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

Lecture 2: Quantum Math Basics

September 14, 2015

Lecturer: John Wright *Scribe: Yongshan Ding*

1 Complex Numbers

From last lecture, we have seen some of the essentials of the quantum circuit model of computation, as well as their strong connections with classical randomized model of computation. Today, we will characterize the quantum model in a more formal way. Let's get started with the very basics, complex numbers.

Definition 1.1. A *complex number* $z \in \mathbb{C}$ is a number of the form $a + bi$, where $a, b \in \mathbb{R}$, and i is the imaginary unit, satisfying $i^2 = -1$.

It's always convenient to picture a complex number $z = a + bi$ as a point (a, b) in the two-dimensional *complex plane*, where the horizontal axis is the real part and the vertical axis is the imaginary part:

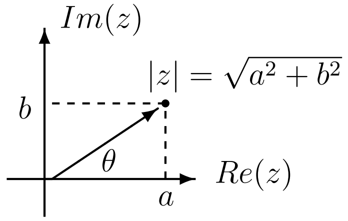


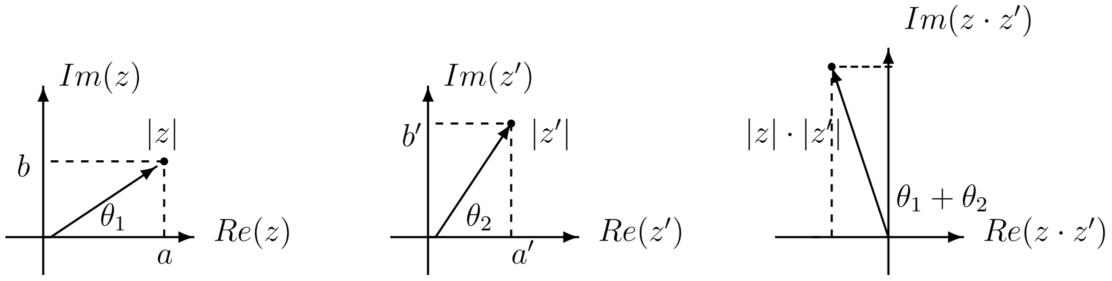
Figure 1: Geometric representation of complex number $z = a + bi$

Another common way of parametrizing a point in the complex plane, instead of using Cartesian coordinates a and b, is to use the *radial coordinate* r (the Euclidean distance of the point from the origin $|z| = \sqrt{a^2 + b^2}$), together with the *angular coordinate* θ (the angle from the real axis). In particular, it can help us visualize geometrically what the *multiplication* operation does:

Observation 1.2. *The product of two complex numbers z_1, z_2 has magnitude $|z_1| \cdot |z_2|$ and angle $\theta_1 + \theta_2$.*

Figure 2 is the geometric visualization of the multiplication of two complex numbers $z = a + bi$ and $z' = a' + b'i$. Another important operation on complex numbers is the complex conjugate:

Definition 1.3. The *complex conjugate* of a complex number $z = a + bi$ is defined as $\bar{z} = a - bi$, also denoted as z^* or $z^\dagger$.



(a) $z = a + bi$ (b) $z' = a' + b'i$ (c) $z \cdot z'$

Figure 2: Geometric representation of $z \cdot z'$

As a convention for complex numbers, we call the product of a complex number with its complex conjugate the *square* of that complex number, which is essentially the square of its magnitude:

$$z \cdot z^\dagger = (a + bi)(a - bi) = a^2 + b^2 = |z|^2$$

Notice that the result is always a real number, which becomes obvious when we realize that $z^\dagger$ is basically a reflection of z about the real axis. Since the sum of their angles in the complex plane is 0, $z \cdot z^\dagger$ always lands on the axis. We can therefore naturally generalize the inner product for complex vectors.

Definition 1.4. The *inner product (or dot product)* of two d-dimensional vectors is defined as $(z_1, \ldots, z_d) \cdot (w_1, \ldots, w_d) = z_1^\dagger w_1 + \cdots + z_d^\dagger w_d$.

