CS 294 Qubits, Gates, Superdense Coding, Teleportation, Bell Inequalities 9/2/16
Fall 2016 Lecture 1

In this lecture we shall consider simple systems of one or two (or three) qubits, and see how to describe their states and operations on them. These simple systems already exhibit interesting properties...

0.1 The superposition principle

Consider a system with k distinguishable (classical) states. For example, the electron in a hydrogen atom is only allowed to be in one of a discrete set of energy levels, starting with the ground state, the first excited state, the second excited state, and so on. If we assume a suitable upper bound on the total energy, then the electron is restricted to being in one of k different energy levels — the ground state or one of $k-1$ excited states. As a classical system, we might use the state of this system to store a number between 0 and $k-1$. The superposition principle says that if a quantum system can be in one of two states then it can also be placed in a linear superposition of these states with complex coefficients.

Let us introduce some notation. We denote the ground state of our qubit by $|0\rangle$, and the successive excited states by $|1\rangle, \ldots, |k-1\rangle$. These are the k possible classical states of the electron. The superposition principle tells us that, in general, the (quantum) state of the electron is $\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{k-1}|k-1\rangle$, where $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ are complex numbers normalized so that $\sum_j |\alpha_j|^2 = 1$. α_j is called the *amplitude of the state* $|j\rangle$.

For instance, if $k = 3$, the state of the electron could be
$1/\sqrt{2}|0\rangle + 1/2|1\rangle + 1/2|2\rangle$ or
$1/\sqrt{2}|0\rangle - 1/2|1\rangle + i/2|2\rangle$ or
$(1+i)/3|0\rangle - (1-i)/3|1\rangle + (1+2i)/3|2\rangle$, where $i = \sqrt{-1}$.

The superposition principle is one of the most mysterious aspects about quantum physics — it flies in the face of our intuitions about the physical world. One way to think about a superposition is that the electron does not make up its mind about whether it is in the ground state or each of the $k-1$ excited states, and the amplitude α_0 is a measure of its inclination towards the ground state. Of course we cannot think of α_0 as the probability that an electron is in the ground state — remember that α_0 can be negative or imaginary. The measurement principle, which we will see shortly, will make this interpretation of α_0 more precise.

0.2 The Geometry of Hilbert Space

We saw above that the quantum state of the k-state system is described by a sequence of k complex numbers $\alpha_0, \ldots, \alpha_{k-1} \in \mathscr{C}$, normalized so that $\sum_j |\alpha_j|^2 = 1$. So it is natural to write the state of the system as a k dimensional vector:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{k-1} \end{pmatrix}$$

The normalization on the complex amplitudes means that the state of the system is a unit vector in a k dimensional complex vector space — called a Hilbert space.

But hold on! Earlier we wrote the quantum state in a very different (and simpler) way as: $\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{k-1}|k-1\rangle$. Actually this notation, called Dirac's ket notation, is just another way of writing a vector. Thus $|0\rangle = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}$ and $|k-1\rangle = \begin{pmatrix} 0 \\ 0 \\ . \\ . \\ 1 \end{pmatrix}$.

So we have an underlying geometry to the possible states of a quantum system: the k distinguishable (classical) states $|0\rangle, \ldots, |k-1\rangle$ are represented by mutually orthogonal unit vectors in a k-dimensional complex vector space. i.e. they form an orthonormal basis for that space (called the standard basis). Moreover, given any two states, $\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{k-1}|k-1\rangle$, and $\beta|0\rangle + \beta|1\rangle + \cdots + \beta k-1|k-1\rangle$, we can compute the inner product of these two vectors, which is $\sum_{j=0}^{k-1} \bar{\alpha}_j \beta_j$. The absolute value of the inner product is the cosine of the angle between these two vectors. You should verify that the inner product of any two vectors in the standard basis is 0, showing that they are orthogonal.

