Chapter 2

Entanglement

What are the allowable quantum states of systems of several particles? The answer to this is enshrined in the addendum to the first postulate of quantum mechanics: the superposition principle. In this chapter we will consider a special case, systems of two qubits. In keeping with our philosophy, we will first approach this subject naively, without the formalism of the formal postulate. This will facilitate an intuitive understanding of the phenomenon of quantum entanglement — a phenomenon which is responsible for much of the "quantum weirdness" that makes quantum mechanics so counter-intuitive and fascinating.

2.1 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:

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

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

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

Measurement

As in the case of a single qubit, even though the state of two qubits is specified by four complex numbers, most of this information is not accessible by measurement. In fact, a measurement of a two qubit system can only reveal 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 $|x\rangle$. 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 $|j\rangle$ and the state of the second is $|k\rangle$.

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: $\Pr\{\text{1st bit } = 0\} = \Pr\{00\} + \Pr\{01\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. Ok, but how does this partial measurement disturb the state of the system?

The answer is obtained by an elegant generalization of our previous rule for obtaining the new state after a measurement. The new superposition is obtained by crossing out all those terms of $|\psi\rangle$ 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:

$$|\phi_{\text{new}}\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Entanglement

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

Can every state of two qubits be decomposed in this way? Our classical intuition would suggest that the answer is obviously affirmative. After all each of the two qubits must be in some state $\alpha\,|0\rangle + \beta\,|1\rangle$, and so the state of the two qubits must be the product. In fact, there are states such as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 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. When the two qubits are entangled, we cannot determine the state of each qubit separately. The state of the qubits has as much to do with the relationship of the two qubits as it does with their individual states.

If the first (resp. second) qubit of $|\Phi^+\rangle$ 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. This is true no matter how large the spatial separation between the two particles.

The state $|\Phi^+\rangle$, which is one of the Bell basis states, has a property which is even more strange and wonderful. The particular correlation between the measurement outcomes on the two qubits holds true no matter which rotated basis a rotated basis $|v\rangle, \left|v^\perp\right\rangle$ the two qubits are measured in, where $|0\rangle = \alpha|v\rangle + \beta\left|v^\perp\right\rangle$ and $|1\rangle = -\beta|v\rangle + \alpha\left|v^\perp\right\rangle$. This can bee seen as,

$$\begin{aligned}
\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(\left(\alpha|v\rangle + \beta\left|v^\perp\right\rangle\right) \otimes \left(\alpha|v\rangle + \beta\left|v^\perp\right\rangle\right)\right) \\
&\quad - \frac{1}{\sqrt{2}}\left(\left(-\beta|v\rangle + \alpha\left|v^\perp\right\rangle\right) \otimes \left(-\beta|v\rangle + \alpha\left|v^\perp\right\rangle\right)\right) \\
&= \frac{1}{\sqrt{2}}\left(\left(\alpha^2+\beta^2\right)|vv\rangle + \left(\alpha^2+\beta^2\right)\left|v^\perp v^\perp\right\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|vv\rangle + |v^\perp v^\perp\rangle\right)
\end{aligned}$$

Two Qubit Gates

Recall that the third axiom 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. In particular it does not change the length of the state vector.

Let us consider what this means for the evolution of a two qubit system. A unitary transformation on the Hilbert space $\mathbb{C}^4$ is specified by a $4x4$ matrix U that satisfies the condition $UU^\dagger = U^\dagger U = I$. The four columns of U specify the four orthonormal vectors $|v_{00}\rangle$, $|v_{01}\rangle$, $|v_{10}\rangle$ and $|v_{11}\rangle$ that the basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ are mapped to by U.