The dot product of a vector with itself now becomes:

$$(z_1, \ldots, z_d) \cdot (z_1, \ldots, z_d) = |z_1|^2 + \cdots + |z_d|^2.$$

2 Quantum Bits

Just as a classical bit can have a state of either 0 or 1, the two most common states for a **qubit** *(quantum bit)* are the states $|0\rangle$ and $|1\rangle$. For now, let's just see the notation "$|\ \rangle$" as a way of distinguishing qubits from classical bits. The *actual* difference though is that a qubit can be in *linear combinations* of states, also know as *superpositions.* In other words, we can write a quantum state in a more general form:

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

where $\alpha, \beta \in \mathbb{C}$, and $|\alpha|^2 + |\beta|^2 = 1$. Two other famous states that we will see very often in this class are:

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,, \quad |-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\,.$$

We can also think of $|\psi\rangle$ as a vector in the two-dimensional complex plane spanned by the two basis states $|0\rangle$ and $|1\rangle$. As mentioned last time, often we can view α and β as *real numbers* without losing much. The reason we can sometimes ignore the fact that they are complex numbers is that $\mathbb{C}$ can be easily simulated by $\mathbb{R}^2$. That's in fact exactly what we did when we imagined the two-dimensional complex plane in the previous section. Then, why do we even use complex numbers at all? Well, there are two major reasons: firstly, complex phases are intrinsic to many quantum algorithms, like the Shor's Algorithm for prime factorization. Complex numbers can help us gain some intuitions on those algorithms. Secondly, complex numbers are often just simpler in terms of describing unknown quantum states, and carrying out computations.

We have been talking about qubits for a while, but how are they *implemented*? In fact many different physical systems can accomplish this. Although we won't cover the entire physics behind them, a general idea of how the qubits are realized physically can sometimes help us understand the procedures and algorithms we are dealing with. In particular, they might be represented by two states of an electron orbiting an atom; by two directions of the spin (*intrinsic angular momentum*) of a particle; by two polarizations of a photon. Let's take a spin-$\frac{1}{2}$ particle as an example. If we were to measure its spin along the z-axis, we would observe that it is either *up* (in $+z$ direction) or *down* (in $-z$ direction). In many physics papers, the two states are denoted as $|z+\rangle$ and $|z-\rangle$, or $|\uparrow\rangle$ and $|\downarrow\rangle$. For computational purposes, we can simply regard them as our good old friends $|0\rangle$ and $|1\rangle$.

2.1 Multiple Qubits and the Qudit System

Let's begin the discussion on multiple-qubit system from the simpliest: a *two-qubit system.* Just as classical 2-bit system, we have four possible computational basis states, namely $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. We can thus write a general form of the two-qubit state as follows:

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

where the amplitudes satisfy $|\alpha_{00}|^2 + \cdots + |\alpha_{00}|^2 = 1$. For instance, we can have a *uniformly mixed state* where the scalar coefficients are the same: $\alpha_{00} = \alpha_{01} = \alpha_{10} = \alpha_{11} = \frac{1}{2}$. Or more interestingly, we can have the following state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Note that this is a system where the two qubit are *correlated*! In particular, they seem to be always in the same state. We will come back to this interesting state very often in the future.

Now, it's time to the extend this to a more general case: *the qudit system.* Specifically, a state in the **d**-dimensional qu**d**it system is a superposition of d basis states. We can write:

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_d|d\rangle,$$

where $|\alpha_1|^2 + \cdots + |\alpha_d|^2 = 1$ as always.

How is a qudit system implemented in physical reality? In fact, particles are allowed to have *spin quantum number* of $0, \frac{1}{2}, 1, \frac{3}{2}, 2,$ etc. For example, a spin-$\frac{1}{2}$ particle, like an electron, is a natural "*qubit*" system, whereas a spin-1 particle, like a photon or a gluon, is a "*qutrit*" system. Although no fundamental particle has been experimentally found to have spin quantum number higher than 1, the two-qubit system we mentioned earlier behaves exactly the same as a qudit system where $d = 4$. In theory, we could construct any qudit system using only qubits.

