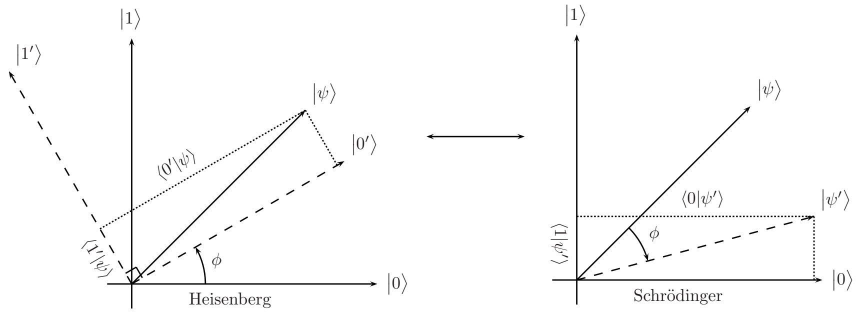
Entanglement, Bell States, EPR Paradox, Bell Inequalities.

1 One qubit:

Recall that the state of a single qubit can be written as a superposition over the possibilities 0 and 1: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Measuring in the standard basis, then, there is probability $|\alpha|^2$ that we get 0 and the new state is $|\psi'\rangle = |0\rangle$, and probability $|\beta|^2$ that we get 1 and $|\psi'\rangle = |1\rangle$.

More generally, we can measure the qubit in any orthonormal basis simply by projecting $|\psi\rangle$ onto the two basis vectors. The new state of the system $|\psi'\rangle$ is the outcome of the measurement. This is known as the Heisenberg picture.

The Schrodinger picture is equivalent. Instead of measuring the system in a rotated basis, we rotate the system (in the opposite direction) and measure it in the original, standard basis.



Rotations over a complex vector space are called unitary transformations. For example, rotation by θ is unitary. Reflection about the line $\theta/2$ is also unitary.

Hadamard gate:

The Hadamard gate is a reflection about the line $\theta = \pi/8$. This reflection maps the x-axis to the 45° line, and the y-axis to the $-45°$ line. That is

$$|0\rangle \xrightarrow{H} \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \equiv |+\rangle \tag{1}$$

$$|1\rangle \xrightarrow{H} \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle \equiv |-\rangle \quad . \tag{2}$$

In matrix form, we write

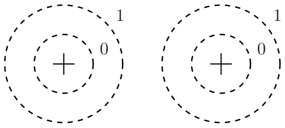
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad .$$

Notice that, starting in $|\psi\rangle$ either $|0\rangle$ or $|1\rangle$, $H|\psi\rangle$ when measured is equally likely to give 0 and 1. There is no longer any distinguishing information in the bit. This information has moved to the phase (in the computational basis).

In a quantum circuit diagram, we imagine the qubit travelling from left to right along the wire. The following diagram shows the application of a Hadamard gate.

2 Two qubits:

Now let us examine the case of two qubits. Consider the two electrons in two hydrogen atoms:



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. Quantum mechanically, they are in a superposition of those four 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 $\sum_{ij}|\alpha_{ij}|^2 = 1$. Again, this is just Dirac notation for the unit vector in $\mathscr{C}^4$:

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

where $\alpha_{ij} \in \mathscr{C}$, $\sum|\alpha_{ij}|^2 = 1$.

Measurement:

If the two electrons (qubits) are in state $\left|\psi\right\rangle$ and we measure them, then the probability that the first qubit is in state i, and the second qubit is in state j is $P(i,j) = |\alpha_{ij}|^2$. Following the measurement, the state of the two qubits is $\left|\psi'\right\rangle = \left|ij\right\rangle$. What happens if we measure just the first qubit? What is the probability that the first qubit is 0? In that case, the outcome is the same as if we had measured both qubits: $\Pr\{\text{1st bit } = 0\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. The new state of the two qubit system now consists of those terms in the superposition that are consistent with the outcome of the measurement – but normalized to be a unit vector:

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

.

A more formal way of describing this partial measurement is that the state vector is projected onto the subspace spanned by $\left|00\right\rangle$ and $\left|01\right\rangle$ with probability equal to the square of the norm of the projection, or onto the orthogonal subspace spanned by $\left|10\right\rangle$ and $\left|11\right\rangle$ with the remaining probability. In each case, the new state is given by the (normalized) projection onto the respective subspace.

