Mathematical Preliminaries of Quantum Computing

Jara Juana Bermejo-Vega
University de Granada

EM TCCM Master Course on
Advanced Computational Techniques
Barcelona, October 23rd – 27th, 2023

Foto: Erik Lucero/Google

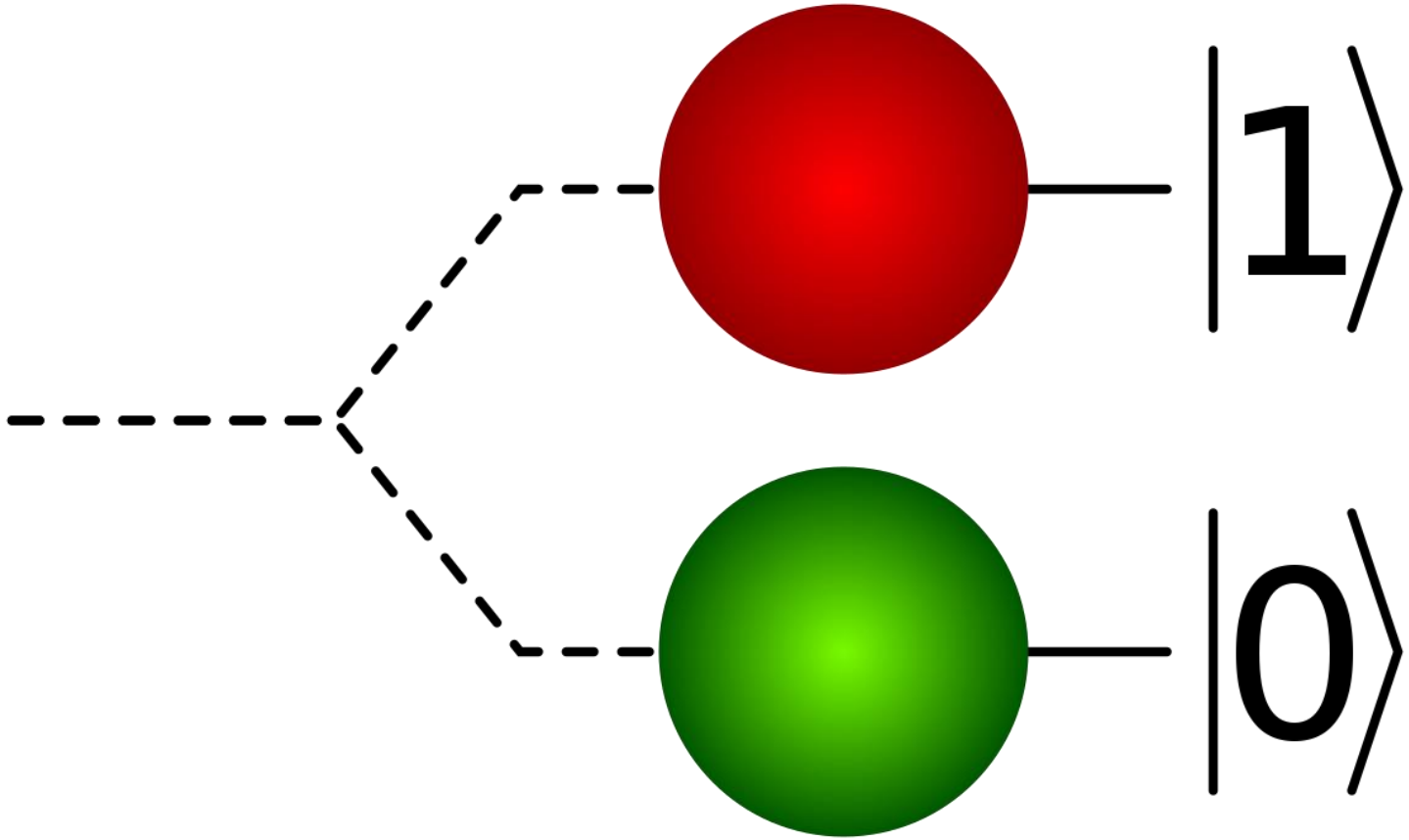
Outline

1. Quantum states
2. Quantum operations
3. Quantum measurement
4. Many-body Quantum Systems & Entanglement
5. Quantum circuits

Reference

IQC Introduction to Quantum Computing - Petros Wallden, Raul García Patrón, The University of Edinburgh Open Course Materials
https://opencourse.inf.ed.ac.uk/iqc/

Quantum States



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)

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

  - $p_i \geq 0$ (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

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

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

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

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

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

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

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

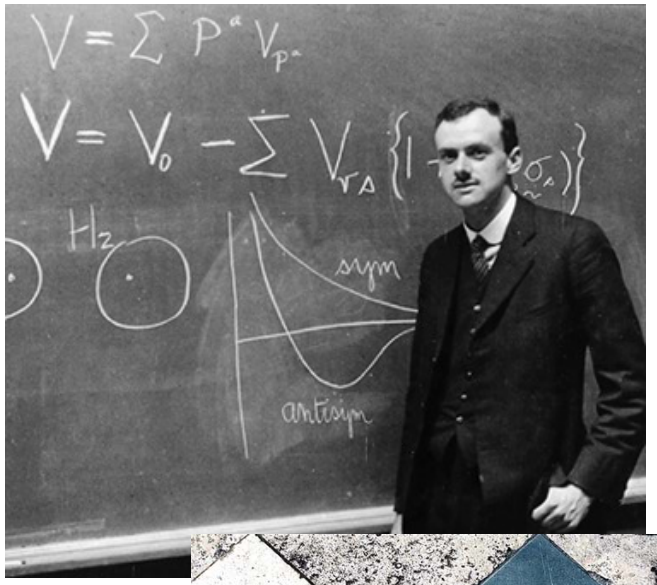
Linearity of QM allows us to write any qubit state a a linear combination of logical 0 or 1, as they are a basis for the qubit state space.

Dirac Notation

Dirac notation

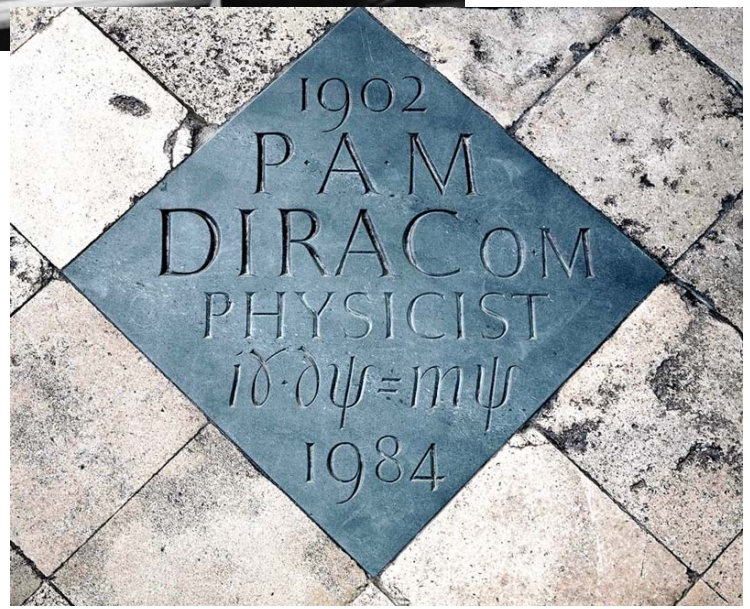
$|\psi\rangle$ ket

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



Paul Dirac: Nobel Prize 1933
Fundamental contributions to:

- quantum mechanics
- quantum electrodynamics



Westminster Abbey (London)

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 $|\psi\rangle \equiv \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{d-1} \end{bmatrix}$ A d-dimensional vector of complex numbers

ψ_i : Probability amplitude of degree of freedom i

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

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

Inner-product in a nutshell

- $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$

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

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

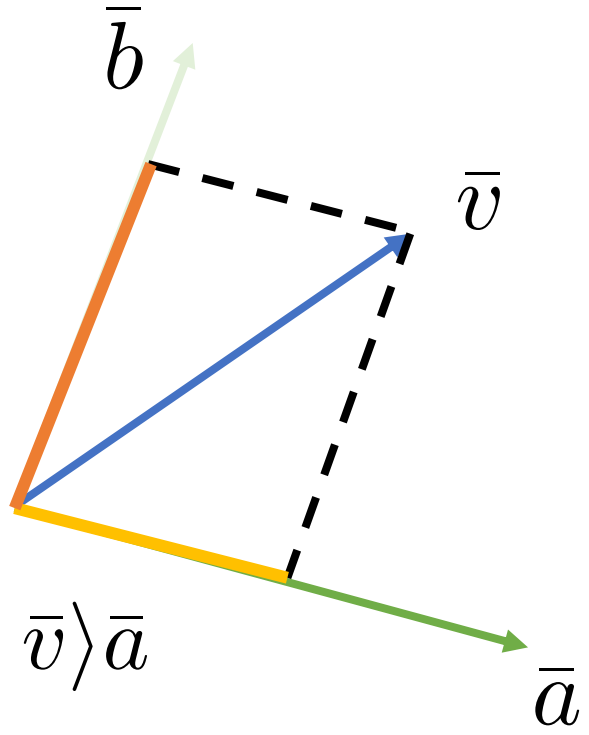
$\langle \bar{a}, \bar{a} \rangle = \langle \bar{b}, \bar{b} \rangle = 1$

$\langle \bar{a}, \bar{b} \rangle = 0$

$$\bar{v} = \langle \bar{a}, \bar{v} \rangle \bar{a} + \langle \bar{b}, \bar{v} \rangle \bar{b}$$

P_x is projector on subspace span by $\bar{x}$

$$P_b \bar{v} = \langle \bar{b}, \bar{v} \rangle \bar{b}$$



$$P_a \bar{v} = \langle \bar{a}, \bar{v} \rangle \bar{a}$$

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

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.)

