THE UNIVERSITY of EDINBURGH informatics

Quantum Cyber Security

Lecture 2: Math supplement

Petros Wallden (slides credit: Raul Garcia-Patron Sanchez)

Postulate I: Quantum states

A quantum state with d degrees of freedom is described by a complex vector space with inner-product (Hilbert space) with norm 1.

$$|\psi\rangle \in \mathcal{H} \equiv \mathbb{C}^d \qquad \langle\psi|\psi\rangle = 1$$

Hilbert space = Complex Vector Space + Inner-product

State vector $|\psi\rangle \equiv \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_d \end{bmatrix}$ A d-dimensional vector of complex numbers

α_i : Probability amplitude of degree of freedom i

Complex number in a nutshell

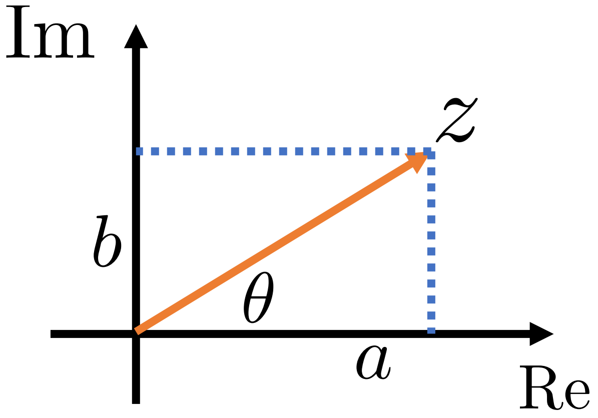
- $\mathbb{C} = \{z = a + ib | (a, b) \in \mathbb{R}^2 \text{ and } i^2 = -1\}$

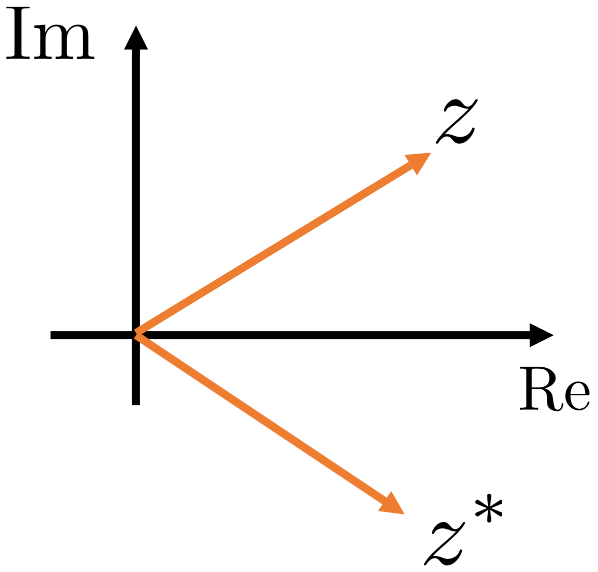
  Trigonometric form: $z = |z|(\cos\theta + i\sin\theta)$

- Addition: $z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2)$
- Multiplication: $z_1 z_2 = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2)$
- Conjugation: $z^* = a - ib$

  $(z_1 + z_2)^* = z_1^* + z_2^* \qquad (z_1 z_2)^* = z_1^* z_2^*$

- Norm: $|z| = \sqrt{zz^*}$
- Euler equation: $e^{i\theta} = (\cos\theta + i\sin\theta) \Rightarrow z = |z|e^{i\theta}$
- Multiplication: $z_1 z_2 = |z_1||z_2|e^{i(\theta_1 + \theta_2)}$





Hilbert Space: Complex vector space $\mathcal{H} \equiv \mathbb{C}^d$

Addition: $\mathcal{H} \times \mathcal{H} \to \mathcal{H}$

$$|\psi\rangle + |\phi\rangle \equiv \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{d-1} \end{bmatrix} + \begin{bmatrix} \phi_0 \\ \phi_1 \\ \vdots \\ \phi_{d-1} \end{bmatrix} = \begin{bmatrix} \psi_0 + \phi_0 \\ \psi_1 + \phi_1 \\ \vdots \\ \psi_{d-1} + \phi_{d-1} \end{bmatrix}$$

Associativity: $|\psi_1\rangle + (|\psi_2\rangle + |\psi_3\rangle) = (|\psi_1\rangle + |\psi_2\rangle) + |\psi_3\rangle$

Commutativity: $|\psi_1\rangle + |\psi_2\rangle = |\psi_2\rangle + |\psi_1\rangle$

Neutral element: $|\psi\rangle + |\emptyset\rangle = |\psi\rangle$

The zero vector: $|\emptyset\rangle \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

Inverse element: $\forall |\psi\rangle, \exists |\nu\rangle$ s.t. $|\psi\rangle + |\nu\rangle = |\emptyset\rangle$