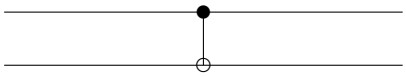
A very basic two qubit gate is the controlled-not gate or the CNOT:

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 called the "control bit," and the second the "target bit." This is because (in the standard basis) the control bit does not change, while the target bit flips if and only if 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:

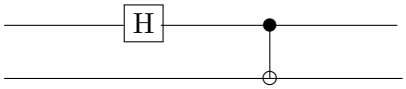
$$\begin{aligned} |0\rangle &\to 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle \\ |1\rangle &\to 1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle\,. \end{aligned}$$

So

$$\begin{aligned} |\psi\rangle &\to 1/2\sqrt{2}\,|00\rangle + 1/2\sqrt{2}\,|01\rangle - i/2\,|00\rangle + i/2\,|01\rangle + 1/2\,|10\rangle - 1/2\,|11\rangle \\ &= (1/2\sqrt{2} - i/2)\,|00\rangle + (1/2\sqrt{2} + i/2)\,|01\rangle + 1/2\,|10\rangle - 1/2\,|11\rangle\,. \end{aligned}$$

Bell states

We can generate the Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$ with the following simple quantum circuit 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

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

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

Notice that the action of the CNOT gate is not so much copying, as our classical intuition would suggest, but rather to entangle.

The state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is one of four Bell basis states:

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

These maximally entangled states on two qubits form an orthonormal basis for $\mathbb{C}^4$. Exercise: give a simple quantum circuit for generating each of these states, and prove that the Bell basis states form an orthonormal basis for $\mathbb{C}^4$.

So far we have avoided a discussion of the addendum to the superposition axiom, which tells us the allowable states of a composite quantum system consisting of two subsystems. The basic question for our example of a two qubit system is this: how do the 2-dimensional Hilbert spaces corresponding to each of the two qubits relate to the 4-dimensional Hilbert space corresponding to the composite system? i.e. how do we glue two 2-dimensional Hilbert spaces to get a 4-dimensional Hilbert space? This is done by taking a tensor product of the two spaces.

Let us describe this operation of taking tensor products in a slightly more general setting. Suppose we have two quantum systems - a k-state system with associated k-dimensional Hilbert space V with orthonormal basis $|0\rangle, \ldots, |k-1\rangle$ and a l-state system with associated l-dimensional Hilbert space W with orthonormal basis $|0\rangle, \ldots, |l-1\rangle$. What is resulting Hilbert space obtained by gluing these two Hilbert spaces together? We can answer this question as follows: there are kl distinguishable states of the composite system — one for each choice of basis state $|i\rangle$ of the first system and basis state $|j\rangle$ of the second system. We denote the resulting of dimension kl Hilbert space by $V \otimes W$ (pronounced "V tensor W"). The orthonormal basis for this new Hilbert space is given by:

$$\{|i\rangle \otimes |j\rangle : 0 \leq i \leq k-1, 0 \leq j \leq l-1\},$$

So a typical element of $V \otimes W$ will be of the form $\sum_{ij} \alpha_{ij}(|i\rangle \otimes |j\rangle)$.

In our example of a two qubit system, the Hilbert space is $\mathbb{C}^2 \otimes \mathbb{C}^2$, which is isomorphic to the four dimensional Hilbert space $\mathbb{C}^4$. Here we are identifying $|0\rangle \otimes |0\rangle$ with $|00\rangle$.

EPR Paradox:

Everyone has heard Einstein's famous quote "God does not play dice with the Universe". The quote is a summary of the following passage from Einstein's 1926 letter to Max Born: "Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot, but does not really bring us any closer to the secret of the Old One. I, at any rate, am convinced that He does not throw dice." Even to the end of his life, Einstein held on to the view that quantum physics is an incomplete theory and that some day we would learn a more complete and satisfactory theory that describes nature.

In what sense did Einstein consider quantum mechanics to be incomplete? To understand this better, let us imagine that we were formulating a theory that would explain the act of flipping a coin. A simple model of a coin flip is that its outcome is random — heads 50% of the time, and tails 50% of the time. This model seems to be in perfect accordance with our experience with flipping a coin, but it is incomplete. A more complete theory would say that if we were able to determine the initial conditions of the coin with perfect accuracy (position, momentum), then we could solve Newton's equations to determine the eventual outcome of the coin flip with certainty. The coin flip amplifies our lack of knowledge about the initial conditions, and makes the outcome seem completely random. In the same way, Einstein believed that the randomness in the outcome of quantum measurements reflected our lack of knowledge about additional degrees of freedom of the quantum system.

