Introduction to Quantum Computing

Lecture 2

The rules and math of quantum mechanics

Enter the Qubit

First we start out with the basic block of quantum computing. Analogous to the bit in classical computing, there is a quantum bit in quantum computing. A classical bit is a 2 state system, with the states denoted 0 and 1. A classical bit is always in one of those states or the other, and measuring the state return a 0 or 1 with certainty. n bits can be in exactly one of 2^n different ordered states, usually denoted $000\ldots00$, $000\ldots01$,...,$111\ldots11$.[a]

Quantum bits (which we shall call qubits) similarly can exist in two states, which we call $|0\rangle$ and $|1\rangle$. However, they behave as if existing in many "in between" states. A quantum bit can be physically represented by any two state (or more) system, such as electron spin up and down, photon energy states, atomic energy levels, molecular vibrational freedom, and many others. For our purposes we assume physical representations are available (they are).

To make the concept of a qubit precise, we define

Definition 1 (Qubit). *A* **qubit** *(or quantum-bit) is a unit vector in* $\mathbb{C}^2$.

Definition 2 (State vector). *The* **state** *of a quantum system is a (column) vector in some vector space, written* $|\psi\rangle$.

Copyright Chris Lomont 2003. Email corrections or questions to clomont@math.purdue.edu.

[a] "There are only 10 kinds of people in the world. Those who understand binary and those who don't."

With this definition, we fix an orthonormal basis of (column) vectors, labelled $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$. It will turn out that physically, *we can only distinguish orthogonal quantum states*, thus the orthogonal requirement. And considerations of probability will make the normality convenient, thus we fix an orthonormal basis. Any such basis of $\mathbb{C}^2$ will work, but we choose the above representations since they are good to work with. Finally, we make a qubit a unit vector because, again, it makes calculations cleaner, and has some physical significance.

Now for the differences from classical bits. A qubit can be *any* unit vector, not just those corresponding to $|0\rangle$ and $|1\rangle$. A qubit can be in the state

$$\alpha|0\rangle + \beta|1\rangle \tag{1}$$

where α and β are complex numbers, with $|\alpha|^2 + |\beta|^2 = 1$. While it only takes one "bit" to fully describe the state of a classical bit, it takes two complex numbers to completely describe the state of one qubit, which intuitively is infinitely more information! However we will see there are practical limitations to the amount of "information" one can store in a single qubit.

This gives us the first of four postulates of quantum mechanics:

Quantum Mechanics Postulate 1: State Space Associated to an isolated physical system is a complex vector space with inner product (a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space[b]. Thus a n qubit system is a unit vector in $\mathbb{C}^{2^n}$.

We will explain the inner product below (we can use the Euclidean one).

[b] Postulate taken verbatim from Neilsen and Chuang. The rest is Lomont-ized

How to "Measure" a Qubit

In principle you could store the knowledge in the Library of Congress on one qubit, but *you could never retrieve it.* When you read out the value in a qubit in the state in equation 1, it returns $|0\rangle$ with probability $|\alpha|^2$, or it returns $|1\rangle$ with probability $|\beta|^2$, and then the qubit assumes the state just returned.

For example, suppose we have a qubit in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2}$$

What are the odds that it returns a $|1\rangle$ when measured? A $|0\rangle$?

This generalizes to multiple qubits as we soon see.

One last point is worth mentioning - there is a useful way to visualize operations on a single qubit, using the **Bloch sphere**. It will turn out that under obervation, states $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ have the same behavior, so we can modify a state up to the phase $i\theta$, where $i = \sqrt{-1}$. So given a single qubit state $\alpha|0\rangle + \beta|1\rangle$, we can remove a phase to write

$$\alpha|0\rangle + \beta|1\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{3}$$

Since the phase out front has no effect on measurements, we can use θ and φ for spherical

coordinates

$$x = \cos\varphi\sin\theta \tag{4}$$

$$y = \sin\varphi\sin\theta \tag{5}$$

$$z = \cos\theta \tag{6}$$

This allows us to picture a qubit as a point on a three dimensional sphere, and visualize operations upon a qubit.

