Quantum Algorithms TA 2025-6

Itai Leigh

Autumn 2025

Recitation 1: BraKet and Linear Algebra

1.1 Refresher: Euclidean space

As Gil said in the lecture, the mathematics in this course is simple. It's linear algebra. So let's recall some basic concepts that underlie what we do.

Note to sole-note-readers: In order to balance between recalling all the concepts we need while not going over the too basic notions, I will have in the notes much more than I'll cover in class. Feel free to skip the linear-algebra parts you remember and focus on the Bra-Ket notation if you are comfortable with the concepts.

Zoneout. For those of you who whiz through the Euclidean space on a daily basis and will be bored in the next few minutes: take this time to make sure you find **2 answers** to question 1.1-2-b in Exercise 1, i.e. what is $\langle v| := (|v\rangle)^\dagger = \overline{(|v\rangle)^t}$ to $|v\rangle$?

Definition 1.1 (*Inner Product*)

Let V be a complex vector space. A function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ is called an Inner Product *if it is:*

1. *Non-negative: $\forall v \in V, 0 \leq \langle v, v \rangle \in \mathbb{R}$ and equality holds iff $v = 0$,*
2. *Conjugate-symmetric: $\forall u, v \in V, \langle u, v \rangle = \overline{\langle v, u \rangle}$ where $\overline{a + ib} = a - ib$ is the complex conjugate, which is also written as $(a + ib)^*$, and*
3. *Linear in the ~~first~~second variable:*

$$\forall u, v, w \in V, a, b \in \mathbb{C}, \langle u, av + bw \rangle = a\langle u, v \rangle + b\langle u, w \rangle$$

4. *$\implies$ (implied) Conjugate-linear in the ~~second~~first variable:*

$$\forall u, v, w \in V, a, b \in \mathbb{C}, \langle au + bv, w \rangle = \overline{a}\langle u, w \rangle + \overline{b}\langle v, w \rangle$$

Inner products are a way to generalise angles and lengths. To see how length comes up, look at the first property of inner product. Using this property, every inner product induces a function that generalises lengths, called a norm.

Definition 1.2 (*Norm*)

Let V be a complex vector space. A function $\|\cdot\| : V \to \mathbb{R}$ is called a Norm *if it is:*

1. *Non-negative:* $\forall v \in V, \|v\| \geq 0$, *and equality holds iff* $v = 0$,
2. *Absolute-value-homogeneous:* $\forall v \in V, a \in \mathbb{C}, \|av\| = |a| \cdot \|v\|$ *and*
3. *Satisfying the triangle inequality:* $\forall u, v \in V, \|u + v\| \leq \|u\| + \|v\|$

In general, not all normed spaces are inner-product spaces. But for those that are inner-product spaces the norm and the inner product determine each other: $\|v\| = \sqrt{\langle v, v\rangle}$ and $\langle\psi|\varphi\rangle = \frac{1}{2}(\langle\psi| + i\langle\varphi|)(|\psi\rangle - i|\varphi\rangle) + \frac{1}{2}(\langle\psi| - i\langle\varphi|)(|\psi\rangle + i|\varphi\rangle) - \langle\psi|\psi\rangle - \langle\varphi|\varphi\rangle = \frac{1}{2}\||\psi\rangle + |\varphi\rangle\|^2 + \frac{1}{2}\||\psi\rangle + i|\varphi\rangle\|^2 - \||\psi\rangle\|^2 - \||\varphi\rangle\|^2$. We will be only looking at finite-dimensional complex vector spaces with the standard inner product, also called the scalar inner product. Some people call it the complex Euclidean space while others reserve the term "Euclidean" to real spaces.

Definition 1.3 (*Finite Dimensional Complex Euclidean Space*)

For $d \in \mathbb{N}$, the d-dimensional complex Euclidean space is $\mathbb{C}^d$ with the scalar inner product:

$$\langle \begin{pmatrix} u_1 \\ \vdots \\ u_d \end{pmatrix}, \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} \rangle = \sum_{i=1}^{d} \overline{u_i} v_i = \begin{pmatrix} u_1^*, \cdots, u_d^* \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}$$

The induced norm is $\|v\| = \sqrt{\langle v, v\rangle}$.

