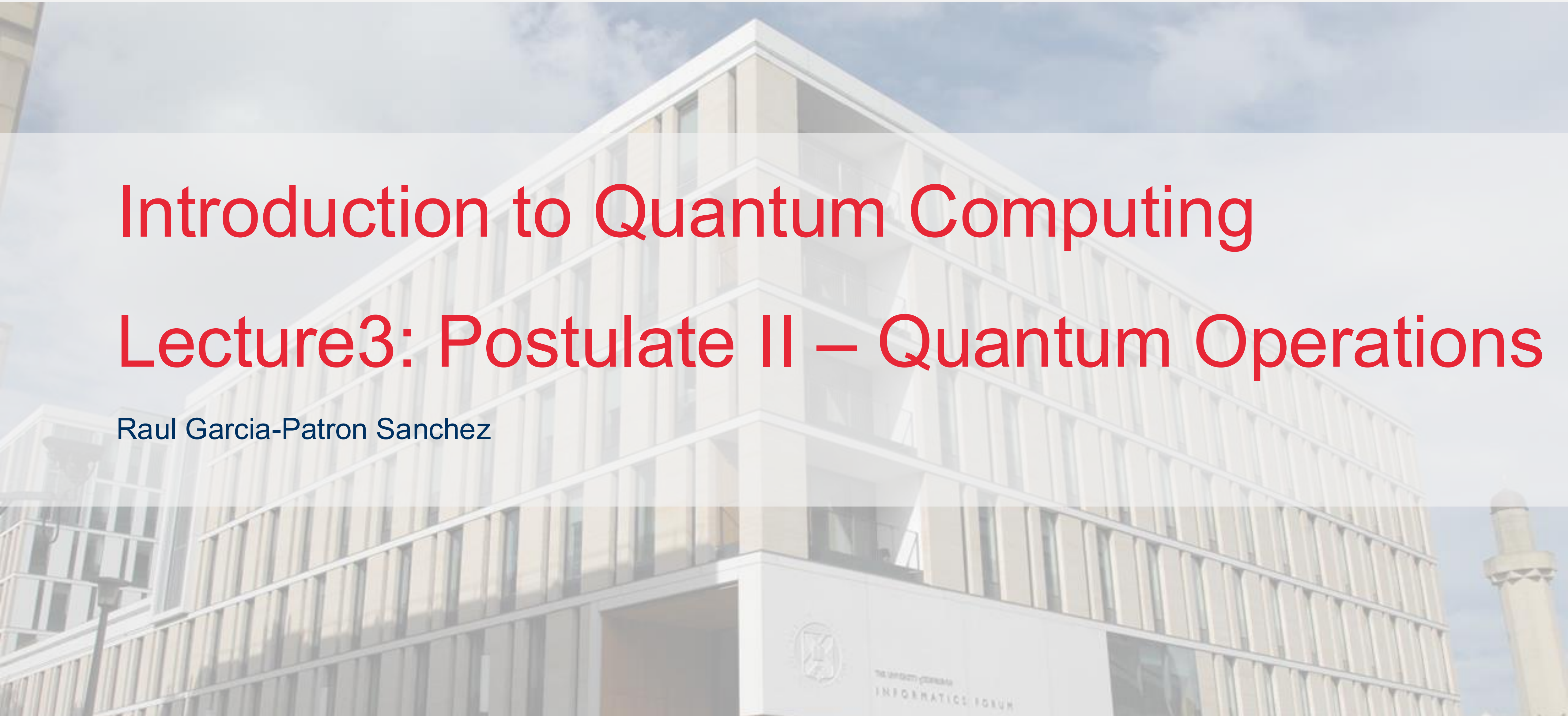
THE UNIVERSITY of EDINBURGH
informatics

Introduction to Quantum Computing

Lecture3: Postulate II – Quantum Operations

Raul Garcia-Patron Sanchez



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: $d = 2^N$

ψ_i : Probability amplitude of degree of freedom i $\qquad P(i) = |\psi_i|^2$

The ideal life of a qubit in a nutshell

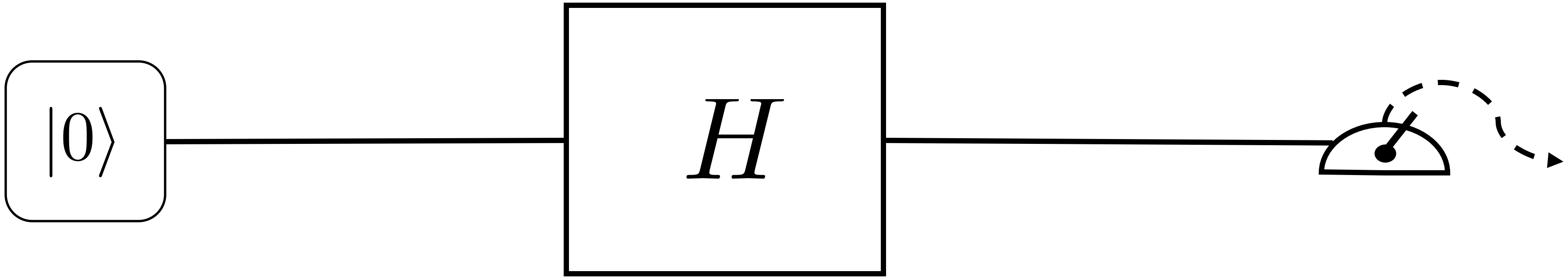
State preparation

Source of quantum states

Operation

Circuit/Gates

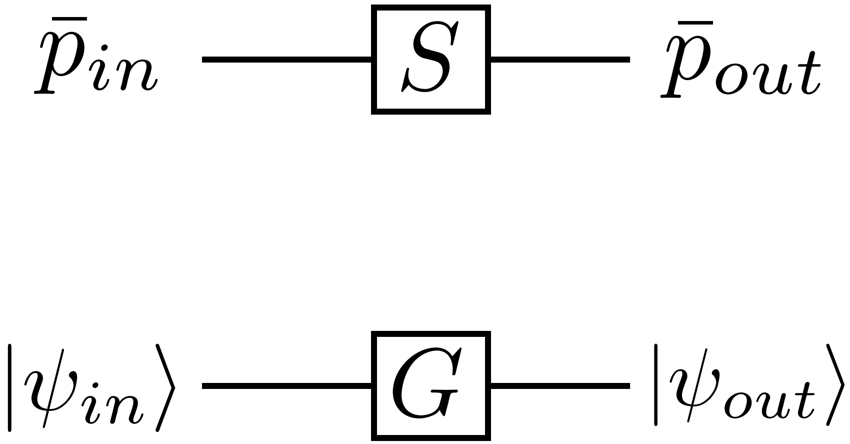
Measurement



Quantum random number generator circuit

Quantum operations: the intuition

- An operation maps an input state into an output state



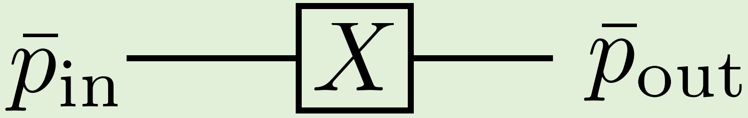
- If input and output are vectors, what is the transformation?

Matrices!!

NOT gate

$$\bar{p} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = p_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + p_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = p_0 \bar{v}_0 + p_1 \bar{v}_1$$

NOT gate



$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

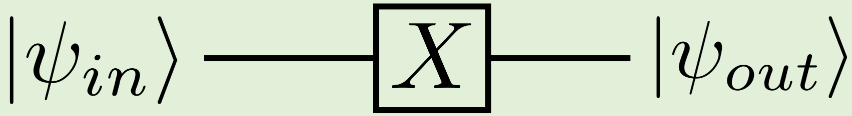
$$\bar{p}_{\text{out}} = X \bar{p}_{\text{in}}$$

$$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{\bar{v}_0} = \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{\bar{v}_1}$$

