $\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$ |
| 3 | $\psi_3 = (Z \otimes I)\psi_0$ | $\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$ |

Alice then sends her qubit to Bob.

*Bob* Bob applies a controlled-NOT to the two qubits of the entangled pair.

| Initial state | Controlled-NOT | First bit | Second bit |
|---|---|---|---|
| $\psi_0 = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$ | $\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$ | $\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ | $\|0\rangle$ |
| $\psi_1 = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$ | $\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$ | $\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$ | $\|1\rangle$ |
| $\psi_2 = \frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$ | $\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$ | $\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$ | $\|1\rangle$ |
| $\psi_3 = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$ | $\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$ | $\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$ | $\|0\rangle$ |

Note that Bob can now measure the second qubit without disturbing the quantum state. If the measurement returns $|0\rangle$ then the encoded value was either 0 or 3, if the measurement returns $|1\rangle$ then the encoded value was either 1 or 2.

Bob now applies $H$ to the first bit:

| Initial state | First bit | $H$(First bit) |
|---|---|---|
| $\psi_0$ | $\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ | $\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)) = \|0\rangle$ |
| $\psi_1$ | $\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$ | $\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)) = \|0\rangle$ |
| $\psi_2$ | $\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$ | $\frac{1}{\sqrt{2}}(-\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle) + \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)) = \|1\rangle$ |
| $\psi_3$ | $\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$ | $\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle) - \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)) = \|1\rangle$ |

Finally, Bob measures the resulting bit which allows him to distinguish between 0 and 3, and 1 and 2.

## IV. QUANTUM ERROR CORRECTION

One fundamental problem in building quantum computers is the need to isolate the quantum state. An interaction of particles representing qubits with the external environment disturbs the quantum state, and causes it to decohere, or transform in an unintended and often non-unitary fashion. Adding error correction protocols mitigates the effect of decoherence, quantum error correction is going to be a key component of quantum computation and communications algorithms.

On the surface quantum error correction is similar to classical error correcting codes in that redundant bits are used to detect and correct errors. But the situation for quantum error correction is somewhat more complicated than in the classical case since we are not dealing with binary data but with quantum states.

Quantum error correction must reconstruct the exact encoded quantum state. Given the impossibility of cloning or copying the quantum state, this reconstruction appears harder than in the classical case. However, it turns out that classical techniques can be modified to work for quantum systems.

### A Characterization of Errors

In the following it is assumed that all errors are the result of quantum interaction between a set of qubits and the environment. The possible errors for each single qubit considered are linear combinations of no errors ($I$), bit flip errors ($X$), phase errors ($Z$), and bit flip phase errors ($Y$). A general single bit error is thus a transformation $e_1 I + e_2 X + e_3 Y + e_4 Z$. Interaction with the environment transforms single qubits according to

$$|\psi\rangle \rightarrow (e_1 I + e_2 X + e_3 Y + e_4 Z)|\psi\rangle = \sum_i e_i E_i |\psi\rangle.$$

For the general case of quantum registers, possible errors are expressed as linear combinations of unitary error operators $E_i$. These could be combinations of single bit errors, like tensor products of the single bit error transformations $\{I, X, Y, Z\}$, or more general multi-bit transformations. In any case, an error can be written as $\sum_i e_i E_i$ for some error operators $E_i$ and coefficients $e_i$.

## B Recovery of Quantum State

An error correcting code for a set of errors $E_i$ consists of a mapping $C$ that embeds $n$ data bits in $n+k$ code bits together with a syndrome extraction operators $S_C$ that maps $n+k$ code bits to the set of indices of correctable errors $E_i$ such that $i = S_C(E_i(C(x)))$. If $y = E_j(C(x))$ for some unknown but correctable error, then error $S_C(y)$ can be used to recover a properly encoded value $C(x)$, i.e. $E^{-1}_{S_C(y)}(y) = C(x)$.

Now consider the case of a quantum register. First, the state of the register can be in a superposition of basis vectors. Furthermore, the error can be a combination of correctable error operators $E_i$. It turns out that it is still possible to recover the encoded quantum state.

Given an error correcting code $C$ with syndrome extraction operator $S_C$, an $n$-bit quantum state $|\psi\rangle$ is encoded in a $n+k$ bit quantum state $|\phi\rangle = C|\psi\rangle$. Assume that decoherence leads to an error state $\sum_i e_i E_i|\phi\rangle$ for some combination of correctable errors $E_i$. The original encoded state $|\phi\rangle$ can be recovered as follows:

1. Apply the syndrome extraction operator $S_C$ to the quantum state padded with sufficient $|0\rangle$ bits:

$$S_C(\sum_i e_i E_i|\phi\rangle) \otimes |0\rangle = \sum_i e_i (E_i|\phi\rangle \otimes |i\rangle).$$

   Quantum parallelism gives a superposition of different errors each associated with their respective error index $i$.

