Complex Vector Spaces

- **complex vector space:** non-empty set $\mathbb{V}$ of vectors
  - (A) operations: addition, negation, scalar multiplication
  - (A) zero vector $\mathbf{0} \in \mathbb{V}$
- **properties:**
  - (A) commutative addition
  - (A) associative addition
  - (A) zero is an additive identity
  - (A) every vector has an inverse $V + (-V) = \mathbf{0}$
  - scalar multiplication has a unit: $1 \cdot V = V$
  - scalar multiplication respects complex multiplication
  - scalar multiplication distributes over addition $c \cdot (V + W) = c \cdot V + c \cdot W$
  - scalar multiplication distributes over complex addition $(c_1 + c_2) \cdot V = c_1 \cdot V + c_2 \cdot V$
- any set with properties marked *(A)* is an **Abelian group**
- **real vector space:** non-empty set $\mathbb{V}$ of vectors
  - operations: additions, negation
    - scalar multiplication uses $\mathbb{R}$ not $\mathbb{C}$
  - properties: analogous to complex vector space properties
- real vector space is like a complex vector space, except scalar multiplication is defined for scalars in $\mathbb{R} \subset \mathbb{C}$
  - as $\mathbb{R} \subset \mathbb{C}$, for every $\mathbb{V}$, $\mathbb{R} \times \mathbb{V} \subset \mathbb{C} \times \mathbb{V}$
  - for a given scalar multiplication $\cdot : \mathbb{C} \times \mathbb{V} \to \mathbb{V}$, you have: $\mathbb{R} \times \mathbb{V} \hookrightarrow \mathbb{C} \times \mathbb{V} \to \mathbb{V}$
  - *every complex vector space can automatically be given a real vector space structure*

Complex matrices

- e.g. $\mathbb{C}^{m \times n}$, the set of m by n matrices with complex entries is a complex vector space
- consider $A \in \mathbb{C}^{m \times n}$. Then we can perform these operations on A:
- **transpose:** A^T, with $A^T_{ij} = A_{ji}$
- **conjugate:** $\bar{A}$ or A^*, with element-wise conjugation

- **adjoint/dagger:** $A^\dagger = \overline{(A^T)} = (\bar{A})^T$
- $\forall A, B \in \mathbb{C}^{m \times n}, c \in \mathbb{C}$ all 3 operations are: (let the operation be denoted x)
  - idempotent: $(A^x)^x = A$
  - respect addition: $(A + B)^x = A^x + B^x$
  - respect scalar multiplication $(c \cdot A)^x = c^x \cdot A^x$

Matrix Multiplication

- matrix multiplication is a binary operation:

$$* : \mathbb{C}^{m \times n} \times \mathbb{C}^{n \times p} \to \mathbb{C}^{m \times p}$$

- properties
  - **not** commutative
  - associative
  - I_n is a unit
  - distributes over addition
  - respects scalar multiplication
  - relates to transpose: $(A * B)^T = B^T * A^T$
  - respects the conjugate
  - relates to adjoint: $(A * B)^\dagger = B^\dagger * A^\dagger$
- complex vector space $\mathbb{V}$ with multiplication $*$ satisfying these properties is a **complex algebra**
- let $A \in \mathbb{C}^{n \times n}$. For any $B \in \mathbb{C}^n$ (a complex vector), $A * B \in \mathbb{C}^n$
  - i.e. multiplication by A gives a function: $A : \mathbb{C}^n \to \mathbb{C}^n$
  - A acts on vectors to yield new vectors

Linear maps

- **linear map** between complex vector spaces $\mathbb{V}, \mathbb{V}'$ is a function $f : \mathbb{V} \to \mathbb{V}'$ s.t. $\forall V, V_1, V_2 \in \mathbb{V}, c \in \mathbb{C}$
  - f respects addition: $f(V_1 + V_2) = f(V_1) + f(V_2)$
  - f respects scalar multiplication: $f(c \cdot V) = c \cdot f(V)$
- **operator:** linear map from a complex vector space to itself
  - if $F : \mathbb{C}^n \to \mathbb{C}^n$ is an operator on $\mathbb{C}$, A is an n-by-n matrix s.t. $\forall V F(V) = A * V$, then say F is **represented** by A