The advantage of the ket notation is that the it labels the basis vectors explicitly. This is very convenient because the notation expresses both that the state of the quantum system is a vector, while at the same time explicitly writing out the physical quantity of interest (energy level, position, spin, polarization, etc).

0.3 Measurement Principle

This linear superposition $|\psi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle$ is part of the private world of the electron. Access to the information describing this state is severely limited — in particular, we cannot actually measure the complex amplitudes α_j. This is not just a practical limitation; it is enshrined in the measurement postulate of quantum physics.

A measurement on this k state system yields one of at most k possible outcomes: i.e. an integer between 0 and $k-1$. Measuring $|\psi\rangle$ in the standard basis yields j with probability $|\alpha_j|^2$.

One important aspect of the measurement process is that it alters the state of the quantum system: the effect of the measurement is that the new state is exactly the outcome of the measurement. I.e., if the outcome of the measurement is j, then following the measurement, the qubit is in state $|j\rangle$. This implies that you cannot collect any additional information about the amplitudes α_j by repeating the measurement.

Intuitively, a measurement provides the only way of reaching into the Hilbert space to probe the quantum state vector. In general this is done by selecting an orthonormal basis $|e_0\rangle, \ldots, |e_{k-1}\rangle$. The outcome of the measurement is j with probability equal to the square of the length of the projection of the state vector ψ on $|e_j\rangle$. A consequence of performing the measurement is that the new state vector is $|e_j\rangle$. Thus measurement may be regarded as a probabilistic rule for projecting the state vector onto one of the vectors of the orthonormal measurement basis.

0.4 Qubits

The basic entity of quantum information is a qubit (pronounced "cue-bit"), or a quantum bit. Qubits are 2-state quantum systems. For example, if we set $k = 2$, the electron in the Hydrogen atom can be in the ground state or the first excited state, or any superposition of the two. We shall see more examples of qubits soon.

The state of a qubit can be written as a unit (column) vector $\binom{\alpha}{\beta} \in \mathscr{C}^2$. In Dirac notation, this may be written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha,\beta \in \mathscr{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1$$

This linear superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is part of the private world of the electron. For us to know the electron's state, we must make a measurement. Making a measurement gives us a single classical bit of information — 0 or 1. The simplest measurement is in the standard basis, and measuring $|\psi\rangle$ in this $\{|0\rangle, |1\rangle\}$ basis yields 0 with probability $|\alpha|^2$, and 1 with probability $|\beta|^2$. The measurement alters the state of the qubit: if the outcome of the measurement is 0, then following the measurement, the new state of the qubit is $|0\rangle$. This implies that you cannot collect any additional information about α, β by repeating the measurement.

More generally, we may choose any orthogonal basis $\{|v\rangle, |w\rangle\}$ and measure the qubit in that basis. To do this, we rewrite our state in that basis: $|\psi\rangle = \alpha'|v\rangle + \beta'|w\rangle$. The outcome is v with probability $|\alpha'|^2$, and $|w\rangle$ with probability $|\beta'|^2$. If the outcome of the measurement on $|\psi\rangle$ yields $|v\rangle$, then as before, the the qubit is then in state $|v\rangle$.

0.4.1 Measurement example: phase estimation

Consider the quantum state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle)$. If we were to measure this qubit in the standard basis, the outcome would be 0 with probability $1/2$ and 1 with probability $1/2$. Is there any measurement that yields information about the phase θ?

Let us consider a measurement in a different basis: the $\{|+\rangle, |-\rangle\}$-basis. Here $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. What does $|\phi\rangle$ look like in this new basis? This can be expressed by first writing $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$.
Now,

$$\begin{aligned} |\psi\rangle &= \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{e^{i\theta}}{\sqrt{2}}|1\rangle) \\ &= \tfrac{1}{2}(|+\rangle + |-\rangle) + \tfrac{e^{i\theta}}{2}(|+\rangle - |-\rangle) \\ &= \tfrac{1+e^{i\theta}}{2}|+\rangle + \tfrac{(1-e^{i\theta})}{2}|-\rangle \ . \end{aligned}$$

Writing $e^{i\theta} = cos\theta + isin\theta$, we see that the probability of measuring $|+\rangle$ is $\frac{1}{4}((1+cos\theta)^2 + sin^2\theta)$. This can be further simplified to $\frac{1}{2}(1+cos\theta) = cos^2\frac{\theta}{2}$. A similar calculation reveals that the probability of measuring $|-\rangle$ is $sin^2\frac{\theta}{2}$. Measuring in the $\{|+\rangle, |-\rangle\}$-basis therefore reveals some information about the phase θ.

