THE UNIVERSITY *of* EDINBURGH
informatics

Introduction to Quantum Computing

Lecture 2: Postulate I – Quantum States

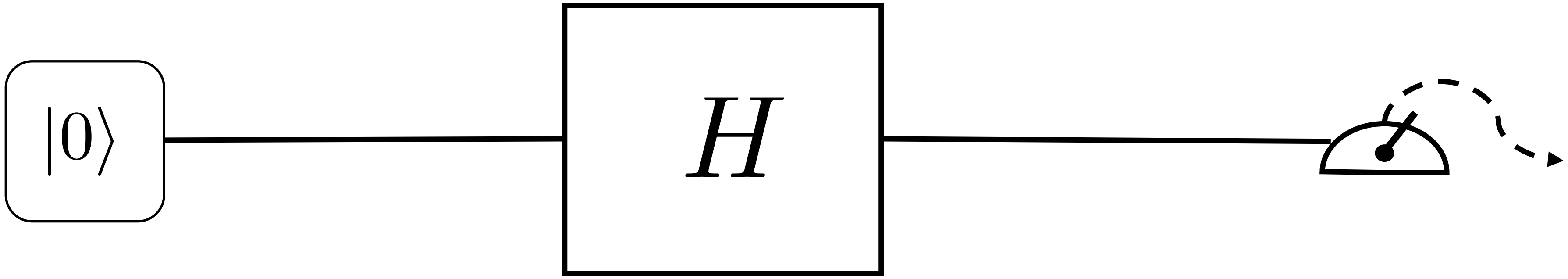
Raul Garcia-Patron Sanchez

The ideal life of a qubit in a nutshell

State preparation | Operation | Measurement

Source of quantum states

Circuit/Gates

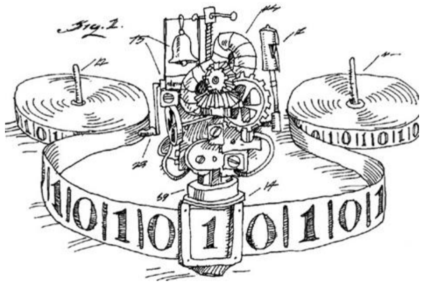


Quantum random number generator circuit

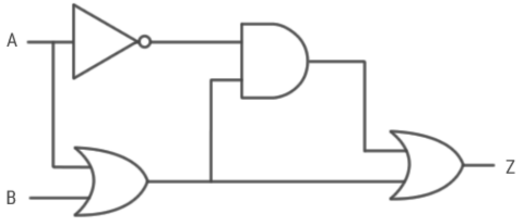
Classical bits

Today computation is base on the computation on binary registers (bits)

- Turing machines

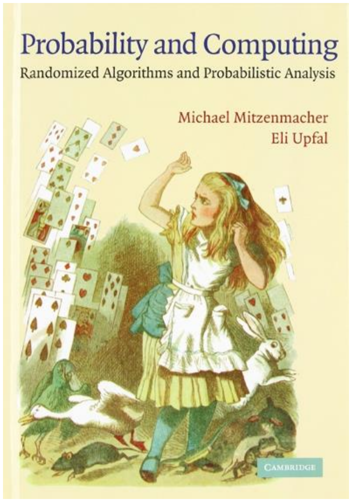


- Circuits



- Probabilistic computation

  - Simulated Annealing
  - Primality Test



A discrete probability space

- Sample space Ω : the set of all possible outcomes.

$\Omega = \{0, 1, ..., d-1\}$ $\qquad$ n bits $: d = 2^n$

- Axioms (state of the system)

  - $$\bar{p} = \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{d-1} \end{bmatrix} \in \mathbb{R}^d$$

$$\bar{p} = \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{d-1} \end{bmatrix} = p_0 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + p_1 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + ... + p_{d-1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

  - $p_i \geq 0$ (Positiveness)
  - $P(\Omega) = \sum_{i=0}^{d-1} p_i = 1$ (Normalization)

Classical bit

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = p_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + p_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Quantum Bit or Qubit

Logical zero $|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Logical one $|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

These two states (logical 0 and 1) form an orthonormal basis of a qubit.