Hilbert Space: Inner-product (Dirac Notation)

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

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

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

Bra

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

Ket

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

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

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

Basis: Computational basis

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

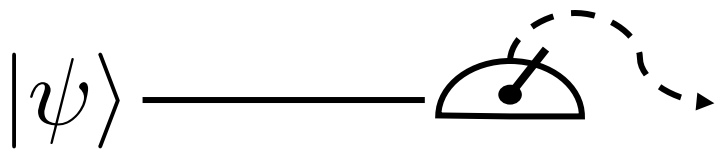
Computational basis

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

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

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

Computational basis measurement



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

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

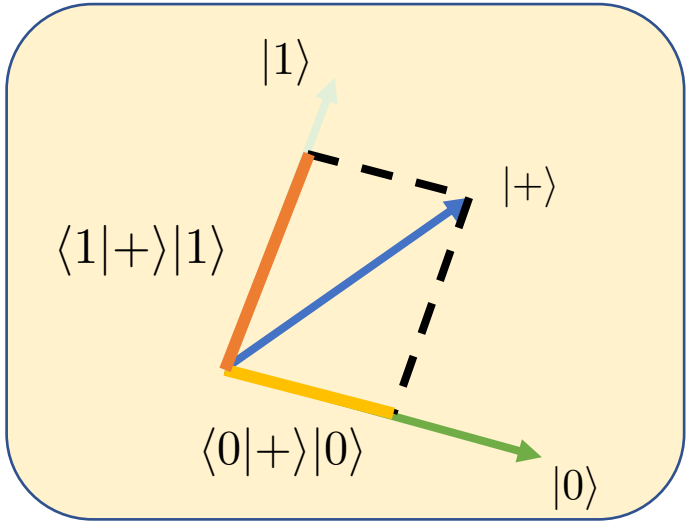
The amplitudes of the quantum state on the logical basis (0 and 1) are associated with the outcome probabilities of the computational basis measurement (logical 0 or 1).

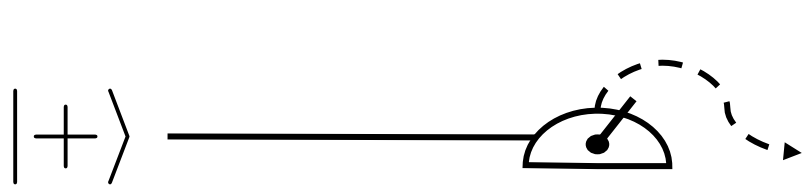
Quantum randomness generation

Computational basis measurement

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

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





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

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

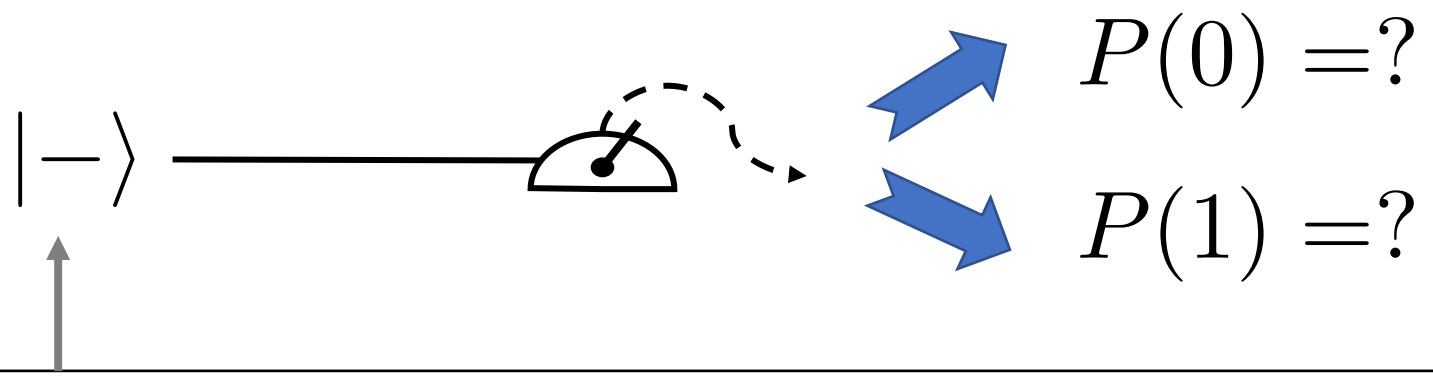
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

Quantum randomness generation

Computational basis measurement

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

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



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

Quantum randomness generation

Computational basis measurement

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

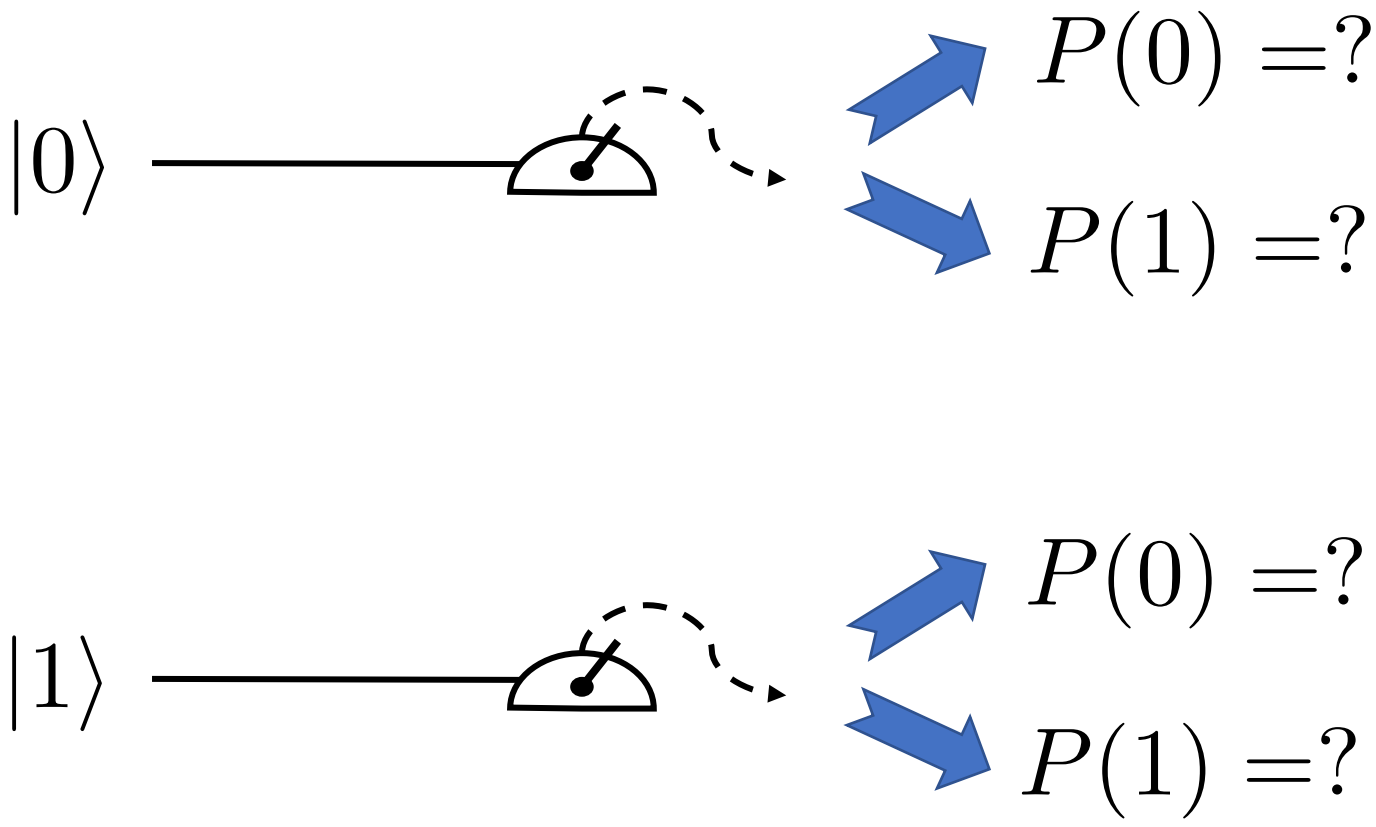
$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$

