Quantum Computing
Lecture 2

Review of Linear Algebra

Maris Ozols

Linear algebra

States of a quantum system form a vector space and their transformations are described by linear operators.

Vector spaces and linear operators are studied in linear algebra.

This lecture reviews definitions from linear algebra that we will need in the rest of the course!

Unless stated otherwise, all vector spaces are over $\mathbb{C}$.

Recall: Any $z \in \mathbb{C}$ is of the form $z = a + ib$ for some $a, b \in \mathbb{R}$.

Matrices

An $n \times m$ matrix is an array of numbers a_{ij} arranged as follows:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

For any A, we write A_{ij} to denote the entry in the i-th row and the j-th column of A. In the matrix above we have $A_{ij} = a_{ij}$.

We denote the set of all $n \times m$ complex matrices by $\mathrm{M}_{n,m}(\mathbb{C})$.

Basic matrix operations

Matrices can be added (if they are of the same shape) and multiplied by a constant (scalar). Both operations are performed entry-wise.

If $A, B \in \mathrm{M}_{n,m}(\mathbb{C})$ and $c \in \mathbb{C}$ then

$$(A + B)_{ij} = A_{ij} + B_{ij} \qquad\qquad (cA)_{ij} = cA_{ij}$$

Example:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & a_{13} + b_{13} \\ a_{21} + b_{21} & a_{22} + b_{22} & a_{23} + b_{23} \end{pmatrix}$$

$$c \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} = \begin{pmatrix} ca_{11} & ca_{12} & ca_{13} \\ ca_{21} & ca_{22} & ca_{23} \end{pmatrix}$$

Conjugate transpose

For $A \in \mathrm{M}_{n,m}(\mathbb{C})$ we define

- complex conjugate: A^* and $\bar{A}$

$$(A^*)_{ij} = (A_{ij})^* \qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}^* = \begin{pmatrix} a_{11}^* & a_{12}^* & a_{13}^* \\ a_{21}^* & a_{22}^* & a_{23}^* \end{pmatrix}$$

- transpose: A^T

$$(A^\mathsf{T})_{ij} = A_{ji} \qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}^\mathsf{T} = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{pmatrix}$$

- conjugate transpose (adjoint): $A^\dagger = (A^*)^\mathsf{T}$

$$(A^\dagger)_{ij} = A_{ji}^* \qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}^\dagger = \begin{pmatrix} a_{11}^* & a_{21}^* \\ a_{12}^* & a_{22}^* \\ a_{13}^* & a_{23}^* \end{pmatrix}$$

Warning: mathematicians often use A^* to denote $A^\dagger$.

Vectors and inner product

Vector is a matrix that has only one row or one column:

$$\begin{array}{cc} \text{row vector} & \text{column vector} \\ \begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} & \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \end{array}$$

Just like matrices, vectors of the same shape can be added and multiplied by scalars. They form a vector space denoted $\mathbb{C}^n$.

A row vector and a column vector can be multiplied together if they have the same number of entries. The result is a number:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n = \sum_{i=1}^{n} a_i b_i$$

This is a special case of matrix product. . .

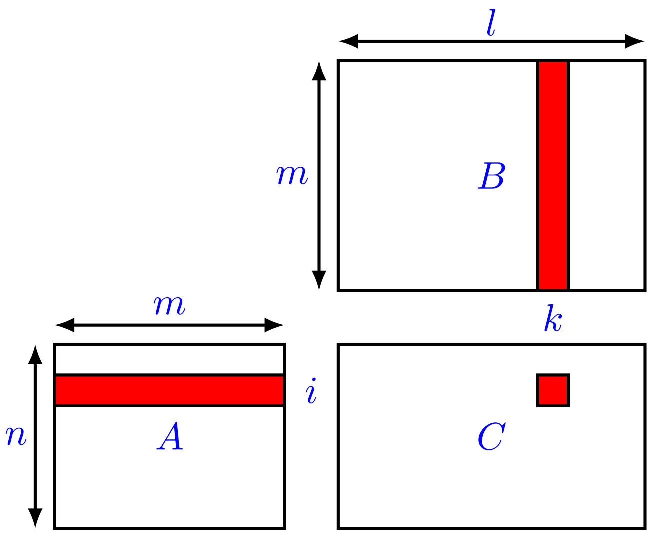
Matrix multiplication

If A is $n \times m$ and B is $m \times l$ matrix then $C = A \cdot B$ 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 $k = 1, \ldots, l$. Note that C_{ik} is just the product of the i-th row of A and the k-th column of B:

Note: It is possible to multiply A and B only if the number of columns of A agrees with the number of rows of B:
$[n \times m] \cdot [m \times l] = [n \times l]$



Properties of matrix multiplication

- *Associativity:* $(A \cdot B) \cdot C = A \cdot (B \cdot C) = ABC$
- *Distributivity:* $A(B + C) = AB + AC$ and $(A + B)C = AB + BC$
- *Scalar multiplication:* $\lambda(AB) = (\lambda A)B = A(\lambda B) = (AB)\lambda$
- *Complex conjugate:* $(AB)^* = A^* B^*$
- *Transpose:* $(AB)^\mathsf{T} = B^\mathsf{T} A^\mathsf{T}$ (reversed order!)
- *Conjugate transpose:* $(AB)^\dagger = B^\dagger A^\dagger$ (reversed order!)

Warning: Matrix multiplication is not commutative: $AB \neq BA$.
In fact, BA might not even make sense even if AB is well-defined (e.g., when A is 3×2 and B is 2×1).

Dirac bra-ket notation

Column vector (ket) Row vector (bra)

$$|\psi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \qquad \langle\psi| = \begin{pmatrix} a_1^* & a_2^* & \dots & a_n^* \end{pmatrix}$$

Note: Ket and bra are conjugate transposes of each other:

$$|\psi\rangle^\dagger \equiv \langle\psi| \qquad \langle\psi|^\dagger \equiv |\psi\rangle$$

For $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^n$ and $A \in \mathrm{M}_{n,n}(\mathbb{C})$ the following are valid products:

- inner product: $\langle\psi| \cdot |\varphi\rangle \equiv \langle\psi|\varphi\rangle \in \mathbb{C}$
- outer product: $|\psi\rangle \cdot \langle\varphi| \equiv |\psi\rangle\langle\varphi| \in M_{n\times n}(\mathbb{C})$
- matrix-vector product: $A \cdot |\psi\rangle \equiv A|\psi\rangle$ and $\langle\psi| \cdot A \equiv \langle\psi|A$

Quiz

Let $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^n$ and $A \in \mathrm{M}_{n,n}(\mathbb{C})$. Which of these make sense?

(a)	$\|\psi\rangle + \langle\varphi\|$	(h)	$\|\psi\rangle\langle\varphi\|A$
(b)	$\|\psi\rangle\langle\varphi\|$	(i)	$\|\psi\rangle A\langle\varphi\|$
(c)	$A\langle\psi\|$	(j)	$\langle\psi\|A\|\varphi\rangle$
(d)	$\|\psi\rangle A$	(k)	$\langle\psi\|A\|\varphi\rangle + \langle\psi\|\varphi\rangle$
(e)	$\langle\psi\|A$	(l)	$\langle\psi\|\varphi\rangle\langle\psi\|$
(f)	$\langle\psi\|A + \langle\varphi\|$	(m)	$\langle\psi\|\varphi\rangle A$
(g)	$\|\psi\rangle\|\varphi\rangle$	(n)	$\|\psi\rangle\langle\psi\|\varphi\rangle = \langle\psi\|\varphi\rangle\|\psi\rangle$

Inner product

The complex number $\langle u|v\rangle$ is called the inner product of $|u\rangle, |v\rangle \in \mathbb{C}^n$.

If $|u\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ and $|v\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ then their inner product is

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

Simple observations:

- $\langle u|v\rangle = \big(\langle v|u\rangle\big)^\dagger = \overline{\langle v|u\rangle}$
- $\langle u|u\rangle = \sum_{i=1}^{n} |a_i|^2$ is a real number
- $\langle u|u\rangle \geq 0$ and $\langle u|u\rangle = 0$ iff $|u\rangle = \mathbf{0}$ (the all-zeroes vector)

Norm and orthogonality

The norm of a vector $|u\rangle$ is the non-negative real number

$$\| |u\rangle \| = \sqrt{\langle u|u\rangle} = \sqrt{\sum_{i=1}^{n} |a_i|^2} \geq 0$$

A unit vector is a vector with norm 1, i.e., $\sum_{i=1}^{n} |a_i|^2 = 1$.