General state of a qubit $|\psi\rangle \equiv \begin{bmatrix} \psi_0 \\ \psi_1 \end{bmatrix}$

$\psi_i \in \mathbb{C}$: probability amplitudes

where $|\psi_0|^2 + |\psi_1|^2 = 1$ (Normalization)

$$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle \equiv \psi_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \psi_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

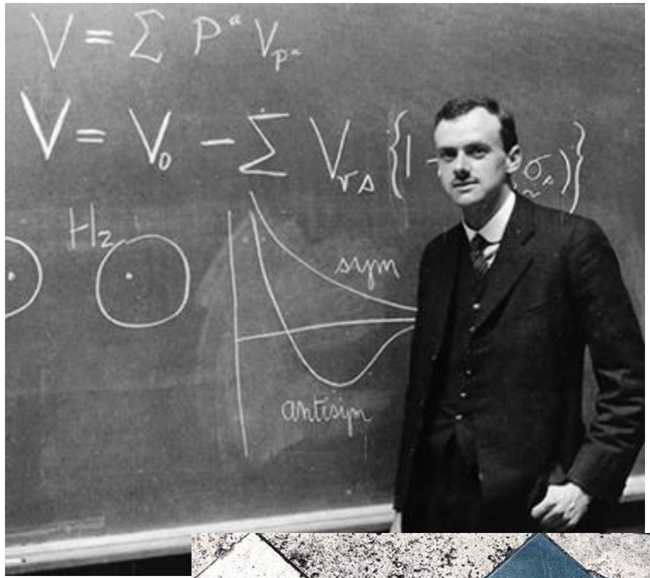
Linearity of QM allows us to write any qubit state a a linear combination of logical 0 or 1, as they are a basis for the qubit state space.

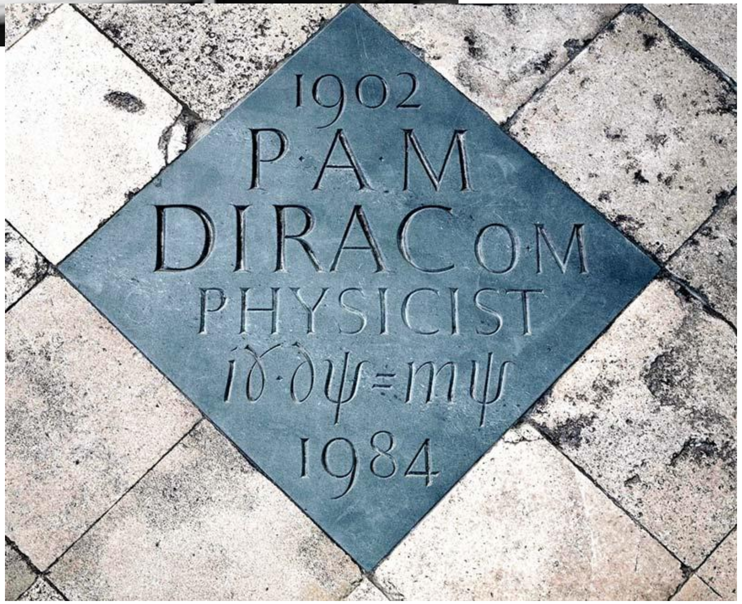
Dirac Notation

Dirac notation

$|\psi\rangle$ ket

$$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle \equiv \psi_0 \begin{bmatrix}1\\0\end{bmatrix} + \psi_1 \begin{bmatrix}0\\1\end{bmatrix}$$





Westminster Abbey (London)

Paul Dirac: Nobel Prize 1933
Fundamental contributions to:

- quantum mechanics
- quantum electrodynamics

Postulate I: Quantum states

A quantum state with d degrees of freedom is a vector belonging to a Hilbert space of dimension d and norm 1.