Unfortunately, this has no known generalization to multiple qubits

Qubits Galore

Similar to concatenating classical bit to get n-bit "bitstrings", we concatenate qubits to get larger systems. Two qubits form a space spanned by four vectors

$$|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad \text{and } |1\rangle \otimes |1\rangle \tag{7}$$

where we will define the "tensor product" $\otimes$ in a moment. Shorthand for the above expressions is

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad \text{and } |11\rangle \tag{8}$$

Definition 3. *The* **tensor product** *of two vectors* $x = (x_1, x_2, \ldots, x_n)^T$ *and* $y = (y_1, y_2, \ldots, y_m)^T$ *as the vector in* nm *dimensional space given by*

$$x \otimes y = \begin{pmatrix} x_1 y \\ x_2 y \\ \cdots \\ x_n y \end{pmatrix} = \begin{pmatrix} x_1 y_1 \\ x_1 y_2 \\ \cdots \\ x_1 y_m \\ x_2 y_1 \\ \cdots \\ x_n y_m \end{pmatrix} \tag{9}$$

Homework 1. *Check this definition does not depend on a choice of basis.*

Now we can check the second basis element (dictionary ordering)

$$|01\rangle = |0\rangle \otimes |1\rangle \tag{10}$$

$$= \tbinom{1}{0} \otimes \tbinom{0}{1} \tag{11}$$

$$= \begin{pmatrix} 1\binom{0}{1} \\ 0\binom{0}{1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{12}$$

and we get the second usual basis element of $\mathbb{C}^4$. This works in general; that is, the vector corresponding to the state $|n\rangle$ where n is a binary number, is the $(n+1)^{\text{th}}$ standard basis element. We also use the decimal shorthand sometimes: $|32\rangle$ is the 33rd standard basis vector in some space which would be clear from context.

Back to the inner product from postulate 1: We write it using the "braket" notation, where the symbol $|k\rangle$ is called a ket, and the dual $\langle j|$ is a bra. Given a state (ket) $|\psi\rangle = \sum \alpha_j |j\rangle$, we define the dual (bra) as the conjugate transpose, that is,

$$\langle \psi| = |\psi\rangle^\dagger = \sum \alpha_j^* \langle j| \tag{13}$$

Together we write $\langle j|k\rangle$, which is the "braket" of states $|j\rangle$ and $|k\rangle$. Since the states are orthonormal, $\langle j|k\rangle$ is 1 if and only if $j = k$, otherwise it is zero. We extend this inner product $\langle -, -\rangle$ to general states via linearity. Thus states $|\psi_1\rangle = \sum \alpha_j|j\rangle$ and $|\psi_2\rangle = \sum \beta_k|k\rangle$ give

$$\begin{aligned}\langle\psi_1|\psi_2\rangle &= \textstyle\sum_j \alpha_j^* \langle j| \sum_k \beta_k|k\rangle \\ &= \textstyle\sum_{j,k} \alpha_j^*\beta_k\langle j|k\rangle \qquad = \displaystyle\sum_m \alpha_m^*\beta_m\end{aligned}$$

So we have the equivalent notations for a 5 qubit state:

$$\begin{aligned}|1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle = &\quad |10010\rangle \\ = &\quad |18\rangle\end{aligned}$$

It is worth noting that not all composite states are simple tensor products of single states. One of the simplest is one of the 2 qubit Bell states, $\beta_{00} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. This is an example of an *entangled state* which turns out to be a very useful computational resource later.

Homework 2. *Prove β_{00} is not of the form $|\psi\rangle \otimes |\varphi\rangle$.*

When appropriate, we may drop the normalization factor to clean up calculations. Then we could write $\beta_{00} = |00\rangle + |11\rangle$, with the understanding this needs to be normalized.

Measuring revisited

Now - how about measuring these states? An arbitrary 2 qubit state is

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

with complex valued α_{ij}. Requiring $\sum_{ij} |\alpha_{ij}|^2 = 1$ is called the "normalization requirement", and we assume all states are normalized. Sometimes to avoid clutter we will drop the coefficients.

