Chapter 3

Quantum Gates, Circuits & Teleportation

Unitary Operators

The third postulate of quantum physics states that the evolution of a quantum system is necessarily unitary. Geometrically, a unitary transformation is a rigid body rotation of the Hilbert space, thus resulting in a transformation of the state vector that doesn't change its length.

Let us consider what this means for the evolution of a qubit. A unitary transformation on the Hilbert space $\mathbb{C}^2$ is specified by mapping the basis states $|0\rangle$ and $|1\rangle$ to orthonormal states $|v_0\rangle = a\,|0\rangle + b\,|1\rangle$ and $|v_1\rangle = c\,|0\rangle + d\,|1\rangle$. It is specified by the linear transformation on $\mathbb{C}^2$:

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

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

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

then it is easily verified that $UU^\dagger = U^\dagger U = I$. Indeed, we can turn this around and say that a linear transformation U is unitary if and only if it satisfies this condition, that

$$UU^\dagger = U^\dagger U = I.$$

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

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$ in the real plane. In the complex plane it is actually a π-rotation about the $\pi/8$ axis.

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

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

- Rotation Gate. This rotates the plane by θ.

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

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

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

- Phase Flip.

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

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

How do we physically effect such a (unitary) transformation on a quantum system? To explain this we must first introduce the notion of the Hamiltonian acting on a system; you will have to wait for three to four lectures before we get to those concepts.

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.

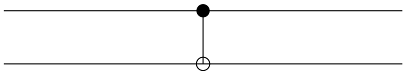
A very basic two qubit gate is the controlled-not gate or the CNOT:

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:

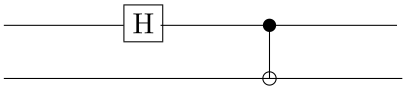
$$\begin{aligned} |0\rangle &\to 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle \\ |1\rangle &\to 1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle\,. \end{aligned}$$

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

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

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 $\mathbb{C}^4$.

Tensor Products

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 $|00\rangle$.

Tensor product of operators

Suppose we have two quantum systems: a k-state system with associated Hilbert space V and a l-state system with associated Hilbert space W. Suppose we apply a unitary transformation A to the first system and B to the second system. What is the resulting transformation on the combined system $V \otimes W$? To figure this out, let us first see how the combined transformation acts on basis states of $V \otimes W$. Consider a basis state $|i\rangle \otimes \{ketj$ where $0 \leq i \leq k-1$ and $0 \leq j \leq l-1$. Since A is only acting on V and B only on W, this state is transformed to $A|i\rangle \otimes B|j\rangle$.

Suppose $|v\rangle$ and $|w\rangle$ are unentangled states on $\mathbb{C}^m$ and $\mathbb{C}^n$, respectively. The state of the combined system is $|v\rangle \otimes |w\rangle$ on $\mathbb{C}^{mn}$. If the unitary operator A is applied to the first subsystem, and B to the second subsystem, the combined state becomes $A|v\rangle \otimes B|w\rangle$.

In general, the two subsystems will be entangled with each other, so the combined state is not a tensor-product state. We can still apply A to the first subsystem and B to the second subsystem. This gives the operator $A \otimes B$ on the combined system, defined on entangled states by linearly extending its action on unentangled states.

(For example, $(A \otimes B)(|0\rangle \otimes |0\rangle) = A|0\rangle \otimes B|0\rangle$. $(A \otimes B)(|1\rangle \otimes |1\rangle) = A|1\rangle \otimes B|1\rangle$. Therefore, we define $(A \otimes B)(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle)$ to be $\frac{1}{\sqrt{2}}(A \otimes B)|00\rangle + \frac{1}{\sqrt{2}}(A \otimes B)|11\rangle = \frac{1}{\sqrt{2}}(A|0\rangle \otimes B|0\rangle + A|1\rangle \otimes B|1\rangle)$.)

Let $|e_1\rangle, \ldots, |e_m\rangle$ be a basis for the first subsystem, and write $A = \sum_{i,j=1}^{m} a_{ij} |e_i\rangle\langle e_j|$ (the i,jth element of A is a_{ij}). Let $|f_1\rangle, \ldots, |f_n\rangle$ be a basis for the second subsystem, and write $B = \sum_{k,l=1}^{n} b_{kl} |f_k\rangle\langle f_l|$. Then a basis for the combined system is $|e_i\rangle \otimes |f_j\rangle$, for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. The operator $A \otimes B$ is

$$\begin{aligned}
A \otimes B = & \left(\sum_{ij} a_{ij} \left| e_i \middle\rangle\!\middle\langle e_j \right| \right) \otimes \left(\sum_{kl} b_{kl} \left| f_k \middle\rangle\!\middle\langle f_l \right| \right) \\
= & \sum_{ijkl} a_{ij} b_{kl} \left| e_i \middle\rangle\!\middle\langle e_j \right| \otimes \left| f_k \middle\rangle\!\middle\langle f_l \right| \\
= & \sum_{ijkl} a_{ij} b_{kl} (|e_i\rangle \otimes |f_k\rangle)(\langle e_j| \otimes \langle f_l|) \ .
\end{aligned}$$

Therefore the $(i,k),(j,l)$th element of $A \otimes B$ is $a_{ij}b_{kl}$. If we order the basis $|e_i\rangle \otimes |f_j\rangle$ lexicographically, then the matrix for $A \otimes B$ is

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \ ;$$

in the i,jth sub-block, we multiply a_{ij} by the matrix for B.

3.1 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 $|\psi\rangle$:

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

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_1b_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 $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$!

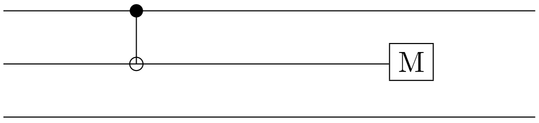
But hold on a moment, doesn't this violate the no cloning theorem?! No, because Alice's qubit was destroyed by measurement before Bob created his copy. Let us build our way to the teleportation protocol in a couple of simple stages:

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 $a/\sqrt{2}(|0\rangle + |1\rangle)\,|0\rangle + b/\sqrt{2}(|0\rangle - |1\rangle)\,|1\rangle = 1/\sqrt{2}\,|0\rangle\,(a\,|0\rangle + b\,|1\rangle) + 1/\sqrt{2}\,|1\rangle\,(a\,|1\rangle - b\,|1\rangle)$. 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

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

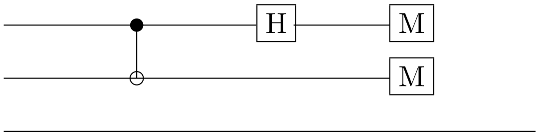
Now A measures the middle qubit. Suppose it is measured as l; then $l = i \oplus j \implies j = i \oplus l$. The state is now

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

Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip, X, on his qubit, resulting in the desired state

$$\sum_i a_i \big|i, i\big\rangle.$$

We already saw how to teleport once we achieved this state. Putting it all together, the following quantum circuit describes the resulting teleportation protocol. The topmost qubit is the unknown qubit that Alice wishes to teleport, the second and third qubits are initially in a Bell state:



The measurement of the middle qubit after performing the CNOT gate sets up the state $\sum_j a_j \big|j, j\big\rangle$ on the first and third qubit. Moreover, A's application of the Hadamard gate on the first qubit induces the transformation

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

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.