Quantum Information Processing

Lecture 2

Dr. Ahmad Khonsari

Uiversity of Tehran

Fall 2022

September 20, 2022

Slides Prepared by Mahdi Dolati

The need for linear algebra and Hilbert space

Quantum phenomena are described using linear algebra, which is the study of vector spaces and linear operations thereon. That is, states of a quantum system form a vector space and their transformations are described by linear operators.
A finite-dimension vector space with a defined inner product is also known as a **Hilbert space**, which is the most usual term used in the literature.

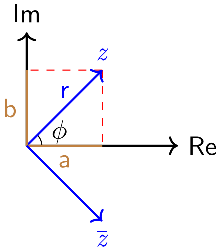
Source: www.math.ucdavis.edu

Representation:

- algebraic: $z = a + ib$
- exponential: $z = re^{i\phi} = r(\cos\phi + i\sin\phi)$

Operations:

- addition and subtraction:
  $(a + ib) \pm (c + id) = (a \pm c) + i(b \pm d)$
- multiplication:
  $(a + ib) \times (c + id) = (ac - bd) + i(ad + bc)$
  $re^{i\phi} \times r' e^{i\phi'} = rr' e^{i(\phi+\phi')}$
- complex conjugate: $z^* = \bar{z} = a - ib = re^{-i\phi}$
- absolute value:
  $|z| = \sqrt{a^2 + b^2} = r$, $|z_1 \times z_2| = |z_1| \times |z_2|$
- absolute value squared: $|z|^2 = a^2 + b^2 = r^2$
  important: $|z|^2 = z\bar{z}$
- inverse: $1/z = \bar{z}/|z|^2$



In general, we require complex numbers to describe quantum phenomena. Any $z \in \mathbb{C}$ is of the form $z = a + ib$ for some $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$.

$\mathbb{C}^n$ is the vector space of n-tuples of complex numbers $\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix}$.

With addition: $\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} z_1 + w_1 \\ z_2 + w_2 \\ \vdots \\ z_n + w_n \end{bmatrix}$.

and scalar multiplication: $w \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} wz_1 \\ wz_2 \\ \vdots \\ wz_n \end{bmatrix}$.

Matrices

A matrix is an array of (in general) complex numbers:

$$A = \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \\ a_{n1} & & a_{nm} \end{bmatrix}$$

With addition:

$$\begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \\ a_{n1} & & a_{nm} \end{bmatrix} + \begin{bmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \ddots & \\ b_{n1} & & b_{nm} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & \dots & a_{1m}+b_{1m} \\ \vdots & \ddots & \\ a_{n1}+b_{n1} & & a_{nm}+b_{nm} \end{bmatrix}$$

and scalar multiplication:

$$b \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \\ a_{n1} & & a_{nm} \end{bmatrix} = \begin{bmatrix} ba_{11} & \dots & ba_{1m} \\ \vdots & \ddots & \\ ba_{n1} & & ba_{nm} \end{bmatrix}$$

Matrix multiplication

If A is a $n \times m$ matrix and B is a $m \times l$ matrix then $C = A \times B$ is the $n \times l$ matrix with entries given by

$$C_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$$

for all $i = 1, \ldots, n$ and $k = 1, \ldots, l$.
Matrix multiplication is

- associative: $(A \times B) \times C = A \times (B \times C) = ABC$
- distributive: $A(B + C) = AB + AC$; $(A + B)C = AC + BC$
- not commutative: $AB \neq BA$

Tensor multiplication

As well as scalar multiplication and matrix multiplication, to describe quantum computation we must consider a third form of multiplication on matrices, *tensor multiplication*. Let A and B be matrices of any dimension:

$$A \otimes B = \begin{bmatrix} Ba_{11} & \dots & Ba_{1m} \\ \vdots & \ddots & \\ Ba_{n1} & & Ba_{nm} \end{bmatrix}$$

where $\otimes$ denotes the tensor product. For example:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 4 & 6 \end{bmatrix}$$

In general if A is $n \times m$ and B is $n' \times m'$ then $A \otimes B$ is $nn' \times mm'$.