2.2 Qubits - the Mathematics

As we saw earlier, a quantum state in the qubit system can be represented as a unit (*column*) vector in the $\mathbb{C}^2$ plane, spanned by the following two basis state:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

With a little bit of algebra, we can write a general state $|\psi\rangle$ as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

where $|\alpha|^2 + |\beta|^2 = 1$. Before we look into the properties of quantum states, let's first introduce the style of notations we use: *the Bra-ket notation*, also called *the Dirac notation.*

Notation 2.1. *A quantum state $|\psi\rangle$ is a (column) vector, also known as a* **ket**, *whereas a state $\langle\psi|$ is the (row) vector dual to $|\psi\rangle$, also know as a* **bra**.

To get a bra vector from a ket vector, we need to take the *conjugate transpose.* Thus we can write:

$$\langle\psi| = (|\psi\rangle)^\dagger = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}^\dagger = \begin{bmatrix} \alpha^\dagger & \beta^\dagger \end{bmatrix}.$$

Now, suppose we have two quantum states: $|x_1\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$ and $|x_2\rangle = \beta_0\,|0\rangle + \beta_1\,|1\rangle$. One possible operation we can do is of course multiplication.

Definition 2.2. The *inner product (or dot product)* of two quantum states $|x_1\rangle$ and $|x_2\rangle$ is defined as $\langle x_1| \cdot |x_2\rangle$, which can be further simplified as $\langle x_1|x_2\rangle$.

For example, the inner product of $|x_1\rangle$ and $|x_2\rangle$ can be carried out:

$$\langle x_1|x_2\rangle = \begin{bmatrix} \alpha_0^\dagger & \alpha_1^\dagger \end{bmatrix} \cdot \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \alpha_0^\dagger\beta_0 + \alpha_1^\dagger\beta_1.$$

What if we take the inner product of $|x_1\rangle$ with itself? Actually, it turns out to be the same as the sum of squares of the amplitudes, which is always 1.

$$\langle x_1|x_1\rangle = \alpha_0^\dagger\alpha_0 + \alpha_1^\dagger\alpha_1 = |\alpha_0|^2 + |\alpha_1|^2 = 1$$

Definition 2.3. The *outer product* of two quantum states $|x_1\rangle$ and $|x_2\rangle$ is defined as $|x_1\rangle \cdot \langle x_2|$, which is often written as $|x_1\rangle\,\langle x_2|$.

This time the result would be in fact a *matrix*, instead of a complex number. Take the outer product of $|x_2\rangle$ and $|x_1\rangle$:

$$|x_2\rangle\langle x_1| = \begin{bmatrix}\beta_0\\ \beta_1\end{bmatrix} \cdot \begin{bmatrix}\alpha_0^\dagger & \alpha_1^\dagger\end{bmatrix} = \begin{bmatrix}\alpha_0^\dagger\beta_0 & \alpha_1^\dagger\beta_0\\ \alpha_0^\dagger\beta_1 & \alpha_1^\dagger\beta_1\end{bmatrix}$$

Observation 2.4. *The relationship between the outer and the inner product:* $tr(|x_2\rangle\langle x_1|) = \langle x_1|x_2\rangle$.

Now let's take a look at some concrete examples:

$$\langle 0|1\rangle = \begin{bmatrix}1 & 0\end{bmatrix} \cdot \begin{bmatrix}0\\ 1\end{bmatrix} = 0,$$

$$\langle +|-\rangle = \begin{bmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix} \cdot \begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix} = \frac{1}{2} - \frac{1}{2} = 0.$$

It means $|0\rangle$ and $|1\rangle$ are orthogonal to each other, so are $|+\rangle$ and $|-\rangle$. Therefore, we say that they both form an *orthonormal basis* for $\mathbb{C}^2$. For any quantum state $|\psi\rangle$ in $\mathbb{C}^2$, it can be expressed using either basis:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_+|+\rangle + \alpha_-|-\rangle,$$

where again $|\alpha_0|^2 + |\alpha_1|^2 = |\alpha_+|^2 + |\alpha_-|^2 = 1$.

