CS 294-6, Quantum Computing (Umesh Vazirani) September 6, 2002
Fall 2000, University of California, Berkeley.
Lecture #2 (Tensor products, entanglement, quantum gates and teleportation.) **DRAFT**
Notes by Galen Huntington and Aaron Segel

1 Introduction

We will continue to discuss the four main properties of quantum physics that we shall exploit in quantum computation:

- Superpositions.
- Interference.
- Entanglement.
- Measurement.

1.1 Young's Double-Slit Experiment

To be added.

2 Qubits

2.1 Discrete Quantum Systems

We will study *discrete* quantum systems. We have already seen one example of a discrete quantum system: The energy states of an electron in a hydrogen atom. There are many other naturally occuring discrete quantum systems. For example, associated to every photon is its *polarization* which is a qubit (whose state may be written as $\alpha|0\rangle + \beta|1\rangle$). When the photon passes through a polarizing lens, only photons of a certain polarization (say $|0\rangle$) may pass through — thus the photon is transmitted through the lens with probability $|\alpha|^2$. Another example of a qubit is a nuclear spin, which we will not discuss now but might return to later in the course.

2.2 Inner Product Spaces

Associated to a qubit $|\psi\rangle \in \mathbb{C}^2$ are notions of angle, inner product and length, which we have already seen. More generally we make the following definitions:

- An *inner product* on a (complex) vector space V is a map $(\cdot,\cdot) : V \times V \to \mathbb{C}$ satisfying for each $\vec{u},\vec{v},\vec{w} \in V$ and $\alpha,\beta \in \mathbb{C}$:

  (i) $(\vec{v},\vec{v}) \geq 0$, and $(\vec{v},\vec{v}) = 0$ if and only if $\vec{v} = \vec{0}$;

  (ii) $(\alpha\vec{u} + \beta\vec{v},\vec{w}) = \alpha(\vec{u},\vec{w}) + \beta(\vec{v},\vec{w})$;

  (iii) $(\vec{v},\vec{w}) = \overline{(\vec{w},\vec{v})}$.

  An *inner product space* is a vector space together with an inner product.

- Vectors $\vec{v},\vec{w} \in V$ are *orthogonal* if $(\vec{v},\vec{w}) = 0$.

- A *basis* for V is a set $\{\vec{v_1},\cdots,\vec{v_d}\}$ such that each $\vec{v} \in V$ can be written uniquely in the form $\vec{v} = \alpha_1\vec{v_1} + \cdots + \alpha_n\vec{v_n}$. The basis is said to be *orthonormal* if $(\vec{v_i},\vec{v_j}) = \delta_{ij}$ for each i,j. (Here $\delta_{ij} = 1$ if $i = j$ and 0 if $i \neq j$.)

Note that we can associate to each inner product space a canonical norm, defined by $||\vec{v}|| = \sqrt{(\vec{v},\vec{v})}$. A *Hilbert space* is an inner product space which is complete with respect to its norm. If V is finite-dimensional (i.e. it has a finite basis), then completeness is automatically satisfied. Furthermore, there is only one Hilbert space of each dimension (up to isomorphism.)

Note also that if $\vec{v} = \sum_i \alpha_i\vec{v_i}$ and $\vec{w} = \sum_i \beta_i\vec{v_i}$ (written in terms of an orthonormal basis) then $(\vec{v},\vec{w}) = \sum_i \overline{\alpha_i}\beta_i$.

2.3 Dirac's Braket Notation

In representing elements of complex vector spaces it is convenient to use notation invented by Dirac. We write $|v\rangle$ for an element of the vector space, and $|i\rangle$ for the i^{th} element of the canonical orthonormal basis.

If $|v\rangle = \sum_i \alpha_i|i\rangle$ and $|w\rangle = \sum_i \beta_i|i\rangle$, then we have already observed that

$$(\vec{v},\vec{w}) = \begin{pmatrix} \overline{\alpha_1} & \overline{\alpha_2} & \cdots & \overline{\alpha_d} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_d \end{pmatrix}.$$

We denote the row vector $(\overline{\alpha_1}\cdots\overline{\alpha_d})$ by $\langle v|$ and the inner product $(\vec{v},\vec{w})$ by $\langle v|w\rangle$.

$\langle v|$ is a *bra*, and $|w\rangle$ is a *ket*, so $\langle v|w\rangle$ is a *braket.*

To demonstrate the utility of this notation, let $|v\rangle$ be a vector of norm 1. Define $P = |v\rangle\langle v|$. Then for any $|w\rangle$ we have $P|w\rangle = |v\rangle\langle v|w\rangle$, so P is the projection operator onto $|v\rangle$ (see diagram.) Note that $P^2 = |v\rangle\langle v|v\rangle\langle v| = P$ since $|v\rangle$ has norm 1.