In class you saw the BraKet (Dirac) notation, invented by Dirac and proposed in his paper "A New Notation for Quantum Mechanics".I like to think of it as an inner product that grew to recognise its individual parts' different roles and giving them a life of their own: $\langle u, v\rangle \to \langle u|v\rangle \to \langle u| \cdot |v\rangle$ (see the vectors' product above, in the definition of the complex Euclidean space). $|v\rangle$ is a column vector called "v", and $\langle u|$ is a row vector called "u". This notation is the standard in quantum computation and quantum information research. It is very convenient and promotes thinking in terms of operators acting on vectors, rather than matrices. They are equivalent, but emphasise different aspects. For example, operator and Bra-Ket are quite coordinate-free, whereas matrices are all about representation in specific bases. Another advantage of the Bra-Ket notation is in dealing with systems that are combined of several smaller sub-systems. This is a major aspect of quantum computation, as it is in any computation, using qubits as the subsystems usually. We will continue recalling linear algebra using the Bra-Ket notation, but for that we need to make sure we understand the basics of the notation.

1.2 Getting used to BraKet (Dirac) notation

From the exercise:

1. Rewrite the following expressions, equations and statements using as much bra-ket notation as you can:

   (a) $\begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}$

   (b) $\begin{pmatrix} 0 & 5 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

   (c) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

   (d) $\frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

2. What are the relations between any two of the following:

   (a) For any $v, w \in V$, the relation between $\langle v|w\rangle$ and $\langle w|v\rangle$

   (b) For any $v \in V$, the relation between $|v\rangle$ and $\langle v|$

   (c) For any two orthonormal bases $v_1 \ldots, v_n$ and $w_1, \ldots, w_n$ of V, the relation between $\sum_{i=1}^{n} |v_i\rangle\langle w_i|$ and $\sum_{i=1}^{n} |w_i\rangle\langle v_i|$

We can answer the questions above in a technically correct way, without getting any insight. Instead, let's dive deeper into the Bra-Ket notation and the understandings we can glean from its operational perspective.

1.3 Linear Algebra Using BraKet

Definition 1.4 (*Dual space*)

> *Let V be a complex vector space. Its dual space $V^* = \{f : V \to \mathbb{C} | f \text{ is linear}\}$ is the set of linear functionals (functions to the field) on V.*

The dual space is also a complex vector space (why?).

Example 1.5 (Linear Functional)**.** For any $|v\rangle \in V$, $\langle v, \cdot\rangle : V \to \mathbb{C}$ is linear. In Bra-Ket notation this functional is: $\langle v|$.

Can we think of a different example? No! All (continuous) linear functionals have this form. Let's prove it in the finite case[1].

In fact we proved something stronger: that for any orthonormal basis $|v_1\rangle, \cdots, |v_d\rangle$, $\langle v_1|, \cdots, \langle v_d|$ is a basis for V^*. This basis is called the *dual basis* of $|v_1\rangle, \cdots, |v_d\rangle$.

This gives us the first operational interpretation of $\langle v|$: for a normalised $|v\rangle$, we can think of $\langle v|$ as its "dual vector".

It also implies that in the case where V is finite dimensional, V^* is of the same dimension as V.

We could have similarly shown the existence of a dual basis for any given basis, but the relation between the primal and dual basis elements is not as elegant as in the orthonormal case.

Proposition 1.6 (*Dual Basis*)

> *Let* $|v_1\rangle, \cdots, |v_d\rangle$ *be a basis of* V. *Then there is a corresponding basis* $\langle u_1|, \cdots, \langle u_d|$ *of* V^*, *called the* dual basis, *where* $\forall i, j \in [d], \langle u_i|v_j\rangle = \delta_{ij}$.

This covered 2-b from the questions above, gaining some further insight into the relation between $|v\rangle$ and $\langle v|$.

Now that we can think of Bras of normalised vectors as their duals, meaning linear functionals that "pick up a component of a specific direction", we can understand 1-b, 1-c and 1-d in a more operational perspective as well: the outer product, or in our terminology the Ket-Bra $|u\rangle\langle v|$ for normalised vectors, is the linear operator that gives the vector $|u\rangle$, scaled by the component of the input in the direction of $|v\rangle$, i.e. $|w\rangle \mapsto \langle v|w\rangle |u\rangle$. $\langle v|w\rangle$ and sometimes $|\langle v|w\rangle|$ are called "the overlap" between $|v\rangle$ and $|w\rangle$. Insisting on normalised vectors makes presentation of operators clear as mapping directions to directions, with explicit "stretch", such as $5|0\rangle\langle 1|$, which is 1-b, showing us that 1-b is an operator that maps the span of the second standard basis element in the domain to the span of the first in the range, stretched by a factor of 5.

How about 1-c? We know it's $|0\rangle\langle 0| + |1\rangle\langle 1|$. We know this is the orthogonal projection to the subspace spanned by $\{|0\rangle, |1\rangle\}$ primarily because we are familiar with this matrix already, but in the Bra-Ket notation it becomes very immediate: the components of $|0\rangle$ and $|1\rangle$ are untouched, while the orthogonal component to them, that of $|2\rangle$, is annihilated as it has no $\langle 2|$ to catch it.