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

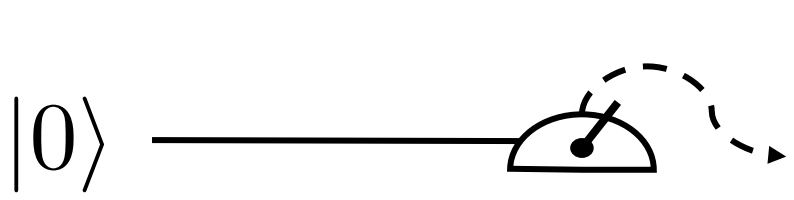
$$P(1) = |\langle 1|-\rangle|^2 = 1/2$$

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

Quantum randomness generation

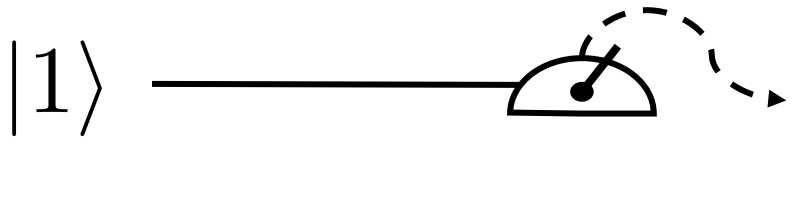


Quantum randomness generation



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

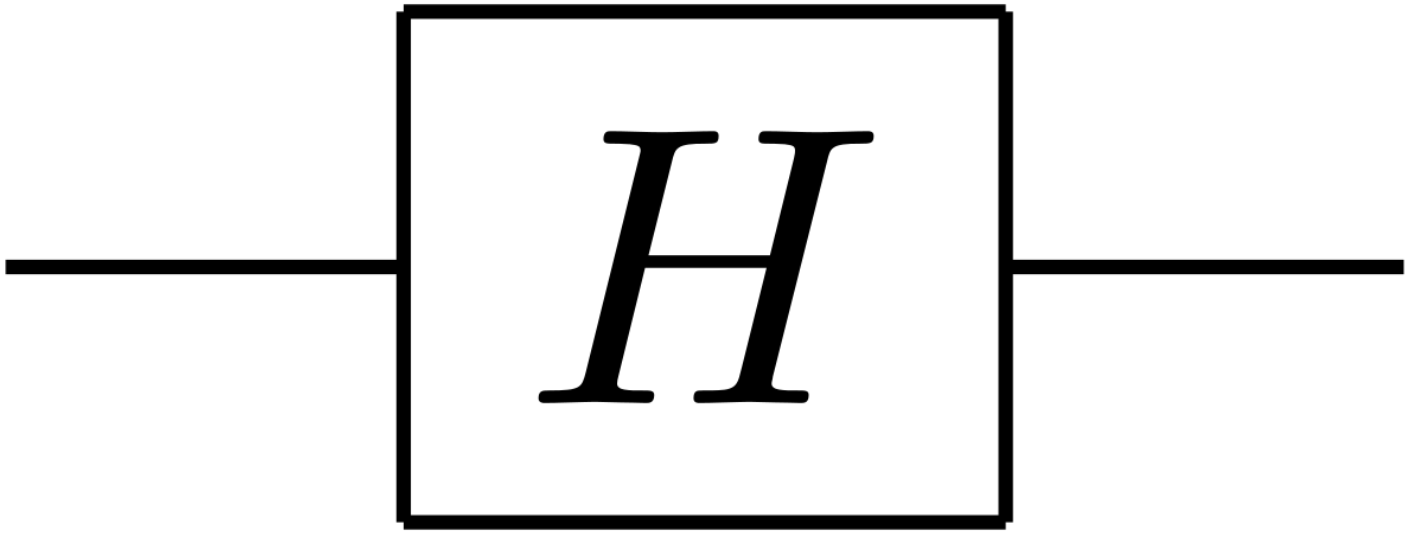
$$P(1) = |\langle 1|0\rangle|^2 = 0$$



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

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

Quantum Operations



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

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

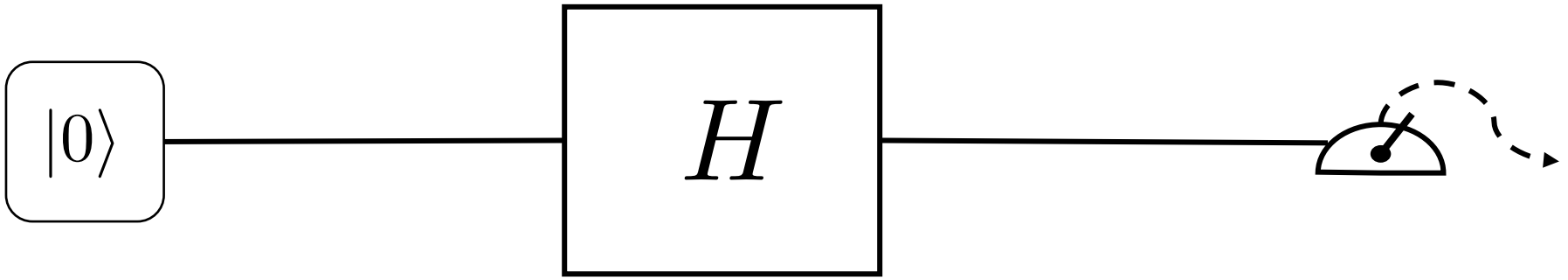
State preparation

Source of quantum states

Operation

Circuit/Gates

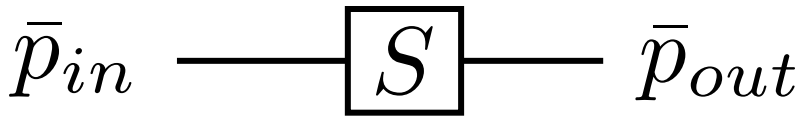
Measurement



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

$\bar{p}_{\text{in}}$ — $[X]$ — $\bar{p}_{\text{out}}$

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

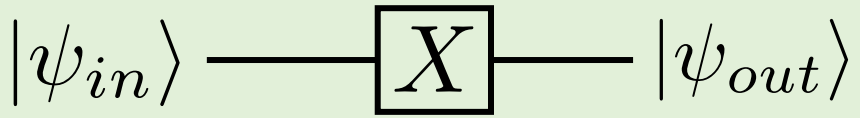
$$\bar{p}_{\text{out}} = X \bar{p}_{\text{in}}$$

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

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

Example 1: Quantum NOT gate

NOT gate



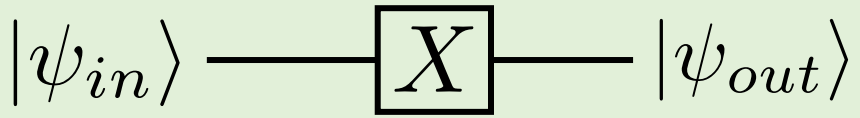
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- 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



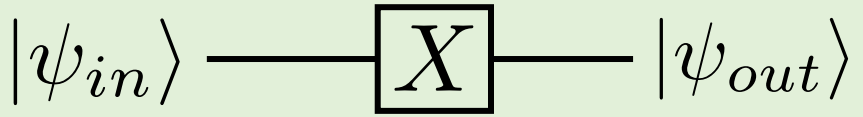
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- 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 $|v_1\rangle, |v_2\rangle, ..., |v_n\rangle$

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

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

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

- Basis: $\text{Span}\{|v_i\rangle\} = \mathcal{H} \Leftrightarrow n = d$
  + Lin. ind.
- Orthonormal: $\forall i, j \in \{1, ..., d\}\,, \langle v_i | v_j \rangle = \delta_{i,j}$
- Has an associated measurement

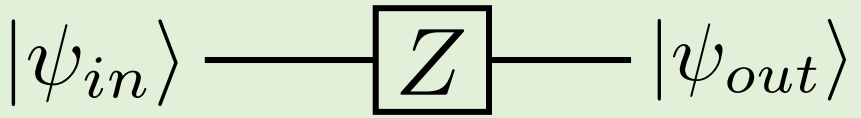
Example

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

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

Example 2: Z gate

Z gate



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

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

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

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

- 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

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

- 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: $|0/1\rangle \Leftrightarrow |\pm\rangle$

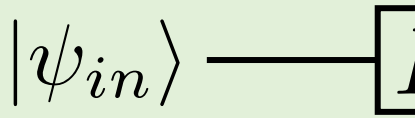
$|\pm\rangle$ basis:

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

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

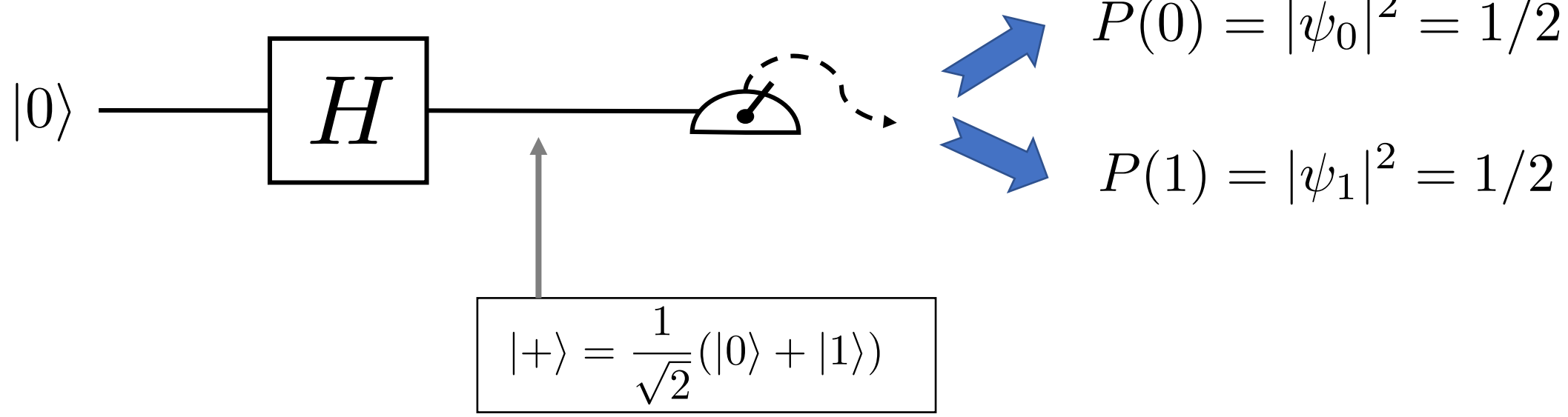
Quantum randomness generation

Hadamard gate



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

- Quantum random number generator circuit



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

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

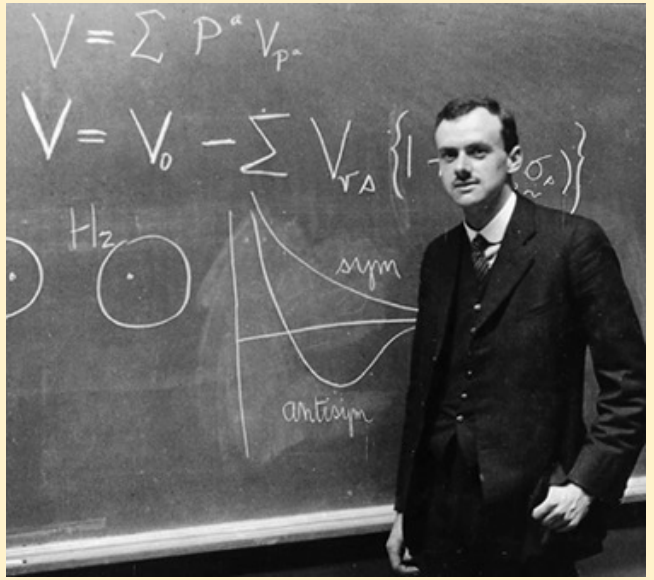
- Linear operator $U : \mathcal{H} \to \mathcal{H}$
- Preserves the inner-product
- Equivalent of orthogonal matrices on real vector spaces

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

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)

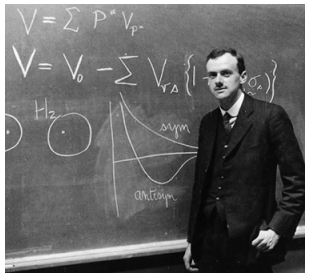
$$\begin{bmatrix} a_{01} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} = a_{00}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{01}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{10}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{11}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

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

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

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

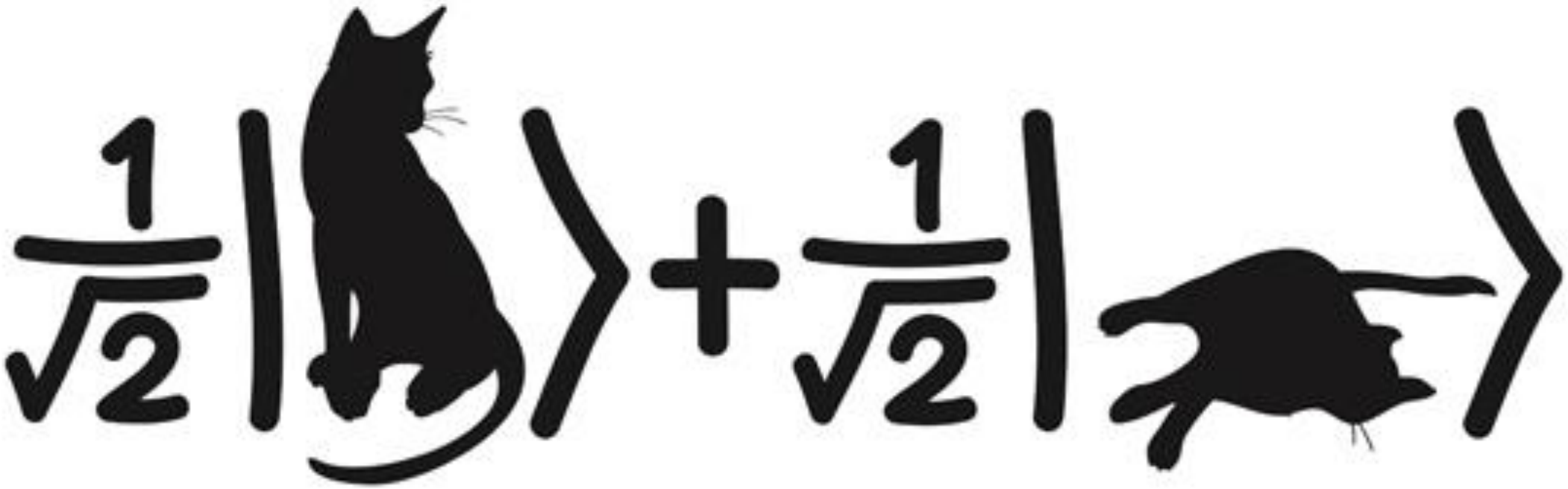
References

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)