0.5 Uncertainty Principle

The Uncertainty Principle limits the amount of information it is possible to maintain about a quantum system in any given moment. Sometimes, the act of precisely measuring one observable invalidates previously held knowledge of a different observable.

For example, it is fundamentally impossible to simultaneously know the bit and the sign of a two-level system. If I measure a bit value of "0", the sign is now equal to $(|+\rangle + |-\rangle)/\sqrt{2}$. If I now measure the sign and return a value of "+", it is tempting to conclude that my system is fully characterized: the bit is zero and the sign is "+". However, this is not the case. After returning "+", the system collapses into the

state $(|0\rangle + |1\rangle)/\sqrt{2}$, an equal superposition of both possible bit states. My previous information about the bit value is no longer valid.

0.6 Unitary Operators

One of the basic postulates of quantum physics states that the evolution of a quantum system is necessarily unitary. Intuitively, a unitary transformation is a rigid body rotation of the Hilbert space. For a qubit the unitary transformation is given by:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

If we denote by $U^\dagger$ the conjugate transpose of this matrix:

$$U^\dagger = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \quad .$$

then U is unitary iff $UU^\dagger = U^\dagger U = I$.

Let us now consider some examples of unitary transformations on single qubits or equivalently single qubit quantum gates:

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$, or a rotation around $\pi/4$ followed by a reflection.

  $$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

  The Hadamard Gate is one of the most important gates. Note that $H^\dagger = H$ – since H is real and symmetric – and $H^2 = I$.

- Rotation Gate. This rotates the plane by θ.

  $$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

- NOT Gate. This flips a bit from 0 to 1 and vice versa.

  $$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase Flip.

  $$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  The phase flip is a NOT gate acting in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis. Indeed, $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

1 Two qubits:

Now let us examine a system of two qubits. Consider the two electrons in two hydrogen atoms, each regarded as a 2-state quantum system:

Since each electron can be in either of the ground or excited state, classically the two electrons are in one of four states – 00, 01, 10, or 11 – and represent 2 bits of classical information. By the superposition principle, the quantum state of the two electrons can be any linear combination of these four classical states:

$$\left|\psi\right\rangle = \alpha_{00}\left|00\right\rangle + \alpha_{01}\left|01\right\rangle + \alpha_{10}\left|10\right\rangle + \alpha_{11}\left|11\right\rangle \ ,$$

where $\alpha_{ij} \in \mathscr{C}$, $\sum_{ij} |\alpha_{ij}|^2 = 1$. Again, this is just Dirac notation for the unit vector in $\mathscr{C}^4$:

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

Measurement:

Measuring $\left|\psi\right\rangle$ now reveals two bits of information. The probability that the outcome of the measurement is the two bit string $x \in \{0,1\}^2$ is $|\alpha_x|^2$. Moreover, following the measurement the state of the two qubits is $\left|x\right\rangle$. i.e. if the first bit of x is j and the second bit k, then following the measurement, the state of the first qubit is $\left|j\right\rangle$ and the state of the second is $\left|k\right\rangle$.

An interesting question comes up here: what if we measure just the first qubit? What is the probability that the outcome is 0? This is simple. It is exactly the same as it would have been if we had measured both qubits: $\Pr\{1\text{st bit } = 0\} = \Pr\{00\} + \Pr\{01\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. Ok, but how does this partial measurement disturb the state of the system?