Suppose we only the first qubit of $|\psi\rangle$. We will obtain $|0\rangle$ with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, that is, we obtain a state with probability equal to the sum of the magnitudes of all states that contribute. After measuring, we know the first qubit is $|0\rangle$, so only those type of states are left, causing the new state to be

$$|\psi^*\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Notice the new normalization factor in the denominator. Again, this idea generalizes to arbitrary (finite) dimension.

Thus we have a way to denote arbitrary quantum states on n qubits:

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j|j\rangle \tag{14}$$

where the α_i are complex numbers satisfying the normalization requirement. Measuring $|\psi\rangle$ returns state $|j\rangle$ with probability $|\alpha_j|^2$, and then becomes state $|j\rangle$

Qubit evolution

We would like our quantum computers to work similar to classical computers. Classically, a very basic operation at the bit level is the NOT gate, which flips bits, that is 0 becomes 1 and 1 becomes 0. So the quantum version would take the state $\alpha|0\rangle + \beta|1\rangle \xrightarrow{NOT} \beta|0\rangle + \alpha|1\rangle$. It is east to check the matrix

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{15}$$

performs the desired operation, by multiplying X on the left of the state. The name X is historical, and we will see the exponential of X rotates qubits around the x-axis on the Bloch sphere. Since X acts like a NOT gate on a qubit, it is often called the NOT operator.

For fun, we compute "the square root of NOT." We want an operator $\sqrt{\text{NOT}}$ that when applied twice to a qubit, has the effect of NOT. This procedure will be useful when we need to construct quantum circuits and when we explain exponentials.

In general, given a function $f(t)$ of one complex variable, we extend this definition to diagonalizable matrices $M = \text{diag}(m_1, m_2, \dots m_n)$ via:

$$f(M) = \text{diag}(f(m_1), f(m_2), \dots, f(m_n)) \tag{16}$$

Since we want $\sqrt{\text{X}}$, we need to diagonalize X. Note the eigenvectors of X are $\binom{1}{1}$ and $\binom{1}{-1}$. Setting a matrix P with these as column vectors, we have under this basis change the diagonal

matrix

$$\begin{aligned} PXP^{-1} &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

Applying $f(t) = \sqrt{t}$, and changing the basis back gives

$$\begin{aligned} P^{-1} f \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} P &= \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \\ &= \sqrt{\text{NOT}} \end{aligned}$$

It is an easy check to see that $\sqrt{\text{NOT}}^2 = X$.

This process of diagonalizing an operator, applying a function, and restoring the basis will be invaluable later.

Homework 3. *What is the effect of $e^{-i\theta X/2}$ on the Bloch sphere, where θ is a real number?*

A universal quantum gate?

It is a basic result in computer science that any circuit can be built with NAND gates, which performs the following operation on two bits a and b:

$a \setminus b$	0	1
0	1	1
1	1	0

Any function on n bits can be built up from NAND gates. However the general function requires exponentially many gates, so in practice we are restricted in the functions we utilize.

So is there a similar "gate" for quantum computing? Yes, and no. It will take a while to answer this precisely, but there are finite (and small) sets of gates sufficient to *approximate* any desired quantum operation to any degree of accuracy in an efficient manner.[a]

To understand what operations we can physcially apply to a qubi (or set of qubits), we are led to study rules from quantum mechanics. It has become clear that abstract models of computation and information theory should be derived from physical law, rather than as standalone mathematical structures, since it is ultimately physical law that determines computability and information. Observation has led researchers to believe that at the quantum level, the following two facts hold:

[a]The Solovay-Kitaev theorem says that for any gate U on a single qubit, and given any $\epsilon > 0$, it is possible to approximate U to a precision ϵ using $\Theta(\log^c(1/\epsilon))$ gates from a fixed, finite set, where $1 \leq c \leq 2$. Detemining c is an open problem.