Einstein sharpened this line of reasoning in a paper he wrote with Podolsky and Rosen in 1935, where they introduced the famous Bell states. Recall that for Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, when you measure first qubit, the second qubit is determined. However, if two qubits are far apart, then the second qubit must have had a determined state in some time interval before measurement, since the speed of light is finite. By the rotational symmetry of the Bell state, which we saw earlier, this fact holds in every basis. This appears analogous to the coin flipping example. EPR therefore suggested that there is a more complete theory where "God does not throw dice." Until his death in 1955, Einstein tried to formulate a more complete "local hidden variable theory" that would describe the predictions of quantum mechanics, but without re-

sorting to probabilistic outcomes. But in 1964, almost three decades after the EPR paper, John Bell showed that properties of Bell (EPR) states were not merely fodder for a philosophical discussion, but had verifiable consequences: local hidden variables are not the answer. He showed that there is a particular experiment that could be performed on two qubits entangled in a Bell state such no local hidden variable theory [1] could possibly match the outcome predicted by quantum mechanics. The Bell experiment has been performed to increasing accuracy, originally by Aspect, and the results have always been consistent with the predictions of quantum mechanics and inconsistent with local hidden variable theories.

2.2 Bell's Thought Experiment

Bell considered the following experiment: let us assume that two particles are produced in the Bell state $|\Phi^+\rangle$ in a laboratory, and the fly in opposite directions to two distant laboratories. Upon arrival, each of the two qubits is subject to one of two measurements. The decision about which of the two experiments is to be performed at each lab is made randomly at the last moment, so that speed of light considerations rule out information about the choice at one lab being transmitted to the other. The measurements are cleverly chosen to distinguish between the predictions of quantum mechanics and any local hidden variable theory. Concretely, the experiment measures the correlation between the outcomes of the two experiments. The choice of measurements is such that any classical hidden variable theory predicts that the correlation between the two outcomes can be at most 0.75, whereas quantum mechanics predicts that the correlation is $\cos^2 \pi/8 \approx 0.8$. Thus the experiment allows us to distinguish between the predictions of quantum mechanics and any local hidden variable theory! We now describe the experiment in more detail.

The two experimenters A and B (for Alice and Bob) each receives one qubit of a Bell state $|\Phi^+\rangle$, and measures it in one of two bases depending upon the value of a random bit r_A and r_B respectively. Denote by a and b respectively the outcomes of the measurements. We are interested in the highest achievable correlation between the two quantities $r_A \times r_B$ and $a + b(mod 2)$. We will see below that there is a particular choice of bases for the quantum measurements made by A and B such that $P[r_A \times r_B = a + b(mod 2)] = \cos^2 \pi/8 \approx .8$. Before we do so, let us see why no classical hidden variable theory allows a correlation of over 0.75. i.e. $P[r_A \times r_B = a + b(mod 2)] \leq 0.75$.

[1] We will describe what we mean by a local hidden variable theory below after we start describing the actual experiment

We can no longer postpone a discussion about what a local hidden variable theory is. Let us do so in the context of the Bell experiment. In a local hidden variable theory, when the Bell state was created, the two particles might share an arbitrary amount of classical information, x. This information could help them coordinate their responses to any measurements they are subjected to in the future. By design, the Bell experiment selects the random bits r_A an r_B only after the two particles are too far apart to exchange any further information before they are measured. Thus we are in the setting, where A and B share some arbitrary classical information x, and are given as input independent, random bits x_A an x_B as input, and must output bits a and b respectively to maximize their chance of achieving $r_A \times r_B = a + b(mod 2)$. It can be shown that the shared information x is of no use in increasing this correlation, and indeed, the best they can do is to always output $a = b = 0$. This gives $P[r_A \times r_B = a + b(mod 2)] \leq .75$.