The new superposition is obtained by crossing out all those terms of $\left|\psi\right\rangle$ that are inconsistent with the outcome of the measurement (i.e. those whose first bit is 1). Of course, the sum of the squared amplitudes is no longer 1, so we must renormalize to obtain a unit vector:

$$\left|\phi\right\rangle_{new} = \frac{\alpha_{00}\left|00\right\rangle + \alpha_{01}\left|01\right\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

.

This is just the projection of $\left|\psi\right\rangle$ onto the two dimensional subspace spanned by $\left|00\right\rangle, \left|01\right\rangle$.

Entanglement

Suppose the first qubit is in the state $3/5\left|0\right\rangle + 4/5\left|1\right\rangle$ and the second qubit is in the state $1/\sqrt{2}\left|0\right\rangle - 1/\sqrt{2}\left|1\right\rangle$, then the joint state of the two qubits is $(3/5\left|0\right\rangle + 4/5\left|1\right\rangle)(1/\sqrt{2}\left|0\right\rangle - 1/\sqrt{2}\left|1\right\rangle) = 3/5\sqrt{2}\left|00\right\rangle - 3/5\sqrt{2}\left|01\right\rangle + 4/5\sqrt{2}\left|10\right\rangle - 4/5\sqrt{2}\left|11\right\rangle$

But there are states such as $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$ which cannot be decomposed in this way as a state of the first qubit and that of the second qubit. Can you see why? Such a state is called an entangled state.

If the first (resp. second) qubit of $\left|\Phi^+\right\rangle$ is measured then the outcome is 0 with probability $1/2$ and 1 with probability $1/2$. However if the outcome is 0, then a measurement of the second qubit results in 0 with certainty. Furthermore this is true even if both qubits are measured in a rotated basis $\left|v\right\rangle, \left|v^\perp\right\rangle$, where $\left|v\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ and $\left|v^\perp\right\rangle = -\beta\left|0\right\rangle + \alpha\left|1\right\rangle$ (for $\alpha, \beta \in R$).

Claim: $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$
$= \frac{1}{\sqrt{2}}\left(\left|vv\right\rangle + \left|v^\perp v^\perp\right\rangle\right)$.

Proof: Then $\frac{1}{\sqrt{2}}(\left|vv\right\rangle + \left|v^\perp v^\perp\right\rangle)$
$= \frac{1}{\sqrt{2}}(\alpha^2\left|00\right\rangle + \alpha\beta\left|01\right\rangle + \alpha\beta\left|10\right\rangle + \beta^2\left|11\right\rangle) + \frac{1}{\sqrt{2}}(\beta^2\left|00\right\rangle - \alpha\beta\left|01\right\rangle - \alpha\beta\left|10\right\rangle + \alpha^2\left|11\right\rangle)$

$= \frac{1}{\sqrt{2}}(\alpha^2+\beta^2)(|00\rangle + |11\rangle)$
$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

1.1 Two Qubit Gates

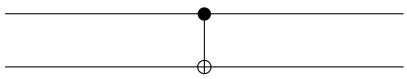
A very basic two qubit gate is the controlled-not gate or the CNOT:

- Controlled Not (CNOT).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

  The first bit of a CNOT gate is the "control bit;" the second is the "target bit." If the inputs to the CNOT gate are standard basis states, then the control bit remains unchanged, while the target bit is flipped iff the control bit is 1.

