Quantum Computation **(CMU 18-859BB, Fall 2015)**

Lecture 3: The Power of Entanglement

September 9, 2015

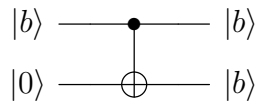
Lecturer: Ryan O'Donnell *Scribe: Joshua Brakensiek*

1 Copying bits

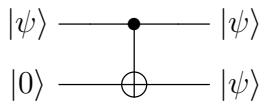
In lecture 2, we demonstrated that every quantum circuit can be thought of as a unitary matrix acting on the space of quantum states as well as described the rules for measurement and partial measurement. In this lecture, we build on these ideas to show how quantum entanglement gives quantum computers an advantage over classical computers in certain settings.

1.1 No-cloning theorem

To start, we describe a way in which quantum computation is *not* superior to classical computation. In classical computation, it is quite easy to copy information, even in a reversible manner.



This leads to a natural question: given a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, is it possible to copy $|\psi\rangle$ so that two *unentangled* qubits each have state $|\psi\rangle$? This would require the two qubits to be in a joint state of $|\psi\rangle \otimes |\psi\rangle$. As a first attempt, it seems that the classical circuit above meets our needs in the quantum setting, too.



To check, before the CNOT gate, the qubits are in the joint state of $(\alpha|0\rangle+\beta|1\rangle)\otimes(|0\rangle) = \alpha|00\rangle + \beta|10\rangle$. After the CNOT, gate the qubit are then in the joint state of $\alpha|00\rangle + \beta|11\rangle$. Unfortunately, this is not equal to our desired state of

$$|\psi\rangle \otimes |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle = \begin{bmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{bmatrix}$$

unless $\alpha = 1$ and $\beta = 0$ or $\alpha = 0$ or $\beta = 1$. That is, the circuit described above fails to copy an arbitrary quantum state into two unentangled copies. It turns out that there does not exist *any* quantum circuit which can take in an arbitrary qubit $|\psi\rangle$ and produce the state $|\psi\rangle \otimes |\psi\rangle$, even when permitted to use ancillas in the input and garbage in the output. This result is call the *No-cloning theorem* and is due to Wootters and Zurek [WZ82] (see also [dW11]).

Theorem 1.1 (No-cloning theorem.)**.** *For all $n \in \mathbb{N}$, there exists no quantum circuit C which upon input $|\psi\rangle \otimes |0^{n-1}\rangle$ outputs $|\psi\rangle \otimes |\psi\rangle \otimes f(|\psi\rangle)$, where $f(\psi)$ (the garbage) is a possibly entangled state of $n-2$ qubits.*

Remark 1.2. We may assume the ancillas are all $|0\rangle$ since we can use a NOT gate to obtain a $|1\rangle$. Additionally, we may assume that there are no measurements in C, since we can defer all measurements until the end of the computation, and we definitely would not want to measure the first two qubits of the output.

Proof. Assume for sake of contradiction that such a C exits. Let U be the unitary matrix representing C. We know that $U(|0^n\rangle) = |00\rangle \otimes f(|0\rangle)$ and $U(|1\rangle \otimes |0^{n-1}\rangle) = |11\rangle \otimes f(|1\rangle)$. Remember that $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. By the linearity of U,

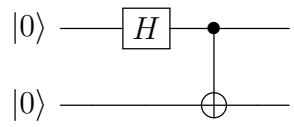
$$U\left(|+\rangle \otimes |0^{n-1}\rangle\right) = \frac{1}{\sqrt{2}}U|0^n\rangle + \frac{1}{\sqrt{2}}U(|1\rangle \otimes |0^{n-1}\rangle) = \frac{1}{\sqrt{2}}|00\rangle \otimes f(|0\rangle) + \frac{1}{\sqrt{2}}|11\rangle \otimes f(|1\rangle).$$

Thus, if we measure the first two qubits, we get the state $|00\rangle$ with probability $1/2$ and $|11\rangle$ with probability $1/2$. If U were copying $|+\rangle$ correctly, we should see each of $|00\rangle, |10\rangle, |01\rangle, |11\rangle$ with probability $1/4$. Hence, U failed to copy $|+\rangle$, so no such unitary U or circuit C exists with the desired properties. □

Although this result may seem unsettling at first, there is an intuitive analogous result in the randomized model of computation: there is no circuit which can take as input a single p-biased random bit (say from a COIN_p gate) and return as output two two independently distributed p-biased bits.