Similarly, for 1-d: $\frac{1}{3}\sum_{i,j=0}^{2} |i\rangle\langle j| = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \cdot \frac{1}{\sqrt{3}}(\langle 0| + \langle 1| + \langle 2|)$, so this is the orthogonal projection onto the span of $\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$.

Finally, let's talk about 2-c.

Definition 1.7 (*Adjoint operator*)

> *Let* $T : V \to W$ *be a linear operator. There exists a unique operator, called the* (Hermitian) adjoint operator *to* T, $T^* : W \to V$, *such that*
>
> $$\forall w \in W, v \in V, \langle w, T(v)\rangle_W = \langle T^*(w), v\rangle_V$$

[1] infinite case is Riss's presentation theorem from Functional Analysis, and that's where the parenthesised caveat regarding continuity of the functional is significant

Proof. $\langle w, T(v)\rangle = \langle w| (T|v\rangle) = (\langle w| T)|v\rangle = \langle w'|v\rangle$ where the second equality can be justified by either thinking in coordinates in the standard basis (which in this case is easier in my opinion), or by realising that operating with T before applying a linear functional is another linear functional, and this mapping is linear (in the functionals – prove it!). Let's call this transformation F for a second. We know that $F(\langle w|)$ as a functional has a vector $|w'\rangle$ for which $F(\langle w|) = \langle w'|$. Call the mapping $T^* : |w\rangle \mapsto |w'\rangle$. We get $\langle w, T(v)\rangle = \langle T^*(w), v\rangle$ and to finish the proof we need to see that T^* is linear and unique. I'll leave uniqueness as an exercise. For linearity, we need to understand what is $|w'\rangle$ in terms of T and $|w\rangle$. For that we can take the conjugate-transpose in the standard basis, the operation we noted by $\cdot^\dagger$, of $\langle w'| = \langle w| T$. We get $T^*|w\rangle := |w'\rangle = (\langle w| T)^\dagger = T^\dagger |w\rangle$. So $T^* = T^\dagger$. In fact, T^* and $T^\dagger$ is used interchangeably and the distinction here was just for presentation clarity. $\square$

This sheds light onto question 2-c: $\sum_{i=1}^n |w_i\rangle\langle v_i|$ is the adjoint operator of $\sum_{i=1}^n |v_1\rangle\langle w_i|$. Additionally, it also illuminates question 2-b in another light:

Example 1.8. If we think of a vector $|v\rangle \in V$ as an operator from the one-dimensional complex space (numbers) to the d dimensional one as $|v\rangle : \mathbb{C} \to V, x \mapsto x|v\rangle$ then $\langle v| : V \to \mathbb{C}, |u\rangle \mapsto \langle v|u\rangle$ is its adjoint operator!

We have two important sets of matrices defined by their relation to their adjoint:

Definition 1.9 (*Unitary and Hermitian operators*)

A linear operator $U : V \to V$ with its inverse as its adjoint $U^\dagger = U^{-1}$ is called Unitary.

A linear operator $H : V \to V$ that is self-adjoint $H^\dagger = H$ is called Hermitian

Let's use 2-c in a proof, the $(e) \implies (a)$ direction from question 1 in the Linear Algebra part of the exercise:

Proposition 1.10

If $U : V \to V$ maps an orthonormal basis to another orthonormal basis then U is unitary $U^\dagger = U^{-1}$.

In question 1 you prove they are actually equivalent conditions, and are equivalent to U preserving norms $\|U|v\rangle\| = \||v\rangle\|$, making the name "Unitary" sensible: the linear operators that keep unit-length vectors unit-length.

Proof. Let $\{|v_i\rangle\}_{i\in[d]}$ and $\{|u_i\rangle\}_{i\in[d]}$ be two orthonormal bases such that $|u_i\rangle = U|v_i\rangle$. Then $U = \sum_{i=1}^d |u_i\rangle\langle v_i|$ while $U^\dagger = \sum_{i=1}^d |v_i\rangle\langle u_i|$. Multiplying them reveals that indeed $UU^\dagger = \sum_{i=1}^d |u_i\rangle\langle v_i| \sum_{j=1}^d |v_j\rangle\langle u_j| = \sum_{i=1}^d |u_i\rangle\langle u_i| = I_d$. $\square$

We can also use Bra-Ket notation to recall Pythagoras, Parseval and Cauchy-Schwarz inequalities, but we will not have enough time for that in the class.