Let's move on to general qudits, as we always do. A qudit state is a unit vector in $\mathbb{C}^d$:

$$|\psi\rangle = \begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_d\end{bmatrix},$$

such that $\langle\psi|\psi\rangle = 1$ as always. Similarly, we have the d-dimensional bases $\{i\}, i \in [d]$:

$$|1\rangle = \begin{bmatrix}1\\ 0\\ \vdots\\ 0\end{bmatrix}, \ldots, |d\rangle = \begin{bmatrix}0\\ 0\\ \vdots\\ 1\end{bmatrix},$$

2.3 Multiple Qubit System - the Mathematics

Suppose we have two qubits $|x\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|y\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. How can we describe their *joint state*? The first guess might be using multiplication of some sort. So, let's try it, maybe using the notation $\otimes$:

$$\begin{aligned}|x\rangle \otimes |y\rangle &= (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)\\ &= \alpha_0\beta_0\underbrace{|0\rangle\otimes|0\rangle}_{|00\rangle} + \alpha_0\beta_1\underbrace{|0\rangle\otimes|1\rangle}_{|01\rangle} + \alpha_1\beta_0\underbrace{|1\rangle\otimes|0\rangle}_{|10\rangle} + \alpha_1\beta_1\underbrace{|1\rangle\otimes|1\rangle}_{|11\rangle}\end{aligned}$$

It seems that if we regard $|0\rangle \otimes |0\rangle = |00\rangle$, etc., as shown above, $|x\rangle \otimes |y\rangle$ looks exactly the same as a linear combination of the four basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. However, we do need to check whether the result of $|x\rangle \otimes |y\rangle$ is *actually* a quantum state:

$$\begin{aligned}&|\alpha_0\beta_0|^2 + |\alpha_0\beta_0|^2 + |\alpha_0\beta_0|^2 + |\alpha_0\beta_0|^2 \\ =&(|\alpha_0|^2 + |\alpha_1|^2) \cdot (|\beta_0|^2 + |\beta_1|^2) = 1\end{aligned}$$

So it is indeed a sensible way of describing joint states!

In general, given kets $|a\rangle = \sum_j \alpha_j |a_j\rangle$ and $|b\rangle = \sum_k \beta_k |b_k\rangle$, we have:

Definition 2.5. The *tensor product* of kets $|a\rangle$ and $|b\rangle$ is

$$|a\rangle \otimes |b\rangle = \sum_j \sum_k \alpha_j \beta_k (|a_j\rangle \otimes |b_k\rangle),$$

where $|a_j\rangle \otimes |b_k\rangle$ can also be written as $|a_j b_k\rangle$ or $|jk\rangle$.

Notice that tensor product is *not commutative*: $|0\rangle \otimes |1\rangle = |01\rangle \neq |10\rangle = |1\rangle \otimes |0\rangle = |00\rangle$. To see what tensor product does more clearly, let's go back to our kets $|x\rangle$ and $|y\rangle$. We can write out the matrix form:

$$|x\rangle \otimes |y\rangle = \begin{bmatrix}\alpha_0 \\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_0 \\ \beta_1\end{bmatrix} = \begin{bmatrix}\alpha_0 \begin{bmatrix}\beta_0 \\ \beta_1\end{bmatrix} \\ \alpha_1 \begin{bmatrix}\beta_0 \\ \beta_1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1\end{bmatrix}$$

For example, we have the four basis of two-qubit system:

$$|00\rangle = \begin{bmatrix}1 \\ 0 \\ 0 \\ 0\end{bmatrix}, |01\rangle = \begin{bmatrix}0 \\ 1 \\ 0 \\ 0\end{bmatrix}, |10\rangle = \begin{bmatrix}0 \\ 0 \\ 1 \\ 0\end{bmatrix}, |11\rangle = \begin{bmatrix}0 \\ 0 \\ 0 \\ 1\end{bmatrix}.$$

We have to remember that not all states in the multiple-qubit system are of tensor product form, namely the *product states.* The most famous example would be:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle.$$

The states that cannot be expressed in terms of a tensor product of two other states are called the *entangled states.* Later in the course, we will see many different interesting properties of the product states and the entangled states.