Quantum Measurements

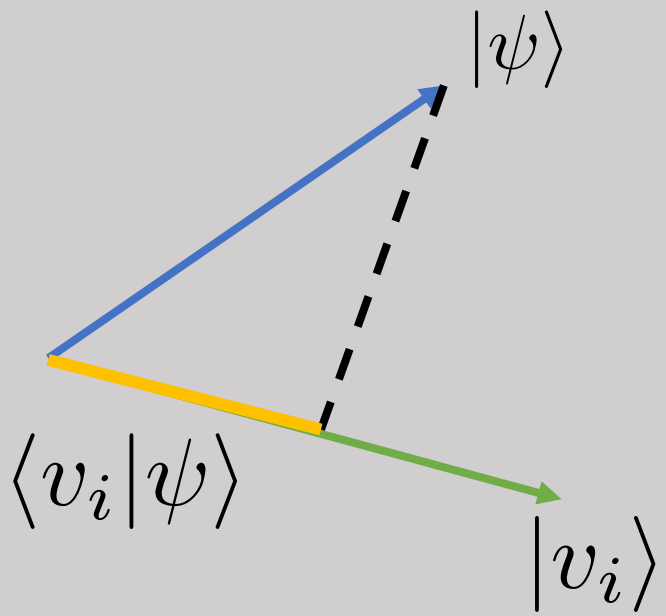


Measurement of orthonormal basis

Any orthonormal basis $\{|v_i\rangle\}$ that span $\mathcal{H}$ has and associated measurement

Probability of outcome i reads: $P(i) = |\langle v_i|\psi\rangle|^2$

The quantum state is updated to $|v_i\rangle$



Basis: Computational basis

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

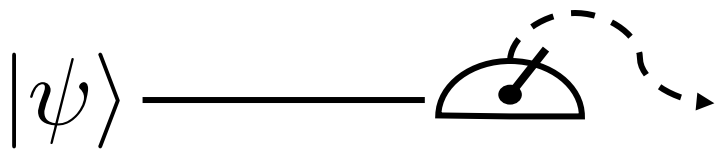
Computational basis

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

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

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

Computational basis measurement



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

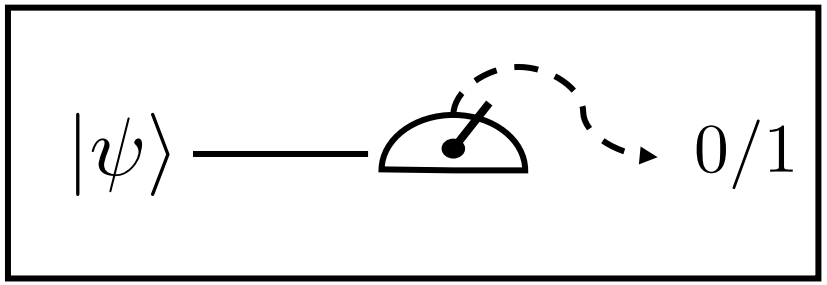
$$P(1) = |\langle 1|\psi\rangle|^2 = |\psi_1|^2$$

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).

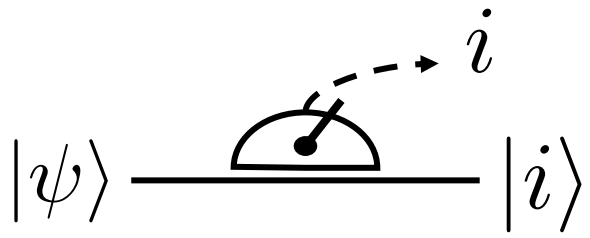
Classical register vs non-demolition measurement

The quantum state is updated to $|v_i\rangle$

- Many times we just care about the outcome. Encoded in a classical register.

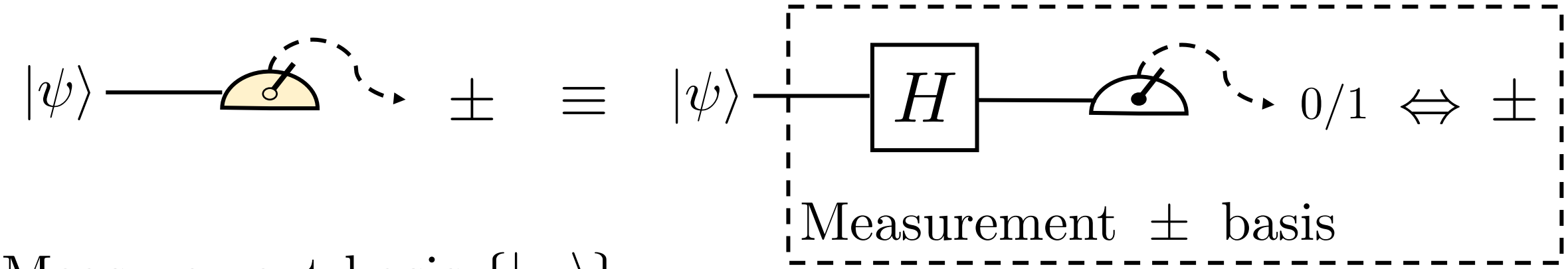


- Non-demolition measurement:

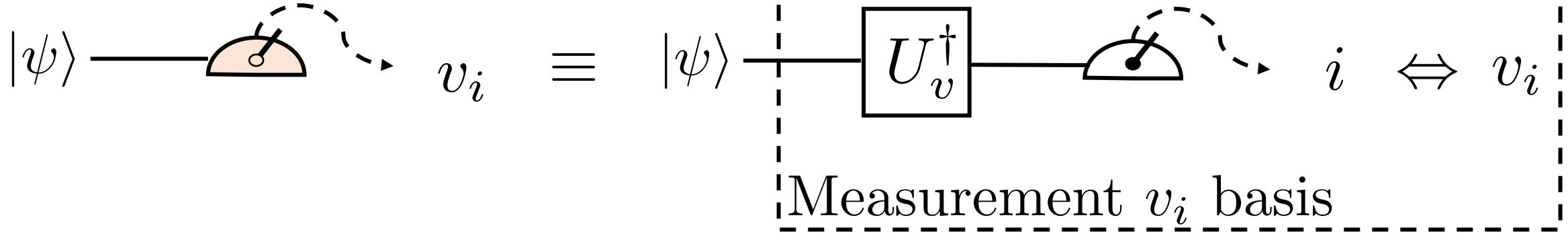


Arbitrary basis measurement

- Measurement basis $\{|\pm\rangle\}$:



- Measurement basis $\{|v_i\rangle\}$:



$\forall$ basis $\{|v_i\rangle\}, \exists U_v$ s.t. $|v_i\rangle = U_v|i\rangle$ $\quad\quad$ $\langle v_i|\psi\rangle = \langle i|U_v^\dagger|\psi\rangle$

Projectors

$$P_{\mathcal{S}}^2 = P_{\mathcal{S}} = P_{\mathcal{S}}^\dagger$$

$$P_{\mathcal{S}} = \sum_{i=0}^{k-1} |u_i\rangle\langle u_i|$$

Projector on vector subspace $\mathcal{S}$ of dim k $(\mathcal{S} \subset \mathcal{H})$

Being a vector space, $\mathcal{S}$ has an orthonormal basis $\{|u_i\}_{i=0}^{k-1}$

Projectors on computational basis

- Projector on computational basis state $|x\rangle\langle x|$
  - $|0\rangle\langle 0| \equiv \begin{bmatrix}1\\0\end{bmatrix} \times \begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$
  - $|1\rangle\langle 1| \equiv \begin{bmatrix}0\\1\end{bmatrix} \times \begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$
- $(|x\rangle\langle x|)|\psi\rangle = |x\rangle \underbrace{\langle x|\psi\rangle}_{\in\mathbb{C}} = \langle x|\psi\rangle|x\rangle = \psi_x|x\rangle$

Projective measurement

A projective measurement consist of a set of projectors P_i

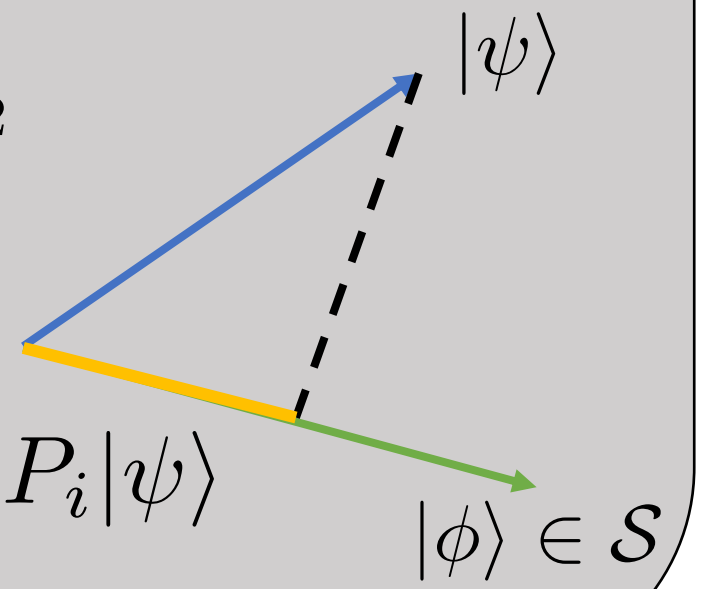
Satisfying a completeness relation: $\sum_{i=0}^{l} P_i = I_d$

Satisfy orthogonal relation: $P_m P_n = \delta_{n,m} P_m$

Probability of outcome i reads: $P(i) = ||P_i|\psi\rangle||^2$

The quantum state is updated to

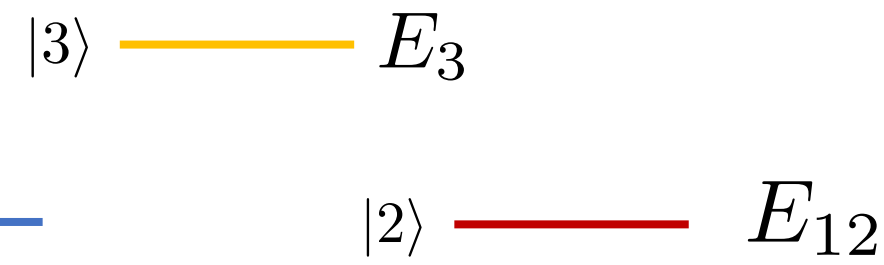
$$\frac{P_i|\psi\rangle}{||P_i|\psi\rangle||}$$

