CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Thursday, January 11 - Lecture 1.2

Today's scribe: Raghav

Reading: Subsections 2.1.7-2.1.9 of Nielsen and Chuang. You should also be wrapping up the front matter and Chapter 1.

Agenda:

1. Proof of spectral theorem
2. Examples of Hilbert spaces
3. Pauli operators

I covered less today than I intended. In particular, I did not get to tensor products or simultaneous diagonalizability, which we will now do Tuesday before discussing the axioms of quantum mechanics.

1 Proof of spectral theorem

Theorem 1. *An operator $A : \mathscr{H} \to \mathscr{H}$ is unitarily diagonalizable if and only if A is normal (i.e. $AA^* = A^*A$).*

Let's give the sketch of the proof. See the book for full details. I want to explain what's going on at, hopefully, a more conceptual level.

Proof. Since this is an "if and only if" statement, we need to prove two things.

$\Longrightarrow$ This is the easy direction. If A is diagonalizable, diagonalize it. In this basis, the matrix of its adjoint is the diagonal matrix whose diagonal entries are the conjugates of the diagonal entries of A; then A is normal because $\mathbb{C}$ is commutative.

$\Longleftarrow$ This is the hard direction. We will use induction on $\dim \mathscr{H}$. (This is why we must assume $\mathscr{H}$ is finite dimensional; it's worth noting that there are generalizations to the infinite dimensional setting.)

Let λ be an eigenvalue of A, and let P_λ be the orthogonal projection onto the λ-eigenspace, $E_\lambda \subseteq \mathscr{H}$.[1] We can write $I_{\mathscr{H}} = P_\lambda + Q$ where Q is the projection onto $E_\lambda^\perp$ (the orthogonal complement of E_λ).[2]

Notice that $A = IAI = P_\lambda A P_\lambda + P_\lambda A Q + QAP_\lambda + QAQ$. Since P_λ and Q are projections onto orthogonal subspaces, $P_\lambda AQ = QAP_\lambda = 0$. Now, since $\mathscr{H}$ is finite dimensional, we can proceed inductively on $\dim \mathscr{H}$. When $\dim \mathscr{H} \in \{0,1\}$, A must be a scalar, which is trivially normal. In the inductive case, since $\dim E_\lambda^\perp < \dim \mathscr{H}$, we know that $QAQ|_{E_\lambda^\perp}$ is unitarily diagonalizable.[3] By a similar argument, $P_\lambda A P_\lambda|_{E_\lambda}$ is also unitarily diagonalizable (in fact, it of course just looks like $\lambda I|_{E_\lambda}$). Hence, there are orthonormal bases $\mathscr{B}_1, \mathscr{B}_2$ in which $QAQ|_{E_\lambda^\perp}$ and $P_\lambda A P_\lambda|_{E_\lambda}$, respectively, are diagonal. It is now easy to check that $\mathscr{B}_1 \cup \mathscr{B}_2$ is an orthonormal basis in which A is diagonal.

□

[1] Here, an operator P is an *orthogonal projection* onto the subspace E if $P(\mathscr{H}) = E$ and $P^2 = P^* = P$.

[2] It is possible that $E_\lambda = \mathscr{H}$ in which case $E_\lambda^\perp$ is trivial, but this implies that $A = \lambda I$, which is already diagonal in EVERY orthonormal basis!

[3] The inequality is strict because E_λ is the subspace corresponding to a honest eigenvalue, hence its dimension is at least 1. This in turn means $E_\lambda^\perp$ has dimension at most $\dim \mathscr{H} - 1$.

2 Examples of Hilbert Spaces

Last time I painstakingly (painfully?) defined Hilbert spaces, but I didn't get you any examples! Let's rectify that.

2.1 The trivial Hilbert space

This is trivial vector space over $\mathbb{C}$ consisting of only a zero vector. The inner product of this vector with itself is 0. Yawn.

2.2 $\mathbb{C}$ itself

Of course $\mathbb{C}$ is a vector space over $\mathbb{C}$. Now define the inner product by $\langle z,w\rangle = z^*w$. You should check this is indeed a Hilbert space, but, also yawn.