- All quantum evolution is reversible. That is very unlike the classical case, where for example NAND is not reversible.[b] This is illustrated by the fact that an electron in orbit does not emit radiation and spiral into the nucleus.
- Quantum evolution is linear. That is, if an experiment is done on the state $|0\rangle$ and on the state $|1\rangle$, then when performed on mixed states the resulting state is the same state as if the initial two answers were added.[c]

So we are left with "reversible" linear operators on the states, that is, matrices! Since the resulting state should satisfy the normalization requirement also, it turns out that any **unitary** operation is allowed. Recall U unitary means $UU^\dagger = I$. We now have :

Quantum Mechanics Postulate 2: State Evolution The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state of a system $|\psi\rangle$ at time t_1 is related to the state $|\psi'\rangle$ at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi\rangle = U|\psi'\rangle \tag{17}$$

Now we know how to specify quantum states and what is legal for manipulating the state.

Intermission - Linear algebra review

[b]Charles Bennett of IBM research showed in the 1970's that energy is used in computations to *destroy* information. Lossless computation can theoretically be done with no energy usage whatsoever!

[c]Seth Lloyd of MIT has shown that any nonlinearity at the quantum level allows the building of computers that can solve **NP** hard problems in polynomial time. Some researchers, most notably Stephen Weingram, try to construct nonlinear quantum mechanics theories, but so far they fail.

We will need several facts, terms, and theorems from linear algebra. It will be easiest to just fire them off: (we also combine some previous facts here for the heck of it)

Definition 4. *Let H, A, B, U be linear operators on a vector space V.*

1. *$H^\dagger$ is the conjugate transpose of H.*
2. *H is **Hermitian** or self-adjoint if $H = H^\dagger$.*
3. *$|\psi\rangle$ is a column vector.*
4. *$\langle\psi|$ is the dual to $|\psi\rangle$, defined $\langle v| \equiv |v\rangle^\dagger$.*
5. *$|\psi\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\rangle \otimes |\phi\rangle$.*
6. *$[A, B] = AB - BA$.*
7. *$\{A, B\} = AB + BA$.*
8. *A is **normal** if $A^\dagger A = AA^\dagger$.*
9. *U is **unitary** if $U^\dagger U = I$.*
10. *A is **positive** if $\langle\psi|A|\psi\rangle \geq 0$ for all ψ.*
11. *$\langle\psi|A|\phi\rangle$ is the inner product of ψ and $A|\phi\rangle$.*

12. *We define specific matrices (the first 4 are the Pauli matrices)*
    $\sigma_0 = I$,
    $$\sigma_1 = \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
    $$\sigma_2 = \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
    $$\sigma_3 = \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
    $$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$$
13. *For a unit vector $\vec{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$, define $\vec{n}.\vec{\sigma} \equiv n_x\sigma_x + n_y\sigma_y + n_z\sigma_z$.*
14. ***Bloch Sphere** Given a state $a|0\rangle + b|1\rangle$ we may assume a is real by phase rotation. Then define for $\phi \in [0, 2\pi]$ and $\theta \in [0, \pi]$*
    $$\cos\left(\frac{\theta}{2}\right) = a \tag{18}$$
    $$e^{i\phi}\sin\left(\frac{\theta}{2}\right) = b \tag{19}$$
    Then the point on the Bloch Sphere is $(\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$.

15. *Define the three rotation matrices:*

$$R_x(\theta) = e^{-\theta X i/2} = \cos\tfrac{\theta}{2} I - i \sin\tfrac{\theta}{2} X = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_y(\theta) = e^{-\theta Y i/2} = \cos\tfrac{\theta}{2} I - i \sin\tfrac{\theta}{2} Y = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_z(\theta) = e^{-\theta Z i/2} = \cos\tfrac{\theta}{2} I - i \sin\tfrac{\theta}{2} Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

16. *For a composite quantum system AB, the* ***partial trace*** *is an operator from density operators on AB to density operators on A defined for $tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle |a_1\rangle\langle a_2|$, and extended by linearity. On matrices: let $\dim A = n$, $\dim B = m$, then it takes a mn by mn matrix, and replaces each m by m sub-block with its trace to give a n by n matrix.*

17. *The* ***Bell States*** *are the 2-qubit basis states*

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{20}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{21}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{22}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{23}$$

Note: The four Pauli matrices (I, X, Y, and Z) have significance, since they form a basis of all linear operators on one qubit, and correspond to similarly named actions on the Bloch sphere.