Hilbert space = Complex Vector Space + Inner-product

State vector $$|\psi\rangle \equiv \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{d-1} \end{bmatrix} = \psi_0|0\rangle + \psi_1|1\rangle + ... + \psi_{d-1}|d-1\rangle$$

$\psi_i \in \mathbb{C}$: Probability amplitude of degree of freedom i

Normalization: $$\sum_{i=0}^{d-1} \psi_i^* \psi_i = \sum_{i=0}^{d-1} |\psi_i|^2 = 1$$

n qubits $: d = 2^n$

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

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

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

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

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

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

Inner-product in a nutshell

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

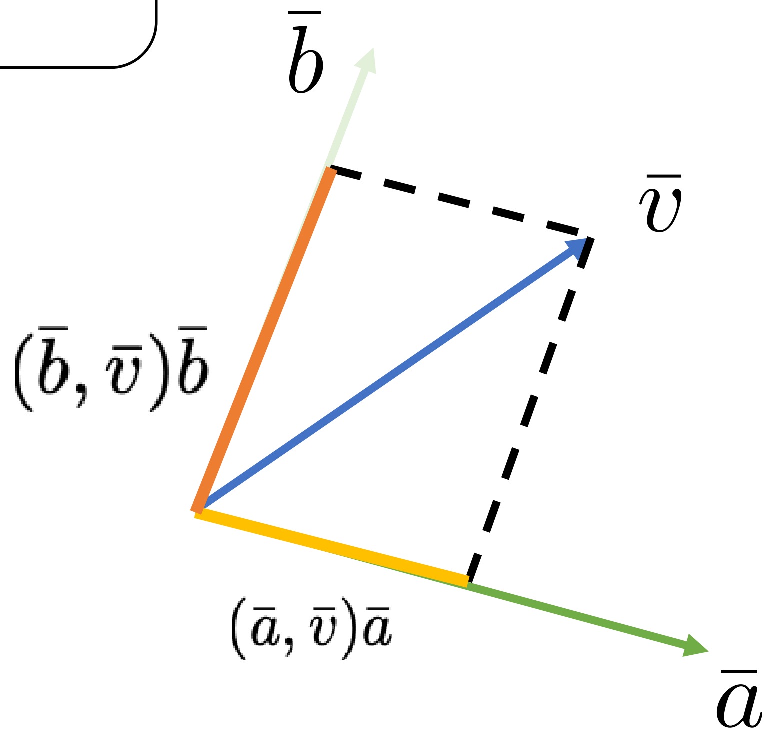
$$(\bar{x},\bar{y}) = \bar{x}\cdot\bar{y} = \sum_{i=0}^{d-1} x_i y_i$$

$\bar{a}$ and $\bar{b}$ orthonormal basis:

$$(\bar{a},\bar{a}) = (\bar{b},\bar{b}) = 1$$

$$(\bar{a},\bar{b}) = 0$$

$$\bar{v} = (\bar{a},\bar{v})\bar{a} + (\bar{b},\bar{v})\bar{b}$$

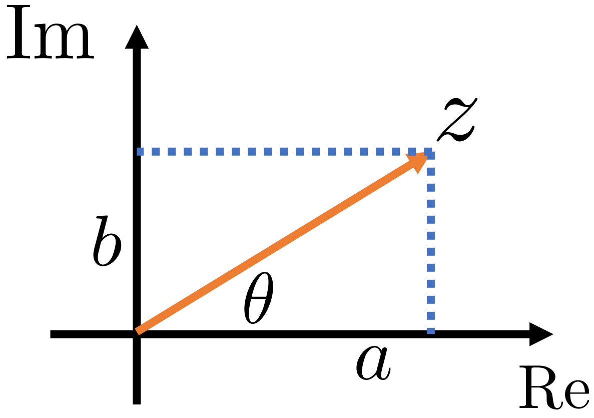


- Norm: $V \to \mathbb{R}^+$ $\quad ||\bar{v}|| = \sqrt{(\bar{v},\bar{v})} \geq 0$
- Orthogonal transformation preserves inner-product

