Sevag Gharibian

Lecture 2: Introduction to Quantum Mechanics

...the "paradox" is only a conflict between reality and your feeling of what reality "ought to be."
— Richard Feynman.

1 The four postulates of quantum mechanics

In this course, our aim is to study computing devices which operate according to the laws of *quantum mechanics*. Developed during the early 20th century by physicists Max Planck, Albert Einstein, Erwin Schrödinger and many others, quantum mechanics is a set of mathematical laws which describe the behaviour of subatomic particles such as protons, electrons, and photons. Although the theory has proven remarkably successful since its inception, it is nevertheless notoriously counterintuitive, an aspect which we shall explore in this lecture.

Quantum mechanics is based on four postulates, which describe the following four intuitive ideas: How to describe a single quantum system, how to perform quantum operations on a quantum system, how to describe multiple quantum systems, and how to measure or extract classical information from a quantum system. In this lecture, we explore the first three of these postulates. The fourth postulate is discussed in the following lecture.

1.1 Postulate 1: Individual quantum systems

Recall that in the classical world, a bit x can take on one of two values: 0 or 1. In the quantum world, we immediately see a radical departure from this statement — a quantum bit, or *qubit*, can take on not just 0 *or* 1, but rather *both* values 0 and 1 simultaneously. This is a very deep and counterintuitive statement, so it worth reflecting on — it is like saying you can be both asleep and awake at the same time, or here on Earth and simultaneously on Mars at the same time. Indeed, relative to life as we know it, *it makes no sense*!

Let us formalize this phenomenon. We begin by encoding bits 0 and 1 via the standard basis vectors $|0\rangle, |1\rangle \in \mathbb{C}^2$. Then, to denote that a qubit is in states $|0\rangle$ and $|1\rangle$ simultaneously, we write

$$|0\rangle + |1\rangle.$$

This is called a *superposition*. More generally, we can change the "extent" to which the qubit is in state $|0\rangle$ versus $|1\rangle$ via *amplitudes* $\alpha, \beta \in \mathbb{C}$, i.e.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

The only restriction is that $|\psi\rangle$ must be a unit vector, i.e. that $|\alpha|^2 + |\beta|^2 = 1$. To summarize, any unit vector in $\mathbb{C}^2$ describes the state of a single qubit.

Exercise. Among the most commonly used single qubit states are $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Verify that these are indeed unit vectors.

Aside: Schrödinger's cat. To demonstrate how strange the concept of quantum superposition is, in 1935 Austrian physicist Erwin Schrödinger devised a thought experiment, nowadays infamously referred to as *Schrödinger's cat*. The experiment, depicted in[1] Figure 1.1, goes as follows (we give a slight variant suitable

[1]Figure due to user Dhatfield, obtained from `https://commons.wikimedia.org/wiki/File:Schrodingers_cat.svg`.

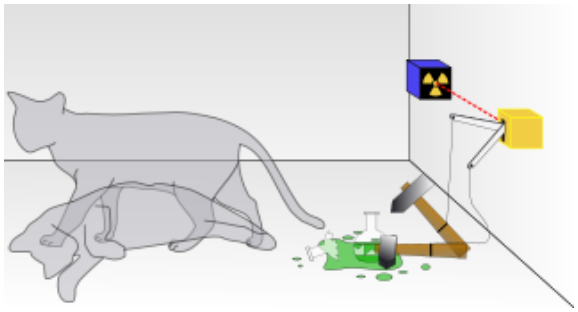


Figure 1: A depiction of Schrödinger's cat.

to our exposition of quantum mechanics here): Suppose that we place a cat in a box and *close* the box (i.e. one cannot look inside the box). In the box, we place a flask of poison, along with a hammer. The hammer is connected to a mechanism outside the box, which is controlled by a computer. If the computer is fed input 0, then nothing happens, and the cat is happy doing whatever it is doing in the box. On the other hand, if the input is 1, then the hammer falls and breaks the flask, releases the poison, and kills the cat.