We can write operators like X in an equivalent operator notation, which is often convienent to use in calculations. Noting that $\langle 0|$ is a row vector, then $|0\rangle\langle 0|$ is a 2×2 matrix. We can write X as:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{24}$$

$$= \tbinom{1}{0}(0\ 1) + \tbinom{0}{1}(1\ 0) \tag{25}$$

$$= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{26}$$

This is interpreted quickly: X sends state 0 to 1, and vice versa.

Example: As an example calculation, we compute $\langle \beta_{00}|I_2 \otimes X|\beta_{10}\rangle$ two different ways. The first way is matrix multiplication: Noting that $|00\rangle = (1,0,0,0)^T$ and $|11\rangle = (0,0,0,1)^T$, we have

$$\langle \beta_{00}|I \otimes X|\beta_{10}\rangle = \left(\tfrac{|00\rangle+|11\rangle}{\sqrt{2}}\right)^\dagger \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \left(\tfrac{|00\rangle-|11\rangle}{\sqrt{2}}\right) \tag{27}$$

$$= \left(\tfrac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \tag{28}$$

$$= 0 \tag{29}$$

For the other method, note as operators we can write $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, and X swaps basis vectors, giving $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. Then we have

$$I \otimes X = (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \tag{30}$$

$$= |00\rangle\langle 01| + |01\rangle\langle 00| + |10\rangle\langle 11| + |11\rangle\langle 10| \tag{31}$$

where we used the fact $|a\rangle\langle b| \otimes |c\rangle\langle d| = |ac\rangle\langle bd|$. Apply this and use orthonormality,

$$\langle \beta_{00}|I \otimes X|\beta_{10}\rangle = \left(\tfrac{\langle 00|+\langle 11|}{\sqrt{2}}\right)(|00\rangle\langle 01| + |01\rangle\langle 00| + |10\rangle\langle 11| + |11\rangle\langle 10|)\left(\tfrac{|00\rangle-|11\rangle}{\sqrt{2}}\right) \tag{32}$$

$$= \left(\tfrac{1}{\sqrt{2}}\right)^2 (0 + 0 + 0 + \cdots + 0) \tag{33}$$

$$= 0 \tag{34}$$

where we get terms like $\langle 00|00\rangle\langle 01|00\rangle = 1 \cdot 0 = 0$.

Homework 4. *Write the matrices above in operator form for practice.*

Homework 5. *Compute the eigen-values and eigen-vectors for the matrices defined above. They will be useful.*

Homework 6. *Understand the behavior of each matrix above on the Bloch sphere representation of a qubit.*

Useful linear algebra theorems

Theorem 5 (Cauchy Schwartz Inequality). $|\langle v|w\rangle|^2 \leq \langle v|v\rangle\langle w|w\rangle$

Theorem 6 (Spectral Decomposition). *Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal.*

Proof. Sketch: Induct on $d = \dim V$. $d = 1$ is trivial. Let λ be an eigenvalue of M, P the projector onto the λ eigenspace, and Q the projector onto the orthogonal complement. $M = PMP + QMQ$ is diagonal with respect to some basis (strip off an eigenvalue one at a time...) □

Check: There is a matrix P, with unit eigenvectors as columns, so that $PMP^\dagger$ is diagonal, with entries the eigenvalues.

Theorem 7 (Simultaneous diagonalization). *Suppose A and B are Hermitian operators on a vector space V. Then $[A, B] = 0 \Leftrightarrow$ there exists an orthonormal basis such that both A and B are diagonal with respect to that basis.*

Theorem 8 (Polar decomposition). *Let A be a linear operator on a vector space V. Then there exists a unitary U and positive operators J and K such that*

$$A = UJ = KU$$

where the unique J and K are given by $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$. Moreover, A invertible implies U is unique.

