Quantum Computing
Lecture 2

Anuj Dawar

Review of Linear Algebra

Linear Algebra

The state space of a quantum system is described as a *vector space*.

Vector spaces are the object of study in *Linear Algebra*.

In this lecture we review definitions from linear algebra that we need in the rest of the course.

We are mainly interested in vector spaces over the *complex number field* – $\mathbb{C}$.

We use the *Dirac notation*—$|v\rangle, |\phi\rangle$ (read as *ket*) for vectors.

Vector Spaces

A vector space over $\mathbb{C}$ is a set $\mathbf{V}$ with

- a commutative, associative addition operation $+$ that has
  - an identity $\mathbf{0}$: $|v\rangle + \mathbf{0} = |v\rangle$
  - inverses: $|v\rangle + (-|v\rangle) = \mathbf{0}$
- an operation of multiplication by a scalar $\alpha \in \mathbb{C}$ such that:
  - $\alpha(\beta|v\rangle) = (\alpha\beta)|v\rangle$
  - $(\alpha+\beta)|v\rangle = \alpha|v\rangle + \beta|v\rangle$ and $\alpha(|u\rangle + |v\rangle) = \alpha|u\rangle + \alpha|v\rangle$
  - $1|v\rangle = |v\rangle$.

$\mathbb{C}^n$

$\mathbb{C}^n$ is the vector space of n-tuples of complex numbers: $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$.

with addition $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1+\beta_1 \\ \vdots \\ \alpha_n+\beta_n \end{bmatrix}$

and scalar multiplication $z \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} z\alpha_1 \\ \vdots \\ z\alpha_n \end{bmatrix}$

Basis

A *basis* of a vector space $\mathbf{V}$ is a *minimal* collection of vectors $|v_1\rangle, \ldots, |v_n\rangle$ such that every vector $|v\rangle \in \mathbf{V}$ can be expressed as a linear combination of these:

$$|v\rangle = \alpha_1 |v_1\rangle + \cdots + \alpha_n |v_n\rangle.$$

n—the size of the basis—is uniquely determined by $\mathbf{V}$ and is called the *dimension* of $\mathbf{V}$.

Given a basis, every vector $|v\rangle$ can be represented as an n-tuple of numbers.

Bases for $\mathbb{C}^n$

The standard basis for $\mathbb{C}^n$ is $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$ (written $|0\rangle, \ldots, |n-1\rangle$).

But other bases are possible: $\begin{bmatrix} 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ -i \end{bmatrix}$ is a basis for $\mathbb{C}^2$.

We'll be interested in *orthonormal* bases. That is bases of vectors of unit length that are mutually orthogonal. Examples are $|0\rangle, |1\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Linear Operators

A linear operator A from one vector space $\mathbf{V}$ to another $\mathbf{W}$ is a function such that:

$$A(\alpha|u\rangle + \beta|v\rangle) = \alpha(A|u\rangle) + \beta(A|v\rangle)$$

If $\mathbf{V}$ is of dimension n and $\mathbf{W}$ is of dimension m, then the operator A can be represented as an $m \times n$-matrix.

The matrix representation depends on the choice of bases for $\mathbf{V}$ and $\mathbf{W}$.

Matrices

Given a choice of bases $|v_1\rangle, \ldots, |v_n\rangle$ and $|w_1\rangle, \ldots, |w_m\rangle$, let

$$A|v_j\rangle = \sum_{i=1}^{m} \alpha_{ij} |w_i\rangle$$

Then, the matrix representation of A is given by the entries α_{ij}.

Multiplying this matrix by the representation of a vector $|v\rangle$ in the basis $|v_1\rangle, \ldots, |v_n\rangle$ gives the representation of $A|v\rangle$ in the basis $|w_1\rangle, \ldots, |w_m\rangle$.

Examples

A 45° rotation of the real plane that takes $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ to $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ to $\begin{bmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ is represented, in the standard basis by the matrix

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

The operator $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ does not correspond to a transformation of the real plane.

Inner Products

An inner product on $\mathbf{V}$ is an operation that associates to each pair $|u\rangle, |v\rangle$ of vectors a *complex number*

$$\langle u|v\rangle.$$

The operation satisfies

- $\langle u|\alpha v + \beta w\rangle = \alpha\langle u|v\rangle + \beta\langle u|w\rangle$
- $\langle u|v\rangle = \langle v|u\rangle^*$ where the * denotes the complex conjugate.
- $\langle v|v\rangle \geq 0$ (note: $\langle v|v\rangle$ is a real number) and $\langle v|v\rangle = 0$ iff $|v\rangle = \mathbf{0}$.