1.2 EPR pairs

Consider the following modification of our classical bit-copying circuit.



The output of this gate is the quantum state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This entangled state is call an *EPR pair*, named after Einstein, Podolsky, and Rosen[EPR35]. Although Einstein did not believe that EPR pairs existed, but they have been confirmed to exist through

experimentation (e.g. [AGR81]). EPR pairs will show up many times throughout the course, including a few times in this lecture.

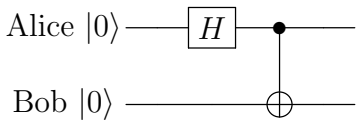
Imagine that we pass an EPR pair $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$ through the quantum gate $\mathrm{H}\otimes\mathrm{H}$; that is, we apply a separate Hadamard gate to each qubit. Recall that $\mathrm{H}|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$ and $\mathrm{H}|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. Thus, we have that

$$\begin{aligned}
(\mathrm{H}\otimes\mathrm{H})\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) &= \frac{1}{\sqrt{2}}(|+\rangle\otimes|+\rangle) + \frac{1}{\sqrt{2}}(|-\rangle\otimes|-\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\
&\quad + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\
&= \frac{1}{2\sqrt{2}}|00\rangle + \frac{1}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle \\
&\quad + \frac{1}{2\sqrt{2}}|00\rangle - \frac{1}{2\sqrt{2}}|01\rangle - \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle \\
&= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle,
\end{aligned}$$

which is our original EPR pair! In general, the bookkeeping of quantum states can be rather unintuitive.

2 Quantum teleportation

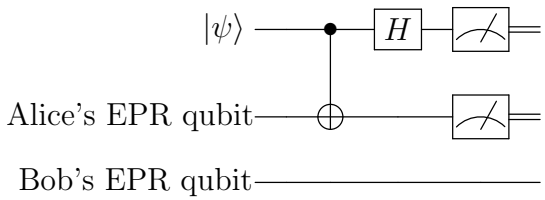
Imagine that two computer scientists, Alice and Bob, each have a qubit initialized to the classical state $|0\rangle$ and that they decide to entangle their qubits into an EPR pair. Thus, their joint state is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, where the first qubit is Alice's and second is Bob's.



Now, even if Alice's and Bob's qubits are physically separated (say they take their qubits to their own homes), the two qubits will still be an EPR pair as long as neither performs a measurement. Additionally, say that Alice has a qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ at her home, and she would like to *give* $|\psi\rangle$ to Bob. It turns out she can do this without leaving her home.

One plausible idea, is that she determines the values of α_0 and α_1 and tells these values to Bob over a *classical* channel (say over the telephone). There are two problems with this idea. First, Alice cannot learn what α_0 and α_1 are without performing a measurement, which would cause her to lose $|\psi\rangle$. Second, even if she did know what α_0 and α_1 were, since they lie in $\mathbb{C}^2$, she would need infinitely many bits of precision to accurately tell Bob what α_0 and α_1 were.

Instead, Alice can cleverly send ψ and her half of the EPR pair through the following quantum circuit.