More generally, in the d dimensional qudit system, we have:

$$\begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_d \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_d \end{bmatrix} = \begin{bmatrix} \alpha_0 \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_1 \end{bmatrix} \\ \vdots \\ \alpha_1 \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_1 \end{bmatrix} \end{bmatrix} = \text{a long vector of length } d^2.$$

3 Quantum Computation

How quantum states are allowed to change over time? We have seen some basic quantum circuits in last lecture, but today we will define them in a more formal way. We will start with our favorite gate, the Hadamard gate H. Recall that H maps $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$. Graphically, it behaves like the following:

$$\begin{aligned} |0\rangle \; -\!\boxed{H}\!- \; \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \\ |1\rangle \; -\!\boxed{H}\!- \; \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

More generally, for any gate U, the circuit will look like this:

$$|\psi\rangle \; -\!\boxed{U}\!- \; U|\psi\rangle$$

But what restrictions do we have on gate U? In fact, in order for the circuit to be physically realizable, we have *two restrictions*:

1. U: $\mathbb{C}^d \to \mathbb{C}^d$ has to map from a *quantum state* to another *quantum state.*
2. U has to be *linear* (i.e. $U(|x_1\rangle + |x_2\rangle) = U|x_1\rangle + U|x_2\rangle$). In other words, U is a matrix.

To satisfy restriction 1, we notice that both the input and the output should be quantum states, and thus

$$\langle\psi|\psi\rangle = 1, \;\; (U|\psi\rangle)^\dagger U|\psi\rangle = 1.$$

Combined with restriction 2, we know that for all $\langle\psi|\psi\rangle = 1$, we need,

$$\begin{aligned} &(U|\psi\rangle)^\dagger U|\psi\rangle = 1 \\ \Rightarrow\; &|\psi\rangle^\dagger U^\dagger U|\psi\rangle = 1 \\ \Rightarrow\; &\langle\psi| U^\dagger U|\psi\rangle = 1 \\ \Rightarrow\; &U^\dagger U = I \end{aligned}$$

In other words, $U \in \mathbb{C}^{d\times d}$ is **unitary**!

Observation 3.1. *The angle between two quantum states preserves under any unitary operations.*

Imagine we take two quantum states $|x_1\rangle$ and $|x_2\rangle$. We send them both through a unitary gate U, resulting in two states $U|x_1\rangle$ and $U|x_2\rangle$. The angle between them can thus be expressed in terms of their inner product:

$$(U|x_1\rangle)^\dagger U|x_2\rangle = \langle x_1| U^\dagger U |x_2\rangle = \langle x_1|x_2\rangle .$$

Observation 3.2. *Unitary operations are invertible (reversible) and its inverse is its conjugate transpose.*

Notice that given $U^\dagger U = I$, we have $I = I^\dagger = (U^\dagger U)^\dagger = UU^\dagger$. So it follows that $U^{-1} = U^\dagger$. Therefore, applying U and $U^\dagger$ back to back brings the state to its original input state back again:

$$|\psi\rangle \; - \boxed{U} - \boxed{U^\dagger} - \; |\psi\rangle$$

Observation 3.3. *Unitary operations are equivalent to changes of basis.*

Suppose $\{|v_1\rangle, \ldots, |v_d\rangle\}$ is any *orthonormal* basis of $\mathbb{C}^d$, and define the following states:

$$|w_1\rangle = U|v_1\rangle, \ldots, |w_d\rangle = U|v_d\rangle .$$

Since we have shown that unitary operations are rotations that preserve relative angles, the set $\{|w_i\rangle\}$ are also *orthonormal*:

$$\langle w_i|w_j\rangle = \langle v_i|v_j\rangle = \begin{cases} 1 & : i = j \\ 0 & : i \neq j \end{cases}$$

And again this is verified by our favorite example, the *Hadamard* gate, which has the matrix form:

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

We can write:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle ,$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = |-\rangle .$$

We can actually construct the Hadamard matrix H from outer products:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = (|+\rangle \langle 0|) + (|-\rangle \langle 1|).$$

