Lecture 8

Comment: Project: I plan to release timeline and list of candidate topics tomorrow (expect minor updates from previous year's), as well as a model project from last year.

Quantum computation. Quantum computation = Input + Ancilla → Quantum circuit → Measurement. (Just like randomized computation!)

Univeral gate set, i.e., a set of gates that allows arbitrary quantum operations to be performed (efficiently and to low error): various examples, common ones include $\{H, \text{CNOT}, T\}$, $\{H, \text{Toffoli}\}$. A non-example $\{H\}$ (obvious), less obvious $\{H, \text{CNOT}\}$.

Bra notation. We previously introduced ket notation, which indicates an object is a column vector. It has a counterpart, the bra notation, which indicates row vectors.

Definition 10 (Bra, braket, norm)**.** Let $|\psi\rangle \in \mathbb{C}^d$ be a column vector. Then $\langle\psi|$ is defined to be $|\psi\rangle^\dagger$. Let $|\phi\rangle \in \mathbb{C}^d$ be a column vector. Then $\langle\phi|\psi\rangle$ is defined to be $\langle\phi| \cdot |\psi\rangle$, which is a complex scalar. The norm of $|\psi\rangle$ is defined to be $\sqrt{\langle\psi|\psi\rangle}$ and written as $\| |\psi\rangle \|$.

Comment: do some examples, one involving complex numbers.

Fact 2 (Complex conjugate $*$, transpose $\top$, and complex conjugate transpose $\dagger$.)**.** For $\text{op} \in \{*, \top, \dagger\}$ and complex matrices A, B, it holds that

$$(A+B)^{\text{op}} = A^{\text{op}} + B^{\text{op}} \qquad \text{(if } A,B \text{ have the same dimensions)}, \tag{43}$$

$$(A \otimes B)^{\text{op}} = A^{\text{op}} \otimes B^{\text{op}}. \tag{44}$$

In addition, if AB is well-defined, then $(AB)^* = A^*B^*, (AB)^\top = B^\top A^\top$, and $(AB)^\dagger = B^\dagger A^\dagger$.

Fact 3. Let $|\psi\rangle \in \mathbb{C}^d$. Suppose $|\psi\rangle = \sum_{i=1}^d \alpha_i |i\rangle$, then $\| |\psi\rangle \|^2 = \langle\psi|\psi\rangle = \sum_{i=1}^d |\alpha_i|^2$

Proof. We have

$$\langle\psi|\psi\rangle = \langle\psi| \cdot |\psi\rangle = \sum_i \alpha_i^* \langle i| \cdot \sum_j \alpha_j |j\rangle = \sum_{i,j} \alpha_i^* \alpha_j \langle i|j\rangle = \sum_i |\alpha_i|^2. \qquad \square$$

Comment: This means $|\psi\rangle$ is a quantum state if and only if $\| |\psi\rangle \| = 1$.

Proposition 2. *Let $|u_1\rangle, \ldots, |u_d\rangle \in \mathbb{C}^d$. Then*

$$\langle u_i|u_j\rangle = \delta_{i,j} \quad \textit{for all } i,j \in \{1,\ldots,d\} \tag{45}$$

if and only if $|u_1\rangle, \ldots, |u_d\rangle \in \mathbb{C}^d$ forms an orthonormal basis.

In particular, a $d \times d$ complex matrix is unitary if and only if its columns are unit vectors and pairwise orthogonal.

Comment: Eq. (45) is often taken as the definition of o.n. basis. This proposition shows it's equivalent to our definition.

Proof. Exercise. Comment: Perhaps do one direction if there is time. $\square$

Proposition 3. *A $d \times d$ complex matrix A maps d-dimensional quantum states to d-dimensional quantum states if and only if A is unitary.*

Notation: for positive integer d, we write $[d] \coloneqq \{1, \ldots, d\}$.

Proof. If direction is easy.

Only if direction. Suppose A maps d-dimensional states to d-dimensional states, then the columns of A are d-dimensional quantum states (unit vectors) since they are of the form $A|a\rangle$ for some $a \in [d]$. To show orthogonality, consider $|a\rangle$, $|b\rangle$ for distinct $a, b \in [d]$. Then

$$\left\| A\frac{|a\rangle + |b\rangle}{\sqrt{2}} \right\|^2 = 1 \implies \frac{\langle a| + \langle b|}{\sqrt{2}} A^\dagger A \frac{|a\rangle + |b\rangle}{\sqrt{2}} = \frac{1}{2}(\langle a| A^\dagger A |a\rangle + \langle b| A^\dagger A |b\rangle + \langle b| A^\dagger A |a\rangle + \langle a| A^\dagger A |b\rangle) = 1, \tag{46}$$

$$\left\| A\frac{|a\rangle + i|b\rangle}{\sqrt{2}} \right\|^2 = 1 \implies \frac{\langle a| - i\langle b|}{\sqrt{2}} A^\dagger A \frac{|a\rangle + i|b\rangle}{\sqrt{2}} = \frac{1}{2}(\langle a| A^\dagger A |a\rangle + \langle b| A^\dagger A |b\rangle - i\langle b| A^\dagger A |a\rangle + i\langle a| A^\dagger A |b\rangle) = 1. \tag{47}$$

But $\langle a| A^\dagger A |a\rangle = \|A|a\rangle\|^2 = 1$ and $\langle b| A^\dagger A |b\rangle = \|A|b\rangle\|^2 = 1$. Therefore,

$$\langle b| A^\dagger A |a\rangle + \langle a| A^\dagger A |b\rangle = 0, \tag{48}$$

$$-i\langle b| A^\dagger A |a\rangle + i\langle a| A^\dagger A |b\rangle = 0. \tag{49}$$

This implies $\langle b| A^\dagger A |a\rangle = 0$ as required. $\square$

Comment: this proof seems clever, is there a systematic way of thinking of this proof? Yes, look up polarization identity for complex vector spaces.