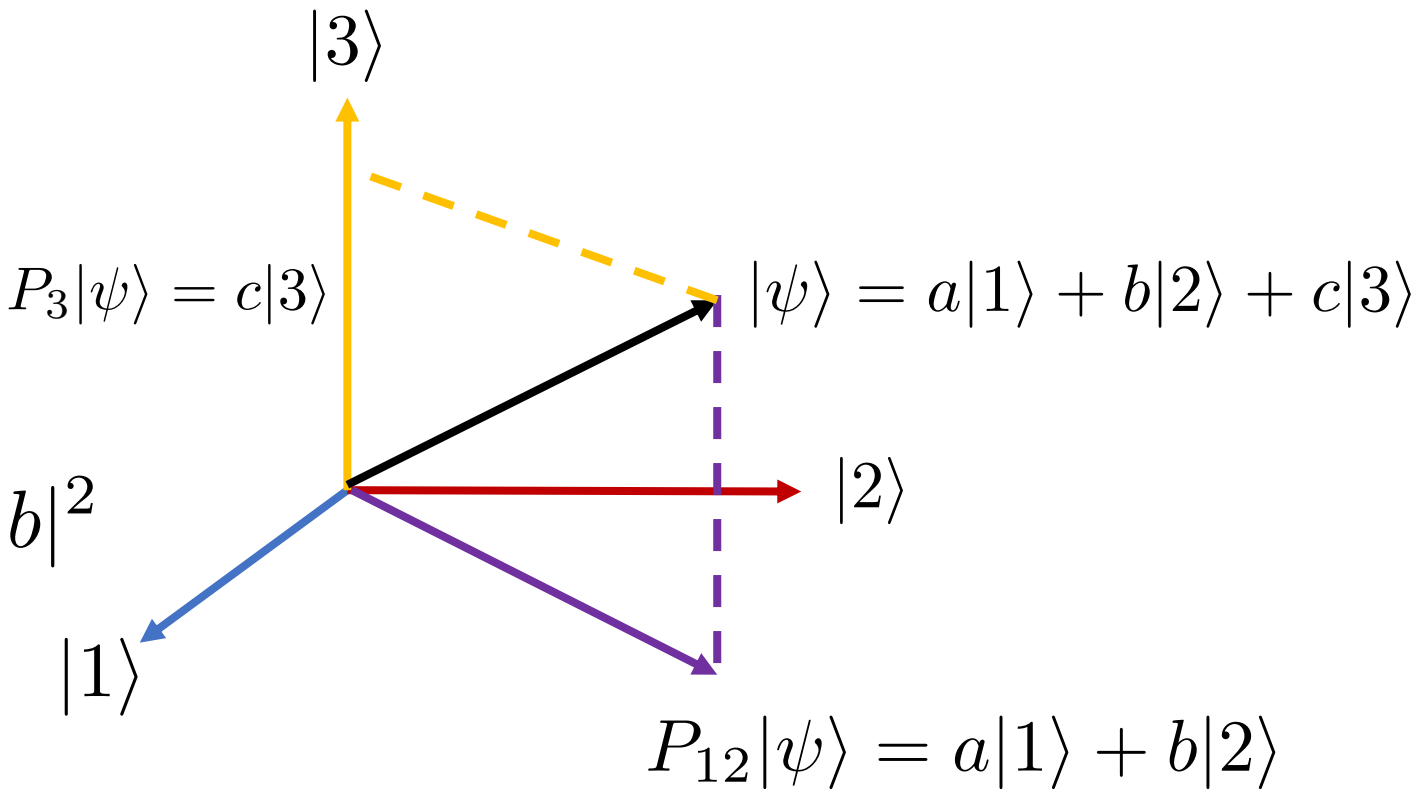


A degenerate 3 dimensional quantum system

- Orthonormal basis:
- Completeness:
  - $P_3 + P_{12} = I$
  - $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Rank 2 projector





- $P(12) = ||P_{12}|\psi\rangle||^2 = |a|^2 + |b|^2$

Update: $|\psi'\rangle = \frac{1}{\sqrt{|a|^2 + |b|^2}}(a|1\rangle + b|2\rangle)$

Projective measurement

Completeness relation

$$\sum_{i=0}^{l} P_l = I_d$$

Completeness implies probabilities add to 1:

$$\begin{aligned}\sum_i P(i) &= \sum_i ||P_i|\psi\rangle||^2 \\ &= \sum_i \langle\psi|P_i^\dagger P_i|\psi\rangle = \langle\psi|\sum_i P_i^\dagger P_i|\psi\rangle \\ &= \langle\psi|\sum_i P_i|\psi\rangle = \langle\psi|\psi\rangle = 1\end{aligned}$$

We use:

- $P(i) = ||P_i|\psi\rangle||^2$
- Linearity
- $P_{\mathcal{S}}^2 = P_{\mathcal{S}} = P_{\mathcal{S}}^\dagger$

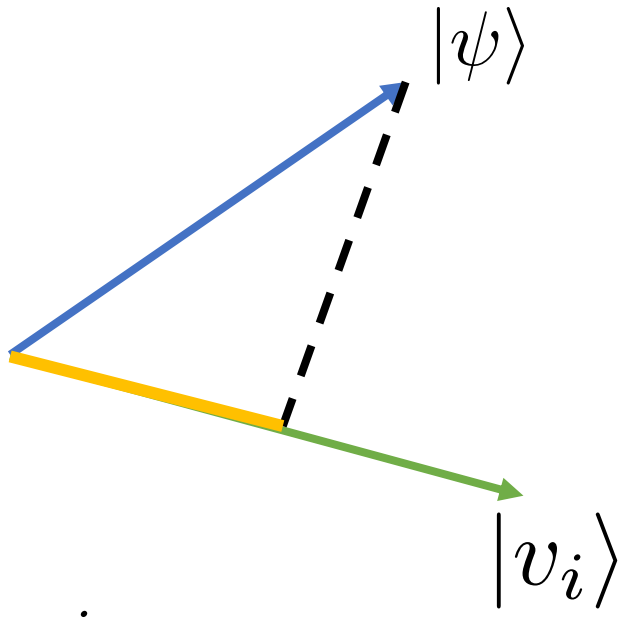
Reproducibility of measurement + Global phase

- *Repeating the same measurement immediately after, gives the same answer.*

$$P_i^2 = P_i$$

$$P_i|v_i\rangle = |v_i\rangle\langle v_i|v_i\rangle = |v_i\rangle$$

$$P_j|v_i\rangle = |v_j\rangle\langle v_j|v_i\rangle = 0 \text{ if } i \neq j$$



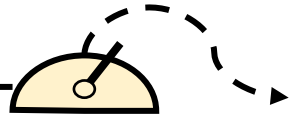
- Define a state up to a global phase: $|\tilde{\psi}\rangle \equiv e^{i\varphi}|\psi\rangle$

Output probability: $P(i) = ||P_i|\tilde{\psi}\rangle||^2 = |e^{i\varphi}\langle v_i|\psi\rangle|^2 = |\langle v_i|\psi\rangle|^2$

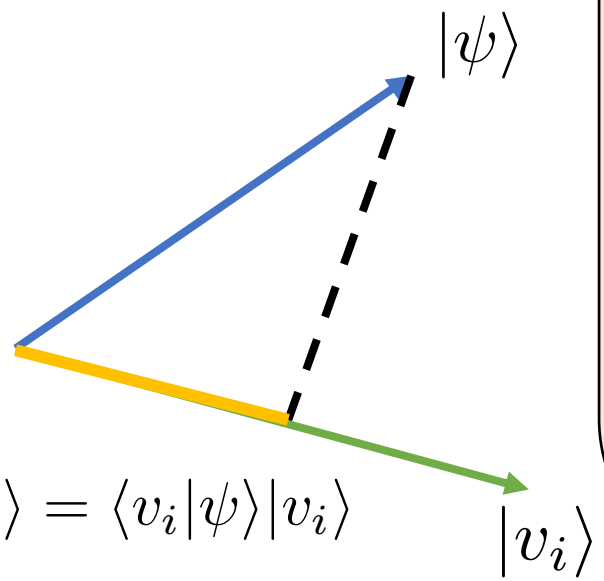
Example:+/- basis

$\mathcal{H}_Q = \text{Span}\{|+\rangle, |-\rangle\}$

- Completeness: $|+\rangle\langle+| + |-\rangle\langle-| \equiv \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix} + \frac{1}{2}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \equiv I_2$

- $|\psi\rangle$ 

$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$



$P(-) = ||P_{|-\rangle}|\psi\rangle||^2$ Updated state: $\frac{P_{|-\rangle}|\psi\rangle}{||P_{|-\rangle}|\psi\rangle||}$

$P_{|-\rangle} = |-\rangle\langle-| \equiv \begin{bmatrix}1/\sqrt{2}\\ -1/\sqrt{2}\end{bmatrix} \times \begin{bmatrix}1/\sqrt{2} & -1/\sqrt{2}\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}$

$P_{|-\rangle}|\psi\rangle = \frac{1}{2}\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}\begin{bmatrix}\psi_0\\ \psi_1\end{bmatrix} = \frac{\psi_0 - \psi_1}{\sqrt{2}}\begin{bmatrix}1/\sqrt{2}\\ -1/\sqrt{2}\end{bmatrix} = \frac{\psi_0 - \psi_1}{\sqrt{2}}|-\rangle$

$P(-) = |\psi_0 - \psi_1|^2/2$ Updated state: $|-\rangle$

Measurement of orthonormal basis

Any orthonormal basis $\{|v_i\rangle\}$ that span $\mathcal{H}$ has and associated measurement

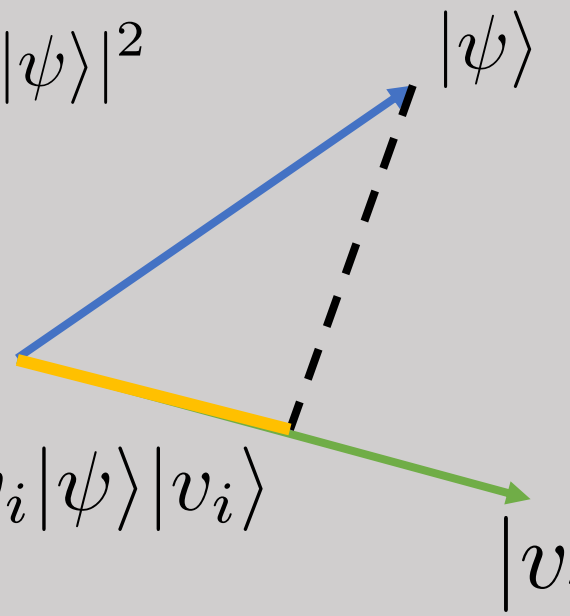
Satisfying a completeness relation: $\sum_{i=0}^{d-1} |v_i\rangle\langle v_i| = I_d$