And now Schrödinger asked the key question: *What if we input a* superposition *of* 0 *and* 1 *to the computer, i.e. the state* $|0\rangle + |1\rangle$*?* If we interpret quantum mechanics literally, then we conclude that the cat is both alive and dead, *at the same time*! Of course, this makes absolutely no sense. Moreover, common sense tells us that if you simply *open* the box and look inside, we will find either a cat which is alive or dead, not both. How can this paradox be resolved? Read on to Postulate 4 to find out!

Finally, thus far we have described the state of a single (2-dimensional) qubit. More generally, the state of a d-dimensional quantum system, called a qu$d$it, is described by a unit vector $|\psi\rangle \in \mathbb{C}^d$, which can be described as

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{d-1}|d-1\rangle = \sum_{i=0}^{d-1} \alpha_i|i\rangle,$$

where recall $|i\rangle \in \mathbb{C}^d$ denotes the ith computational basis vector and $\alpha_i \in \mathbb{C}$. Since $|\psi\rangle$ is a unit vector, we have $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$.

1.2 Postulate 2: Quantum operations

We next ask: What types of operations or maps can we perform on a qubit? Since a qubit is a vector, the natural choice is a linear map, i.e. multiplication by a matrix. However, not all matrices are fair game — it turns out that nature only allows a special class of matrices known as *unitary* matrices. A unitary matrix $U \in \mathcal{L}(\mathbb{C}^d)$ is one which satisfies $UU^\dagger = U^\dagger U = I$. In other words, the *inverse* of U is simple to calculate — just take the dagger of U. This immediately yields a key insight — all quantum gates are *reversible*.

Among the most common single qubit gates are the following, known as the *Pauli* gates, after Austrian-Swiss physicist Wolfgang Pauli:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Exercise. Verify that Pauli X, Y, and Z are unitary.

The X gate acts as a "quantum" NOT gate, as we see below:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad \text{and} \qquad X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle.$$

It follows that $|+\rangle$ and $|-\rangle$ are eigenvectors of X, i.e. $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$ (as we calculated in the last lecture). The spectral decomposition of X is hence $X = |+\rangle\langle+| - |-\rangle\langle-|$.

Exercise. Write $|+\rangle\langle+| - |-\rangle\langle-|$ out as a matrix to verify that it indeed equals X.

The Z gate, on the other hand, has no classical analogue. It acts as

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad \text{and} \qquad Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle.$$

In other words, Z leaves $|0\rangle$ invariant, but injects a "phase" of -1 in front of $|1\rangle$. This also immediately shows that $|0\rangle$ and $|1\rangle$ are eigenvectors of Z with eigenvalues 1 and -1, respectively.

Exercise. Write down the spectral decomposition of Z.

The Z gate is special in that it allows us to inject a *relative phase* into a quantum state. For example,

$$Z|+\rangle = Z\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}Z|0\rangle + \frac{1}{\sqrt{2}}Z|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle.$$

By relative phase, we mean that only the amplitude on $|1\rangle$ had its sign changed (or more generally, was multiplied by a phase $e^{i\pi} = -1$). If *all* the amplitudes in the state were instead multiplied by $e^{i\pi}$, then we could simply factor out the $e^{i\pi}$ from the entire state — in this case, we would call $e^{i\pi}$ a *global* phase. It turns out that a global phase is insignificant in that it cannot be experimentally detected. A relative phase may seemingly also look unimportant - yet, as we shall see in this course, it is one of the features of quantum mechanics which allows quantum computers to outperform classical ones!

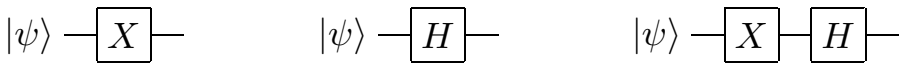
Finally, we come to a fourth important unitary gate, the *Hadamard* gate:

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

The Hadamard gate is special in that it creates superpositions for us. Namely, we have $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. It can also "erase" superpositions, i.e. $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$. In other words, H is self-inverse — we have that $H^2 = I$ for I the identity matrix. In fact, the Pauli matrices are also self-inverse.

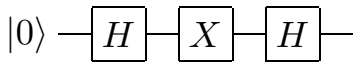
Exercise. Verify that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. Also verify that $H^2 = I$.