Tensor products (informal):

Suppose the first qubit is in the state $\left|\phi_1\right\rangle = \alpha_1\left|0\right\rangle + \beta_1\left|1\right\rangle$ and the second qubit is in the state $\left|\phi_2\right\rangle = \alpha_2\left|0\right\rangle + \beta_2\left|1\right\rangle$. How do we describe the joint state of the two qubits?

$$\begin{aligned} \left|\phi\right\rangle &= \left|\phi_1\right\rangle \otimes \left|\phi_2\right\rangle \\ &= \alpha_1\alpha_2\left|00\right\rangle + \alpha_1\beta_2\left|01\right\rangle + \beta_1\alpha_2\left|10\right\rangle + \beta_1\beta_2\left|11\right\rangle \ . \end{aligned}$$

We have simply multiplied together the amplitudes of $|0\rangle_1$ and $|0\rangle_2$ to determine the amplitude of $|00\rangle_{12}$, and so on. The two qubits are not entangled with each other and measurements of the two qubits will be distrbuted independently.

Given a general state of two qubits can we say what the state of each of the individual qubits is? The answer is usually no. For a random state of two qubits is entangled — it cannot be decomposed into state of each of two qubits. In next section we will study the Bell states, which are maximally entangled states of two qubits.

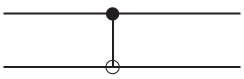
CNOT gate: The controlled-not (CNOT) gate exors the first qubit into the second qubit ($|a,b\rangle \rightarrow |a,a\oplus b\rangle = |a,a+b \bmod 2\rangle$). Thus it permutes the four basis states as follows:

$$\begin{array}{ll} 00 \rightarrow 00 & 01 \rightarrow 01 \\ 10 \rightarrow 11 & 11 \rightarrow 10 \end{array} .$$

As a unitary 4×4 matrix, the CNOT gate is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

In a quantum circuit diagram, the CNOT gate has the following representation. The upper wire is called the control bit, and the lower wire the target bit.



It turns out that this is the only two qubit gate we need to think about ...

3 Spooky Action at a Distance

Consider a state known as a EPR pair (also called a Bell state)

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Measuring the first bit of $|\Psi^-\rangle$ in the standard basis yields a 0 with probability 1/2, and 1 with probability 1/2. Likewise, measuring the second bit of $|\Psi^-\rangle$ yields the same outcomes with the same probabilities. Measuring one bit of this state yields a perfectly random outcome.

However, determining either bit exactly determines the other.

Furthermore, measurement of $|\Psi^-\rangle$ in any basis will yield opposite outcomes for the two qubits. To see this, check that $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|vv^\perp\rangle - |v^\perp v\rangle\right)$, for any $|v\rangle = \alpha|0\rangle + \beta|1\rangle$, $|v^\perp\rangle = \bar{\alpha}|1\rangle - \bar{\beta}|0\rangle$.

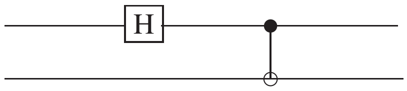
Bell states:

Including $|\Psi^-\rangle$, there are four Bell states:

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

These are maximally entangled states on two qubits. They cannot be product states because there are no cross terms.

We can generate the Bell states with a Hadamard gate and a CNOT gate. Consider the following diagram:



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

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

and after the CNOT gate the state becomes $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the Bell state $|\Phi^+\rangle$. In fact, one can verify that the four possible inputs produce the four Bell states:

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle; \qquad |01\rangle \mapsto \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle;$$
$$|10\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle; \qquad |11\rangle \mapsto \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle.$$

3.1 EPR Paradox:

In 1935, Einstein, Podolsky and Rosen (EPR) wrote a paper ”Can quantum mechanics be complete?” [Phys. Rev. 47, 777, Available online via PROLA: `http://prola.aps.org/abstract/PR/v47/i10/p777_1`]

For example, consider coin-flipping. We can model coin-flipping as a random process giving heads 50% of the time, and tails 50% of the time. This model is perfectly predictive, but incomplete. With a more accurate experimental setup, we could determine precisely the range of initial parameters for which the coin ends up heads, and the range for which it ends up tails.

For Bell state, 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. Moreover this holds in any 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.”

What would such a theory look like? Here is the most extravagant framework... When the entangled state is created, the two particles each make up a (very long!) list of all possible experiments that they might be subjected to, and decide how they will behave under each such experiment. When the two particles separate and can no longer communicate, they consult their respective lists to coordinate their actions.

But in 1964, almost three decades later, Bell showed that properties of EPR states were not merely fodder for a philosophical discussion, but had verifiable consequences: local hidden variables are not the answer.

4 Bell’s Inequality

Bell’s inequality states: There does not exist any local hidden variable theory consistent with these outcomes of quantum physics.

Consider the following communication protocol in the classical world: Alice (A) and Bob (B) are two parties who share a common string S. They receive independent, random bits X_A, X_B, and try to output bits a, b respectively, such that $X_A \wedge X_B = a \oplus b$. (The notation $x \wedge y$ takes the AND of two binary variables x and y, i.e., is one if $x = y = 1$ and zero otherwise. $x \oplus y \equiv x + y \bmod 2$, the XOR.)