- Action on $\bar{v}_0 : X\bar{v}_0 = \bar{v}_1$

Example 1: Quantum NOT gate

NOT gate



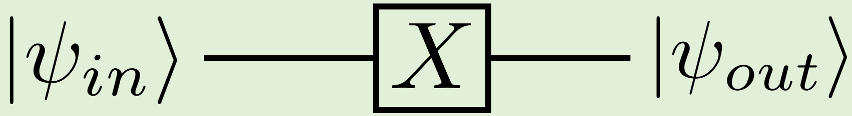
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Action on $|0\rangle$: $X|0\rangle = |1\rangle$

$$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{|0\rangle} = \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{|1\rangle}$$

Example 1: Quantum NOT gate

NOT gate



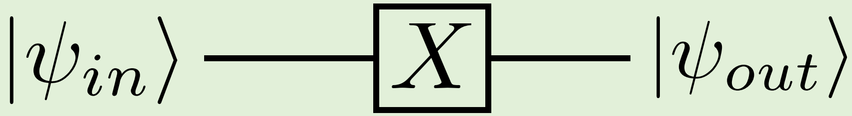
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Action on $|0\rangle : X|0\rangle = |1\rangle$
- Action on $|1\rangle : X|1\rangle = |0\rangle$

$$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{|0\rangle} = \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{|1\rangle}$$

Example 1: Quantum NOT gate

NOT gate



$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Action on $|0\rangle$: $X|0\rangle = |1\rangle$

$$\underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{X} \underbrace{\begin{bmatrix} 1 \\ 0 \end{bmatrix}}_{|0\rangle} = \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{|1\rangle}$$

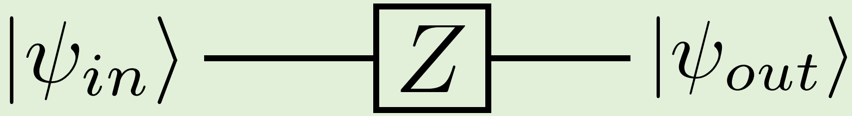
- Action on $|1\rangle$: $X|1\rangle = |0\rangle$

- Action on $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \beta|0\rangle + \alpha|1\rangle$$

Example 2: Z gate

Z gate



$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Action on $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$

Basis: General case

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

- Spanning set of $\mathcal{H}$: set of vectors $|v_1\rangle, |v_2\rangle, \ldots, |v_n\rangle$

  $\forall |\psi\rangle \in \mathcal{H} : |\psi\rangle = \sum_{i=1}^{n} \psi_{v_i} |v_i\rangle$ where amplitudes are given by: $\psi_{v_i} = \langle v_i|\psi\rangle$

- Linearly independent: $\nexists\, a_1, a_2, \ldots, a_n \neq 0$ complex numbers

  $a_1|v_1\rangle + \ldots + a_n|v_n\rangle = 0$

- Basis: $\text{Span}\{|v_i\rangle\} = \mathcal{H} \Leftrightarrow n = d$

  + Lin. ind.

- Orthonormal: $\forall i, j \in \{1, \ldots, d\}, \langle v_i|v_j\rangle = \delta_{i,j}$

- Has an associated measurement

Example

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Example 2: Z gate

Z gate

$$|\psi_{in}\rangle \text{ — } \boxed{Z} \text{ — } |\psi_{out}\rangle \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Action on $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$$

- Action on $|\pm\rangle$ basis: $Z|\pm\rangle = |\mp\rangle$

- Z gate is a "NOT gate" in the $|\pm\rangle$ basis!