Isomorphism

- two complex vector spaces $\mathbb{V}, \mathbb{V}'$ are **isomorphic** if there is a bijective (one-to-one + onto) linear map $f : \mathbb{V} \rightarrow \mathbb{V}'$
  - call f an **isomorphism**
- when two vector spaces are isomorphic: the names of the elements of the vector space are renamed, but the structure of the 2 vector spaces are the same: the vector spaces are *essentially the same*, or *the same up to isomorphism*
- for complex vector spaces $\mathbb{V}, \mathbb{V}'$: $\mathbb{V}$ is a **complex subspace** of $\mathbb{V}'$ if $\mathbb{V} \subseteq \mathbb{V}$, and operations of $\mathbb{V}$ are restrictions of operations of $\mathbb{V}'$
- equivalently: $\mathbb{V}$ is a **complex subspace** of $\mathbb{V}'$ if $\mathbb{V} \subseteq \mathbb{V}$, and
  - $\mathbb{V}$ closed under addition and scalar multiplication

Isomorphism Example

- e.g. all matrices of the following form comprise a real subspace of $\mathbb{R}^{2\times 2}$

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

- this subspace is isomorphic to $\mathbb{C}$ via map $f : \mathbb{C} \rightarrow \mathbb{R}^{2\times 2}$ defined as:

$$f(x + iy) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

Basis and Dimension

- a set of vectors $\{V_0, ..., V_{n-1}\} \in \mathbb{V}$ is **linearly independent** if

$$\mathbf{0} = c_0 \cdot V_0 + ... + c_{n-1} \cdot V_{n-1}$$

implies $c_0 = ... = c_{n-1} = 0$. - i.e. the only way a linear combination of the vectors can be the zero vector is if all c_i are zero - linearly independent i.e. each vector in the set cannot be expressed as a linear combination of the other vectors in the set - equivalent to saying for any non-zero vector $V \in \mathbb{V}$ there are unique coefficients $c_i \in \mathbb{C}$ s.t. V is a linear combination of these vectors multiplied by these coefficients - a set of vectors $\mathcal{B} \subseteq \mathbb{V}$ forms a **basis** of complex vector space $\mathbb{V}$ if - every $V \in \mathbb{V}$ can be written as a linear combination of vectors from $\mathcal{B}$, and - $\mathcal{B}$ is linearly independent - every basis of a vector space has the same number of vectors, its **dimension**

Change of basis

- **change of basis/transition matrix:** from basis $\mathcal{B}$ to $\mathcal{D}$ is a matrix $M_{\mathcal{D} \leftarrow \mathcal{B}}$ s.t. for any matrix $\mathbb{V}$:

$$V_{\mathcal{D}} = M_{\mathcal{D} \leftarrow \mathcal{B}} * V_{\mathcal{B}}$$

- i.e. the matrix gets the coefficients with respect to one basis from the coefficients with respect to another basis

Hadamard Matrix

- in $\mathbb{R}^2$, the transition matrix from the canonical basis to the following basis:

$$\left\{ \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \right\}$$

is the **Hadamard matrix**

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

- $H * H = I_2$, so the transition back to the canonical basis is also H
- H is commonly used for change of basis in quantum computing calculations

Inner Products and Hilbert Spaces

- **inner product/dot product/scalar product** on a complex vector space $\mathbb{V}$ is a function

$$\langle -, - \rangle = \mathbb{V} \times \mathbb{V} \to \mathbb{C}$$

- $\forall V, V_1, V_2, V_3 \in \mathbb{V}, \forall a, c \in \mathbb{C}$ the inner product has the properties
- non-degenerate:
  - $\langle V, V \rangle \geq 0$
  - $\langle V, V \rangle = 0 \iff V = 0$ (only degenerate when it is 0)
- respects addition
  - $\langle V_1 + V_2, V_3 \rangle \langle V_1, V_3 \rangle + \langle V_2, V_3 \rangle \geq 0$, and vice versa

- respects scalar multiplication
  - $\langle c \cdot V_1, V_2 \rangle = c \cdot \langle V_1, V_2 \rangle$, and vice versa
- skew symmetric
  - $\langle V_1, V_2 \rangle = \overline{\langle V_2, V_1 \rangle}$, and vice versa
- a **complex inner product space** $\mathbb{V}, \langle -, - \rangle$ is a complex vector space along with an inner product

Norm and Distance

- for every complex inner product space you can define a **norm/length** which is a function

$$|| : \mathbb{V} \to \mathbb{R}$$

defined as $|V| = \sqrt{\langle V, V \rangle}$

- **intuition:** norm of a vector in any vector space is its length
- properties:
  - nondegenerate
  - satisfies triangle inequality $|V + W| \leq |V| + |W|$
  - respects scalar multiplication
- for every complex inner product space you can define a **distance function**

$$d(,) : \mathbb{V} \to \mathbb{R}$$

where

$$d(V_1, V_2) = |V_1 - V_2| = \sqrt{\langle V_1 - V_2 \rangle, \langle V_1 - V_2 \rangle}$$