It is very useful to graphically depict sequences of quantum gates via *quantum circuits*. For example, here are three circuits:



They correspond to evolutions $X|\psi\rangle$, $H|\psi\rangle$, and $HX|\psi\rangle$, respectively. Each wire in such a diagram denotes a quantum system, and a box labelled by gate U depicts the action of unitary U. We think of time going from left to right; for the last circuit above, note that the X appears on the "left" in the circuit diagram but on the "right" in the expression $HX|\psi\rangle$; this is because X should be applied first to $|\psi\rangle$, then H.

Exercise. What single-qubit state does the following circuit output? (Hint: Rather than explicitly calculating this, try to use your knowledge of the action of H on states $|0\rangle$ and $|+\rangle$, and the eigenvectors of X.)



1.3 Postulate 3: Composite quantum systems

Thus far, we have considered only single quantum systems, i.e. states $|\psi\rangle \in \mathbb{C}^d$ for $d \geq 2$. But a computer with just a single qubit might be rather uninteresting! What we would instead like is to discuss *multiple* qubits simultaneously. How can we mathematically describe, for example, the joint state of two qubits?

The correct Linear Algebraic tool for this task is the *tensor product*, denoted $\otimes$. The tensor product allows us to "stitch together" two vectors, say $|\psi\rangle, |\phi\rangle \in \mathbb{C}^2$, to obtain a larger 4-dimensional vector $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^4$. Formally, we have $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^{2\times 2}$. In other words, the entries of a vector $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ can be referenced via a pair of indices (i, j) for $i, j \in \{0, 1\}$, and the specific rule for doing so is

$$(|\psi\rangle \otimes |\phi\rangle)(i, j) := \psi_i \phi_j,$$

where recall ψ_i and ϕ_j are the entries of $|\psi\rangle$ and $|\phi\rangle$, respectively. Here, you should think of the pair (i, j) as representing the bits of a single index $x \in \{0, 1, 2, 3\}$. So for example, $(0, 0)$ is equivalent to index 0, $(0, 1)$ to index 1, and $(1, 1)$ to index 3. This implies that we can think of $|\psi\rangle \otimes |\phi\rangle$ as having four entries, i.e. $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^4$. Let us demonstrate with some examples:

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Exercise. Verify that

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Note that in the four equations above, the four-dimensional vectors obtained are just the computational basis vectors for $\mathbb{C}^4$! This hints at an important fact: If we take orthonormal bases $B_1 = \{|\psi_0\rangle, |\psi_1\rangle\}$ and $B_2 = \{|\phi_0\rangle, |\phi_1\rangle\}$ for $\mathbb{C}^2$, then we can obtain an orthonormal basis for $\mathbb{C}^4$ by tensoring together the elements of B_1 and B_2 in all four possible combinations, i.e. $\{|\psi_0\rangle \otimes |\phi_0\rangle, |\psi_0\rangle \otimes |\phi_1\rangle, |\psi_1\rangle \otimes |\phi_0\rangle, |\psi_1\rangle \otimes |\phi_1\rangle\}$ forms an orthonormal basis for $\mathbb{C}^4$. For brevity, we shall often drop the notation $\otimes$ and simply write $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle$.

Exercise. Compute the 4-dimensional vectors corresponding to $|1\rangle \otimes |-\rangle$ and $|+\rangle \otimes |+\rangle$.

Our discussion thus far generalizes straightforwardly to the case of $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$. Specifically, for $|\psi\rangle \in \mathbb{C}^{d_1}$ and $|\phi\rangle \in \mathbb{C}^{d_2}$, we have that $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^{d_1 d_2}$. Then, for $i \in \{0, \ldots, d_1 - 1\}$ and $j \in \{0, \ldots, d_2 - 1\}$, we have $(|\psi\rangle \otimes |\phi\rangle)(i, j) := \psi_i \phi_j$. Thus, for example, if we add a third qubit to our existing two qubit system, then we have a state which lives in $\mathbb{C}^4 \otimes \mathbb{C}^2 = \mathbb{C}^8$. In fact, for each qubit we add to our system, the dimension grows by a factor of 2, i.e. it grows exponentially — in general, an n-qubit state will correspond to a vector $|\psi\rangle \in (\mathbb{C})^{2^n}$! It is precisely this exponential growth in complexity which makes it difficult for classical computers to simulate the mechanics of an n-qubit quantum state — indeed, this was the reason why physicist Richard Feynman proposed the concept of a quantum computer in 1982 to begin with!