Let us now describe the quantum measurements that achieve greater correlation. They are remarkably simple to describe:

- if $r_A = 0$, then Alice measures in the $-\pi/16$ basis.
- if $r_A = 1$, then Alice measures in the $3\pi/16$ basis.
- if $r_B = 0$, then Bob measures in the $\pi/16$ basis.
- if $r_B = 1$, then Bob measures in the $-3\pi/16$ basis.

The analysis of the success probability of this experiment is also beautifully simple. We will show that in each of the four cases $r_A = r_B = 0$, etc, the success probability $P[r_A \times r_B = a + b(mod 2)] = \cos^2 \pi/8$.

We first note that if Alice and Bob measure in bases that make an angle θ with each other, then the chance that their measurement outcomes are the same (bit) is exactly $\cos^2 \theta$. This follows from the rotational invariance of $|\Phi^+\rangle$ and the following observation: if the first qubit is measured in the standard basis, then the outcome is outcome is an unbiased bit. Moreover the state of the second qubit is exactly equal to the outcome of the measurement — $|0\rangle$ if the measurement outcome is 0, say. But now if the second qubit is measured in a basis rotated by θ, then the probability that the outcome is also 0 is exactly $\cos^2 \theta$.

Now observe that in three of the four cases, where $x_A \cdot x_B = 0$, Alice and Bob measure in bases that make an angle of $\pi/8$ with each other. By our observation above, $P[a + b \equiv 0 \mod 2] = P[a = b] = \cos^2 \pi/8$.

In the last case $x_A \cdot x_B = 1$, and they measure in bases that make an angle of $3\pi/8$ with each other. Now, $P[a + b \equiv 1 \mod 2] = P[a \neq b] = \sin^2 3\pi/8 = \cos^2 5\pi/8$.

2.3 No Cloning Theorem and Quantum Teleportation

The axioms of quantum mechanics are deceptively simple. Our view is that to begin to understand and appreciate them you have to be exposed to some of their most counterintuitive consequences. Paradoxically, this will help you build a better intuition for quantum mechanics.

In this chapter we will study three very simple but counterintuitive consequences of the laws of quantum mechanics. The theme of all three vignettes is the copying or transmission of quantum information.

No Cloning Theorem

Given a quantum bit in an unknown state $|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, is it possible to make a copy of this quantum state? i.e. create the state $|\phi\rangle \otimes |\phi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle)$? The axioms of quantum mechanics forbid this very basic operation, and the proof of the no cloning theorem helps gain insight into this.

To be more precise, we are asking whether it is possible to start with two qubits in state $|\phi\rangle \otimes |0\rangle$ and transform them to the state $|\phi\rangle \otimes |\phi\rangle$? By the third axiom of quantum mechanics, for this to be possible there must be a unitary transformation U such that $U |\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle$. We will show that no unitary transformation can achieve this simultaneously for two orthogonal states $|\phi\rangle$ and $|\psi\rangle$.

Recall that a unitary transformation is a rotation of the Hilbert space, and therefore necessarily preserves angles. Let us make this more precise. Consider two quantum states (say on a single qubit): $|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and $|\psi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$. The cosine of the angle between them is given by (the absolute value of) their inner product: $\alpha_0^* \beta_0 + \alpha_1^* \beta_1$.

Now consider the quantum states (on two qubits) $|\phi\rangle \otimes |\phi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle)(\alpha_0 |0\rangle + \alpha_1 |1\rangle)$ and $|\psi\rangle \otimes |\phi\rangle = (\beta_0 |0\rangle + \beta_1 |1\rangle)(\beta_0 |0\rangle + \beta_1 |1\rangle)$. Their inner product is: $(\alpha_0^* \beta_0 + \alpha_1^* \beta_1)^2$. i.e. $\langle\phi| \psi\rangle^2 = \langle\phi\phi| \psi\psi\rangle$.