2.3 Qubits and qudits, kets and bras

This is where the fun begins.

A *qubit* is any 2-dimensional Hilbert space. All qubits are isomorphic to the vector space $\mathbb{C}^2$, which is often (in elementary linear algebra classes) defined as "columns of complex numbers of length 2" with the inner product defined by the (conjugate linear) dot product:

$$\left\langle \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \right\rangle := z_1^* w_1 + z_2^* w_2$$

I prefer to define it a slightly different way. But, since I can't help myself, let's do things a little more generally.

A *qudit* is any d-dimensional Hilbert space. (Taking $d=2$ yields a qubit.) All qudits are isomorphic to the vector space $\mathbb{C}^d$, which I will define to be the unique Hilbert space with an orthonormal basis consisting of the set of symbols $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. We sometimes call these symbols "kets." More generally, any vector in any Hilbert space can be called a "ket."[4]

More concretely, with this definition, $\mathbb{C}^d$ is the vector space consisting of (formal) linear combinations of the symbols $|0\rangle, |1\rangle, \ldots, |d-1\rangle$. This means a general vector—or ket—in $\mathbb{C}^d$, which I will denote by $|x\rangle$ where x is some other symbol (that is, x is not (necessarily) one of the indices $0,1,\ldots,d-1$) looks like

$$|x\rangle = \sum_{i=0}^{d-1} z_i |i\rangle.$$

where $z_i \in \mathbb{C}$. The inner product of $\mathbb{C}^d$ is defined on the defining basis in a way that makes it orthonormal. That is

$$\langle |i\rangle, |j\rangle\rangle = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}.$$

Since this is patently absurd notation, we will clean it up, by defining

$$\langle i|j\rangle := \langle |i\rangle || j\rangle\rangle.$$

This is called bra-ket notation.[5] Note that knowing the definition of the inner product is enough to know it on any two general vectors. Indeed, let

$$|x\rangle = \sum_{i=0}^{d-1} z_i |i\rangle$$

[4] There is no definition to make here, other than to say that "ket" is simply a synonym for vector. Bras are a different story that you will see on your homework.

[5] Note that the ket $|j\rangle$ is the right "half" of the bra-ket $\langle i|j\rangle$. You will make sense of the left "half" $\langle i|$ on your homework; it is called a bra, and, techincally speaking, is an element of the dual Hilbert space.

and

$$|y\rangle = \sum_{i=0}^{d-1} w_i |i\rangle$$

be two arbitrary vectors in $\mathbb{C}^d$. Then, because the basis kets are orthogonal, when we expand out the bra-ket $\langle x|y\rangle$ using sesquilinearity, the cross terms cancel and we are left with

$$\langle x|y\rangle = \sum_{i=0}^{d-1} z_i^* w_i.$$

Worth reiterating: every finite dimensional Hilbert space is isomorphic to $\mathbb{C}^d$ for some non-negative integer d.

2.4 Infinite dimensional Hilbert spaces

Infinite dimensional Hilbert spaces won't play a very large role in this class; one can also arrange to avoid them in most quantum computing discussion. However, sometimes this is unnatural. So, I will discuss these only to be sure you have good culture.

Probably the most important example of a Hilbert space (indeed, even more important than a qubit!) is L^2-integrable functions on $\mathbb{R}^k$. That is, we can define an (infinite dimensional) vector space over $\mathbb{C}$ by looking at

$$L^2(\mathbb{R}^k) := \{f : \mathbb{R}^k \to \mathbb{C} \mid \int_{\mathbb{R}^k} |f(x)|^2 dx < \infty\}/\sim$$

where $f \sim g$ if $f(x) = g(x)$ for x in a set of full measure. (Equivalence classes of) functions in $L^2(\mathbb{R}^k)$ are what physicists had in mind when they invented the terminology "wavefunction," since it's things like these that, for example, describe electrons as "waves" permeating space; in particular, allowing one to formalize the idea that an electron's "position" is really a probability distribution over all of space!