Finally, the tensor product has the following important properties for any $|a\rangle, |b\rangle \in \mathbb{C}^{d_1}$ and $|c\rangle, |d\rangle \in \mathbb{C}^{d_2}$, which we will use repeatedly:

$$\begin{aligned}
(|a\rangle + |b\rangle) \otimes |c\rangle &= |a\rangle \otimes |c\rangle + |b\rangle \otimes |c\rangle && (1)\\
|a\rangle \otimes (|c\rangle + |d\rangle) &= |a\rangle \otimes |c\rangle + |a\rangle \otimes |d\rangle && (2)\\
c(|a\rangle \otimes |c\rangle) &= (c|a\rangle) \otimes |c\rangle = |a\rangle \otimes (c|c\rangle) && (3)\\
(|a\rangle \otimes |c\rangle)^\dagger &= |a\rangle^\dagger \otimes |c\rangle^\dagger = \langle a| \otimes \langle c| && (4)\\
(\langle a| \otimes \langle c|)(|b\rangle \otimes |d\rangle) &= \langle a|b\rangle\langle c|d\rangle. && (5)
\end{aligned}$$

Exercise. What is the inner product of $|0\rangle|1\rangle$ and $|1\rangle|0\rangle$? How about the inner product of $|0\rangle|0\rangle$ and $|+\rangle|-\rangle$?

Quantum entanglement. Now that we know how to stitch together a pair of single qubit states, it turns out we have opened Pandora's box. For we can now talk about the two-qubit state which troubled Einstein to the end of his days — the innocuous-looking *Bell state*:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

This state demonstrates a quantum phenomenon known as *entanglement* — intuitively, if a pair q_0 and q_1 of qubits are entangled, then they are so "tightly bound" that one cannot accurately describe the state of q_0 or q_1 alone — only the *joint* state of q_0 and q_1 can be described precisely. In the language of tensor products, this is captured by the following statement: There do not exist $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$ such that $|\Phi^+\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. In 1935, Einstein, Podolsky and Rosen published a famous paper nowadays referred to as the "EPR" paper, in which they argue that quantum mechanics cannot be a complete physical theory because it allows the existence of states such as $|\Phi^+\rangle$. Fast forwarding a number of decades, we now not only believe entanglement is real, but we know that is is a *necessary resource* for quantum computers to outperform classical ones.

We shall later return to the topic of entanglement, but for now let us remark that there are three other such Bell states:

$$\begin{aligned}
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}.
\end{aligned}$$

Note that here we have further simplified notation by letting (e.g.) $|0\rangle|0\rangle = |00\rangle$. The four Bell states $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ form an orthonormal basis for $\mathbb{C}^4$ known as the *Bell* basis, after Northern Irish physicist John Bell.

Exercise. Verify that the Bell basis indeed forms an orthonormal basis, i.e. check that the Bell states are pairwise orthogonal unit vectors.

Two-qubit quantum gates. We have seen that two-qubit quantum states are described by unit vectors in $\mathbb{C}^4$. We can thus discuss two-qubit quantum gates, i.e. unitary operators $U \in \mathcal{L}(\mathbb{C}^4)$. There are two types of such gates: The first are simply tensor products of one-qubit gates, such as $X \otimes Z$ or $H \otimes H$. Here, the tensor product is defined analogously for matrices as it is for vectors. (The formal description is cumbersome, but we follow with a helpful illustration to clarify.) For any $A \in \mathcal{L}(\mathbb{C}^{d_1})$, $B \in \mathcal{L}(\mathbb{C}^{d_2})$, $A \otimes B$ is a $d_1 d_2 \times d_1 d_2$ complex matrix whose entries are indexed by $([d_1] \times [d_2], [d_1] \times [d_2])$ (where $[d] = \{0, \ldots, d-1\}$ here), such that

$$(A \otimes B)((i_1, j_1), (i_2, j_2)) := A(i_1, i_2)B(j_1, j_2).$$

To clarify this definition, suppose

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

Then, $A \otimes B$ is given by

$$A \otimes B = \begin{pmatrix} a_1 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_2 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \\ a_3 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} & a_4 \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \end{pmatrix}.$$

In other words, $A \otimes B$ is obtained by taking four copies of B, each time multiplying by a different scalar entry of A.