2.4 Tensor Products

Much of the computational power of quantum systems comes from the fact that as the number of qubits increases linearly, the amount of information stored increases exponentially. For example, a single-qubit state $|\psi\rangle \in \mathbb{C}^2$ is represented by a pair of complex numbers: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The composite state of two qubits is an element of $\mathbb{C}^4$:

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

The composite state of three qubits is in $\mathbb{C}^8$, and so on. So in order to represent the composite state of n qubits, we need 2^n complex numbers.

More generally, suppose $V = \mathbb{C}^k$ and $W = \mathbb{C}^l$. We will describe a space $V \otimes W$ (pronounced "V tensor W"). Given a state in V and a state in W, their composite will be in $V \otimes W$.

Fix bases $|v_1\rangle, \ldots, |v_k\rangle$ and $|w_1\rangle, \ldots, |w_l\rangle$ for V, W respectively. Then a basis for $V \otimes W$ is given by

$$\{|v_i\rangle \otimes |w_j\rangle : 1 \leq i \leq k, 1 \leq j \leq l\},$$

so that $\dim(V \otimes W) = kl$. So a typical element of $V \otimes W$ will be of the form $\sum_{ij} \alpha_{ij}(|v_i\rangle \otimes |w_j\rangle)$. We can define an inner product on $V \otimes W$ by

$$(|v_1\rangle \otimes |w_1\rangle, |v_2\rangle \otimes |w_2\rangle) = (|v_1\rangle, |v_2\rangle) \cdot (|w_1\rangle, |w_2\rangle),$$

which extends uniquely to the whole space $V \otimes W$.

For example, consider $V = \mathbb{C}^2 \otimes \mathbb{C}^2$. V is a Hilbert space of dimension 4, so $V \cong \mathbb{C}^4$. So we can write $|00\rangle$ alternatively as $|0\rangle \otimes |0\rangle$. More generally, for n qubits we have $\mathbb{C}^2 \otimes \cdots$ (n times) $\otimes \cdots \mathbb{C}^2 \cong \mathbb{C}^{2^n}$. A typical element of this space is of the form

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle.$$

A word of caution: Not all elements of $V \otimes W$ can be written as $|v\rangle \otimes |w\rangle$ for $|v\rangle \in V$, $|w\rangle \in W$. As an example, consider the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

2.5 A Brief Digression

Classically, if we combine a system that stores k bits of information with one that stores l bits of information, the new system stores $k+l$ bits of information. However, if one quantum state requires k complex numbers to describe, and another requires l complex numbers to describe, then their composite requires kl complex numbers. In a sense, then, the amount of information stored by the composite system is multiplicative with respect to its components.

This fact is so subtle and counter-intuitive that it was consciously realized only after a series of incremental historical developments:

- 1935 - The EPR Paradox

- 1964 - Bell's Theorem
- 1981 - Feynman's paper on the multiplicative aspect of quantum computation

Feynman presented his paper at the first quantum computation conference in 1981, some eighty years after the discovery of quantum mechanics. Recently it has emerged as the fundamental source of the computational power of quantum systems.

Finally, note that when we actually a measure an n-qubit quantum state, we see only an n-bit string - so we can recover from the system only n, rather than 2^n, bits of information.

3 Quantum Gates and Teleportation

3.1 Unitary Operators

A postulate of quantum physics is that quantum evolution is unitary. That is, if we have some arbitrary quantum system U that takes as input a state $|\phi\rangle$ and outputs a different state $U|\phi\rangle$, then we can describe U as a *unitary linear transformation*, defined as follows.

If U is any linear transformation, the *adjoint* of U, denoted U^T, is defined by $(U\vec{v}, \vec{w}) = (\vec{v}, U^T\vec{w})$. We say that U is *unitary* if $U^T = U^{-1}$. An example of a unitary operator is rotation.

Some properies of a unitary transformation U:

- U preserves inner products, i.e. $(\vec{v}, \vec{w}) = (U\vec{v}, U\vec{w})$.
- The eigenvalues of U are all of the form $e^{i\theta}$ (since U is length-preserving, i.e., $(\vec{v}, \vec{v}) = (U\vec{v}, U\vec{v})$).
- U can be diagonalized into the form

$$\begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & e^{i\theta_d} \end{pmatrix}$$

- The rows of U form an orthonormal basis.
- The colums of U form an orthonormal basis.

In general a "quantum computation" will mean a measurement of $U|\phi\rangle$ for some quantum system U and input $|\phi\rangle$.

3.2 Quantum Gates

We give some examples of simple unitary transforms, or "quantum gates."