Complex number in a nutshell

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

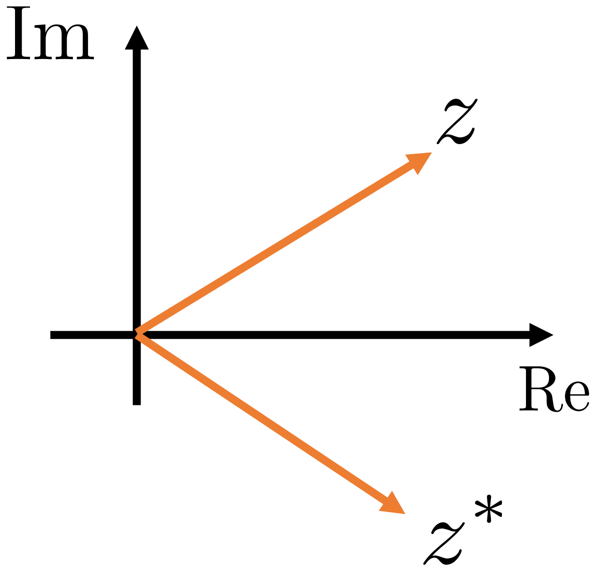
  Trigonometric form: $z = |z|(\cos\theta + i\sin\theta)$



- 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: $z^* = a - ib$



- Norm: $|z| = \sqrt{zz^*}$

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

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

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

Bra

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

$$\langle\psi| = |\psi\rangle^\dagger = (|\psi\rangle^T)^*$$

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

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

$$\langle|\psi\rangle, |\phi\rangle\rangle = \begin{bmatrix}\psi_0^* & \psi_1^* & \dots & \psi_{d-1}^*\end{bmatrix} \times \begin{bmatrix}\phi_0 \\ \phi_1 \\ \vdots \\ \phi_{d-1}\end{bmatrix} = \sum_{i=0}^{d-1} \psi_i^* \phi_i$$

Bra

$$\langle\psi| \equiv \begin{bmatrix}\psi_0^* & \psi_1^* & \dots & \psi_{d-1}^*\end{bmatrix}$$

Ket

$$|\phi\rangle \equiv \begin{bmatrix}\phi_0 \\ \phi_1 \\ \vdots \\ \phi_{d-1}\end{bmatrix}$$

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

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

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

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

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

Bra

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

$$\langle\psi| = |\psi\rangle^\dagger = (|\psi\rangle^T)^*$$

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

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

- $|||\psi\rangle + |\phi\rangle|| \leq ||\,|\psi\rangle|| + ||\,|\phi\rangle||$ 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.)

Basis: Computational basis $\mathcal{H} \equiv \mathbb{C}^d$

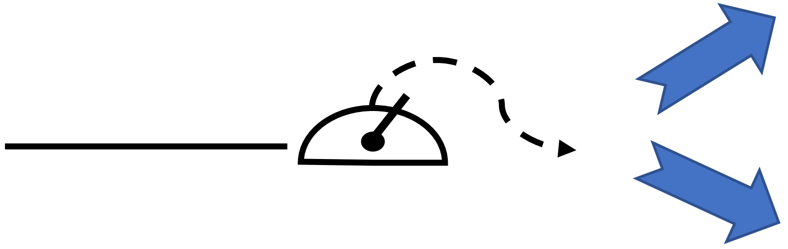
Computational basis $\quad \mathcal{H}_{\mathcal{Q}} = \text{Span}\{|0\rangle, |1\rangle\}$

- $\forall |\psi\rangle, \exists \psi_0 \text{ and } \psi_1 : |\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$
- $\langle 0|1\rangle = 0 \text{ (Orthogonal basis)}$
- $|| \, |0\rangle|| = || \, |1\rangle|| = 1 \text{ (Normalized basis)}$

This ensure logical 0 and 1 is an orthonormal basis of a Hilbert space of dim 2.