The inner product is defined by integration via

$$\langle f|g\rangle := \int_{\mathbb{R}^k} f^*(x)g(x)\, dx.$$

A fun fact is that all "separable" (roughly, meaning NOT uncountably infinite-dimensional) Hilbert spaces are isomorphic. In particular, $L^2(\mathbb{R}^k) \cong L^2(\mathbb{R}^l)$ even if $k \neq l$. In other words, up to isomorphism, there is basically only one (separable) infinite-dimensional Hilbert space.

2.5 Hilbert space generated by a (finite) set

Let S be a finite set. Exactly as for $\mathbb{C}^d$, we can define $\mathbb{C}[S]$ to be the Hilbert space spanned by S with the inner product defined (as above) using $\langle s|t\rangle = \delta_{st}$. In this notation, $\mathbb{C}^d = \mathbb{C}[\{0,1,2,\ldots,d-1\}]$.

What if S is not finite? Then we can stil eke something out, similar to L^2:

$$\mathbb{C}[S] := \left\{ \sum_{s\in S} z_s|s\rangle : \sum_{s\in S} |z_s|^2 < \infty \right\}.$$

If S is countably infinite, then $\mathbb{C}[S] \cong \mathbb{C}[\mathbb{N}] := \ell_2$, the Hilbert space of all square-sumable sequences. Moreover, $\ell_2 \cong L^2(\mathbb{R})$.

3 Pauli operators

The *Pauli operators* are important examples of linear operators on qubits. They are defined as matrices:[6]

[6] Unless otherwise stated, any time we define an operator on a qudit using a matrix, we assume we are using the standard (ordered) basis $|0\rangle,\ldots,|d-1\rangle$

$$\sigma_0 = I$$

$$\sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ (bit swap)}$$

$$\sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ (composite error)}$$

$$\sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ (relative phase error)}$$

Example: If $|\phi\rangle = a|0\rangle + b|1\rangle$, then $X|\phi\rangle = b|0\rangle + a|1\rangle$. $Z|\phi\rangle = a|0\rangle - b|1\rangle$.

All the Pauli operators are both Hermitian and unitary. It's not easy to explain or justify now why they are important. But they do have some nice formal properties, one of which I can explain now.

Definition. *If $\mathscr{H}$ is a finite-dimensional Hilbert space, then let $\mathscr{B}(\mathscr{H})$ be the set of all linear operators on $\mathscr{H}$, that is,*

$$\mathscr{B}(\mathscr{H}) := \{A : \mathscr{H} \to \mathscr{H}\}.$$

Let me reiterate that $\mathscr{B}(\mathscr{H})$ is *all* operators on $\mathscr{H}$. Then $\mathscr{B}(\mathscr{H})$ is a complex vector space with dimension $\dim \mathscr{H}^2$.

Let $\mathscr{B}^{sa}(\mathscr{H})$ denote the *subset* of $\mathscr{B}(\mathscr{H})$ consisting of all self-adjoint operators. Note that it really does not make sense to call $\mathscr{B}^{sa}(\mathscr{H})$ a subspace of $\mathscr{B}(\mathscr{H})$ because it is not closed under scalar multiplication by imaginary numbers. However, this is essentially the *only* reason that $\mathscr{B}^{sa}(\mathscr{H})$ is not a subspace. In other words, if we only look at *real* linear combinations of elements of $\mathscr{B}^{sa}(\mathscr{H})$, then we get a *real* subspace of $\mathscr{B}(\mathscr{H})$, considered as a real vector space.

With this all in mind, one can check very easily that $\{I, X, Y, Z\}$ is a basis of $\mathscr{B}^{sa}(\mathbb{C}^2)$.

More is true. $\mathscr{B}(\mathscr{H})$ can be made into a Hilbert space by equipping it with the "Hilbert-Schmidt inner product" (aka "trace product"; see Exercise 2.39 in Nielsen and Chuang). Then $\{I, X, Y, Z\}$ is an orthogonal basis.