Recall: qubit states $\alpha|0\rangle + \beta|1\rangle$ are unit vectors since $|\alpha|^2 + |\beta|^2 = 1$.

Cauchy–Schwarz inequality: $|\langle u|v\rangle| \leq \| |u\rangle \| \, \| |v\rangle \|$ for any $|u\rangle, |v\rangle \in \mathbb{C}^n$.

If $|u\rangle$ and $|v\rangle$ are unit vectors then $|\langle u|v\rangle| \in [0, 1]$, so $|\langle u|v\rangle| = \cos\theta$ for some angle $\theta \in [0, \pi/2]$.

Vectors $|u\rangle$ and $|v\rangle$ are orthogonal if $\langle u|v\rangle = 0$ (i.e., $\theta = \pi/2$).

Basis

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

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

for some coefficients $\alpha_i \in \mathbb{C}$. In particular, $|v_1\rangle, \ldots, |v_n\rangle$ are linearly independent, meaning that no $|v_i\rangle$ can be expressed as a linear combination of the rest.

The number n (the size of the basis) is uniquely determined by the vector space and is called its dimension. The dimension of $\mathbb{C}^n$ is n.

Given a basis, every vector $|v\rangle$ can be uniquely represented as an n-tuple of scalars $\alpha_1, \ldots, \alpha_n$, called the coordinates of $|v\rangle$ in this basis.

An orthonormal basis is a basis made up of unit vectors that are pairwise orthogonal:

$$\langle v_i|v_j\rangle = \delta_{ij} \equiv \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

Standard basis for $\mathbb{C}^n$

The following are all bases for $\mathbb{C}^2$ (the last two are orthonormal):

$$\begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ -i \end{pmatrix} \qquad \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

The standard or computational basis for $\mathbb{C}^n$ is

$$|1\rangle \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad |2\rangle \equiv \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \cdots \quad |n\rangle \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

(Sometimes we will use $|0\rangle, |1\rangle, \ldots, |n-1\rangle$ instead, e.g., when $n = 2$.)

Any vector can be expanded in the standard basis:

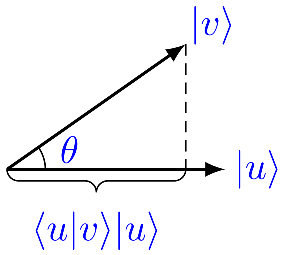
$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^{n} a_i|i\rangle$$

Outer product and projectors

With every pair of vectors $|u\rangle \in \mathbb{C}^n$, $|v\rangle \in \mathbb{C}^m$ we can associate a matrix $|u\rangle\langle v| \in \mathrm{M}_{n,m}(\mathbb{C})$ known as the outer product of $|u\rangle$ and $|v\rangle$.
For any $|w\rangle \in \mathbb{C}^m$, it satisfies the property

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

If $|u\rangle$ is a unit vector then $|u\rangle\langle u|$ is the projector on the one-dimensional subspace generated by $|u\rangle$. This can be easily seen if $|u\rangle$ and $|v\rangle$ are real and we set $\cos\theta = \langle u|v\rangle$. Then $|u\rangle\langle u|v\rangle = \langle u|v\rangle|u\rangle$.



Expanding a matrix in the standard basis

$$|1\rangle\langle 2| = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\begin{pmatrix}0 & 1 & \cdots & 0\end{pmatrix} = \begin{pmatrix}0 & 1 & \cdots & 0\\0 & 0 & \cdots & 0\\\vdots & \vdots & \ddots & \vdots\\0 & 0 & \cdots & 0\end{pmatrix}$$

Similarly, $|i\rangle\langle j|$ has 1 at coordinates (i,j) and zeroes everywhere else.