Proof. $J \equiv \sqrt{A^\dagger A}$ is positive, so spectral gives $J = \sum_i \lambda_i |i\rangle\langle i|$, $(\lambda_i \geq 0)$. Let $|\phi_i\rangle = A|i\rangle$. For $\lambda_i \neq 0$, let $|e_i\rangle = |\phi_i\rangle/\lambda_i$. Extend to orthogonal basis $|e_i\rangle$, and define unitary $U \equiv \sum_i |e_i\rangle\langle i|$. This satisfies $A = UJ$. Multiply on left by adjoint $A^\dagger = JU^\dagger$ giving $J^2 = A^\dagger A$, so $J = \sqrt{A^\dagger A}$.

Then $A = UJ = UJU^\dagger U = KU$ with $K = UJU^\dagger$. This $K = \sqrt{AA^\dagger}$. □

Theorem 9 (Singular value decomposition). *Let A be a square matrix. Then there exists unitary U and V, and diagonal D, such that*

$$A = UDV$$

The diagonal elements of D are called singular values of A.

Proof. By polar decomposition, $A = SJ$ for S unitary and J positive. By spectral $J = TDT^\dagger$, T unitary, D diagonal with nonnegative entries. $U \equiv ST$ and $V \equiv T^\dagger$ completes the proof. □

Theorem 10. *Every unitary 2×2 matrix can be expressed as*

$$\begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \cdot \begin{pmatrix} e^{\frac{i\beta}{2}} & 0 \\ 0 & e^{-\frac{i\beta}{2}} \end{pmatrix} \cdot \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \cdot \begin{pmatrix} e^{\frac{i\delta}{2}} & 0 \\ 0 & e^{-\frac{i\delta}{2}} \end{pmatrix} \tag{35}$$

Note: Notice the third matrix is a usual rotation in the plane. The 2nd and 4th matrices are Z-axis rotation on the Bloch sphere, and the first matrix is merely a phase shift of the entire state. This decomposition gives some intuition of how a single qubit operator acts.

Theorem 11 (Z-Y decomposition for a single qubit). *U is a unitary operation on a single qubit. Then there are real numbers $\alpha, \beta, \delta, \gamma$ such that*

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

Note: Similarly there are **X-Y**, **Z-X**, etc. decomposition theorems.

Theorem 12 (ABC corollary). *Suppose U is a unitary gate on a single qubit. Then there are unitary operators A, B, and C, such that $ABC = I$, and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.*

Proof. Apply theorem 11 with $A \equiv R_z(\beta)R_y(\gamma/2)$, $B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$, and $C \equiv R_z((\delta-\beta)/2)$. □

This weird looking theorem becomes very useful when trying to construct quantum circuts. It allows one to use a Controlled NOT gate (a circut that flips a qubit based on the state of another qubit) to contruct arbitrary controlled U gates.

Useful linear algebra facts!

Here are some facts that help in computations and proofs when dealing with quantum computing.

1. Any complex $n \times n$ matrix A can be written as a sum of 4 positive Hermitian matrices: $A = B + iC$ with B, C Hermitian $B = \frac{1}{2}(A^* + A)$, and C accordingly. Then any Hermitian B can be written as the sum of 2 positive Hermitian matrices $B = (B + \lambda I) - \lambda I$ where $-\lambda$ is the most negative eigenvalue of B.
2. Every positive A is of the form BB^*.
3. $|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2| = |a_1 b_1\rangle\langle a_2 b_2|$ (useful in partial trace operations).
4. Trace of kets: $|\psi\rangle = \sum_{i,j} a_{ij}|ij\rangle$, when converted to a density matrix $\rho = |\psi\rangle\langle\psi|$, and then trace is taken over the j, gives $tr_B(p) = \sum_i \left(\sum_j |a_{i,j}|^2\right) |i\rangle\langle i|$, so it seems $tr_B(|\psi\rangle)$ should be something like $\sum_i \sqrt{\sum_j |a_{i,j}|^2}\, |i\rangle$. In particular, tracing out some columns in $|011010\rangle$ removes those columns, but the new kets are not a simple sum of the previous ones... It may be ok to sum probabilities, then sqrt when collapsing, but I am not clear.
5. Unitary also satisfies $UU^\dagger = I$, so U is normal and has spectral decomposition (all QC ops unitary!).
6. Unitary preserves inner products.
7. **Positive** $\Rightarrow$ **Hermitian** $\Rightarrow$ **normal**.
8. $A^\dagger A$ is positive for any linear operator A.
9. Tensor of unitary (resp Hermitian, positive, projector) is unitary (resp,...).