2. Measure the $|i\rangle$ component of the result. This yields some (random) value $i_0$ and projects the state to

$$E_{i_0}|\phi, i_0\rangle$$

3. Apply the inverse error transformation $E^{-1}_{i_0}$ to the first $n+k$ qubits of $E_{i_0}|\phi, i_0\rangle$ to get the corrected state $|\phi\rangle$.

Note that step 2 projects a superposition of multiple error transformations into a single error. Consequently, only one inverse error transformation is required in step 3.

## C Error Correction Example

Consider the trivial error correcting code $C$ that maps $|0\rangle \rightarrow |000\rangle$ and $|1\rangle \rightarrow |111\rangle$. $C$ can correct single bit flip errors

$$E = \{I \otimes I \otimes I, X \otimes I \otimes I, I \otimes X \otimes I, I \otimes I \otimes X\}.$$

The syndrome extraction operator is

$$S : |x_0, x_1, x_2, 0, 0, 0\rangle \rightarrow |x_0, x_1, x_2, x_0 \bigoplus x_1, x_0 \bigoplus x_2, x_1 \bigoplus x_2\rangle,$$

with the corresponding error correction operators shown in the table. Note that $E_i = E_i^{-1}$ for this example.

| Bit flipped | Syndrome | Error correction |
|---|---|---|
| none | $\|000\rangle$ | none |
| 0 | $\|110\rangle$ | $X \otimes I \otimes I$ |
| 1 | $\|101\rangle$ | $I \otimes X \otimes I$ |
| 2 | $\|011\rangle$ | $I \otimes I \otimes X$ |

Consider the quantum bit $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ that is encoded as

$$C|\psi\rangle = |\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

, a three qubit entangled state and the error

$$E = \frac{4}{5}X \otimes I \otimes I + \frac{3}{5}I \otimes X \otimes I.$$

The resulting error state is

$$\begin{aligned}
E|\phi\rangle &= (\frac{4}{5}X \otimes I \otimes I + \frac{3}{5}I \otimes X \otimes I)(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)) \\
&= \frac{4}{5}X \otimes I \otimes I(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)) + \frac{3}{5}I \otimes X \otimes I(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)) \\
&= \frac{4}{5\sqrt{2}}X \otimes I \otimes I(|000\rangle - |111\rangle) + \frac{3}{5\sqrt{2}}I \otimes X \otimes I(|000\rangle - |111\rangle) \\
&= \frac{4}{5\sqrt{2}}(|100\rangle - |011\rangle) + \frac{3}{5\sqrt{2}}(|010\rangle - |101\rangle)
\end{aligned}$$

Next apply the syndrome extraction to $(E|\phi\rangle) \otimes |000\rangle$ as follows:

$$\begin{aligned}
&S_C((E|\phi\rangle) \otimes |000\rangle) \\
&= S_C(\frac{4}{5\sqrt{2}}(|100000\rangle - |011000\rangle) + \frac{3}{5\sqrt{2}}(|010000\rangle - |101000\rangle)) \\
&= \frac{4}{5\sqrt{2}}(|100110\rangle - |011110\rangle) + \frac{3}{5\sqrt{2}}(|010101\rangle - |101101\rangle) \\
&= \frac{4}{5\sqrt{2}}(|100\rangle - |011\rangle) \otimes |110\rangle + \frac{3}{5\sqrt{2}}(|010\rangle - |101\rangle) \otimes |101\rangle
\end{aligned}$$

Measuring the last three bits of this state yields either $|110\rangle$ or $|101\rangle$. Assuming the measurement produces the former, the state becomes

$$\frac{1}{\sqrt{2}}(|100\rangle - |011\rangle) \otimes |110\rangle.$$

The measurement has the almost magical effect of causing all but one summand of the error to disappear. The remaining part of the error can be removed by applying the inverse error operator $X \otimes I \otimes I$, corresponding to the measured value $|110\rangle$, to the first three bits, to produce

$$\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = C|\psi\rangle = |\phi\rangle.$$

## v. CONCLUSIONS

Quantum computing and communications are novel ways of engineering quantum systems and are proving to dramatically change the way we think about computation, complexity, information, and communication. Quantum entanglement is one of the most important consequences of quantum mechanics and ,as we have seen, introduces a new dimension to computation and communications.

## VI. REFERENCES

1. R. P. Feynman. Simulating physics with computers, International Journal of Theoretical Physics, **(21)** 467, 1982.

2. A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete, Physical Review, **(47)**, 777-780, 1935.

3. M. A. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

4. D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation, Nature, **(390)**, 575-579, 1997.

5. J. Preskill, Quantum Compuation and Information, California Institute of Technology, 1998, http://www.theory.caltech.edu/people/preskill/ph229.

6. N. Gershenfeld and I. L. Chuang, Bulk spin resonance quantum computation, Science, **(275)**, 350, 1999.

7. C. H. Bennett and D. P. DiVincenzo, Quantum information and computation, Nature, **(404)**, 247, 2000.

8. E. Schrodinger, Probability relations between separated systems, Proceedings of Cambridge Philosophical Society, **(32)**, 446, 1936.