At the beginning of the circuit, the three qubits are in the joint state of

$$|\psi\rangle \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{\alpha_0}{\sqrt{2}}|011\rangle + \frac{\alpha_0}{\sqrt{2}}|000\rangle + \frac{\alpha_1}{\sqrt{2}}|100\rangle + \frac{\alpha_1}{\sqrt{2}}|111\rangle.$$

After passing the qubits through the quantum gates, but before the measurement, the state of the circuit ends up being

$$\frac{\alpha_0}{2}|000\rangle + \frac{\alpha_1}{2}|001\rangle + \frac{\alpha_1}{2}|010\rangle + \frac{\alpha_0}{2}|011\rangle + \frac{\alpha_0}{2}|100\rangle - \frac{\alpha_1}{2}|101\rangle - \frac{\alpha_1}{2}|110\rangle + \frac{\alpha_0}{2}|111\rangle.$$

After Alice measures her two qubits. What could the possible states be? These are summarized in the following table. Recall that $|\alpha_0|^2 + |\alpha_1|^2 = 1$

Alice's measurement	Prob. of meas.	Collapsed state
$\|00\rangle$	$\frac{\|\alpha_0\|^2}{4} + \frac{\|\alpha_1\|^2}{4} = \frac{1}{4}$	$\|00\rangle \otimes (\alpha_0\|0\rangle + \alpha_1\|1\rangle)$
$\|01\rangle$	$\frac{\|\alpha_1\|^2}{4} + \frac{\|\alpha_0\|^2}{4} = \frac{1}{4}$	$\|01\rangle \otimes (\alpha_1\|0\rangle + \alpha_0\|1\rangle)$
$\|10\rangle$	$\frac{\|\alpha_0\|^2}{4} + \frac{\|-\alpha_1\|^2}{4} = \frac{1}{4}$	$\|10\rangle \otimes (\alpha_0\|0\rangle - \alpha_1\|1\rangle)$
$\|11\rangle$	$\frac{\|-\alpha_1\|^2}{4} + \frac{\|\alpha_0\|^2}{4} = \frac{1}{4}$	$\|11\rangle \otimes (-\alpha_1\|0\rangle + \alpha_0\|1\rangle)$

Note that for every possible partial measurement Alice makes, the resulting state of Bob's qubit is equal to or very close to Alice's original $|\psi\rangle$. To finish the job, Alice can call up Bob on the telephone and tell him what her partial measurement was. What Bob does next then splits into four cases.

- If Alice says $|00\rangle$, then Bob knows his qubit is in state $\begin{bmatrix}\alpha_0\\ \alpha_1\end{bmatrix} = |\psi\rangle$.
- If Alice says $|01\rangle$, then Bob applies a NOT gate, $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, to $\begin{bmatrix}\alpha_1\\ \alpha_0\end{bmatrix}$ to get $|\psi\rangle$.
- If Alice says $|10\rangle$, then Bob applies a $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ gate to $\begin{bmatrix}\alpha_0\\ -\alpha_1\end{bmatrix}$ to get $|\psi\rangle$.
- If Alice says $|11\rangle$, then Bob applies a $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, to $\begin{bmatrix}-\alpha_1\\ \alpha_0\end{bmatrix}$ to get $|\psi\rangle$.

Thus, using only an EPR pair and two classical bits, Alice was able to send to Bob her quantum state. This experiment is *not* a violation of the no-cloning theorem since Alice no longer has a copy of the quantum state. Additionally, this is a not a violation of Einstein's special/general relativity since the necessary classical bits could not have been communicated faster than the speed of light. One though could counter this with the following thought experiment. Imagine that Bob measured his qubit *immediately* after Alice measures hers (faster than the time it takes light to travel from Alice's house to Bob's house). Doesn't Bob then learn something about $|\psi\rangle$ faster than the speed of light? It turns out the answer to that question is no. Before Alice sent her qubits through the quantum circuit, if Bob were to measure his EPR-pair, he would see $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. After Alice uses her quantum circuit (including the measurement), the probability Bob sees $|0\rangle$ after his measurement is

$$\frac{1}{4}|\alpha_0|^2 + \frac{1}{4}|\alpha_1|^2 + \frac{1}{4}|\alpha_0|^2 + \frac{1}{4}|-\alpha_1|^2 = \frac{1}{2}(|\alpha_0|^2 + |\alpha_1|^2) = \frac{1}{2},$$

which is the exact same probability as before. Thus, until Alice tells Bob her two classical bits, Bob cannot learn anything about $|\psi\rangle$, and thus relativity is not violated in this example.