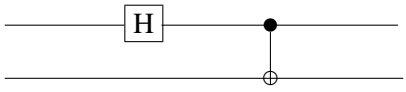
  The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



Though the CNOT gate looks very simple, any unitary transformation on two qubits can be closely approximated by a sequence of CNOT gates and single qubit gates. This brings us to an important point. What happens to the quantum state of two qubits when we apply a single qubit gate to one of them, say the first? Let's do an example. Suppose we apply a Hadamard gate to the superposition: $|\psi\rangle = 1/2|00\rangle - i/\sqrt{2}|01\rangle + 1/\sqrt{2}|11\rangle$. Then this maps the first qubit as follows: $|0\rangle \rightarrow 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$, and
$|1\rangle \rightarrow 1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle$.
So $|\psi\rangle \rightarrow 1/2\sqrt{2}|00\rangle + 1/2\sqrt{2}|01\rangle - i/2|00\rangle + i/2|01\rangle + 1/2|10\rangle - 1/2|11\rangle$
$= (1/2\sqrt{2} - i/2)|00\rangle + (1/2\sqrt{2} + i/2)|01\rangle + 1/2|10\rangle - 1/2|11\rangle$.

Bell states:

We can generate the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with the following simple quantum circuit, call it the Bell gate, consisting of a Hadamard and CNOT gate:



The first qubit is passed through a Hadamard gate and then both qubits are entangled by a CNOT gate.

If the input to the system is $|0\rangle \otimes |0\rangle$, then the Hadamard gate changes the state to

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{sqrt2}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \ ,$$

and after the CNOT gate the state becomes $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the Bell state $|\Phi^+\rangle$.

Indeed, the output of the circuit on input each of the four standard basis states are the four Bell basis states:

$$\begin{aligned} |\Phi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \\ |\Psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \quad . \end{aligned}$$

These are maximally entangled states on two qubits.

2 No Cloning Theorem

The *No Cloning Theorem* states that it is impossible to clone an arbitrary quantum state. A successful cloning procedure would copy qubit $|$ A $\rangle$ onto qubit $|$ B $\rangle$, leaving qubit $|$ A $\rangle$ unchanged. The initial state of the system can be expressed as:

$$|AB\rangle_i = \alpha|00\rangle + \beta|10\rangle$$

After cloning is complete, states $|$ A $\rangle$ and $|$ B $\rangle$ must be separable and identical:

$$|AB\rangle_f = \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle = (\alpha|0\rangle_A + \beta|1\rangle_A)(\alpha|0\rangle_B + \beta|1\rangle_B)$$

Quantum systems evolve linearly and thus obey the linear superposition principle: if input A produces output B and input C produces output D, then input (A+C) must produce output (B+D). This requirement leads to the following:

$$\begin{aligned} |00\rangle &\Longrightarrow |00\rangle \\ |10\rangle &\Longrightarrow |11\rangle \\ \alpha|00\rangle + \beta|10\rangle &\Longrightarrow \alpha|00\rangle + \beta|11\rangle \end{aligned}$$

This output state is not consistent with the output of quantum cloning for arbitrary values of α and β. It does, however, allow for the cloning of basis states.

$$\alpha|00\rangle + \beta|11\rangle \neq \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$$

The *No Cloning Theorem* is a critical restriction because quantum clones would allow us to communicate faster than the speed of light and violate causality.

Suppose Alice and Bob share Bell state $|AB\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Alice tells Bob that she will measure in the bit basis to communicate "1", and will measure in the sign basis to communicate "0". After a pre-specified amount of time, Alice measures her bit, Bob clones his bit, and Bob measures his clones in the bit basis.

If Alice measures in the bit basis, the Bell pair will collapse into either state $|$ 00 $\rangle$ or $|$ 11 $\rangle$. When Bob clones his bit, the system will be in either state $|$ 0000...0 $\rangle$ or $|$ 1111...1 $\rangle$, and the results of all of his measurements will be identical.

If Alice measures in the sign basis, the Bell pair will collapse into either state $\left| \text{++} \right\rangle$ or $\left| \text{- -} \right\rangle$, and the full system will be in either state $\left| \text{++++...+} \right\rangle$ or $\left| \text{- - - - ... -} \right\rangle$. When Bob measures in the bit basis, he will find half ones and half zeros.

Since Bob can use his local bit to determine Alice's chosen basis, Alice can transmit a string of bits over an arbitrarily long distance in an arbitrarily small amount of time! This procedure is prohibited by the impossibility of cloning.