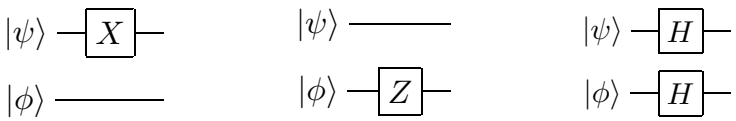
Exercise. What is $X \otimes I$? How about $Z \otimes H$?

The tensor product for matrices shares the properties of the tensor product for vectors, with the addition of two rules below:

$$(A \otimes B)(C \otimes D) = AC \otimes BD \qquad \text{and} \qquad \mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B).$$

Exercise. What is $(Y \otimes Y)(Y \otimes Y)$? How about $\mathrm{Tr}(X \otimes X)$?

The circuit diagrams for tensor products of unitaries are depicted below: We consider the cases of $X \otimes I$, $I \otimes Z$, and $H \otimes H$, respectively.



Exercise. What is the circuit diagram for $Z \otimes Z$? What is $(X \otimes X)|0\rangle \otimes |1\rangle$? How about $(Z \otimes Z)|1\rangle \otimes |1\rangle$?

Finally, we can also consider genuinely two-qubit gates, i.e. gates which are not the tensor product of single qubit gates. One important such gate is the *controlled-NOT* gate, denoted CNOT. The CNOT treats one qubit as the *control* qubit, and the other as the target *qubit*. It then applies the Pauli X gate to the target qubit only if the control qubit is set to $|1\rangle$. More precisely, the action of the CNOT on a two-qubit basis is given as follows, where qubit 1 is the control and qubit 2 is the target:

$$\mathrm{CNOT}\,|00\rangle = |00\rangle \quad \mathrm{CNOT}\,|01\rangle = |01\rangle \quad \mathrm{CNOT}\,|10\rangle = |11\rangle \quad \mathrm{CNOT}\,|11\rangle = |10\rangle.$$

Exercise. What is $\mathrm{CNOT}\,|\Phi^+\rangle$ for $|\Phi^+\rangle$ the Bell state? Can you simplify the result to get answer $|+\rangle|0\rangle$?

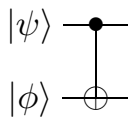
The CNOT gate is given by matrix:

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix},$$

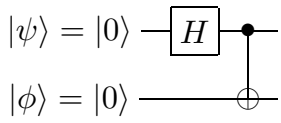
where the second expression is in block matrix form with I and X the identity and X matrices.

Exercise. Verify that multiplying $|11\rangle$ by the matrix for CNOT indeed yields $|10\rangle$.

The circuit diagram for the CNOT is given by



With this in hand, we can do our first interesting computation — we can prepare the Bell state $|\Phi^+\rangle$ starting from an initial state of $|0\rangle|0\rangle$! The preparation circuit is given as:



To see that this works, note that this diagram is equivalent to

$$\begin{aligned}
\text{CNOT}(H \otimes I)|0\rangle|0\rangle &= \text{CNOT}\,|+\rangle|0\rangle \\
&= \text{CNOT}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle \\
&= \frac{1}{\sqrt{2}}\,\text{CNOT}\,(|00\rangle + |10\rangle) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= |\Phi^+\rangle.
\end{aligned}$$

Exercise. Show that applying the preparation circuit above on initial states $|01\rangle$, $|10\rangle$, and $|11\rangle$ yields the remaining Bell basis states $|\Psi^+\rangle$, $|\Phi^-\rangle$, and $|\Psi^-\rangle$, respectively.