Computational basis measurement

$|\psi\rangle$



$$P(0) = |\langle 0|\psi\rangle|^2 = |\psi_0|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$

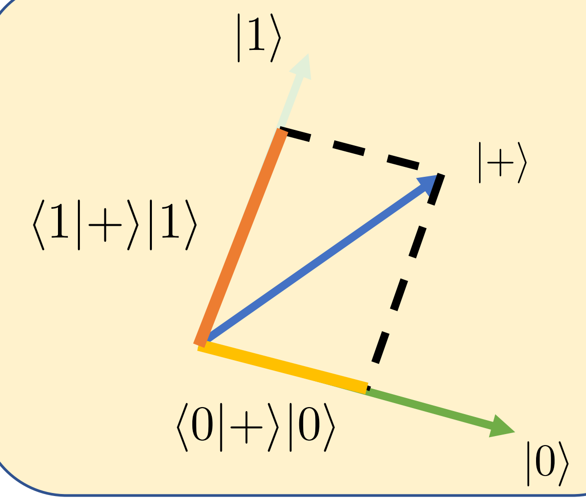
The amplitudes of the quantum state on the logical basis (0 and 1) are associated with the outcome probabilities of the computational basis measurement (logical 0 or 1).

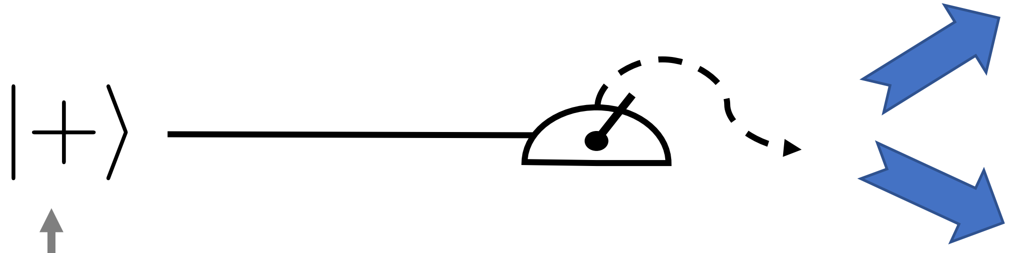
Quantum randomness generation

Computational basis measurement

$$P(0) = |\langle 0|\psi\rangle|^2 = |\psi_0|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$





$$P(0) = ?$$

$$P(1) = ?$$

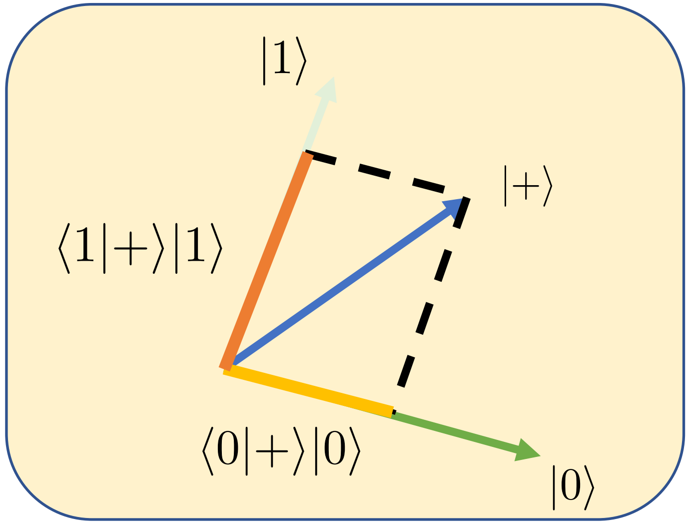
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

Quantum randomness generation

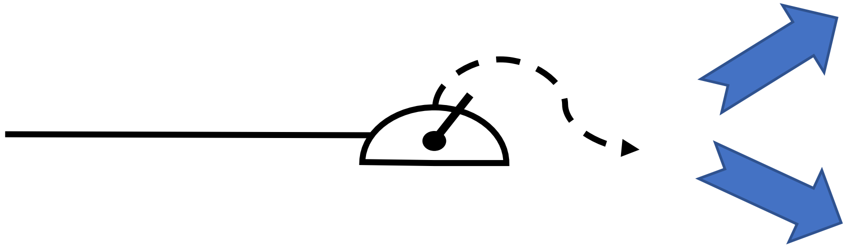
Computational basis measurement

$$P(0) = |\langle 0|\psi\rangle|^2 = |\psi_0|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$