10. If $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, then $P^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
11. Given eigenvectors v_1 and v_2 of B, with eigenvalues λ_1 and λ_2, let $P = \begin{pmatrix} v_1 & v_2 \end{pmatrix}$. Then the diagonal D is
$$D = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = P^{-1}BP$$
12. W is a subspace of V with basis $|i\rangle$. Projection to W is $P = \sum_i |i\rangle\langle i|$. $Q = I - P$ is the orthogonal complement.
13. Eigenvectors with distinct eigenvalues of a Hermitian operator are orthogonal.
14. $\vec{n}.\vec{\sigma}$ has eigenvalues ± 1 with corresponding eigenvectors $\begin{pmatrix} n_z \pm 1 \\ n_x + in_y \end{pmatrix}$.
15. U unitary $\Rightarrow$ U has a spectral decomposition $\Rightarrow$ U is diagonal in some orthonormal basis $\Rightarrow$ $U = \text{diag}(e^{i\alpha_1}, e^{i\alpha_2}, \ldots, e^{i\alpha_n}) \Rightarrow U$ has a *unitary* n^{th} root V, $V^n = U$.
16. tr $(|\psi\rangle\langle\phi|) = \langle\phi|\psi\rangle$.
17. For unit vectors $\vec{r}$ and $\vec{s}$, $(\vec{r}.\vec{\sigma}) \cdot (\vec{s}.\vec{\sigma}) = \vec{r} \cdot \vec{s} I + (\vec{r} \times \vec{s}).\vec{\sigma}$.

Some basic identities

There are lots of identities between the operators we have above which will be useful in reducing circuits later on. This is a good place to list some.

$$[X,Y] = 2iZ \quad [Y,Z] = 2iX \quad [Z,X] = 2iY$$

$$\{\sigma_i, \sigma_j\} = 2\delta ij \text{ if } i,j \neq 0 \quad \sigma_i^2 = I$$

$$R_z(\frac{\pi}{2})R_x(\frac{\pi}{2})R_z(\frac{\pi}{2}) = e^{-i\pi/2}H$$

$$XYX = -Y \Rightarrow XR_y(\theta)X = R_y(-\theta)$$

$$HXH = Z \quad HYH = -Y \quad HZH = X$$

$$HTH = phase * R_x(\frac{\pi}{4})$$

C is CNOT, X_j is X acting on qubit j, etc.

$$\begin{aligned} CX_1X &= X_1X_2 & \qquad CY_1C &= Y_1X_2 \\ CZ_1C &= Z_1 & \qquad CX_2C &= X_2 \\ CY_2C &= Z_1Y_2 & \qquad CZ_2C &= Z_1Z_2 \\ R_{z,1}(\theta)C &= CR_{z,1}(\theta) & \qquad R_{x,2}(\theta)C &= CR_{x,2}(\theta) \end{aligned}$$

For $i,j = 1,2,3$, $\sigma_j\sigma_k = \delta_{jk}I + i\sum_{l=1}^{3}\epsilon_{jkl}\sigma_l$ where ϵ_{jkl} is the antisymmetric tensor on 3 indices.[a]

Homework 7. *Check these identities using the matrix form and the operator form to gain mastery of these calculations.*

[a] Exercise 2.43 in Neilsen and Chuang. All of these identites appear in the book, as exercises or in the text.

Measuring the qubits

The final operation we need to understand about qubits is, how can we get information back out of them? The process is called measurement, and there are several equivalent ways to think about it. We will cover the easiest to understand, intuitively and mathematically. However, to gain the precise control over measurements, we will have to resort later to an equivalent, yet more complicated, measurement framework.

Quantum Mechanics Postulate 3: State Measurement[a] Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of a system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{36}$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}} \tag{37}$$

The measurement operators satisfy the *completeness equation*

$$\sum_m M_m^\dagger M_m = I \tag{38}$$

Cascaded measurements are single measurements

[a] Verbatim from Neilsen and Chuang.