It turns out this procedure (see [Die82]), called *quantum teleportation*does not merely works in theory but has also been verified to work in practice. This was first verified in 1992 by Bennett, et. al., [BBC$^+$93]. In 2012, Ma, et. al., [MHS$^+$12] performed quantum teleportation at a distance of 143 kilometers. One drawback though to quantum teleportation is that it does not help someone 'believe' in quantum mechanics. That is, in order to interpret the results of these experiments one needs to already accept quantum mechanics. Soon, we discuss another experiment called the CHSH game which *does* give definitive proof that our world is quantum mechanical.

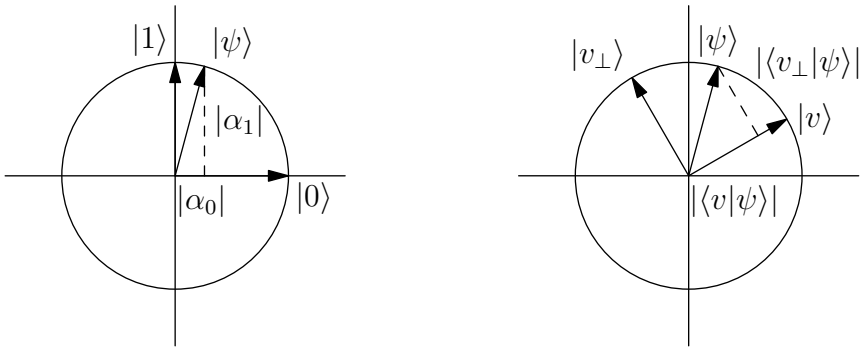
3 Measuring in a different basis

3.1 Measuring in an orthonormal basis

When we write $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, we are expressing $|\psi\rangle$ in terms of the basis $\{|0\rangle, |1\rangle\}$. This basis is called the *standard* or *computational* basis. When we perform a measurement on $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, we see $|0\rangle$ with probability $|\alpha_0|^2$ and $|1\rangle$ with probability $|\alpha_1|^2$. Since $\alpha_0 = \langle 0|\psi\rangle$ and $\alpha_1 = \langle 1|\psi\rangle$, we can rewrite these probabilities as

$$|\alpha_0|^2 = \alpha_0^\dagger \alpha_0 = \langle\psi|0\rangle\langle 0|\psi\rangle$$
$$|\alpha_1|^2 = \alpha_1^\dagger \alpha_1 = \langle\psi|1\rangle\langle 1|\psi\rangle.$$

To visualize this, imagine that $\alpha_0, \alpha_1 \in \mathbb{R}$, thus we can image $|\psi\rangle = \begin{bmatrix}\alpha_0 \\ \alpha_1\end{bmatrix}$ as a vector on the unit circle.



If we project $|\psi\rangle$ onto the x (or $|0\rangle$)-axis, the length of the resulting vector is $|\alpha_0|^2$. Furthermore, the distance from $|\psi\rangle$ to the projection is $|\alpha_1|^2$. Since the two resulting segments for a right triangle, we have from the Pythagorean theorem that $|\alpha_0|^2 + |\alpha_1|^2 = 1$, which is a familiar formula.

We can extend this analogy to an arbitrary orthonormal basis $\{|v\rangle, |v^\perp\rangle\}$. If we write $|\psi\rangle = \beta_v|v\rangle + \beta_{v^\perp}|v^\perp\rangle$, then we have that $\beta_v = \langle v|\psi\rangle$ and $\beta_{v^\perp} = \langle v^\perp|\psi\rangle$. Thus, projecting $|\psi\rangle$ onto vectors $|v\rangle$ and $|v^\perp\rangle$ results in a right triangle with legs $|\beta_v|$ and $|\beta_{v^\perp}|$.