Combining matrix and tensor multiplication

As a (column) vector is just a $n \times 1$ matrix, we can equally well apply tensor products to vectors. This reveals an important property of tensor products when combined with matrix products. Let A and B be $n \times m$ and $n' \times m'$ matrices respectively, and x and y be m and m' dimension column vectors respectively:

$$(A \otimes B)(x \otimes y) = (Ax) \otimes (By)$$

Complex conjugation, transpose and conjugate transpose

A complex number $z = a + bi$ has a conjugate, defined as $z^* = a - bi$.
Letting A be the $n \times m$ matrix:

$$A = \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \\ a_{n1} & & a_{nm} \end{bmatrix}$$

its transpose is defined as the $m \times n$ matrix:

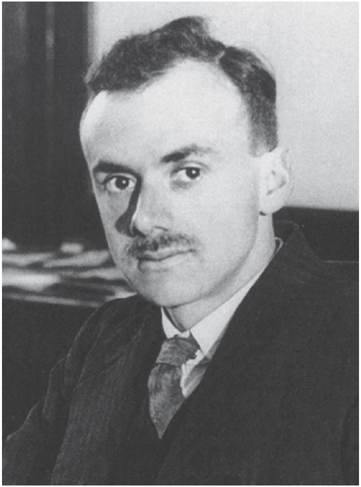
$$A^{\intercal} = \begin{bmatrix} a_{11} & \dots & a_{n1} \\ \vdots & \ddots & \\ a_{1m} & & a_{nm} \end{bmatrix}$$

Combining these two, we get the conjugate transpose or adjoint of a matrix:

$$A^{\dagger} = (A^*)^{\intercal} = \begin{bmatrix} a_{11}^* & \dots & a_{n1}^* \\ \vdots & \ddots & \\ a_{1m}^* & & a_{nm}^* \end{bmatrix}$$

Note that $(AB)^{\dagger} = B^{\dagger} A^{\dagger}$.

Dirac notation



Source: www.alchetron.com

Virtually all teaching and research on the subject of quantum information and computation expresses the linear algebra using **Dirac** notation (also known as "Bra-Ket" notation), and we will also adopt this convention.
By doing so, the expressions are compact, thus helping us to focus on the actual quantum states that are being represented

"Bras" and "Kets"

A "Ket" is a column vector:

$$|\psi\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$$

Each "Ket" has a corresponding "Bra", which is its conjugate transpose, the row vector:

$$\langle\psi| = \begin{bmatrix} a_1^* & a_2^* & \dots & a_n^* \end{bmatrix}$$

We continue to denote matrix operations with a capital letter, i.e., the matrix A operating on the state $|u\rangle$ would be written $A|u\rangle$.
When tensor multiplying vectors expressed as kets, the following are all equivalent: $|\psi\rangle \otimes |\phi\rangle$, $|\psi\rangle|\phi\rangle$, $|\psi\phi\rangle$. Note also that tensor multiplication is associative, so $(|\psi\rangle \otimes |\phi\rangle) \otimes |\omega\rangle = |\psi\rangle \otimes (|\phi\rangle \otimes |\omega\rangle) = |\psi\phi\omega\rangle$.

Inner products, orthogonality and norms

Let $|u\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$, and $|v\rangle = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$, we define the inner product:

$$\langle u|v\rangle = \langle u| \times |v\rangle = \begin{bmatrix} a_1^* & \dots & a_n^* \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \sum_{i=1}^{n} a_i^* b_i$$

If each of $|u\rangle$ and $|v\rangle$ have at least one non-zero element:

- $\langle u|v\rangle = (\langle v|u\rangle)^*$
- If $\langle u|v\rangle = 0$ then $|u\rangle$ and $|v\rangle$ are orthogonal.
- $\langle u|u\rangle = \sum_{i=1}^{n} |a_i|^2$, which is a positive real number.
- $|||u\rangle|| = \sqrt{\langle u|u\rangle}$ is defined as the norm of $|u\rangle$, unit vectors have norm $= 1$.

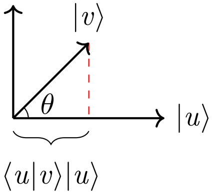
Outer products and projectors

As well as inner products, vectors can be multiplied by outer-products, for which they need no longer have the same dimension. Let $|u\rangle = \begin{bmatrix} a_1 & \dots & a_n \end{bmatrix}^{\mathsf{T}}$ and $|v\rangle = \begin{bmatrix} b_1 & \dots & b_m \end{bmatrix}^{\mathsf{T}}$, the outer product is defined as the $n \times m$ complex matrix: $|u\rangle\langle v|$.