- **intuition:** $d(V_1, V_2)$ is the distance from the end of vector V_1 to the end of vector V_2
- properties
  - non-degenerate
  - satisfies triangle inequality
  - symmetric

Orthogonal Basis

- two vectors $V_1, V_2 \in \mathbb{V}$, an inner product space, are **orthogonal** if $\langle V_1, V_2, \rangle = 0$
- **intuition:** two vectors are orthogonal if they are perpendicular to each other
- a basis $\mathbb{B} = \{V_0, ..., V_{n-1}\}$ for an inner product space $\mathbb{V}$ is called an **orthogonal basis** if the vectors are pairwise orthogonal to each other: $j \neq k \implies \langle V_j, V_k \rangle = 0$
- **orthonormal basis:** orthogonal basis of norm 1 (Kronecker delta, $\delta_{j,k}$)

Eigenvalues and Eigenvectors

- for certain vectors, the action of a matrix upon it merely changes its length, while the direction remains the same
- such vectors are eigenvectors, and the scalar multiples are eigenvalues (for the matrix)
- formally: for a matrix $A \in \mathbb{C}^{n \times n}$, if $\exists c \in \mathbb{C}$ and a non-zero vector $V \in \mathbb{C}^n$, such that:

$$AV = c \cdot V$$

- c: **eigenvalue** of A
- V: **eigenvector** of A associated with c
- **eigenspace:** every eigenvector determines a complex subvector space of the vector space

Hermitian Matrices

- a matrix $A \in \mathbb{R}^{n \times n}$ is **symmetric** if $A^T = A$
- generalising to the complex numbers: a matrix $A \in \mathbb{C}^{n \times n}$ is **Hermitian** if $A^\dagger = A$
  - $A_{jk} = \overline{A_{kj}}$
- if A is hermitian, the operator it represents is called **self-adjoint**
- the diagonal elements of a hermitian matrix must be real
- if A is hermitian, then $\forall V, V' \in \mathbb{C}^n$:

$$\langle AV, V' \rangle = \langle V, AV' \rangle$$

- if A is hermitian, then **all eigenvalues are real**
- for a given hermitian matrix, distinct eigenvectors with distinct eigenvalues are orthogonal
- **diagonal matrix:** square matrix whose only non-zero entries are on the diagonal

- **Spectral Theorem for Finite-Dimensional Self-Adjoint Operators:** every self-adjoint operator A on a finite-dimensional complex vector space $\mathbb{V}$ can be represented by a diagonal matrix whose diagonal entries are the eigenvalues of A, and whose eigenvectors form an orthonormal basis (an **eigenbasis**) for $\mathbb{V}$
- every physical observable of a quantum system has a corresponding hermitian matrix

Unitary Matrices

- a matrix A is **invertible** if $\exists A^{-1}$, such that:

$$A * A^{-1} = A^{-1} * A = I_n$$

- unitary matrices are a flavour of invertible matrix, whose inverse is their adjoint: this ensure unitary matrices preserve the geometry of the space on which they act
- NB: not all invertible matrices are unitary
- formally: a matrix $U \in \mathbb{C}^{n \times n}$ is **unitary** if:

$$U * U^\dagger = U^\dagger * U = I_n$$

- unitary matrices preserve inner products: if U is unitary $\langle UV, UV' \rangle = \langle V, V' \rangle$, for any $V, V' \in \mathbb{C}^n$
- unitary matrices preserve norms: $|UV| = |V|$
- **isometry:** unitary matrices preserve distance: $d(UV_1, UV_2) = d(V_1, V_2)$
- if $|V| = 1$, $|UV| = 1$. The set of all such vectors forms the **unit sphere**
- a unitary matrix performs a rotation of the unit sphere
- if U is unitary, and $UV = V'$
  - we can form $U^\dagger$ and multiply both sides by it: $U^\dagger UV = U^\dagger V'$
  - gives $V = U^\dagger V'$
  - i.e. as U is unitary, there is a related matrix that is able to **undo** the action U performs
  - $U^\dagger$ takes the result of U's action and gets back to the original vector
  - in the quantum world, all actions (other than measurements) are undoable/reversible in this sense

Tensor Products