$P_i = |v_i\rangle\langle v_i|$ are projectors on the states of the basis

Probability of outcome i reads: $P(i) = ||P_i|\psi\rangle||^2 = |\langle v_i|\psi\rangle|^2$

The quantum state is updated to

$$\frac{P_i|\psi\rangle}{||P_i|\psi\rangle||} = \frac{\langle v_i|\psi\rangle}{||P_i|\psi\rangle||}|v_i\rangle = e^{i\phi}|v_i\rangle$$



References

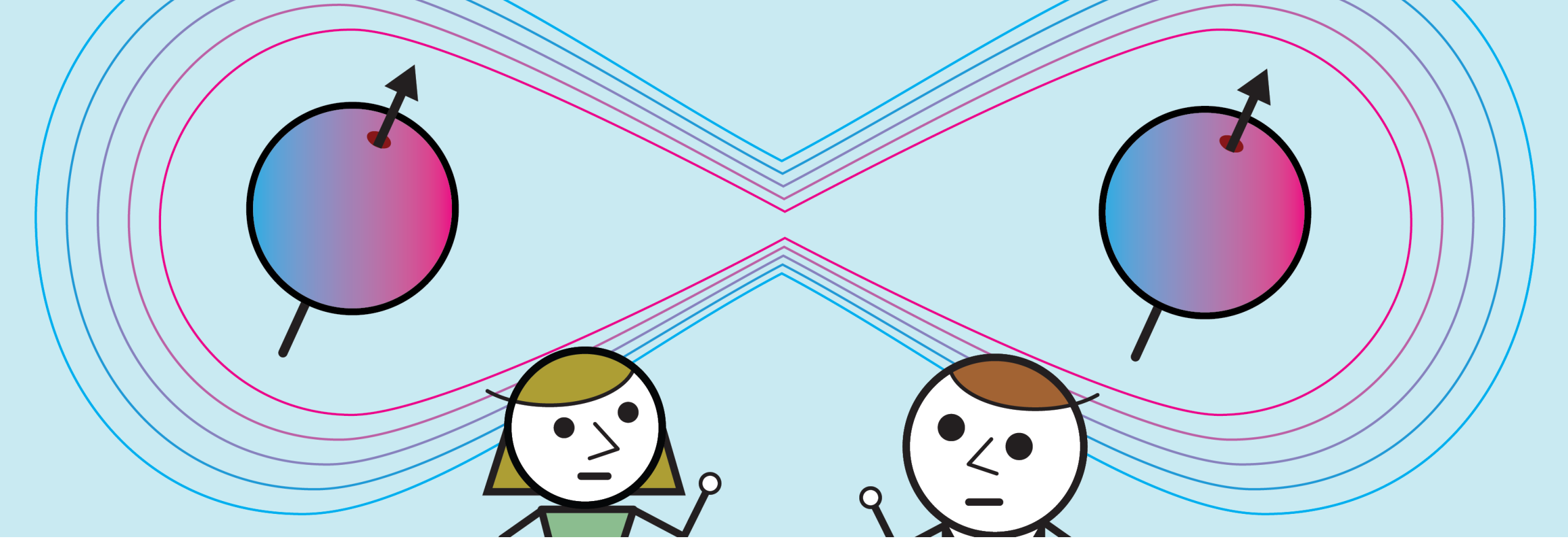
Reading references

1. NC 2.2.3 and 2.2.5

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

There is even a more general concept of measurement in N&C called POVM (2.2.6) that we will not cover in this course.

Even more general is the concept of quantum instrument.



Many-body Quantum Systems & Entanglement

Composition of classical systems

- Two independent perfect coins: $p_{AB}(a,b) = p_A(a)p_B(b)$

$p(0,1)$

A\B	0	1	
0	1/4	1/4	1/2
1	1/4	1/4	1/2
	1/2	1/2	1

$p(a)$

$p(b)$

- Composition of independent coins:

$$\bar{u} \in \mathcal{C}_A, \bar{v} \in \mathcal{C}_B \text{ leads to } \bar{u} \otimes \bar{v} \in \mathcal{C}_A \otimes \mathcal{C}_B$$

$$\text{Vector notation: } \bar{u} \otimes \bar{v} \equiv \begin{bmatrix} u_0 \\ u_1 \end{bmatrix} \otimes \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} = \begin{bmatrix} u_0 v_0 \\ u_0 v_1 \\ u_1 v_0 \\ u_1 v_1 \end{bmatrix} = \begin{bmatrix} p_{00} \\ p_{01} \\ p_{10} \\ p_{11} \end{bmatrix}$$

Composition of quantum systems

Two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ can form a new Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ s.t. $\dim\mathcal{H}_{AB} = \dim\mathcal{H}_A \times \dim\mathcal{H}_B$.

A basis of $\mathcal{H}_{AB}$ is built via tensor product of basis of $\mathcal{H}_A$ and $\mathcal{H}_B$.

An operator $\mathcal{L}(\mathcal{H}_{AB})$ is built via tensor product of operators $\mathcal{L}(\mathcal{H}_A)$ and $\mathcal{L}(\mathcal{H}_B)$.

Tensor product of vectors/states

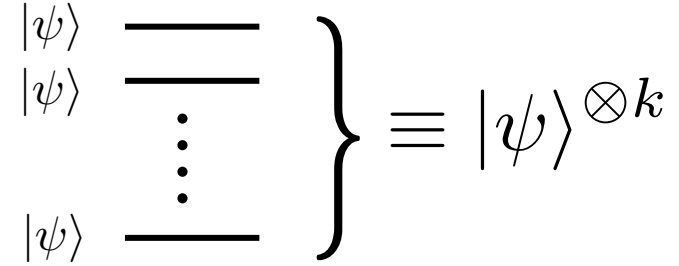
- Tensor product of vectors: $\mathcal{H}_A \times \mathcal{H}_B \rightarrow \mathcal{H}_{A,B} = \mathcal{H}_A \otimes \mathcal{H}_B$
  - $|u\rangle \in \mathcal{H}_A, |v\rangle \in \mathcal{H}_A$ leads to $|u\rangle \otimes |v\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$
  - $c(|u\rangle \otimes |v\rangle) = (c|u\rangle) \otimes |v\rangle = |u\rangle \otimes (c|v\rangle)$
  - $|u\rangle \otimes (|v_1\rangle + |v_2\rangle) = |u\rangle \otimes |v_1\rangle + |u\rangle \otimes |v_2\rangle$

$$|+\rangle \otimes |+\rangle = (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes (\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

  - Vector notation: $|u\rangle \otimes |v\rangle \equiv \begin{bmatrix} u_0 \\ u_1 \end{bmatrix} \otimes \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} = \begin{bmatrix} u_0 v_0 \\ u_0 v_1 \\ u_1 v_0 \\ u_1 v_1 \end{bmatrix} = \begin{bmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{10} \\ \psi_{11} \end{bmatrix}$

Tensor product of vectors/states

- Inner-product: $\mathcal{H}_A \otimes \mathcal{H}_B \times \mathcal{H}_A \otimes \mathcal{H}_B \to \mathbb{C}$
  - $(|v\rangle_A \otimes |w\rangle_B, |v'\rangle_A \otimes |w'\rangle_B) = \langle v|v'\rangle_A \langle w|w'\rangle_B$
  - $(\sum_i a_i |v_i\rangle_A \otimes |w_i\rangle_B, \sum_j b_j |v'_j\rangle_A \otimes |w'_j\rangle_B) = \sum_{i,j} a_i^* b_j \langle v_i|v'_j\rangle_A \langle w_i|w'_j\rangle_B$
- Additional notation:
  - $|\psi\rangle^{\otimes k} = \underbrace{|\psi\rangle \otimes |\psi\rangle \otimes ... \otimes |\psi\rangle}_{k}$
  - $|0^k\rangle = |0\rangle^{\otimes k} = |0\rangle \otimes |0\rangle \otimes ... \otimes |0\rangle$



Entanglement

- $\exists |\psi_{AB}\rangle \in \mathcal{H}_{AB}$ s.t. $\nexists |\phi_A\rangle \in \mathcal{H}_A$ and $|\varphi_B\rangle \in \mathcal{H}_B : |\psi_{AB}\rangle = |\phi_A\rangle \otimes |\varphi_B\rangle$

Bell states: a basis of $\mathcal{H}_Q \otimes \mathcal{H}_Q$ composed of entangled states.

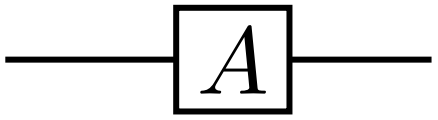
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \qquad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

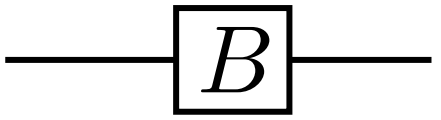
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

- Maximally entangled states of 2 qubits.
- Bell states are entanglement units. Similarly as an unbiased coins is a unit of randomness.

- $\forall |\psi_{AB}\rangle \in \mathcal{H}_{AB} : |\psi_{AB}\rangle = \sum_{i,j} \psi_{i,j} |i\rangle \otimes |j\rangle$

Tensor product of operators

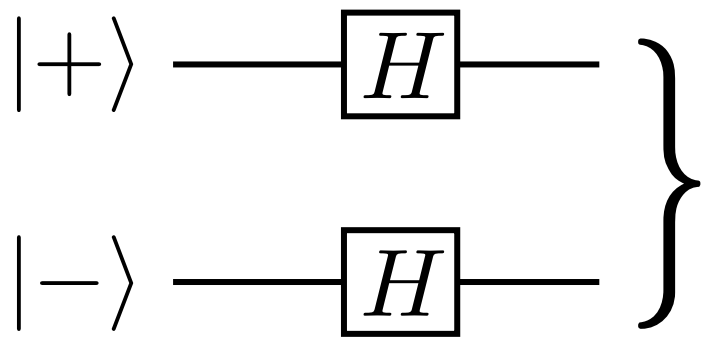




Tensor product of operators

- Tensor product of operators: $\mathcal{L}(\mathcal{H}_A) \times \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_{AB}) = \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$
  - $(A \otimes B)(|v\rangle \otimes |w\rangle) = (A|v\rangle) \otimes (B|w\rangle) = A|v\rangle \otimes B|w\rangle$
  - $(A \otimes B)(\sum_i a_i |v_i\rangle \otimes |w_i\rangle) = \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle$
  - $(\sum_i c_i A_i \otimes B_i)|v\rangle \otimes |w\rangle = \sum_i c_i A_i|v\rangle \otimes B_i|w\rangle$
  - Matrix notation: $A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{n1}B & A_{n2}B & \dots & A_{nn}B \end{bmatrix}$

