

CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, January 16 - Lecture 2.1

Today's scribe: Xiaoyu

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. Bra-ket notation
2. Definition and properties of tensor products
3. Simultaneous diagonalizability theorem

1 Bra-ket notation

1.1 Definitions and relation to the dual Hilbert space

We sometimes call vectors in a Hilbert space *kets*, and will denote them using the notation $|x\rangle$. Here x is just a label/variable name for the ket/vector. Note that there is nothing to define here. Indeed, this really is just notation, no different from how we might write vectors as \vec{x} in a multivariable calculus class.

For example, if $A : \mathcal{H} \rightarrow \mathcal{H}$ is a Hermitian operator with an eigenvalue λ , we might write $|\lambda\rangle$ to denote an eigenvector of A with eigenvalue λ . Then $A|\lambda\rangle = \lambda|\lambda\rangle$. Pretty convenient!

We use *bra-ket* notation to represent the inner product:

$$\langle x|y\rangle := \langle |x\rangle || |y\rangle \rangle.$$

While kets and bra-kets are “just” notation, and since a ket is half of a bra-ket, one might wonder what the “other half” of a bra-ket really is. These are called *bras*, but they are not “just” notation, they require a definition.

Given any Hilbert space \mathcal{H} , the *dual space* \mathcal{H}^* is defined to be the vector space

$$\mathcal{H}^* := \{f : \mathcal{H} \rightarrow \mathbb{C} | f \text{ linear and bounded}\}.$$

Here f is *bounded* if the (operator) norm of f is not infinity:

$$\|f\| := \inf_{|\psi\rangle \in \mathcal{H} - \{0\}} \frac{\|f|\psi\rangle\|}{\| |\psi\rangle \|} < \infty.$$

If \mathcal{H} is finite-dimensional, then all linear maps $f : \mathcal{H} \rightarrow \mathbb{C}$ are bounded, so don't worry too much about understanding the word “bounded” if you haven't already heard about it before.

It is easy to check that \mathcal{H}^* is a vector space. It turns out that the vector space \mathcal{H}^* can be equipped with a unique inner product whose length function agrees with the operator norm, and moreover, the resulting complex inner product on \mathcal{H}^* is complete. In other words, we can make \mathcal{H}^* into a Hilbert space (in a canonical way, in fact). The abstract details of this aren't so important for us, because of what I'm about to say.¹

¹Here is the summary version, if you're interested: the operator norm on \mathcal{H}^* turns it into a so-called *Banach space* (roughly, a vector space with a notion of length, but not necessarily with a notion of angle/inner product). Moreover, this length function satisfies the *polarization identity*, which allows us to define a unique inner product whose length function agrees with the given length function. See Exercise

In mathematics, the elements of \mathcal{H}^* are often called (*bounded*) *linear functionals* on \mathcal{H} , but we will do as in physics, and call them *bras* (or *dual vectors*). Given any ket $|\psi\rangle \in \mathcal{H}$, there is an obvious way to write down a bra, denoted $\langle\psi|$ and defined as follows:

$$\begin{aligned} \langle\psi| : \mathcal{H} &\rightarrow \mathbb{C} \\ |\phi\rangle &\mapsto \langle\psi|\phi\rangle. \end{aligned}$$

In fact, this construction gives rise to a “canonical” map between \mathcal{H} and \mathcal{H}^* :

$$\begin{aligned} \Phi : \mathcal{H} &\longrightarrow \mathcal{H}^* \\ |\psi\rangle &\longmapsto \langle\psi| \end{aligned}$$

The Riesz representation theorem says (in particular) that Φ is a bijection. You will prove this in the finite dimensional case on HW1. (The proof in the infinite dimensional case requires analysis—in particular, one has to use the fact that Hilbert spaces are *complete*.)

Note that even though Φ is a bijection, it is *not* linear—it is actually *conjugate linear*:

$$\Phi(c|\psi\rangle)|\phi\rangle = c^* \langle\psi|\phi\rangle \neq c \langle\psi|\phi\rangle$$

for any scalar $c \in \mathbb{C}$ with non-zero imaginary part.

1.2 Outer products and operators in bra-ket notation

The bra-ket notation is especially useful because we can combine bras and kets in the “wrong order” and get something helpful. In the “correct” order we get the usual *inner product*

$$\begin{aligned} \mathcal{H}^* \times \mathcal{H} &\rightarrow \mathbb{C} \\ (\langle\phi|, |\psi\rangle) &\mapsto \langle\phi|\psi\rangle. \end{aligned}$$

In the “wrong” order we get the *outer product*

$$\begin{aligned} \mathcal{H} \times \mathcal{H}^* &\longrightarrow \mathcal{B}(\mathcal{H}) \\ (|\psi\rangle, \langle\phi|) &\longmapsto |\psi\rangle\langle\phi|, \end{aligned}$$

where, by definition, $|\psi\rangle\langle\phi|$ is the linear operator

$$\begin{aligned} |\psi\rangle\langle\phi| : \mathcal{H} &\longrightarrow \mathcal{H} \\ |x\rangle &\longmapsto |\psi\rangle\langle\phi|x\rangle. \end{aligned}$$

In Homework 2, you will show that the outer product gives rise to an isomorphism $\mathcal{H} \otimes \mathcal{H}^* \rightarrow \mathcal{B}(\mathcal{H})$ (note that the \times is now a \otimes).