Hilbert Space: Complex vector space $\mathcal{H} \equiv \mathbb{C}^d$

Scalar multiplication: $\mathbb{C} \times \mathcal{H} \to \mathcal{H}$

$$\lambda|\psi\rangle \equiv \lambda \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{d-1} \end{bmatrix} = \begin{bmatrix} \lambda\psi_0 \\ \lambda\psi_1 \\ \vdots \\ \lambda\psi_{d-1} \end{bmatrix}$$

Compatibility: $\lambda(\nu|\psi\rangle) = (\lambda\nu)|\psi\rangle$

(Compatibility of product of scalars with scalar multiplication)

Distributivity (vector addition): $\lambda(|\psi_1\rangle + |\psi_2\rangle) = \lambda|\psi_1\rangle + \lambda|\psi_2\rangle$

Distributivity (field addition): $(\lambda + \nu)|\psi\rangle = \lambda|\psi\rangle + \nu|\psi\rangle$

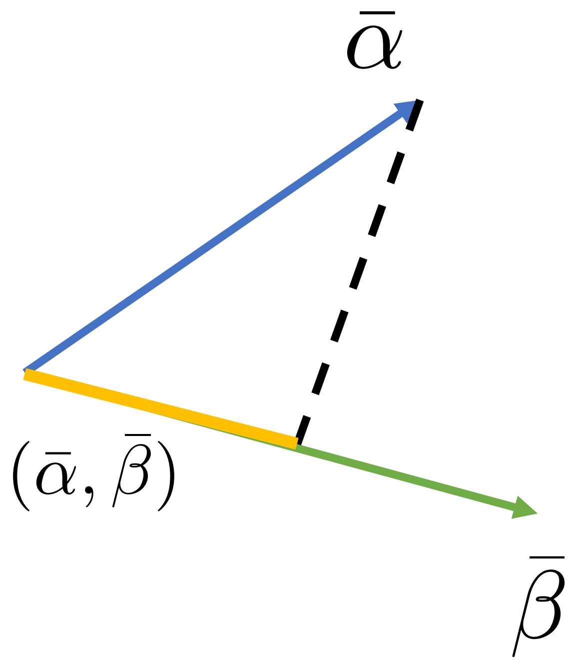
Identity element: $1|\psi\rangle = |\psi\rangle$

Multiplying by zero: $0|\psi\rangle = |\emptyset\rangle$

Inner-product (Math notation) $\mathcal{H} \equiv \mathbb{C}^d$

Inner-product $(\cdot,\cdot) : V \times V \to \mathbb{F}$

$$(\bar{\alpha}, \bar{\beta}) = \begin{bmatrix} \beta_0^* & \alpha_1^* & \dots & \alpha_{d-1}^* \end{bmatrix} \times \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{d-1} \end{bmatrix} = \sum_{i=0}^{d-1} \alpha_i^* \beta_i$$



Linearity: $(\lambda\bar{\alpha}, \bar{\beta}) = \lambda^*(\bar{\alpha}, \bar{\beta})$

$$(\bar{\alpha}_1 + \bar{\alpha}_2, \bar{\beta}) = (\bar{\alpha}_1, \bar{\beta}) + (\bar{\alpha}_2, \bar{\beta})$$

Conjugate symmetry: $(\bar{\alpha}, \bar{\beta}) = (\bar{\beta}, \bar{\alpha})^*$

Positive semi-definiteness: $(\bar{\alpha}, \bar{\alpha}) \geq 0$

$$(\bar{\alpha}, \bar{\alpha}) = 0 \Leftrightarrow \bar{\alpha} = \bar{0}$$

Hilbert Space: Inner-product (Dirac Notation) $\mathcal{H} \equiv \mathbb{C}^d$

Inner-product: $\mathcal{H} \times \mathcal{H} \to \mathbb{C}$

$$\langle\psi|\phi\rangle = \sum_{i=0}^{d-1} \psi_i^* \phi_i$$

Ket $|\psi\rangle \equiv \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{d-1} \end{bmatrix}$

Bra $\langle\psi| = |\psi\rangle^\dagger \equiv \begin{bmatrix} \psi_1^* & \psi_2^* & \dots & \psi_d^* \end{bmatrix}$

Linearity: $(\lambda|\psi\rangle, |\phi\rangle) = \lambda^*\langle\psi|\phi\rangle = (\lambda|\psi\rangle)^\dagger|\phi\rangle = \langle\lambda\psi|\phi\rangle$

$$(|\psi_1\rangle + |\psi_2\rangle) = \langle\psi_1|\phi\rangle + \langle\psi_2|\phi\rangle = \langle\psi_1 + \psi_2|\phi\rangle$$

Dirac notation can lead to some inconsistencies.
We are rarely confronted with those and can be avoided.