We are now ready to state and prove the no cloning theorem:

Assume we have a unitary operator U and two quantum states $|\phi\rangle$ and

$|\psi\rangle$:

$$\begin{aligned} |\phi\rangle \otimes |0\rangle &\xrightarrow{U} |\phi\rangle \otimes |\phi\rangle \\ |\psi\rangle \otimes |0\rangle &\xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \quad . \end{aligned}$$

Then $\langle\phi|\psi\rangle$ is 0 or 1.

$\langle\phi|\psi\rangle = (\langle\phi|\otimes\langle 0|)(|\psi\rangle\otimes|0\rangle) = (\langle\phi|\otimes\langle\phi|)(|\psi\rangle\otimes|\psi\rangle) = \langle\phi|\psi\rangle^2$. In the second equality we used the fact that U, being unitary, preserves inner products.

Superdense Coding

Suppose Alice and Bob are connected by a *quantum* communications channel. By this we mean, for example, that they can communicate qubits over an optical fibre using polarized photons. Is this much more powerful than a classical communication channel, over which only classical bits may be transmitted? The answer seems obvious, since a classical bit is a special case of a quantum bit. And a qubit appears to encode an infinite number of bits of information, since to specify its state we must specify two complex numbers. However, the truth is a little more subtle, since the axioms of quantum mechanics also severely restrict how we may access information about the quantum state by a measurement.

So the question we wish to ask is "how many classical bits can Alice transmit to Bob in a message consisting of a single qubit?" We will show that if Alice and Bob share entanglement in the form of a Bell state, then Alice can transmit two classical bits by transmitting just one qubit over the quantum channel.

The overall idea is this: say Alice and Bob share $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice can transform this shared state to any of the four Bell basis states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ by applying a suitable quantum gate just to her qubit. Now if she transmits her qubit to Bob, he holds both qubits of of a Bell basis state and can perform a measurement in the Bell basis to distinguish which of the four states he holds.

Let's now see the details of Alice's protocol: if Alice wishes to transmit the two bit message $b_1 b_2$, she applies a bit flip X to her qubit if $_1 = 1$ and a phase flip Z to her qubit if $b_2 = 1$. You should verify that in the four cases 00, 01, 10, 11 this results in the two qubits being in the state $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ respectively.

After receiving Alice's qubit, Bob measures the two qubits in the Bell basis by running the circuit we saw in chapter 2 backwards (i.e., applying $(H \otimes I) \circ CNOT$), then measuring in the standard basis.

Note that Alice really did use two qubits total to transmit the two classical bits. After all, Alice and Bob somehow had to start with a shared Bell state. However, the first qubit – Bob's half of the Bell state – could have been sent well before Alice had decided what message she wished to send to Bob.

One can show that it is not possible to do any better. No more than two classical bits can be transmitted by sending just one qubit. To see why you will have to understand our next example.

Quantum Teleportation

After months of effort, Alice has managed to synthesize a special qubit, which she strongly suspects has some wonderful physical properties. Unfortunately, she doesn't explicitly know the state vector $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$. And she does not have the equipment in her lab to carry out a crucial next phase of her experiment. Luckily Bob's lab has the right equipment, though it is at the other end of town. Is there a way for Alice to safely transport her qubit to Bob's lab?

If Alice and Bob share a Bell state, then there is a remarkable method for Alice to transmit her qubit to Bob. The method requires her to make a certain measurement on her two qubits: the qubit she wishes to transmit and her share of the Bell state. She then calls up Bob on the phone and tells him the outcome of her measurement — just two classical bits. Depending upon which of four outcomes Alice announces to him on the phone, Bob performs one of four operations on his qubit, and voila, his qubit is in the state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$!