If $|u\rangle$ is a unit vector, then $|u\rangle\langle u|$ is known as a projector, as $|u\rangle\langle u|$ is an operators that 'projects' an arbitrary vector (of appropriate dimension) $|v\rangle$ onto the subspace $|u\rangle$. That is:

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

which can be seen to be the projection of $|v\rangle$ onto $|u\rangle$ in the following diagram:



Basis

A basis of $\mathbb{C}^n$ is a minimal collection of vectors $|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle$ such that every vector $|v\rangle \in \mathbb{C}^n$ can be expressed as a linear combination of these:

$$|v\rangle = \alpha_1|v_1\rangle + \alpha_2|v_2\rangle + \cdots + \alpha_n|v_n\rangle$$

where the coefficients $\alpha_i \in \mathbb{C}$.

That the basis is a minimal collection of vectors means that $|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle$ are linearly independent, no $|v_i\rangle$ can be expressed as a linear combination of the rest. The size of the basis is n, termed its dimension.

Of particular interest are orthonormal bases, in which each basis vector is a unit vector, and the basis vectors are pairwise orthogonal, that is:

$$\langle v_i|v_j\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Standard 'computational' basis

Here are some bases for $\mathbb{C}^3$:

$$\begin{bmatrix}1\\2\\1\end{bmatrix}, \begin{bmatrix}10\\2+i\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix} \qquad \begin{bmatrix}0\\1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix}, \begin{bmatrix}0\\1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix} \qquad \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}$$

The latter two of these are orthonormal, of which the final one is known as the standard or computational basis. In general, the computational basis for $\mathbb{C}^n$ is

$$|1\rangle = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, |2\rangle = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, \ldots, |n\rangle = \begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$$

Sometimes, especially in the case of $\mathbb{C}^2$, well number these $|0\rangle \ldots |n-1\rangle$.

Expanding vectors and matrices in the standard basis

Any vector $|u\rangle = \begin{bmatrix} a_1 & a_2 & \dots & a_n \end{bmatrix}^\mathsf{T}$ can be expressed as a weighted sum of standard basis vectors:

$$|u\rangle = a_1|1\rangle + a_2|2\rangle + \cdots + a_n|n\rangle$$

Similarly, any matrix can be expressed as a double sum over the outer-products of standard basis vectors:

$$\begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \\ a_{n1} & & a_{nm} \end{bmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij}|i\rangle\langle j|$$

Eigenvectors and eigenvalues

If a $n \times n$ matrix, A, has the effect of scaling a given (non-zero) vector, $|v\rangle$ by a constant, λ, then that vector is known as an eigenvector, with corresponding eigenvalue λ:

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

The eigenvalues of a matrix are the roots of the characteristic polynomial:

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

where det denotes the determinant, and I is the $n \times n$ identity. Each square matrix has at least one eigenvalue.

- The determinant of a matrix is the product of its eigenvalues.
- The trace of a square matrix is the sum of its leading diagonal elements. It is also the sum of its eigenvalues.

Diagonal representation of matrices

If a $n \times n$ complex matrix A can be expressed in the form:

$$A = \sum_{i=1}^{n} \lambda_i |v_i\rangle\langle v_i|$$

where λ_i is the ith eigenvalue, corresponding to the ith eigenvector $|v_i\rangle$, then it is said to be diagonalisable. This is called the eigendecomposition, or spectral decomposition of A.

If A is diagonalisable as above, then it can be written as the diagonal matrix

$$\begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

in the basis of its eigenvectors, $|v_1\rangle$, $|v_2\rangle$, $\ldots$, $|v_n\rangle$. Moreover, the (normalised) eigenvectors form an orthonormal set.

Normal, Hermitian and unitary matrices

- A matrix is normal if $A^\dagger A = AA^\dagger$
  - A matrix is normal if and only if it is diagonalisable.
  - If $A = A^\dagger$ a matrix is Hermitian.
- A matrix is unitary if $A^\dagger A = AA^\dagger = I$ (the identity).
  - Unitary matrices play an important role in quantum computing.
  - Clearly all unitary matrices are normal therefore diagonalisable.
  - All eigenvalues of unitary matrices have absolute value one.
  - Unitary operators preserve inner products: if U is unitary and $|u'\rangle = U|u\rangle$ and $|v'\rangle = U|v\rangle$ then:

$$\begin{aligned}
\langle u'|v'\rangle &= (U|u\rangle)^\dagger (U|v\rangle) \\
&= (\langle u|U^\dagger)(U|v\rangle) \\
&= \langle u|(U^\dagger U)|v\rangle \\
&= \langle u|I|v\rangle \\
&= \langle u|v\rangle
\end{aligned}$$