$|+\rangle$



$$P(0) = |\langle 0|+\rangle|^2 = 1/2$$

$$P(1) = |\langle 1|+\rangle|^2 = 1/2$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

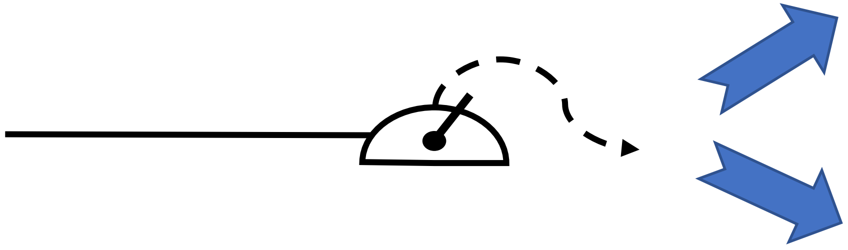
Quantum randomness generation

Computational basis measurement

$$P(0) = |\langle 0|\psi\rangle|^2 = |\psi_0|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$

$$|-\rangle$$



$$P(0) = ?$$

$$P(1) = ?$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$$

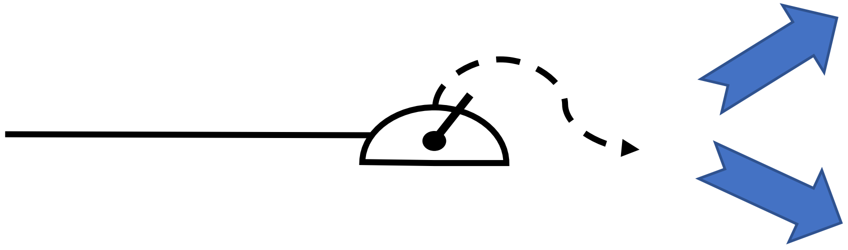
Quantum randomness generation

Computational basis measurement

$$P(0) = |\langle 0|\psi\rangle|^2 = |\psi_0|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$