In general, we can express unitary operations in $\mathbb{C}^d$ as follows:

$$U = \sum_{i=1}^{d} |w_i\rangle \langle v_i| ,$$

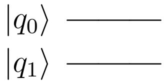
where $\{w_i\}, \{v_i\}$ are the bases of $\mathbb{C}^d$. In fact, the action of U is a change of basis from $\{v_i\}$ to $\{w_i\}$:

$$U |v_j\rangle = \sum_{i=1}^{d} |w_i\rangle \underbrace{\langle v_i| |v_j\rangle}_{\delta_{ij}} = |w_j\rangle ,$$

where $\delta_{ij} = \begin{cases} 1 & : i = j \\ 0 & : i \neq j \end{cases}$. The same rule applies to general states that are in superpositions of basis vectors. We will employ linearity for the states like $|\psi\rangle = \sum_i \alpha_i |v_i\rangle$.

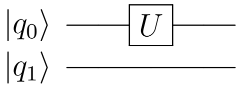
3.1 Mutiple Qubits System

What if we apply unitary operations on multiple qubit systems? What does it mean to apply gates on one of the entangled qubits? Let's again start with the simplest, a two-qubit system. And here is a "*do-nothing*" gate:

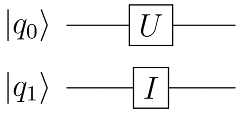


Notice that $|q_0\rangle$ and $|q_1\rangle$ individually would be described as 2×1 column vectors, but when viewing them collectively we have to maintain the joint state of the entire system, which we write as a 4×1 column vector. This is necessary when, e.g., $|q_0\rangle$ and $|q_1\rangle$ are entangled. Now, this "quantum circuit" does essentially nothing to the states, so it's not particularly interesting, but if we wanted to describe how this circuit behaves, what matrix would we use to describe it? The answer is the 4×4 identity matrix I.

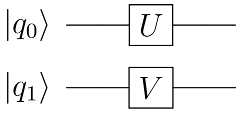
The more interesting case is of course when a unitary is applied to (at least) one of the qubits. For example:



As we repeatedly stressed in Lecture 1, just as in probabilistic computation you have to always maintain the state of all qubits at all times, even though it looks like U is only changing the first qubit. We know that coming in, the state is represented by a height-4 column vector. But U is represented by a 2×2 matrix. And that doesn't type-check (can't multiply 2×2 against 4×1). Well, by the laws of quantum mechanics, the transformation from input to output has to be a big 4×4 (*unitary*) matrix. To clarify things, one might ask oneself – what operation are we applying to the second bit? Well, we're doing nothing, so we're applying an (2×2) I. So we could draw the picture like



So how do U and I get combined into a 4×4 matrix? Or more generally, if we do



how do they get combined?

Well, the short answer is that it's something called $U \otimes V$ (*the Kronecker/tensor product* on matrices), but you can even *tell* what $U \otimes V$ should be. Notice that everything can be spatially separated; perhaps the first qubit coming in is a $|0\rangle$ or a $|1\rangle$ and the second qubit coming in is a $|0\rangle$ or a $|1\rangle$, and they are not in any way entangled, just hanging out in the same room. Clearly after the circuit's over you have $U|q_0\rangle$ and $V|q_1\rangle$ hanging out, not entangled; i.e., we determined that for $|q_0\rangle, |q_1\rangle$ in $\{|0\rangle, |1\rangle\}$, whatever $U \otimes V$ is it must satisfy

$$(U \otimes V)(|q_0\rangle \otimes |q_1\rangle) = (U|q_0\rangle) \otimes (V|q_1\rangle).$$

By linearity, that's enough to exactly tell what $U \otimes V$ must be. This is because for any (possibly entangled) 2-qubit state

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

we have that

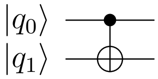
$$(U \otimes V)|\psi\rangle = \alpha_{00}(U \otimes V)|00\rangle + \alpha_{01}(U \otimes V)|01\rangle + \alpha_{10}(U \otimes V)|10\rangle + \alpha_{11}(U \otimes V)|11\rangle,$$

and we have already defined $U \otimes V$ for these four kets.