Conjugate symmetry: $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$

Positive semi-definiteness: $\langle\psi|\psi\rangle \geq 0$

$$\langle\psi|\psi\rangle = 0 \Leftrightarrow |\psi\rangle = |\emptyset\rangle$$

Norm

$\mathcal{H} \equiv \mathbb{C}^d$

Norm: $\mathcal{H} \rightarrow \mathbb{R}^+$

$$|| \, |\psi\rangle || = \sqrt{\langle\psi|\psi\rangle} \geq 0$$

- $|| \, |\psi\rangle || = 0 \Leftrightarrow |\psi\rangle = |\emptyset\rangle$
- $||\lambda|\psi\rangle|| = |\lambda| \, || \, |\psi\rangle||$
- $|||\psi\rangle + |\phi\rangle|| \leq || \, |\psi\rangle|| + || \, |\phi\rangle||$ Triangle inequality
- Quantum states have norm 1: $|||\psi\rangle|| = 1$

Norm being 1 is associated with the fact that measurement outcome probabilities should sum to one. QM equivalent of axiom 3 for classical systems (slide 3.)

Postulate II: Quantum operations

The evolution of a quantum system $|\psi\rangle \in \mathcal{H} \equiv \mathbb{C}^d$ is given by a unitary tranformation $U : \mathcal{H} \to \mathcal{H}$, s.t. $|\psi_{out}\rangle = U|\psi_{in}\rangle$

Unitary matrices

$$UU^\dagger = U^\dagger U = I_d$$

- Linear operator $U : \mathcal{H} \to \mathcal{H}$
- Preserves the inner-product
- Equivalent of orthogonal matrices on real vector spaces

Linearity

- $A \in \mathcal{L}(\mathcal{H}) : \mathcal{H} \to \mathcal{H}$ is linear on its inputs:
  - $A(\sum_i a_i |v_i\rangle) = \sum_i a_i A(|v_i\rangle)$
  - $(A + B)|\psi\rangle = A|\psi\rangle + B|\psi\rangle$
  - Composition: $(BA)|\psi\rangle \equiv B(A|\psi\rangle)$
  - Matrix representation: $A|j\rangle = \sum_i A_{ij} |i\rangle$

Adjoint (Hermitian conjugate)

- Adjoint (Hermitian conjugate): $\forall A, \exists A^\dagger : (|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle)$
  - Matrix representation: $A^\dagger = (A^T)^*$
  - $(BA)^\dagger = B^\dagger A^\dagger$
  - $|\psi\rangle^\dagger \equiv \langle\psi|$
  - $(A|\psi\rangle)^\dagger \equiv \langle\psi|A^\dagger$
  - $(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle) = \langle v|A|w\rangle$

Dirac notation incorporates some equalities by construction!

Unitaries preserve the inner-product

- Adjoint (Hermitian conjugate): $\forall A, \exists A^\dagger : (|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle)$
  - Matrix representation: $A^\dagger = (A^T)^*$
  - $(BA)^\dagger = B^\dagger A^\dagger$
  - $|\psi\rangle^\dagger \equiv \langle\psi|$
  - $(A|\psi\rangle)^\dagger \equiv \langle\psi|A^\dagger$
  - $(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle) = \langle v|A|w\rangle$

Dirac notation incorporates some equalities by construction!

$$UU^\dagger = U^\dagger U = I_d$$

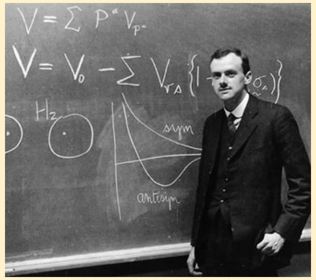
- Preserves the inner-product

$$|\tilde{\psi}\rangle = U|\psi\rangle$$

$$\langle\tilde{\psi}|\tilde{\psi}\rangle = (\langle\psi|U^\dagger)(U|\psi\rangle) = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|I_d|\psi\rangle = \langle\psi|\psi\rangle = 1$$

Outer-product

- Outer-product: $|\phi\rangle\langle\psi| \equiv \begin{bmatrix} \phi_0 \\ \phi_1 \\ \vdots \\ \phi_{d-1} \end{bmatrix} \times \begin{bmatrix} \psi_0^* & \psi_1^* & \dots & \psi_{d-1}^* \end{bmatrix} \in \mathcal{L}(\mathcal{H})$



- $|v_j\rangle\langle w_i| \in \mathcal{L}(\mathcal{H}), \mathcal{H} \to \mathcal{H}:$
  - $(|v_j\rangle\langle w_i|)|\psi\rangle = |v_j\rangle \underbrace{\langle w_i|\psi\rangle}_{\in\mathbb{C}} = \langle w_i|\psi\rangle|v_j\rangle = \psi_{w_i}|v_j\rangle$

- $$A = \sum_{i,j} a_{ij}|i\rangle\langle j| \qquad |2\rangle\langle 3| \equiv \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$