3 Super Dense Coding

As we move away from the physical aspects of quantum mechanics and start thinking of them in mathematical terms, we can start thinking of qubits as quantities of information that can be sent and manipulated. The first question that this evokes, then, is *How much classical information does a qubit carry?*

Since a qubit is just a generalization of a classical bit, there is an intuition that is should carry more information. And since we describe a qubit with two complex numbers that are unlimited in precision, our intuition may say that it should carry *a lot* more. So far, however, we've seen that the measurement principle (our only probe into a qubit) only reveals to us one bit upon viewing. Our next goal then would be to be clever in extracting more information from the qubit. Say, for example, we prepare the state $(\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle....|0\rangle$ and hope that more information about α and β *leaks out* into the attached qubits. Can we hope to learn some of the dense information encoded in α and β through some trick of this nature?

Perhaps surprisingly, the answer is no. Holevo's Theorem in essence states that at most one classical bit of information can be retrieved from a qubit. Our next result is the seemingly unimpressive fact that from two qubits you can recover two classical bits; what's surprising is the unusual chronology you can accomplish this in, somewhat bypassing Holevo's Theorem, by using entanglement.

Consider the following (very high-level) entanglement assisted protocol for Alice, A, to transmit two classical bits to Bob, B by sending one qubit.

0. A and B share an entangled pair
   ⋮
1. A chooses classical bits b_0 and b_1 as her message she wants to convey to B
2. A performs operations on her half of the entangled pair
3. A sends her qubit (her half of the pair)
4. B measures the received qubit and his half of the entangled pair, thus learning what b_0 and b_1 were

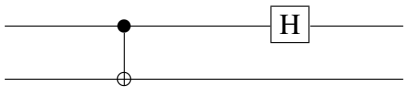
Intuitively, Alice can transform the entangled system into one of the four Bell states depending on which of the four possible messages she wants to send, and Bob, receiving both halves of the pair, can determine which is the case, thus knowing the two bits Alice wanted to send. But before going into the details of the operations and why this works, we should first acknowledge that our protocol unimpressively uses two qubits to recover two classical bits. What is impressive, and surprising, is the chronology in which these qubits are communicated.

The first qubit Bob receives is at Step 0 when the entangled pair is created. But the suggestive ellipsis connotes that this initialization could happen years or decades before the second qubit is sent and, most importantly, *before Alice even decides what message she wants to send!* Morally, then, this "initialization

step" is just that and doesn't convey any information on its own, laying dormant until a message is to be thought of and sent in the protocol; the second qubit really does in essence carry with it the two classical bits.

To slightly formalize the procedure, then, we see that Alice wants to put the system in one of the four Bell states, $\left|\Phi^{\pm}\right\rangle, \left|\Psi^{\pm}\right\rangle$. Assuming we initialize our entangled pair to be $\left|\Phi^{+}\right\rangle$, Alice will then, upon deciding a b_0 and b_1 to send, apply Z to her half if $b_0 = 1$ (and identity otherwise) and then apply X if $b_1 = 1$ (and identity otherwise). Each b_0, b_1 pair then puts us in one of the Bell states with b_0 effectively deciding between $+$ and $-$ and b_1 deciding between Φ and Ψ.

All that's left is for Bob to measure in the Bell basis and recover which state we're in. To do this we convert to the Bell basis so that a measurement in the standard basis then corresponds to a measurement in the Bell basis. And this can be done by reversing the Bell gate to get the gate



Feeding this gate our Bell state will do the reverse of the Bell gate and give us a pure state corresponding to $\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle$, or $\left|11\right\rangle$, effectively taking us to the Bell basis so that a standard basis measurement is as if we measured in the Bell basis to begin with, thus recovering our two bit message.

4 Quantum Teleportation

Quantum teleportation can be thought of as the dual task to super dense coding. Whereas super dense coding is concerned with conveying classical information via a qubit, quantum teleportation is concerned with conveying quantum information with classical bits.