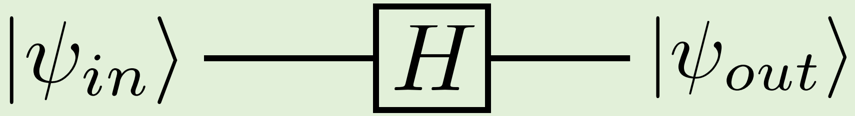
$|\pm\rangle$ basis:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Example 3: Hadamard Gate

Hadamard gate



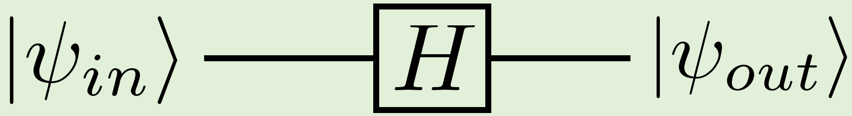
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Action on $|0\rangle : H|0\rangle = |+\rangle$
- Action on $|1\rangle : H|1\rangle = |-\rangle$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} (\alpha + \beta)/\sqrt{2} \\ (\alpha - \beta)/\sqrt{2} \end{bmatrix}$$

Example 3: Hadamard Gate

Hadamard gate



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

- Action on $|0\rangle$: $H|0\rangle = |+\rangle$
- Action on $|1\rangle$: $H|1\rangle = |1\rangle$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} (\alpha+\beta)/\sqrt{2} \\ (\alpha-\beta)/\sqrt{2} \end{bmatrix}$$

- Action on $|\pm\rangle$ basis: $H|+\rangle = |0\rangle$

$$H|-\rangle = |1\rangle$$

$|\pm\rangle$ basis:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Example 3: Hadamard Gate

Hadamard gate

$$|\psi_{in}\rangle \text{ —} \boxed{H} \text{— } |\psi_{out}\rangle \qquad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- Action on $|0\rangle$: $H|0\rangle = |+\rangle$
- Action on $|1\rangle$: $H|1\rangle = |1\rangle$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} (\alpha+\beta)/\sqrt{2} \\ (\alpha-\beta)/\sqrt{2} \end{bmatrix}$$

- Action on $|\pm\rangle$ basis: $H|+\rangle = |0\rangle$

  $H|-\rangle = |1\rangle$

- Hadamard gate is a change of basis: $|0/1\rangle \Leftrightarrow |\pm\rangle$

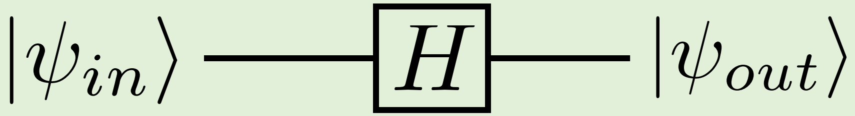
$|\pm\rangle$ basis:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