But hold on a moment, doesn't this violate the no cloning theorem?! No, because Alice's qubit was destroyed by measurement before Bob created his copy. Let us build our way to the teleportation protocol in a couple of simple stages:

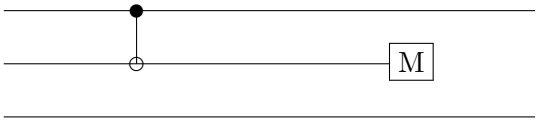
Let us start with the following scenario. Alice and Bob share two qubits in the state $a\,|00\rangle + b\,|11\rangle$. Alice and Bob don't know the amplitudes a and b. How can Bob end up with the state $a\,|0\rangle + b\,|1\rangle$? An easy way to achieve this is to perform a CNOT gate on the two qubits with Bob's qubit as the control, and Alice's qubit as the target. But this requires an exchange of quantum information. What if Alice and Bob can only exchange classical information?

Here is a way. Alice performs a Hadamard on her qubit. The state of the two qubits is now $a/\sqrt{2}(|0\rangle + |1\rangle)\,|0\rangle + b/\sqrt{2}(|0\rangle - |1\rangle)\,|1\rangle = 1/\sqrt{2}\,|0\rangle\,(a\,|0\rangle + b\,|1\rangle) + 1/sqrt2\,|1\rangle\,(a\,|1\rangle - b\,|1\rangle)$. Now if Alice measures her qubit in the standard basis, if the measurement outcome is 0, then Bob's qubit is the desired $a\,|0\rangle + b\,|1\rangle$. If the measurement outcome is 1, then Bob's qubit is $a\,|0\rangle - b\,|1\rangle$.

But in this case if Bob were to apply a phase flip gate (Z) to his qubit, it would end up in the desired state $a\,|0\rangle + b\,|1\rangle$.

Back to teleportation. Alice has a qubit in state $a\,|0\rangle + b\,|1\rangle$, and Alice and Bob share a Bell state. Is there any way for them to convert their joint state to $a\,|00\rangle + b\,|11\rangle$, without exchanging any quantum information? If they succeed, then by our previous discussion Alice can teleport her qubit to Bob.

Consider what happens if Alice applies a CNOT gate with her qubit $a\,|0\rangle + b\,|1\rangle$ as the control qubit, and her share of the Bell state as the target qubit.



$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=0,1} a_i |i\rangle \otimes \sum_{j=0,1} \frac{1}{\sqrt{2}} |j,j\rangle.$$

After passing through the CNOT gate this becomes

$$\sum_{i,j} a_i \big|i, i \oplus j, j\big\rangle.$$

Now A measures the middle qubit. Suppose it is measured as l; then $l = i \oplus j$. The state is now

$$\sum_{j} a_{j\oplus l} \big|j \oplus l, j\big\rangle.$$

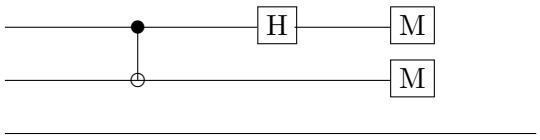
Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip on his qubit (the bottom qubit in the diagram.) A bit flip is just the transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we have

$$\sum_{j} a_{j\oplus l} \big|j, j\big\rangle.$$

Finally, B does a phase flip on his qubit, yielding

$$\sum_{j} a_j \big|j, j\big\rangle.$$

The correct solution is to go back and modify the original diagram, inserting a Hadamard gate and an additional measurement:



Now the algorithm proceeds exactly as before. However A's application of the Hadamard gate now induces the transformation

$$\sum_j a_j|j,j\rangle \longrightarrow \sum_{ij} a_j(-1)^{ij}|i,j\rangle.$$

Finally A measures i and sends the measurement to B. The state is now:

$$\sum_j a_j(-1)^{ij}|j\rangle.$$

If $i = 0$ then we are done; if $i = 1$ then B applies a phase flip. In either case the state is now $a_0|0\rangle + a_1|1\rangle$.

So A has transported the quantum state to B simply by sending two classical bits.