$$|-\rangle$$

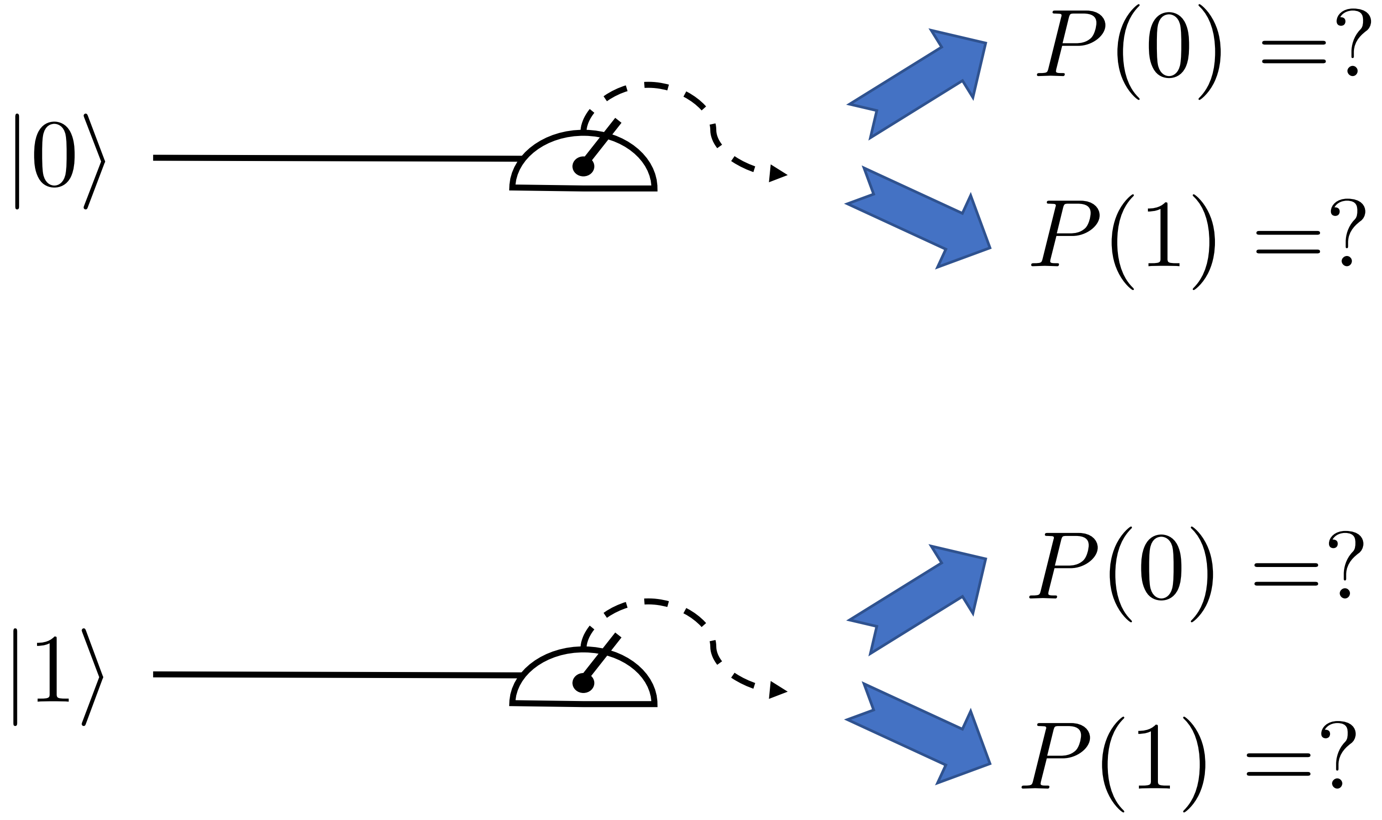


$$P(0) = |\langle 0|-\rangle|^2 = 1/2$$

$$P(1) = |\langle 1|-\rangle|^2 = 1/2$$

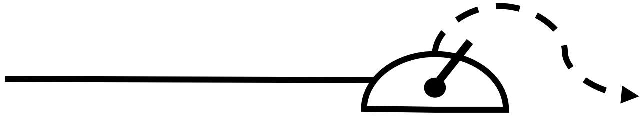
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$$

Quantum randomness generation



Quantum randomness generation

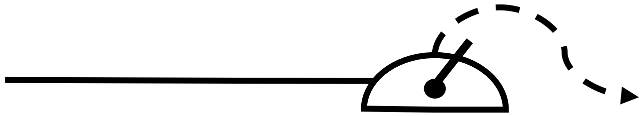
$|0\rangle$



$$P(0) = |\langle 0|0\rangle|^2 = 1$$

$$P(1) = |\langle 1|0\rangle|^2 = 0$$

$|1\rangle$



$$P(0) = |\langle 0|1\rangle|^2 = 0$$

$$P(1) = |\langle 1|1\rangle|^2 = 1$$

Postulate I: Quantum states

A quantum state with d degrees of freedom is represented by a vector in a complex vector space with inner-product (Hilbert space)