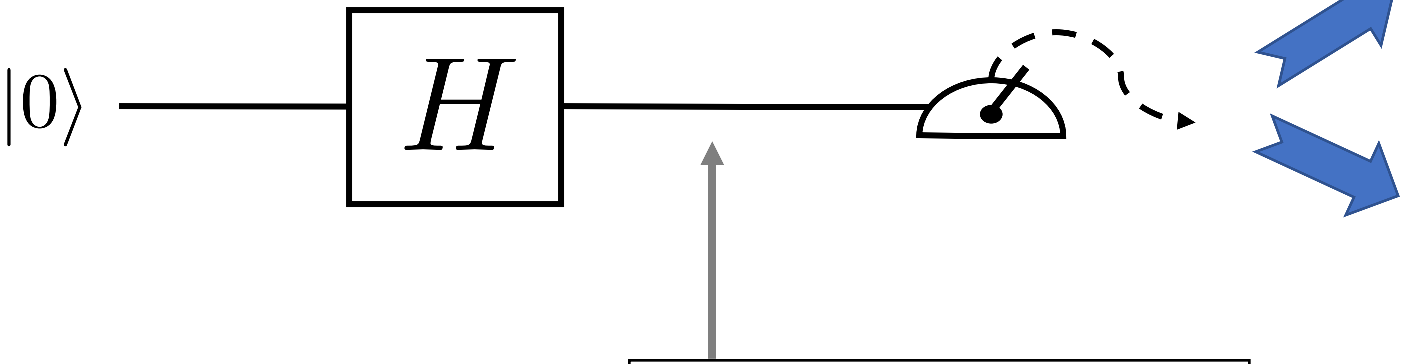
Quantum randomness generation

Hadamard gate



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

- Quantum random number generator circuit



$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$P(0) = |\psi_0|^2 = 1/2$$

$$P(1) = |\psi_1|^2 = 1/2$$

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

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

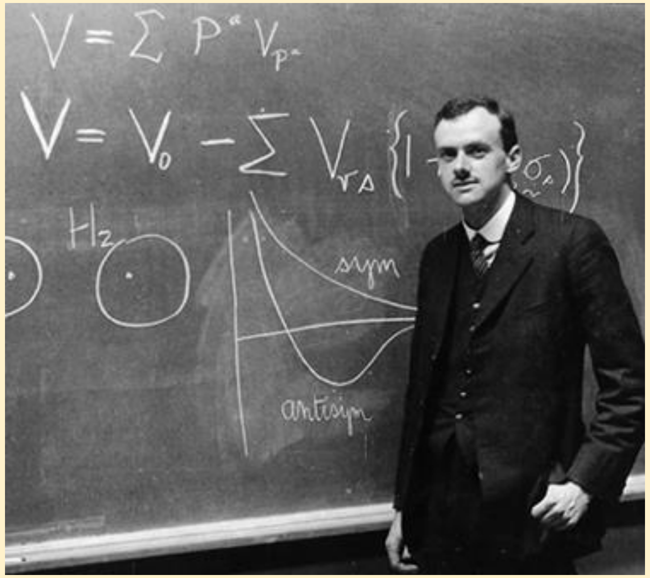
- Linear operator $U : \mathcal{H} \to \mathcal{H}$
- Preserves the inner-product
- Equivalent of orthogonal matrices on real vector spaces

Linearity

- $A \in \mathcal{L}(\mathcal{H}) : \mathcal{H} \rightarrow \mathcal{H}$ 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: $(BA)|\psi\rangle \equiv B(A|\psi\rangle)$
  - Not necessarily commuting: $BA|\psi\rangle \neq AB|\psi\rangle$
  - Matrix representation: $\langle i|A|j\rangle = A_{ij}$

Dirac notation Summary

Dirac notation



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

Bra $\langle\psi| \equiv \begin{bmatrix} \psi_0^* & \psi_1^* & \dots & \psi_{d-1}^* \end{bmatrix} : \mathcal{H} \to \mathbb{C}$

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

Outer-product:

Outer-products (Dirac notation)

$\|0\rangle\langle 0\| \equiv \begin{bmatrix}1\\0\end{bmatrix} \times \begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$	$\|0\rangle\langle 1\| \equiv \begin{bmatrix}1\\0\end{bmatrix} \times \begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}$
$\|1\rangle\langle 0\| \equiv \begin{bmatrix}0\\1\end{bmatrix} \times \begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}$	$\|1\rangle\langle 1\| \equiv \begin{bmatrix}0\\1\end{bmatrix} \times \begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$

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

Outer-products (Dirac notation)

$$\begin{bmatrix} a_{01} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} = a_{00} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{01} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{10} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{11} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Outer-products (Dirac notation)

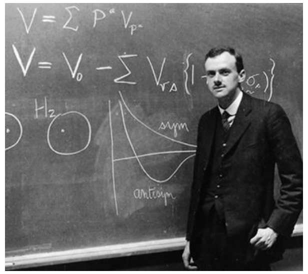
$$\begin{bmatrix} a_{01} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} = a_{00} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{01} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{10} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{11} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= a_{00}|0\rangle\langle 0| + a_{01}|0\rangle\langle 1| + a_{10}|1\rangle\langle 0| + a_{11}|1\rangle\langle 1|$$

$\lvert 0\rangle\langle 0\rvert \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$	$\lvert 0\rangle\langle 1\rvert \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$
$\lvert 1\rangle\langle 0\rvert \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$	$\lvert 1\rangle\langle 1\rvert \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Outer-product

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



Not gate $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$

Z gate $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$

Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1| \right]$

References

Reading references

1. Basis and linear independence NC 2.1.1
2. Linear operators and matrices NC 2.1.2
3. Single qubits gates NC 1.3.1 and NC 4.2

NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)