Notice that since $\{v, v^\perp\}$ is an orthonormal basis,

$$\begin{aligned}
1 &= \langle\psi|\psi\rangle \\
&= (\beta_v^\dagger\langle v| + \beta_{v^\perp}^\dagger\langle v^\perp|)(\beta_v|v\rangle + \beta_{v^\perp}|v^\perp\rangle) \\
&= \beta_v^\dagger\beta_v\langle v|v\rangle + \beta_v^\dagger\beta_{v^\perp}\langle v|v^\perp\rangle + \beta_{v^\perp}^\dagger\beta_v\langle v^\perp|v\rangle + \beta_{v^\perp}^\dagger\beta_{v^\perp}\langle v^\perp|v^\perp\rangle \\
&= |\beta_v|^2 + |\beta_{v^\perp}|^2.
\end{aligned}$$

Thus, it is quite natural to discuss a probability distribution which says '$|v\rangle$' with probability $|\beta_v|^2$ and says '$|v^\perp\rangle$' with probability $|\beta_{v^\perp}|^2$. This is in fact the definition of measuring in a different basis.

Definition 3.1. Let $\{v, v^\perp\}$ be an orthonormal basis. The process of *measuring* $|\psi\rangle = \beta_v|v\rangle + \beta_{v^\perp}|v^\perp\rangle$ *in the basis* $\{v, v^\perp\}$ is a quantum circuit with a measurement which upon input $|\psi\rangle$ outputs $|0\rangle$ (representing an answer of '$|v\rangle$') with probability $|\beta_v|^2$ and outputs $|1\rangle$ (representing an answer of '$|v^\perp\rangle$') with probability $|\beta_{v^\perp}|$.

It turns out that a simple quantum circuit allows us to measure in the basis $\{v, v^\perp\}$, it consists of a one-qubit gate U and a measurement. Clearly this gate should have the property that $U|v\rangle = |0\rangle$ and $U|v^\perp\rangle = |1\rangle$. As discussed in Lecture 2, we must then have that $U = |0\rangle\langle v| + |1\rangle\langle v^\perp|$. It is easy then to see that if $|\psi\rangle = \beta_v|v\rangle + \beta_{v^\perp}|v\rangle$, then measuring $U|\psi\rangle = \beta_v|0\rangle + \beta_{v^\perp}|1\rangle$ yields $|0\rangle$ with probability $|\beta_v|^2$ and $|1\rangle$ with probability $|\beta_{v^\perp}|^2$, as desired.

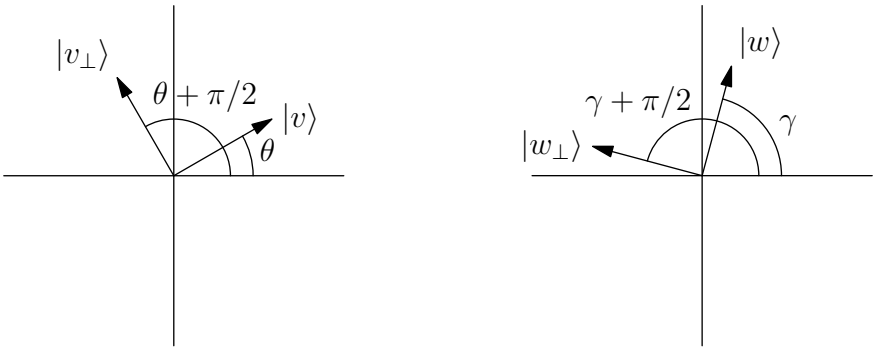
Remark 3.2. It is a standard assumption in quantum computing that all unitary 1-qubit and 2-qubit gates are available to be used at unit cost. This is not necessary since any 1-qubit or 2-qubit gate can be simulated to arbitrary precision with ancillas, CCNOT gates, and Hadamard gates; but this assumption makes quantum circuits easier to reason about.

3.2 Example

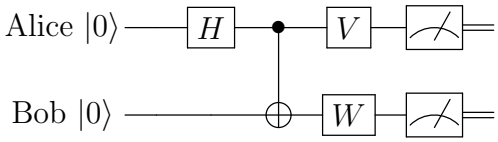
Often, the basis we which to measure in is a counter-clockwise rotation of the standard basis by an angle of θ. Thus, the change of basis matrix we desire for measuring is the *clockwise* rotation matrix by the angle of θ, which we denote as Rot_θ

$$\mathrm{Rot}_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Consider a pair of orthonormal bases $\{v, v^\perp\}$ and $\{w, w^\perp\}$ such that $\{v, v^\perp\}$ is a θ radian counter-clockwise rotation of the standard basis, and $\{w, w^\perp\}$ is a γ radian counter-clockwise rotation of the standard basis.