Example. On the space $\mathbb{C}^2 = \text{span}_{\mathbb{C}}\{|0\rangle, |1\rangle\}$, we have

$$\begin{aligned} |0\rangle\langle 0| &\doteq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}. \\ |1\rangle\langle 0| &\doteq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}. \end{aligned}$$

Similar for $|0\rangle\langle 1|$ and $|1\rangle\langle 1|$. Thus, we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|.$$

More generally, if we write the operator

$$A : \mathbb{C}^d \rightarrow \mathbb{C}^d$$

as the matrix $A = (a_{ij})$ with respect to the standard basis of \mathbb{C}^d , then we have

$$A = \sum_{i=0}^{d-1} a_{ij} |i\rangle \langle j|.$$

Example. $I : \mathbb{C}^d \rightarrow \mathbb{C}^d$ can be written as

$$I = \sum_{i=0}^{d-1} |i\rangle \langle i|.$$

Example. If $D = \text{diag}(\lambda_0, \dots, \lambda_{d-1}) : \mathbb{C}^d \rightarrow \mathbb{C}^d$, then

$$D = \sum_{i=0}^{d-1} \lambda_i |i\rangle \langle i|.$$

2 Tensor Products

2.1 Tensor product of Hilbert spaces

I will define the tensor product \otimes using orthonormal bases.

Let V be a Hilbert space with orthonormal basis $\mathcal{B}_1 = \{v_1, \dots, v_m\}$, and W be another Hilbert space with $\mathcal{B}_2 = \{w_1, \dots, w_n\}$.

Then the *tensor product* is defined to be the Hilbert space $V \otimes W$ with orthonormal basis given by

$$\{|v_i\rangle \otimes |w_j\rangle : 1 \leq i \leq m, 1 \leq j \leq n\}$$

satisfying the following rules:

1. For all $z \in \mathbb{C}$,

$$z(|v_i\rangle \otimes |w_j\rangle) = (z|v_i\rangle) \otimes |w_j\rangle = |v_i\rangle \otimes (z|w_j\rangle).$$

2. For all $1 \leq i \leq m, 1 \leq j \leq m, 1 \leq k \leq n$,

$$(|v_i\rangle + |v_j\rangle) \otimes |w_k\rangle = |v_i\rangle \otimes |w_k\rangle + |v_j\rangle \otimes |w_k\rangle.$$

Similarly, for all $1 \leq i \leq m, 1 \leq j, k \leq n$,

$$|v_i\rangle \otimes (|w_j\rangle + |w_k\rangle) = |v_i\rangle \otimes |w_j\rangle + |v_i\rangle \otimes |w_k\rangle.$$

We can check, that $\{v_i \otimes w_k : i, k\}$ really is a basis. The inner product on $V \otimes W$ is defined so that this is a orthonormal basis.

Sometimes we might write $|v_i, w_k\rangle$ for $|v_i\rangle \otimes |w_k\rangle$.

The curse of dimensionality. Observe that $\dim V \otimes W = (\dim V)(\dim W)$. For example, for a n -qubit quantum memory, $\dim(\mathbb{C}^2)^{\otimes n} = 2^n$. This is a big part of reason why simulating quantum systems with classical computers is typically very difficult.

Binary Representation of Qubit States. Note that even though we defined the tensor product of Hilbert spaces of V and W by using bases, if the bases are *ordered*, then there is still not really a natural way to order the basis of $V \otimes W$. But it's really helpful to have ordered, because matrix representations of operators are made with respect to ordered bases (not unordered ones).

So, we will typically use the convention that if $\{v_0, v_1, \dots, v_{n-1}\}$ and w_0, \dots, w_{m-1} are ordered bases of V and W , respectively, then the basis $\{v_i \otimes w_j\}$ is ordered “lexicographically”², meaning it looks like this:

$$v_0 \otimes w_0, v_0 \otimes w_1, \dots, v_0 \otimes w_{m-1}, v_1 \otimes w_0, \dots, v_1 \otimes w_{m-1}, \dots, v_{n-1} \otimes w_0, \dots, v_{n-1} \otimes w_{m-1}.$$

Of course, we can iterate this construction for a big tensor product of lots of Hilbert spaces: $V_0 \otimes V_1 \otimes \dots \otimes V_{k-1}$.