This, at first, may seem impossible to convey the infinite precision of an arbitrary qubit's amplitudes with classical bits, but again using an entanglement assisted protocol will allows us to achieve this. Even more surprising, the duality is continued since, as were were able to convey two classical bits with one qubit, we will now be able to convey one qubit with only two classical bits!

We describe the high-level quantum teleportation protocol.

0. A and B share an entangled pair, $\left|\Phi^{+}\right\rangle$

   $\vdots$

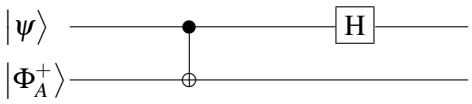
1. A chooses a qubit $\left|\psi\right\rangle$ as her message she wants to convey to B
2. A performs operations on $\left|\psi\right\rangle$ and her half of $\left|\Phi^{+}\right\rangle$
3. A measures $\left|\psi\right\rangle$ and her half of $\left|\Phi^{+}\right\rangle$
4. A sends the two classical bits that were the results of her measurements
5. B uses the two classical bits as directions on how to "correct" his qubit to be $\left|\psi\right\rangle$

Intuitvely, Alice interferes $\left|\psi\right\rangle$ with her half of the Bell pair so that operations on her qubits automatically affect Bob's half of the Bell pair by virtue of an entangled system. To some degree, $\left|\psi\right\rangle$ gets imprinted on

Bob's half of the Bell state. Alice can then measure her two qubits so that the whole system collapses to the single qubit that Bob has had, which, because of Alice's previous actions, is in some way *related* to $|\psi\rangle$. Lastly, Alice knows exactly how Bob's qubit is now related to $|\psi\rangle$ because of her measurements; all she has left to do is convey to Bob her findings so that he also knows how $|\psi\rangle$ is related to his qubit and can apply operations to correct it to be exactly $|\psi\rangle$.

Before we explore the details, we should note that, while operating on her half of the Bell state does instantly affect Bob's half, no faster-than-light communication occurs since Bob still learns nothing from the changes until Alice actually sends the two classical bits to him (which are themselves bounded by the speed of light). Also, the No-Cloning theorem is not violated here either even though Bob has an exact copy of $|\psi\rangle$ since, to get this copy, Alice destroyed her own copy by measuring. Finally, one interesting point is that neither Alice or Bob ever "know" what $|\psi\rangle$ is (in terms of its actual amplitutudes), but simply know that, whatever it was, it was transferred.

To be a little more formal, the full state of the system is $|\psi\rangle \otimes |\Phi^+\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ and Alice has the first bit of $|\Phi^+\rangle$ while Bob has the second. Next Alice applies the reverse of the Bell gate to $|\psi\rangle$ and her half of $|\Phi^+\rangle$, call it $|\Phi_A^+\rangle$, and then measuring in the standard basis:



Now Alice measures the output of this gate in the standard basis. We note that working through the circuit shows us that the form of the whole system's state after this transformation is

$$\frac{\alpha}{2}(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \frac{\beta}{2}(|010\rangle - |110\rangle + |001\rangle - |101\rangle)$$

Now we see from this that when Alice measures her two qubits, of course seeing 00, 01, 10, or 11, she gets each of the four possiblities with probability $\frac{1}{4}$. Furthermore, we see that if 00 is seen, the state collapses to Bob's remaining qubit, $|\Phi_B^+\rangle$, being $\alpha|0\rangle + \beta|1\rangle$, and if instead she sees 01 his state must be $\beta|0\rangle + \alpha|1\rangle$, if she sees 10 his state is $\alpha|0\rangle - \beta|1\rangle$, and, finally, if she sees 11 his state is $\beta|0\rangle - \alpha|1\rangle$.

By sending the two bits she saw to Bob, he knows what operations to perform to transform his current qubit to be $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. That is, looking at the above cases, if $b_0 = 1$ he should apply Z to his qubit and identity otherwise, and if $b_1 = 1$ he should apply X and identity otherwise. Thus, Bob is left with $|\psi\rangle$ as his qubit.