Of course, this just shows how $U \otimes V$ operates on kets, but we know that underlying $U \otimes V$ must be a *unitary* matrix. From the above, it's easy to derive what this unitary matrix looks like. It's given as follows (notice the similarity to the tensor product of two vectors):

$$U \otimes V = \begin{bmatrix} u_{11}V & u_{12}V \\ u_{21}V & u_{22}V \end{bmatrix} = \begin{bmatrix} u_{11}v_{11} & u_{11}v_{12} & u_{12}v_{11} & u_{12}v_{12} \\ u_{11}v_{11} & u_{11}v_{12} & u_{12}v_{21} & u_{12}v_{22} \\ u_{21}v_{11} & u_{21}v_{12} & u_{22}v_{11} & u_{22}v_{12} \\ u_{21}v_{21} & u_{21}v_{22} & u_{22}v_{21} & u_{22}v_{22} \end{bmatrix}.$$

Of course, not all 2-qubit gates are the result of tensoring two 1-qubit gates together. Perhaps the easiest example of this is the CNOT gate.

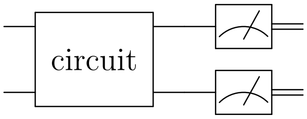


In matrix form, we can write this gate as

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

4 Measurements

We have discussed quantum measurements on a single qubit in last lecture. Briefly, suppose we have a state $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$. Measurements on $|\psi\rangle$ result in 0 or 1, with probability $|\alpha_0|^2$ and $|\alpha_1|^2$, respectively. What happens if we measure a state in a multiple qubit system? Take the 2-qubit system as an example:



Suppose before the measurements were made, we have a joint state in the form of

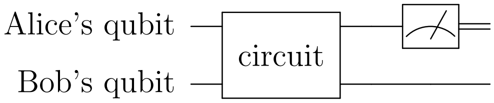
$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \in \mathbb{C}^4,$$

such that $|\alpha_{00}|^2 + \cdots + |\alpha_{11}|^2 = 1$. Then we have the following *measurement rule*:

$$\text{We will observe} \begin{cases} |00\rangle & : \text{ with probability } |\alpha_{00}|^2 \\ |01\rangle & : \text{ with probability } |\alpha_{01}|^2 \\ |10\rangle & : \text{ with probability } |\alpha_{10}|^2 \\ |11\rangle & : \text{ with probability } |\alpha_{11}|^2 \end{cases} .$$

4.1 Partial Measurements

What if we only measure on one of the two qubits? If we measure the second qubit afterwards, how will the outcome of the second measurement be related to the outcome of the first measurement? The circuit for *partial measurements* might look like this:



Say Alice holds on to the first qubit and Bob holds on to the second. If Alice measures the first qubit, her qubit becomes deterministic. We can rewrite the measurement rule as follows:

$$\text{Alice will observe} \begin{cases} |0\rangle & : \text{ with probability } |\alpha_{00}|^2 + |\alpha_{01}|^2 \\ |1\rangle & : \text{ with probability } |\alpha_{10}|^2 + |\alpha_{11}|^2 \end{cases} .$$

Suppose Alice observed $|0\rangle$. The probability rule for Bob's measurements on the second qubit is now the same as the rules of *conditional probability.* In particular, the joint state after Alice measured her qubit becomes:

$$\frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} = |0\rangle \otimes (\frac{\alpha_{00} |0\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}).$$

Notice that, the joint state is now "*unentangled*" to a product state. Now, Bob measures. We can then write his measurement rule as:

$$\text{Bob will observe} \begin{cases} |0\rangle & : \text{ with probability } \frac{|\alpha_{00}|^2}{|\alpha_{00}|^2+|\alpha_{01}|^2} \\ |1\rangle & : \text{ with probability } \frac{|\alpha_{01}|^2}{|\alpha_{00}|^2+|\alpha_{01}|^2} \end{cases} .$$

The conditional probabilities is actually the straightforward consequences of the fact that, once Alice made her measurement (say, she observed $|0\rangle$), the probability of observing $|10\rangle, |11\rangle$ becomes zero.

The action of quantum measurements is in fact a lot more subtle and interesting than what we have briefly discussed above. Sometimes a quantum system is "*destroyed*" during a measurement, but in other cases it continues to exist and preserves certain properties. To analyze the effect of quantum measurements, we often employ the notion of "*wave function collapse*", which we will in detail next time.