In the quantum mechanical analogue of this protocol, A and B share the EPR pair $\left|\Psi^-\right\rangle$. As before, they receive bits X_A, X_B, and try to output bits a, b respectively, such that $X_A \wedge X_B = a \oplus b$.

If the odd behavior of $\left|\Psi^-\right\rangle$ can be explained using some hidden variable theory, then the two protocols give above should be equivalent.

However, Alice and Bob's best protocol for the classical game, as you will prove in the homework, is to output $a = 0$ and $b = 0$, respectively. Then $a \oplus b = 0$, so as long as the inputs $(X_A, X_B) \neq (1,1)$, they are successful: $a \oplus b = 0 = X_A \wedge X_B$. If $X_A = X_B = 1$, then they fail. Therefore they are successful with probability exactly $3/4$.

We will show that the quantum mechanical system can do better. Specifically, if Alice and Bob share an EPR pair, we will describe a protocol for which the probability $\Pr\{X_A \wedge X_B = a \oplus b\}$ is greater than 3/4.

We can setup the following protocol:

- if $X_A = 0$, then Alice measures in the standard basis, and outputs the result.
- if $X_A = 1$, then Alice rotates by $\pi/8$, then measures, and outputs the result.
- if $X_B = 0$, then Bob measures in the standard basis, and outputs the complement of the result.
- if $X_B = 1$, then Bob rotates by $-\pi/8$, then measures, and outputs the complement of the result.

Now we calculate $\Pr\{a \oplus b \neq X_A \wedge X_B\}$. (Recall that if measurement in the standard basis yields $\left|0\right\rangle$ with probability 1, then if a state is rotated by θ, measurement yields $\left|0\right\rangle$ with probability $\cos^2(\theta)$.) There are four cases:

$$\Pr\{a \oplus b \neq X_A \wedge X_B\} \quad = \quad \sum_{X_A, X_B} \tfrac{1}{4} \Pr\{a \oplus b \neq X_A \wedge X_B | X_A, X_B\}$$

Now we claim

$$\begin{aligned}
\Pr\{a \oplus b \neq X_A \wedge X_B | X_A = 0, X_B = 0\} &= 0 \\
\Pr\{a \oplus b \neq X_A \wedge X_B | X_A = 0, X_B = 1\} &= \sin^2(\pi/8) \\
\Pr\{a \oplus b \neq X_A \wedge X_B | X_A = 1, X_B = 0\} &= \sin^2(\pi/8) \\
\Pr\{a \oplus b \neq X_A \wedge X_B | X_A = 1, X_B = 1\} &= \sin^2(\pi/4) = 1/2 \ .
\end{aligned}$$

Indeed, for the first case, $X_A = X_B = 0$ (so $X_A \wedge X_B = 0$), Alice and Bob each measure in the computational basis, without any rotation. If Alice measures $a = 0$, then Bob's measurement is the opposite, and Bob outputs the complement, $b = 0$. Therefore $a \oplus b = 0 = X_A \wedge X_B$, a success. Similarly if Alice measures $a = 1$, they are always successful.

In the second case, $X_A = 0$, $X_B = 1$ ($X_A \wedge X_B = 0$). If Alice measures $a = 0$, then the new state of the system is $\left|01\right\rangle$; Bob's qubit is in the state $\left|1\right\rangle$. In the rotated basis, Bob measures a 1 (and outputs its complement, 0) with probability $\cos^2(\pi/8)$. The probability of *failure* is therefore $1 - \cos^2(\pi/8) = \sin^2(\pi/8)$. Similarly if Alice measures $a = 1$. The third case, $X_A = 1$, $X_B = 0$ is symmetrical.

In the final case, $X_A = X_B = 1$ (so $X_A \wedge X_B = 1$), Alice and Bob are measuring in bases rotated 45 degrees from each other, so their measurements are independent. The probability of failure is $1/2$.

Averaging over the four cases, we find

$$\begin{aligned}
\Pr\{a \oplus b \neq X_A \wedge X_B\} &= 1/4\left(2\sin^2(\pi/8) + 1/2\right) \\
&= 1/4\,(1 - \cos(2 * \pi/8) + 1/2) \\
&= 1/4\left(3/2 - \sqrt{2}/2\right) \\
&\approx 1/8\,(3 - 1.4) \\
&= 1.6/8 = .2 \ .
\end{aligned}$$

The probability of success with this protocal is therefore around .8, better than any protocol could achieve in the classical, hidden variable model.

Exercise: Consider the GHZ (Greenberger-Horne-Zeilinger) state, of 3 qubits:

$$\frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right)$$

Suppose three parties, A, B and C with experiments X_A, X_B, X_C respectively, with the constraint $X_A \oplus X_B \oplus X_C = 0$. Output a, b, c s.t. $X_A \vee X_B \vee X_C = a \oplus b \oplus c$. Show that this can be done with certainty. Hint: you'll need the Hadamard matrix,

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

which takes

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$