Example (Dirac notation)



$|\pm\rangle$ basis:

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

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

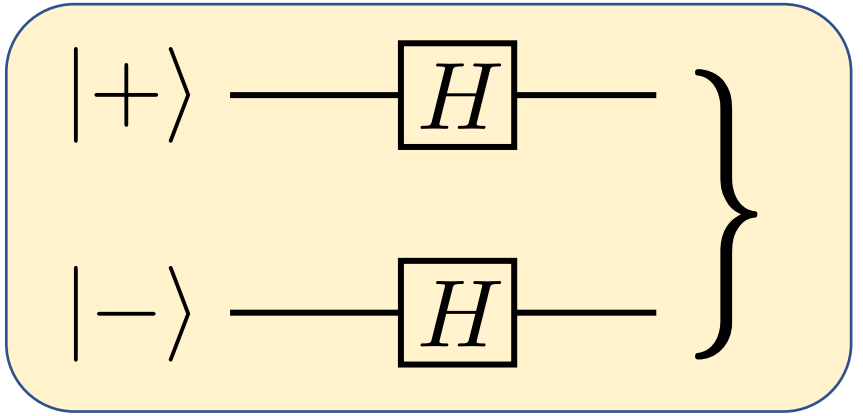
$$(H \otimes H)(|+\rangle \otimes |-\rangle) = (H|+\rangle) \otimes (H|-\rangle)$$

$$= |0\rangle \otimes |1\rangle$$

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

Example (matrix notation)

- $|+\rangle \otimes |-\rangle \equiv \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \otimes \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$

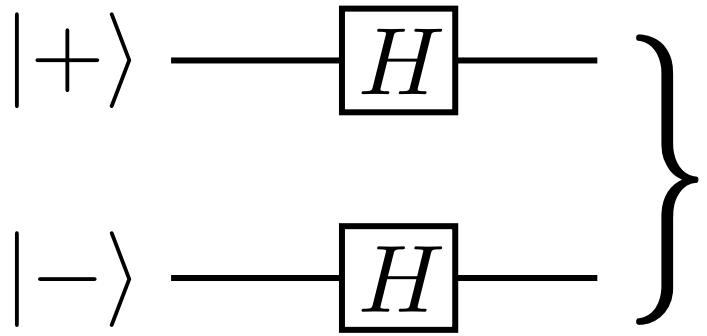


- $H \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} H & H \\ H & -H \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{n1}B & A_{n2}B & \dots & A_{nn}B \end{bmatrix}$$

- $|\psi\rangle = (H \otimes H)(|+\rangle \otimes |-\rangle) \equiv \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \times \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |0\rangle \otimes |1\rangle$

Example (Dirac notation)

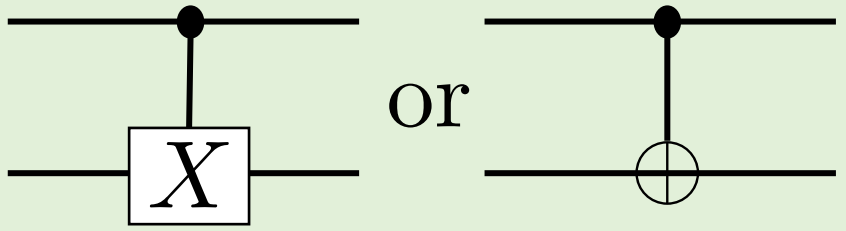


$$(H \otimes H)(|+\rangle \otimes |-\rangle) = (H|+\rangle) \otimes (H|-\rangle) = |0\rangle \otimes |1\rangle$$

Entangling operations

- $\exists U_{AB} \in \mathcal{L}(\mathcal{H}_{AB})$ s.t. $\nexists U_A \in \mathcal{L}(\mathcal{H}_A)$ and $U_B \in \mathcal{L}(\mathcal{H}_B) : U_{AB} = U_A \otimes U_B$

Controlled-NOT gate (CNOT gate):

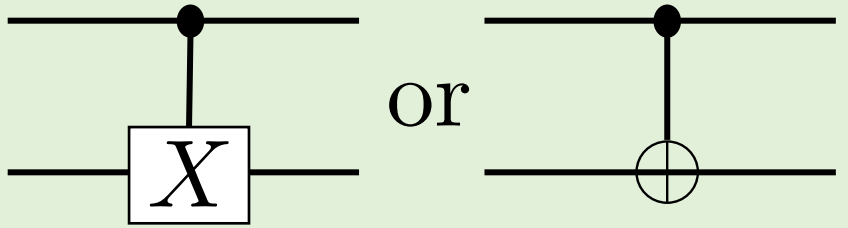


$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes X$$

- $\forall U \in \mathcal{L}(\mathcal{H}_{AB}), \exists \{V_i\} \in \mathcal{L}(\mathcal{H}_A)$ and $\{W_i\} \in \mathcal{L}(\mathcal{H}_B) : U = \sum_i V_i \otimes W_i$

Entangling operations

Controlled-not gate (cnot gate):

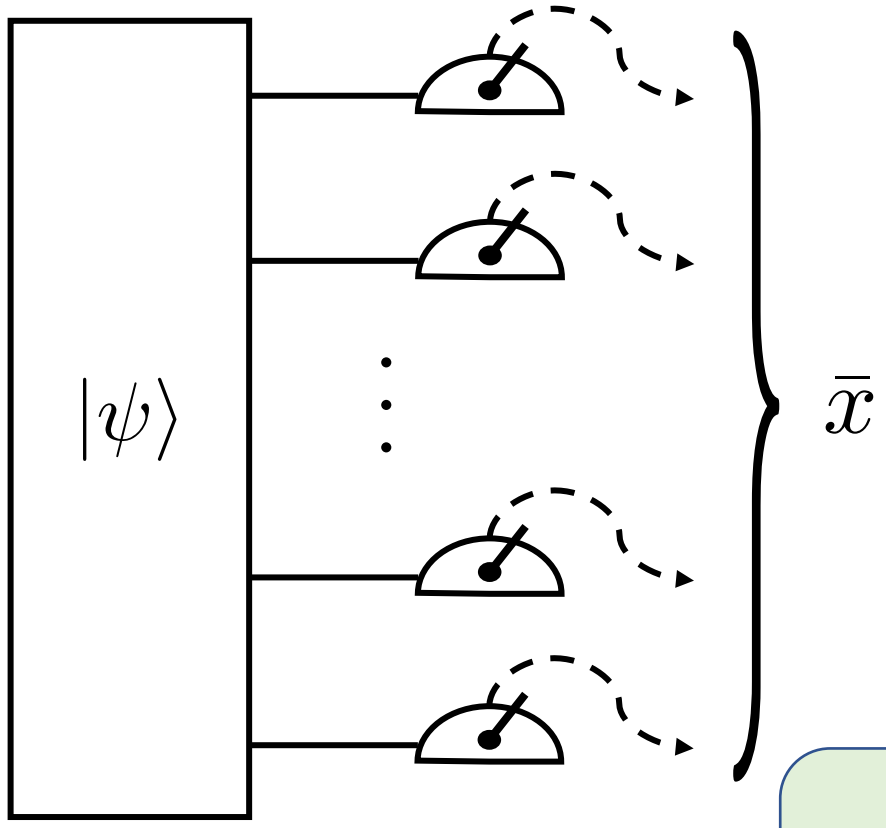


$$U_{CNOT} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes X = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

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

Composition of measurement: computational basis

- Let's $\bar{x}$ encode the outcome of n bits

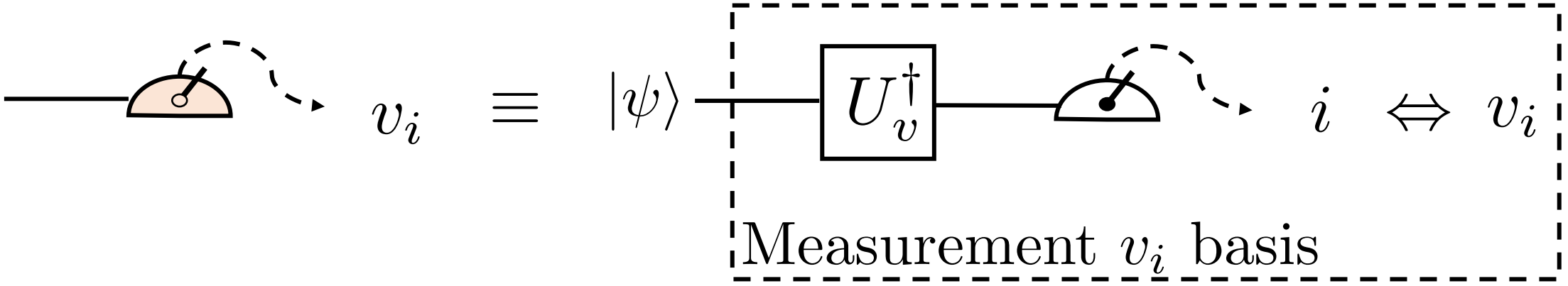


$$|\bar{x}\rangle = |x_1\rangle \otimes |x_2\rangle \otimes .... \otimes |x_n\rangle$$

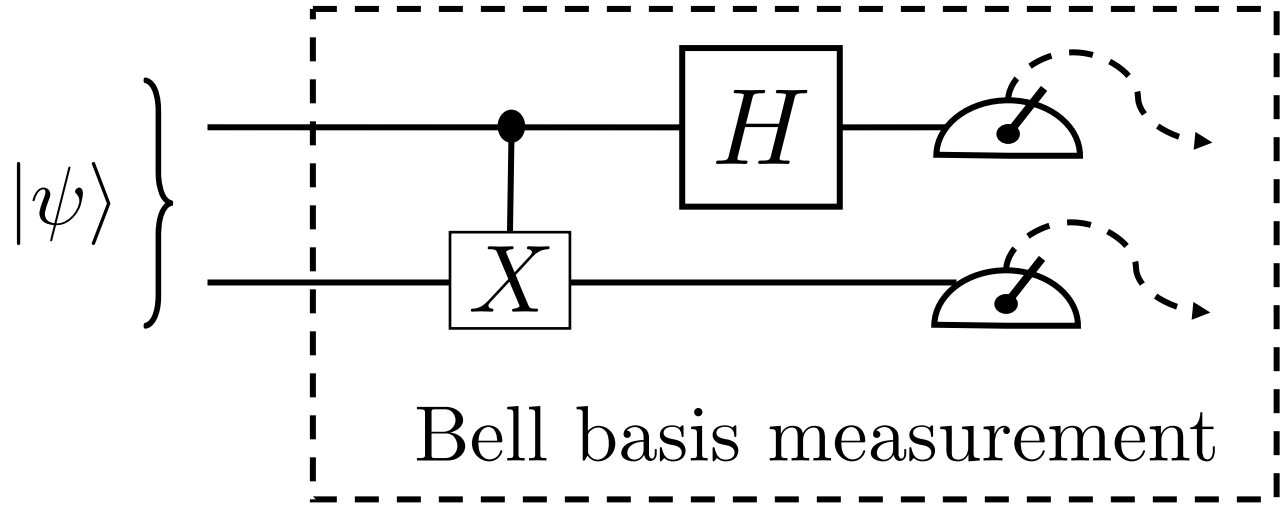
$$|\langle \bar{x}|\psi\rangle|^2 = |\langle \bar{x}| \sum_{\bar{y}\in\{0,1\}^n} \psi_{\bar{y}}|\bar{y}\rangle|^2 = |\psi_{\bar{x}}|^2$$