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

Hilbert space = Complex Vector Space + Inner-product

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

A d-dimensional vector of complex numbers

- Qubit: $d = 2$
- Qudit: $d > 2$
- N qubits: $d = 2^N$

$\psi_i \in \mathbb{C}$: Probability amplitude of degree of freedom i

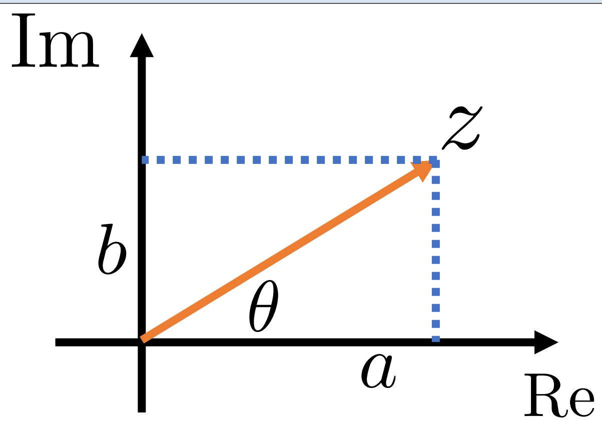
$$P(i) = |\psi_i|^2$$

References

Course Material

1. *Quantum Computing and Quantum Information*, Michael Nielsen and Isaac Chuang, Cambridge University Press (2010) [Sections 1.2, 2.1.1-2.1.4].

Complex number in a nutshell



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

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

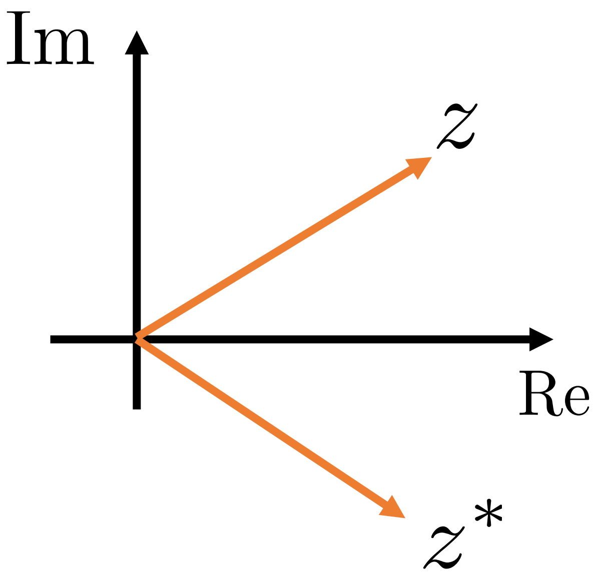
- Norm: $|z|^2 = zz^* = a^2 + b^2$

- 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: $z^* = a - ib$

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



- 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: $|\psi\rangle + |0\rangle = |\psi\rangle$

Inverse element: $\forall|\psi\rangle, \exists|\nu\rangle$ s.t. $|\psi\rangle + |\nu\rangle = |0\rangle$

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

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

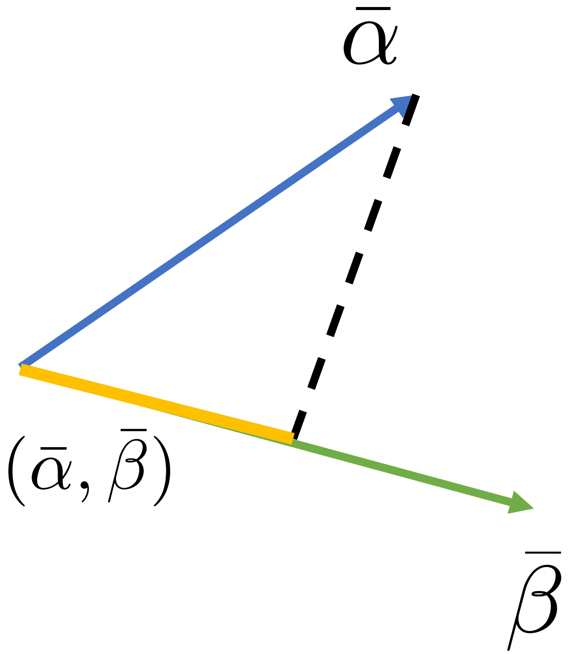
Identity element: $1|\psi\rangle = |\psi\rangle$

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

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: $(\bar{\alpha}, \bar{\alpha}) \geq 0$

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

Norm

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

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

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

- $|| \, |\psi\rangle || = 0 \Leftrightarrow |\psi\rangle = |\emptyset\rangle$
- $||\lambda|\psi\rangle|| = |\lambda| \, || \, |\psi\rangle||$
- $|||\psi\rangle + |\phi\rangle|| \leq || \, |\psi\rangle|| + || \, |\phi\rangle||$ 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.)