Thus, the unitary matrix V which allows us to measure in the basis $\{v, v^\perp\}$ corresponds to a *clockwise* rotation by θ, $V = \mathrm{Rot}_\theta$. Similarly, the unitary matrix W which allows us to measure in the basis $\{w, w^\perp\}$ is $W = \mathrm{Rot}_\gamma$. Imagine again that Alice and Bob share an EPR pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ (Alice owns the first qubit and Bob the second). If Alice applies V to her qubit, and Bob applies W to his qubit.



The resulting state can summarized by the following lemma.

Lemma 3.3. *Let θ and γ be angles and let $\Delta = \theta - \gamma$. Then,*

$$(\mathrm{Rot}_\theta \otimes \mathrm{Rot}_\gamma)\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{\sqrt{2}}(\cos\Delta|00\rangle + \sin\Delta|01\rangle - \sin\Delta|10\rangle + \cos\Delta|11\rangle).$$

Proof. This result can be verified by direct computation.

$$\begin{aligned}
(\mathrm{Rot}_\theta \otimes \mathrm{Rot}_\gamma)\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) &= \frac{1}{\sqrt{2}}(\cos\theta|0\rangle - \sin\theta|1\rangle) \otimes (\cos\gamma|0\rangle - \sin\gamma|1\rangle) \\
&\quad + \frac{1}{\sqrt{2}}(\sin\theta|0\rangle + \cos\theta|1\rangle) \otimes (\sin\gamma|0\rangle + \cos\gamma|1\rangle) \\
&= \frac{1}{\sqrt{2}}(\cos\theta\cos\gamma + \sin\theta\sin\gamma)|00\rangle \\
&\quad + \frac{1}{\sqrt{2}}(-\cos\theta\sin\gamma + \sin\theta\cos\gamma)|01\rangle \\
&\quad + \frac{1}{\sqrt{2}}(-\sin\theta\cos\gamma + \cos\theta\sin\gamma)|01\rangle \\
&\quad + \frac{1}{\sqrt{2}}(\sin\theta\sin\gamma + \cos\theta\cos\gamma)|11\rangle \\
&= \frac{1}{\sqrt{2}}(\cos\Delta|00\rangle + \sin\Delta|01\rangle - \sin\Delta|10\rangle + \cos\Delta|11\rangle).
\end{aligned}$$

□

Note that is $\theta = \gamma$, then $\Delta = 0$, and the resulting state is $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, which implies the operation restored the original EPR pair. Thus, when Alice and Bob measure an EPR pair in the same basis, they always get the same result. The lemma easily yields the following corollary about measuring the qubits.

Corollary 3.4. *After applying* $\mathrm{Rot}_\theta \otimes \mathrm{Rot}_\gamma$ *to an EPR pair, perform a measurement. The probability that both qubits in the collapsed state have the same value is* $\cos^2\Delta = \cos^2(\theta - \gamma)$. *Likewise, the probability that both qubits collapse to different states is* $\sin^2\Delta$.

Proof. The probability of measuring $|00\rangle$ is $\frac{1}{2}\cos^2\Delta$. Similarly, the probability of measuring $|11\rangle$ is $\frac{1}{2}\cos^2\Delta$. Therefore, the probability of both qubits collapsing to the same value is $\cos^2\Delta$. This directly implies that the probability of the qubits collapsing to different values is $1 - \cos^2\Delta = \sin^2\Delta$. □

If $\Delta = \pi/2$, then the probability of both qubits collapsing to different values is 1. This makes sense, since the bases Alice and Bob are measuring in are a $\pi/2$ rotation of each other.