Inner Product on $\mathbb{C}^n$

The standard inner product on $\mathbb{C}^n$ is obtained by taking, for

$$|u\rangle = \sum_i u_i|i\rangle \quad \text{and} \quad |v\rangle = \sum_i v_i|i\rangle$$

$$\langle u|v\rangle = \sum_i u_i^* v_i$$

Note: $\langle u|$ is a *bra*, which together with $|v\rangle$ forms the *bra-ket* $\langle u|v\rangle$.

Norms

The *norm* of a vector $|v\rangle$ (written $||\,|v\rangle||$) is the *non-negative, real number*:

$$||\,|v\rangle|| = \sqrt{\langle v|v\rangle}.$$

A *unit vector* is a vector with norm 1.

Two vectors $|u\rangle$ and $|v\rangle$ are *orthogonal* if $\langle u|v\rangle = 0$.

An *orthonormal* basis for an inner product space $\mathbf{V}$ is a basis made up of *pairwise orthogonal, unit vectors*.

the term *Hilbert space* is also used for an inner product space

Outer Product

With a pair of vectors $|u\rangle \in \mathbf{U}$, $|v\rangle \in \mathbf{V}$ we associate a linear operator $|u\rangle\langle v| : \mathbf{V} \to \mathbf{U}$, known as the *outer product* of $|u\rangle$ and $|v\rangle$.

$$(|u\rangle\langle v|)|v'\rangle = \langle v|v'\rangle|u\rangle$$

$|v\rangle\langle v|$ is the *projection* on the one-dimensional space generated by $|v\rangle$.

Any linear operator can be expressed as a linear combination of outer products:

$$A = \sum_{ij} A_{ij}|i\rangle\langle j|.$$

Eigenvalues

An *eigenvector* of a linear operator $A : \mathbf{V} \to \mathbf{V}$ is a non-zero vector $|v\rangle$ such that

$$A|v\rangle = \lambda|v\rangle$$

for some complex number λ

λ is the *eigenvalue* corresponding to the eigenvector v.

The eigenvalues of A are obtained as solutions of the characteristic equation:

$$\det(A - \lambda I) = 0$$

Each operator has at least one eigenvalue.

Diagonal Representation

A linear operator A is *diagonalisable* if

$$A = \sum_i \lambda_i |v_i\rangle\langle v_i|$$

where the $|v_i\rangle$ are an orthonormal set of eigenvectors of A with corresponding eigenvalues λ_i.

Equivalently, A can be written as a matrix

$$\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

in the basis $|v_1\rangle, \ldots, |v_n\rangle$ of its eigenvectors.

Adjoints

Associated with any linear operator A is its *adjoint* $A^\dagger$ which satisfies

$$\langle v|Aw\rangle = \langle A^\dagger v|w\rangle$$

In terms of matrices, $A^\dagger = (A^*)^T$

where $*$ denotes complex conjugation and T denotes transposition.

$$\begin{bmatrix} 1+i & 1-i \\ -1 & 1 \end{bmatrix}^\dagger = \begin{bmatrix} 1-i & -1 \\ 1+i & 1 \end{bmatrix}$$

Normal and Hermitian Operators

An operator A is said to be *normal* if

$$AA^\dagger = A^\dagger A$$

Fact: An operator is diagonalisable if, and only if, it is normal.

A is said to be *Hermitian* if $A = A^\dagger$

A normal operator is Hermitian if, and only if, it has real eigenvalues.

Unitary Operators

A linear operator A is *unitary* if

$$AA^\dagger = A^\dagger A = I$$

Unitary operators are normal and therefore diagonalisable.

Unitary operators are norm-preserving and invertible.

$$\langle Au|Av\rangle = \langle u|v\rangle$$

All eigenvalues of a unitary operator have modulus 1.

Tensor Products

If $\mathbf{U}$ is a vector space of dimension m and $\mathbf{V}$ one of dimension n then $\mathbf{U} \otimes \mathbf{V}$ is a space of dimension mn.

Writing $|uv\rangle$ for the vectors in $\mathbf{U} \otimes \mathbf{V}$:

- $|(u + u')v\rangle = |uv\rangle + |u'v\rangle$
- $|u(v + v')\rangle = |uv\rangle + |uv'\rangle$
- $z|uv\rangle = |(zu)v\rangle = |u(zv)\rangle$

Given linear operators $A : \mathbf{U} \to \mathbf{U}$ and $B : \mathbf{V} \to \mathbf{V}$, we can define an operator $A \otimes B$ on $\mathbf{U} \otimes \mathbf{V}$ by

$$(A \otimes B)|uv\rangle = |(Au), (Bv)\rangle$$

Tensor Products

In matrix terms,

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