A conceptual point here is that, while we covered teleporation here, we never really talked in terms of "teleporting" some physical quantity but instead talked of transferring information: how to convey a qubit through a classical channel. We may have not even recognized it as teleportation immediately without the title. It's good to note here that, while these concepts tie deeply with physical aspects of our world, it is a rich theory of information in its own right and can be thought of entirely in terms of information manipulation and communication.

5 Bell & CHSH

While we can now think of quantum theory as a rich mathematical framework describing notions of information, the physical perspective of it and its ramifications caused much turmoil as it was being discovered.

With "spooky" notions of randomness in nature, actions at distances via entanglement, and later notions of physical teleportation, there were many who doubted and philosiphized about quantum theory.

Einstein, Podolsky, and Rosen (EPR) were so concerned about the counter-intuitive physical implications that they introduced the Bell state $\left|\Phi^+\right\rangle$ specifically to construct a "paradoxical" thought experiment. There thought was to prepare the state and notice that $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right) = \frac{1}{\sqrt{2}}\left(\left|++\right\rangle + \left|--\right\rangle\right)$, and then separate the two qubits, giving one to Alice and one to Bob. Now have Alice measure her half in the in the standard basis to *recover the bit* and, at the same time, Bob measure his half to *recover the sign*, thus learning the bit and sign and breaking the uncertainty principle!

They proposed this as a paradox and further claimed quantum theory was likely incomplete and that there is a *real underlying reality* that we simply don't have all the variables for to accurately predict and instead see randomness as a result of our lack of knowledge. They wanted a *classical* hidden variable theory to describe reality.

The Bell test is a test that distinguishes a quantum world from one that can be described by a classical hidden variable theory. We show the game being played and how an inequality between strategies in a classical world versus a quantum world allows us to distinguish which we are in. It has since been repeatedly experimentally confirmed that our universe is quantum using this test.

The two experimenters, Alice and Bob, each receive a random bit x and y respectively. Each also receives one half of a Bell state, and makes a suitable measurement described below based on the received random bit. Call the outcomes of the measurements a and b respectively. We are interested in the achievable correlation between the two quantities xy and $a+b(mod 2)$. We will show that for the particular quantum measurements described below $P[xy = a+b(mod 2)] = cos^2\pi/8 \approx .85$.

What would a classical hidden variable theory predict for this setting? Now, when the Bell state was created, the two particles could share an arbitrary amount of information. But by the time the random bits x and y are generated, the two particles are too far apart to exchange information. Thus in any experiment, the outcome can only be a function of the previously shared information and one of the random bits. It can be shown that in this setting the best correlation is achieved by always letting the outcomes of the two experiments be $a = 0$ and $b = 0$ (see homework exercise). This gives $P[xy = a+b(mod 2)] \leq .75$. This experiment therefore distinguishes between the predictions of quantum physics and those of any arbitrary local hidden variable theory. It has now been performed in several different ways, and the results are consistent with quantum physics and inconsistent with any classical hidden variable theory.

Here is the protocol:

- if $X_A = 0$, then Alice measures in the standard basis.
- if $X_A = 1$, then Alice measures in the $\pi/4$ basis.
- if $X_B = 0$, then Bob measures in the $\pi/8$ basis.
- if $X_B = 1$, then Bob measures in the $-\pi/8$ basis.

Now an easy calculation shows that in each of the four cases $X_A = X_B = 0$, etc, the success probability is $cos^2\pi/8$. This is because in the three cases where $x_A \cdot x_B = 0$, Alice and Bob measure in bases that differ by $\pi/8$. In the last case they measure in bases that differ by $3\pi/8$, but in this case they must output different bits. Finally, this works since our Bell state has the special property that we've seen: $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle) = \frac{1}{\sqrt{2}}(\left|v_A v_A\right\rangle + \left|v_A^\perp v_A^\perp\right\rangle)$.