4 CHSH Game

To demonstrate the power of entanglement, we discuss how quantum computation can give the players an edge in the following combinatorial game. Such a game was suspected by John Bell [Bel64], and was formulated by Clauser, et. al., [CHSH69].

4.1 Game formulation

Definition 4.1. The *CHSH Game* consists of a team of two players Alice and Bob who are assisted by two referees Ref. 1 and Ref. 2. Alice and Bob are separated sufficiently far away (say 1 light-second) so that they cannot communicate with each other during the game, but Alice is sufficiently close to Ref. 1 and Bob is sufficiently close to Ref. 2. At the start of the game, Ref. 1 and Ref. 2 pick select uniformly random bits $x, y \in \{0, 1\}$, respectively. Ref. 1 tells Alice x and Ref. 2 tells Bob y. Alice is then to respond with a bit $a \in \{0, 1\}$ and Bob is to respond with a bit $b \in \{0, 1\}$. Alice and Bob win if and only if $a \otimes b = x \wedge y$.

Another way to phrase the winning condition, is that Alice and Bob must produce the same bit when $(x, y) \neq (1, 1)$ and must come up with different bits otherwise. Alice and Bob are allowed to agree to a strategy before hand.

4.2 Classical strategy

It is easy to come up with a strategy in which Alice and Bob win with probability 3/4: have both players always respond with 0. It turns out that no classical strategy can do better.

Lemma 4.2. *No classical deterministic or randomized strategy which allows Alice and Bob to win with probability greater than* 3/4*.*

Proof. First, we prove that any deterministic strategy results in Alice and Bob winning at most 3/4 of the time. In a deterministic strategy, Alice's bit a must be a function of her random bit x. Thus, Alice must choose that either $a(x) = 0$, $a(x) = 1$, $a(x) = x$, or $a(x) = \neg x$. Similarly, Bob must choose between $b(y) = 0$, $b(y) = 1$, $b(y) = y$, and $b(y) = \not{y}$. The winning probability of each pair of strategies is summarized in the following table.

	$a = 0$	$a = 1$	$a = x$	$a = \neg x$
$b = 0$	3/4	1/4	3/4	1/4
$b = 1$	1/4	3/4	1/4	3/4
$b = y$	3/4	1/4	1/4	3/4
$b = \neg y$	1/4	3/4	3/4	1/4

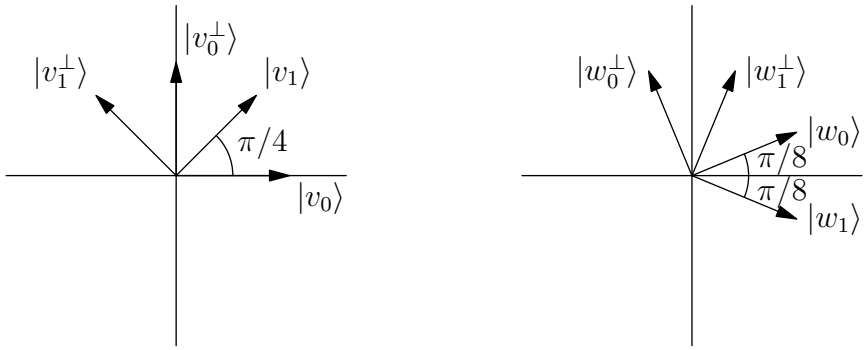
Thus, there is no deterministic strategy which beats 3/4. Since any randomized strategy is a probability distribution of these deterministic strategies, the best a randomized distribution can do is also 3/4. □

4.3 Quantum strategy

We now show how to beat 3/4 using a quantum strategy. For this quantum strategy to work, we will have Alice and Bob each share a qubit of an EPR pair. Alice and Bob will independently decide which basis to measure their qubit in the EPR pair based on the random bit they receive. By exploiting the correlations of the EPR pair, Alice and Bob will get a win probability significantly greater than 3/4.

Theorem 4.3. *There is a quantum strategy which allows Alice and Bob to win with probability* $\cos^2(\pi/8) \approx .85 > 3/4$.