Any $n \times m$ matrix can be expressed as a linear combination of outer products:

$$\begin{pmatrix}a_{11} & a_{12} & \ldots & a_{1m}\\a_{21} & a_{22} & \ldots & a_{2m}\\\vdots & \vdots & \ddots & \vdots\\a_{n1} & a_{n2} & \ldots & a_{nm}\end{pmatrix} = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}|i\rangle\langle j|$$

We can recover the (i,j) entry of A as follows:

$$\langle i|A|j\rangle = a_{ij}$$

Eigenvalues and eigenvectors

An eigenvector of $A \in \mathrm{M}_{n,n}(\mathbb{C})$ is a non-zero vector $|v\rangle \in \mathbb{C}^n$ such that

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

for some complex number λ (the eigenvalue corresponding to $|v\rangle$).

The eigenvalues of A 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 matrix:

$$I = \sum_{i=1}^{n} |i\rangle\langle i|$$

Each $n \times n$ matrix has at least one eigenvalue.

Diagonal representation

Matrix $A \in \mathrm{M}_{n,n}(\mathbb{C})$ is diagonalisable if

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

where $|v_1\rangle, \ldots, |v_n\rangle$ is an orthonormal set of eigenvectors of A with corresponding eigenvalues $\lambda_1, \ldots, \lambda_n$.

This is called spectral decomposition of A.

Equivalently, A can be written as a diagonal matrix

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

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

Normal and Hermitian matrices

Matrix $A \in \mathrm{M}_{n,n}(\mathbb{C})$ is normal if

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

Theorem: A matrix is diagonalisable if and only if it is normal.

A is Hermitian if $A = A^\dagger$.

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

Unitary matrices

Matrix $A \in \mathrm{M}_{n,n}(\mathbb{C})$ is unitary if

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

where I is the $n \times n$ identity matrix.

Unitary operators are normal and therefore diagonalisable.

Unitary operators preserve inner products: if U is unitary and $|u'\rangle = U|u\rangle$ and $|v'\rangle = U|v\rangle$ then

$$\langle u'|v'\rangle = (U|u\rangle)^\dagger (U|v\rangle) = \langle u|U^\dagger U|v\rangle = \langle u|v\rangle$$

All eigenvalues of a unitary operator have absolute value 1.

Tensor product

Let A and B be matrices of arbitrary shape. Their tensor product is the following block matrix:

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1m}B \\ A_{21}B & A_{22}B & \cdots & A_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1}B & A_{n2}B & \cdots & A_{nm}B \end{pmatrix}$$

where the block at coordinates (i, j) is equal to $A_{ij}B$.

If A is $n \times m$ and B is $n' \times m'$ then $A \otimes B$ is $nn' \times mm'$.

Tensor product applies to vectors too, e.g., $|\psi\rangle \otimes |\varphi\rangle$ and $\langle\psi| \otimes \langle\varphi|$.

Note: $|\psi\rangle|\varphi\rangle$ is a shorthand for $|\psi\rangle \otimes |\varphi\rangle$.

Summary

- **Matrix multiplication:** $AB = C$ where $\sum_j A_{ij}B_{jk} = C_{ik}$, A, B, C have dimensions $[n \times m] \cdot [m \times l] = [n \times l]$
- **Conjugate transpose:** $A^\dagger = \bar{A}^\mathsf{T}$, $(AB)^\dagger = B^\dagger A^\dagger$
- **Dirac notation:** $|\psi\rangle^\dagger \equiv \langle\psi|$ and $\langle\psi|^\dagger \equiv |\psi\rangle$
- **Inner product:** $\langle\psi|\varphi\rangle$, it is 0 for orthogonal vectors
- **Norm:** $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$, it is 1 for unit vectors
- **Orthonormal basis:** $\langle v_i|v_j\rangle = \delta_{ij}$
- **Outer product:** $|\psi\rangle\langle\varphi|$, **projector:** $|\psi\rangle\langle\psi|$ where $\||\psi\rangle\| = 1$
- **Eigenvalues and eingevectors:** $A|v\rangle = \lambda|v\rangle$
- **Spectral decomposition:** $A = \sum_i \lambda_i |v_i\rangle\langle v_i|$ iff A is normal
- **Normal:** $AA^\dagger = A^\dagger A$
  - **Hermitian:** $A^\dagger = A$
  - **Unitary:** $AA^\dagger = A^\dagger A = I$
- **Tensor product:** $A \otimes B$ is a block matrix with (i, j)-th block $A_{ij}B$