Distinguishing states TODO:

Combining states and partial states

Quantum Mechanics Postulate 4: State Combining[a] The state space of a composite physical system is the tensor product of the state spaces of the component systems. Moreover, if we have systems numbered 1 through n, and system number j is prepared in the state $|\psi_j\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots |\psi_n\rangle$.

TODO: partial trace

And that is all there is to quantum mechanics (as far as we are concerned). These four postulates form the basis of all that is known about qantum mechanics, a physical theory that has stood for over seven decades, and is used to explain phenomena at many scales.

However, quantum mechanics does not mesh well with the other main intellectual achievement in theoretical physics in the 20th century, relativity. Combining these two theories into a unified framework has occupied the best minds for over 50 years, and good no solution is TODO: clean.

Using the above postulates gives us an important theorem:

[a] Verbatim from Neilsen and Chuang.

The No Cloning Theorem

Theorem 13. ***The No Cloning Theorem.*** *It is impossible to build a machine that can clone any given quantum state.*

This is in stark ccontrast to the classical case, where we copy information all the time.

Proof. Suppose we have a machine with two slots: A for the quantum state $|\psi\rangle$ to be cloned, and B in some fixed initial state $|s\rangle$, and the machine makes a copy of the quantum state A. By the rules of quantum mechanics, the evolution U is unitary, so we have

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \tag{39}$$

Now suppose we have two states we wish to clone, $|\psi\rangle$ and $|\varphi\rangle$, giving

$$\begin{aligned} U\left(|\psi\rangle \otimes |s\rangle\right) = &\quad |\psi\rangle \otimes |\psi\rangle \\ U\left(|\varphi\rangle \otimes |s\rangle\right) = &\quad |\varphi\rangle \otimes |\varphi\rangle \end{aligned}$$

Taking the inner product of these two equations, and using $U^\dagger U + =$:

$$\begin{aligned} \left(\langle\varphi| \otimes \langle s|\right) U^\dagger U \left(|\psi\rangle \otimes |s\rangle\right) = &\quad \left(\langle\varphi| \otimes \langle\varphi|\right)\left(|\psi\rangle \otimes |\psi\rangle\right) \\ \langle\varphi|\psi\rangle\langle s|s\rangle = &\quad \langle\varphi|\psi\rangle\langle\varphi|\psi\rangle \\ \langle\varphi|\psi\rangle = &\quad \left(\langle\varphi|\psi\rangle\right)^2 \end{aligned}$$

This has solutions if and only if $\langle\varphi|\psi\rangle$ is 0 or 1, so cloning cannot be done for general states.[a]

□

[a] There is a lot of research on what can be cloned, how much information can be cloned, etc.

Reasons, Part 1

The reasons we define a qubit and multiple qubits as above is ... TODO:

TODO: evolution via Schrodinger...

TODO: density operator, bell inequality, mixed, pure, reduced state, partial trace, Schmidt decomposition

TODO: explain other measurements

TODO: projective measurements

TODO: add operator form of matrices, and how to compute

TODO: give some formula, etc, and explain decomposition of single qubit formula, and X-Y decomp, etc

TODO: need partial trace operation, etc, density matrix formulation

TODO: problems - and work out some calculations

TODO: next time - classical computing

TODO: Heisenberg - p.89

TODO: then - quantum circuits

Next time

- Definition of Turing machine, computability, Halting problem
- Circut construction - AND, OR, NAND, XOR, FANOUT, half adder, arbitrary function computation.
- Universality of NAND.
- Uniform circuit families.
- Complexity classes: **P**, **NP**, **coNP**, **PSPACE**, **EXP**, **L**, **BPP**.
- Problems: 3SAT, 2SAT, sorting, and more.
- Energy and computation.
- Fractran (how to get all primes from the "program" $\frac{17}{91}, \frac{78}{85}, \frac{19}{51}, \frac{23}{38}, \frac{29}{33}, \frac{77}{29}, \frac{95}{23}, \frac{77}{19}, \frac{1}{17}, \frac{11}{13}, \frac{13}{11}, \frac{15}{2}, \frac{1}{7}, \frac{55}{1}$).
- Fun fun fun.