Some quantum gates with one qubit:

- Rotation Gate. This rotates the plane by θ.

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

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$, or a rotation around $\pi/4$ followed by a reflection.

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

  The Hadamard Gate is one of the most important. Note that H^2 is the identity.

- Phase Flip.

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

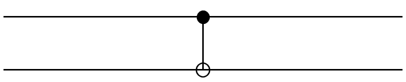
And a two-qubit quantum gate:

- Controlled Not (CNOT).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

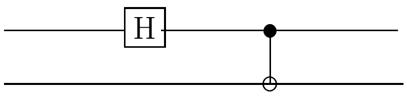
  The first bit of a CNOT gate is the "control bit;" the second is the "target bit." The control bit never changes, while the target bit flips if and only if the control bit is 1.

  The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



3.3 An Example

As an example of a system built from quantum gates, consider the following diagram:



The first qubit is passed through a Hadamard gate and then both qubits are entangled by a CNOT gate.

If the input to the system is $|0\rangle \otimes |0\rangle$, then the Hadamard gate changes the state to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$, and after the CNOT gate the state becomes $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the Bell state $|\phi^+\rangle$. In fact, one can verify that the four possible inputs produce the four Bell states:

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

3.4 Another Example: Quantum Teleportation

The *No Cloning Theorem* states that no quantum system can copy a qubit; that is, there is no transform sending $|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$. However, if we are willing to destroy the original, we can transmit a qubit, even to a remote location.

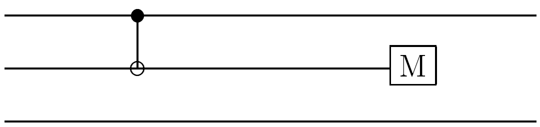
Suppose A has access to a quantum state $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, which she wants to transmit to a remote party B. She can accomplish this by transmitting only classical bits of information, provided A and B share the entangled two-qubit state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The technique is known as *quantum teleportation.*

The basic idea is this. A controls $|\psi\rangle$ and the first qubit of $|\phi\rangle$. A's strategy, roughly speaking, is to forcibly entangle $|\psi\rangle$ with the first qubit $|\phi\rangle$. A then measures the first qubit of $|\phi\rangle$, resolving it completely, and hopes this will cause $|\psi\rangle$ to become entangled with the *second* qubit of $|\phi\rangle$. Presumably, B could then transfer $|\psi\rangle$ to the second qubit of $|\phi\rangle$.

As a first try, consider the following diagram. The top line represents $|\psi\rangle$; the bottom two represent the two qubits of $|\phi\rangle$.



That is, A passes $|\psi\rangle$ and the first qubit of $|\phi\rangle$ through a CNOT gate, and then measures the first qubit of $|\phi\rangle$. Now the input into the system as a whole is

$$|\phi\rangle \otimes |\psi\rangle = \sum_{i=0,1} a_i|i\rangle \otimes \sum_{j=0,1} \frac{1}{\sqrt{2}}|j, j\rangle.$$

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 $l = i \oplus j$. The state is now

$$\sum_{j} a_{j \oplus l} \big| j \oplus l, j \big\rangle.$$

Next, A transmits l to B. If $l = 0$, B takes no action, while if $l = 1$, then B performs a bit flip on his qubit (the bottom qubit in the diagram.) A bit flip is just the transformation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we have

$$\sum_{j} a_{j \oplus l} \big| j, j \big\rangle.$$

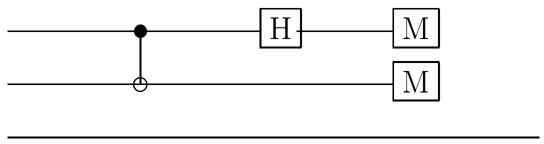
Finally, B does a phase flip on his qubit, yielding

$$\sum_{j} a_j \big| j, j \big\rangle.$$

This is almost exactly what we want. The only problem is that now, the qubit corresponding to $|\psi\rangle$ is entangled with B's qubit. The entanglement that was necessary to get the whole process started is now a liability. One way to disentangle them would be for A to measure her remaining qubit. But this would destroy B's qubit as well.

The ideal solution would be to send the entangle qubits through a CNOT gate—but A controls the first qubit and B controls the second. This would require quantum communication between A and B, which is prohibited.

The correct solution is to go back and modify the original diagram, inserting a Hadamard gate and an additional measurement:



Now the algorithm proceeds exactly as before. However A's application of the Hadamard gate now 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.

These notes are a transcription of the September 6, 2002 meeting of Umesh Vazirani's Quantum Computation course. They were typeset in latex by Aaron Siegel based on notes taken by Galen Huntington and Aaron Siegel.