Proof. Have Alice and Bob share an EPR pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Alice will measure her qubit in either basis $\{v_0, v_0^\perp\} = \{|0\rangle, |1\rangle\}$ or $\{|v_1\rangle, |v_1^\perp\rangle\} = \{|+\rangle, |-\rangle\}$, which is a $\pi/4$ counterclockwise rotation of the standard basis. Similarly, Bob will measure his qubit in either $\{|w_0\rangle, |w_0^\perp\rangle\}$ which is a $\pi/8$ rotation of the standard basis or $\{|w_1\rangle, |w_1^\perp\rangle\}$ which is a $-\pi/8$ rotation of the standard basis.



Now, when Alice and Bob receive x and y, respectively, Alice will measure in basis $\{|v_x\rangle, |v_x^\perp\rangle\}$ to determine a and Bob will measure in basis $\{|w_x\rangle, |w_x^\perp\rangle\}$ to determine b. Applying Corollary 3.4, we have that the possible scenarios are as follows

x	y	Alice's rotation θ	Bob's rotation γ	$\Delta = \theta - \gamma$	$\mathbf{Pr}$[win]
0	0	0	$\pi/8$	$-\pi/8$	$\cos^2(-\pi/8)$
0	1	0	$-\pi/8$	$\pi/8$	$\cos^2(\pi/8)$
1	0	$\pi/4$	$\pi/8$	$\pi/8$	$\cos^2(\pi/8)$
1	1	$\pi/4$	$-\pi/8$	$3\pi/8$	$\sin^2(3\pi/8)$

We take the sine instead of the cosine when $x = y = 1$ since we want $a \neq b$ in that case. In all four scenarios the probability of winning is equal to $\cos^2(\pi/8)$, so that is the overall win probability, as desired. □

4.4 Experimental verification

Like with quantum teleportation, multiple experiments have been done to verify that the quantum strategy beats the classical one. The first such experiment was done in 1981-82 by Aspect et. al. [AGR81, AGR82, ADR82]. Although the these results very much supported quantum mechanics, there were still "classical" explanations of the results. In 2015, this experiment was redone by Hensen, et. al., [HBD+15] at the University of Delft in a "loophole free" manner to essentially eliminate the possibility that our universe is *not* quantum mechanical. For a more detailed discussion, see Aaronson's article on the topic [Aar15].

References

[Aar15] Scott Aaronson. Bell inequality violation finally done right. *Shtetl-Optimized*, sep 2015. URL: http://www.scottaaronson.com/blog/?p=2464.

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental Test of Bell's Inequalities Using Time- Varying Analyzers. *Physical Review Letters*, 49:1804–1807, December 1982. doi:10.1103/PhysRevLett.49.1804.

[AGR81] A. Aspect, P. Grangier, and G. Roger. Experimental Tests of Realistic Local Theories via Bell's Theorem. *Physical Review Letters*, 47:460–463, August 1981. doi:10.1103/PhysRevLett.47.460.

[AGR82] A. Aspect, P. Grangier, and G. Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Physical Review Letters*, 49:91–94, July 1982. doi:10.1103/PhysRevLett.49.91.

[BBC+93] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[Bel64] John S Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1(3):195–200, 1964.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. URL: http://link.aps.org/doi/10.1103/PhysRevLett.23.880, doi:10.1103/PhysRevLett.23.880.

[Die82] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271 – 272, 1982. URL: http://www.sciencedirect.com/science/article/pii/0375960182900846, doi:http://dx.doi.org/10.1016/0375-9601(82)90084-6.

[dW11] Ronald de Wolf. Quantum computing: Lecture notes, 2011. URL: http://homepages.cwi.nl/~rdewolf/qcnotes.pdf.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. URL: http://link.aps.org/doi/10.1103/PhysRev.47.777, doi:10.1103/PhysRev.47.777.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri,

M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km. *ArXiv e-prints*, August 2015. `arXiv:1508.05949`.

[MHS+12] Xiao-Song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexandra Mech, Johannes Kofler, Elena Anisimova, et al. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269–273, 2012.

[WZ82] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.