This is especially useful for understanding states on qubits, since it means that our preferred ordered basis for a system of n qubits is

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle, |0\rangle \otimes |0\rangle \dots \otimes |1\rangle, \dots, |1\rangle \otimes |1\rangle \otimes \dots \otimes |0\rangle, |1\rangle \otimes \dots \otimes |1\rangle.$$

I said that sometimes we would write $|v_i, w_j\rangle$ instead of $|v_i\rangle \otimes |w_j\rangle$. If we do this to the above basis, then we get

$$|0, \dots, 0\rangle, |0, \dots, 1\rangle, |1, 1, \dots, 0\rangle, |1, \dots, 1\rangle.$$

In particular, we will often conflate $(\mathbb{C}^2)^{\otimes n}$ with \mathbb{C}^{2^n} via the preferred/standard isomorphism

$$\begin{aligned} (\mathbb{C}^2)^{\otimes n} &\rightarrow \mathbb{C}^{2^n} \\ |i_{n-1}, i_{n-2}, \dots, i_1, i_0\rangle &\mapsto |i_{n-1}i_{n-2} \dots i_1i_0\rangle \end{aligned}$$

where $i_{n-1}i_{n-2} \dots i_1i_0$ is understood to be the binary expansion of some number $0 \leq b \leq 2^n - 1$, namely,

$$b = \sum_{k=0}^{n-1} i_k 2^k.$$

This allows us to do a very convenient thing. *A priori*, a vector $|x\rangle$ in $(\mathbb{C}^2)^{\otimes n}$ looks like a big multi-sum:

$$|x\rangle = \sum_{i_1=0}^1 \dots \sum_{i_n=0}^1 z_{i_1, \dots, i_n} |i_1\rangle \otimes \dots \otimes |i_n\rangle.$$

But now we can rewrite this as

$$|x\rangle = \sum_{b=0}^{2^n-1} z_b |b\rangle.$$

Example. Let $|x\rangle = |0\rangle + |1\rangle \in \mathbb{C}^2$, $|y\rangle = |0\rangle - |1\rangle \in \mathbb{C}^2$, then

$$\begin{aligned} |x\rangle \otimes |y\rangle &= (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \\ &= |00\rangle - |01\rangle + |10\rangle - |11\rangle. \end{aligned}$$

2.2 Tensor product of operators

Not only can we define tensor products of Hilbert spaces—we can also define tensor products of operators between Hilbert spaces.³ This is sometimes called the Kronecker product when expressed using matrices.

Let $\{v_i\}$ and $\{w_j\}$ be orthonormal bases of V_1 and W_1 , and let $A : V_1 \rightarrow W_1, B : V_2 \rightarrow W_2$ be two operators. Then we define $A \otimes B : V_1 \otimes V_2 \rightarrow W_1 \otimes W_2$ by requiring that

$$(A \otimes B)(v_i \otimes w_j) = (Av_i) \otimes (Bw_j).$$

Alternatively, we can define $A \otimes B$ using a block matrix:

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1m}B \\ A_{21}B & A_{22}B & \dots & A_{2m}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}.$$

²also called the “dictionary” ordering

³Tensor product gives a *bifunctor* on the category whose objects are Hilbert spaces and whose morphisms are (bounded) maps between Hilbert spaces.

Example.

$$Z \otimes X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \neq X \otimes Z.$$

3 Simultaneous diagonalization

Given $A, B : \mathcal{H} \rightarrow \mathcal{H}$, their *commutator* is $[A, B] = AB - BA$. We say A, B are *simultaneously diagonalizable* if there exists an orthonormal basis of \mathcal{H} , with respect to which both A and B are diagonal.

Theorem 1 (Simultaneous diagonalization). *Let A, B be two normal operators. A, B are simultaneously diagonalizable iff they commute.*

Proof. The \Rightarrow direction is trivial.

For the \Leftarrow direction, see the book for the full argument (at least in the case that A and B are Hermitian—I don't remember if the book's argument works for the general case of normal operators). We will make a simplifying assumption: all of the eigenspaces of both A and B are one-dimensional.

Now assume that $AB = BA$. Since A and B are both normal, we can diagonalize both of them:

$$A = \sum \lambda_i |\lambda_i\rangle \langle \lambda_i|$$

$$B = \sum \lambda'_i |\lambda'_i\rangle \langle \lambda'_i|$$

We have

$$AB |\lambda_i\rangle = BA |\lambda_i\rangle = B\lambda_i |\lambda_i\rangle = \lambda_i B |\lambda_i\rangle.$$

Thus, $B|\lambda_i\rangle$ is an eigenvector of A with eigenvalue λ_i . Since we are assuming the eigenspaces of A are all 1-dimensional, there must exist a scalar b_i such that $B|\lambda_i\rangle = b_i |\lambda_i\rangle$. But this means that $|\lambda_i\rangle$ is an eigenvector of B with eigenvalue b_i ! Since we are also assuming that the eigenspaces of B are all 1-dimensional, this means there exists a *unique* index j_i such that $\lambda'_{j_i} = b_i$ and $|\lambda'_{j_i}\rangle = |\lambda_i\rangle$. In other words

$$B \sum_j \lambda'_j |\lambda'_j\rangle \langle \lambda'_j| = \sum_i b_i |\lambda_i\rangle \langle \lambda_i|.$$

Thus B is diagonal with respect to the same basis as A . □