General multi-qubit basis measurement

- Measurement basis $\{|v_i\rangle\}$:



- Bell basis measurement:



Bell basis

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B)$$

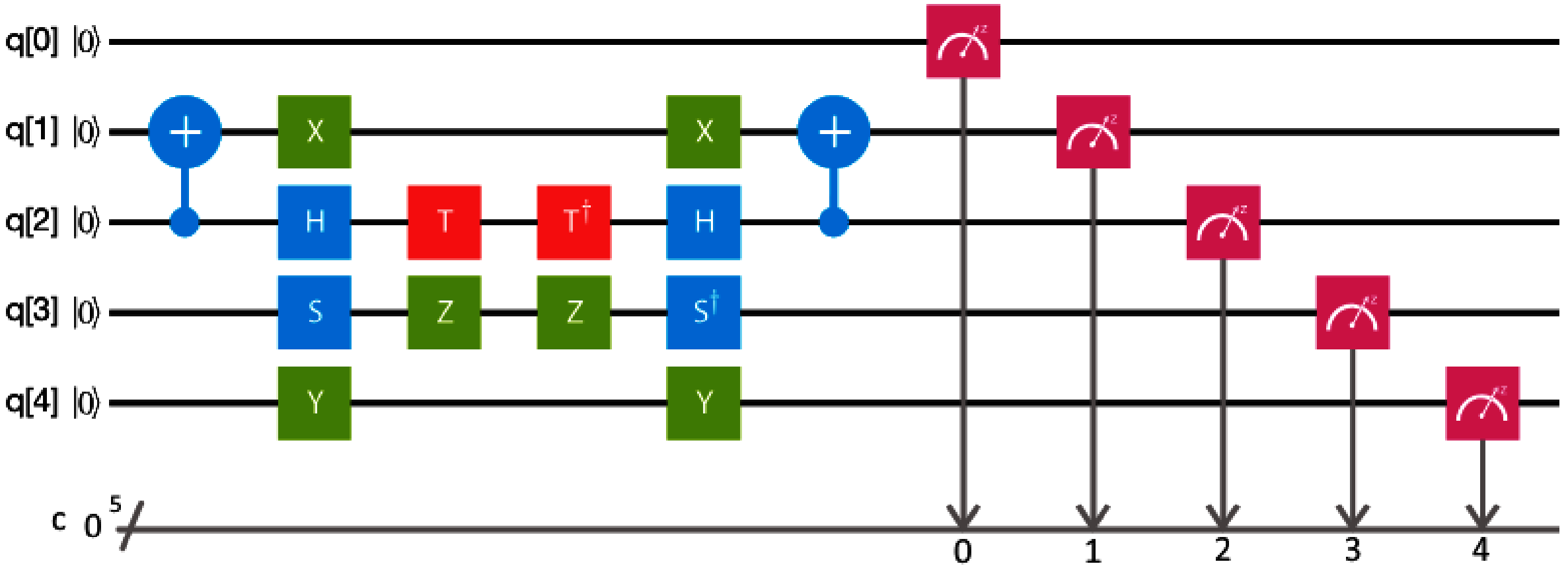
References

Reading references

1. Tensor product NC 2.1.7
2. Outer-product NC 2.1.4 page 67

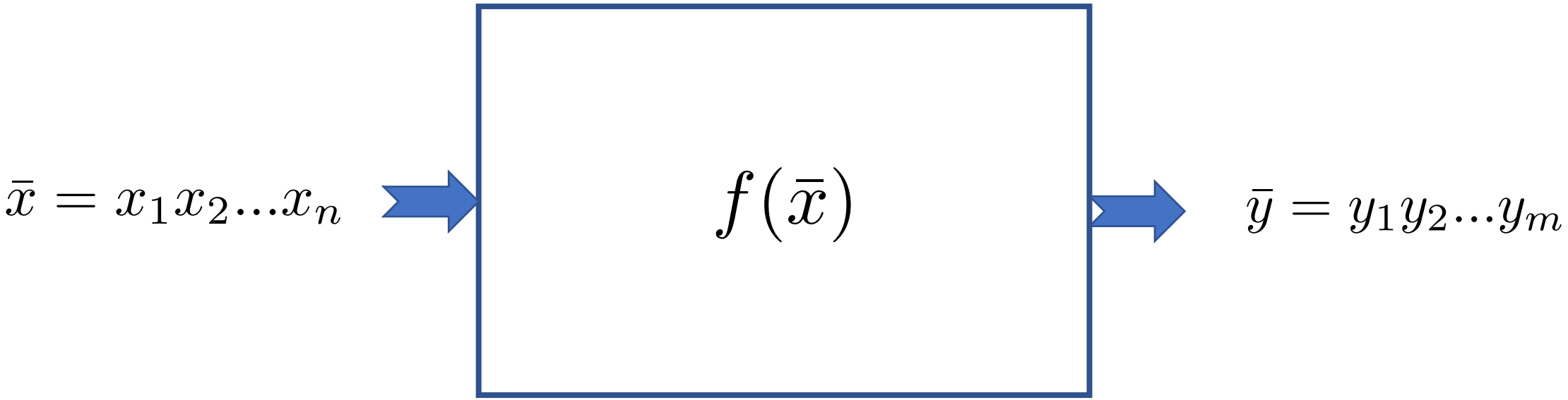
NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)

Quantum Circuit Model



Classical Circuit Model

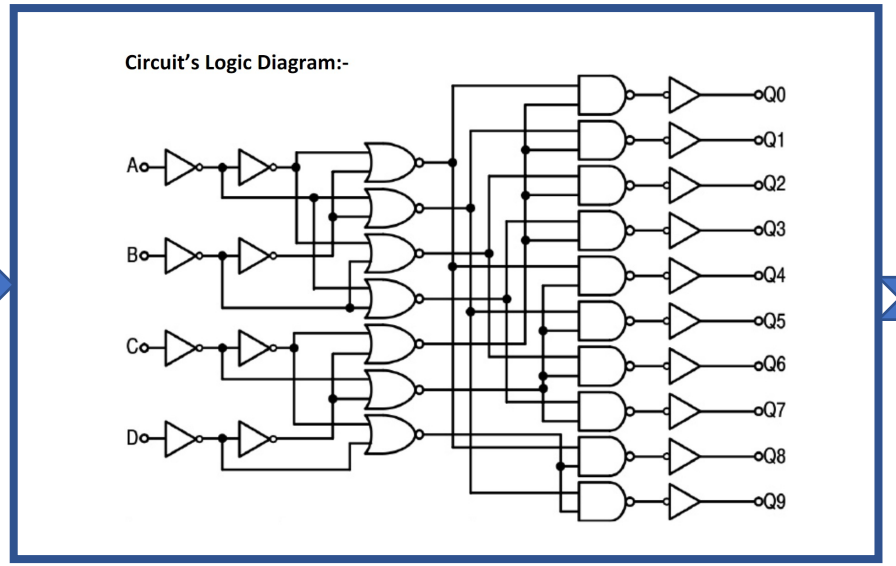
- Classical circuits compute Boolean functions: $f : \{0,1\}^n \rightarrow \{0,1\}^m$



Classical Circuit Model

- Classical circuits compute Boolean functions: $f : \{0,1\}^n \to \{0,1\}^m$

$\bar{x} = x_1 x_2 \ldots x_n$



$\bar{y} = y_1 y_2 \ldots y_m$

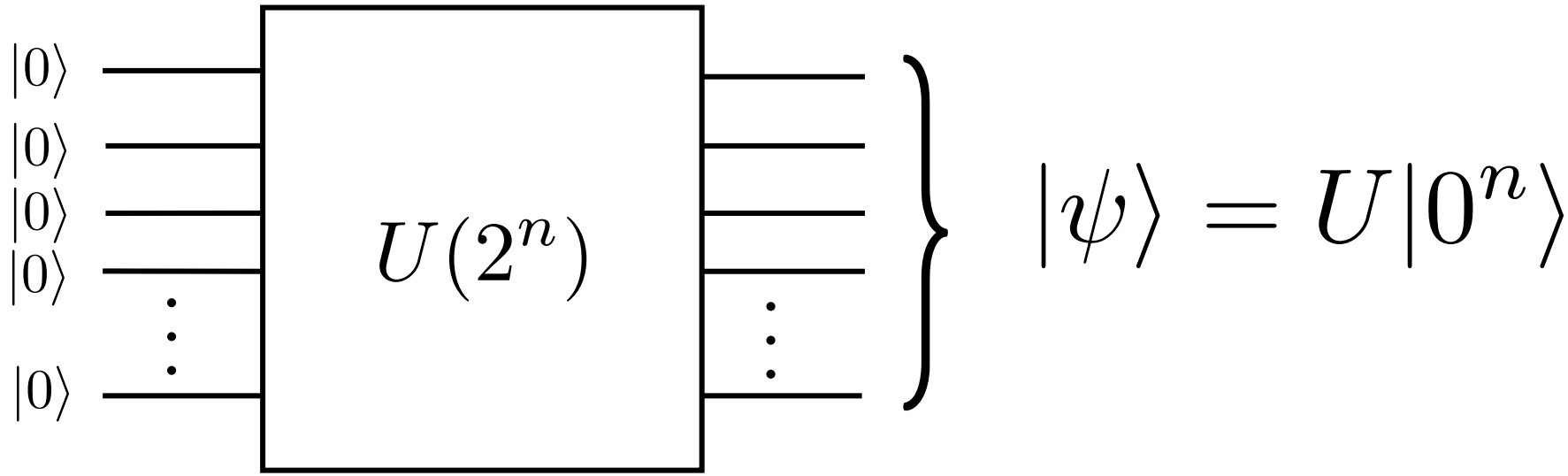
- NAND gates are UNIVERSAL

All Boolean functions can be generated with NAND gates.

- Most circuits are irreversible.
- Resource count: # gates, depth of circuit (# layers of gates).
- Most Boolean functions need exponential number of gates.

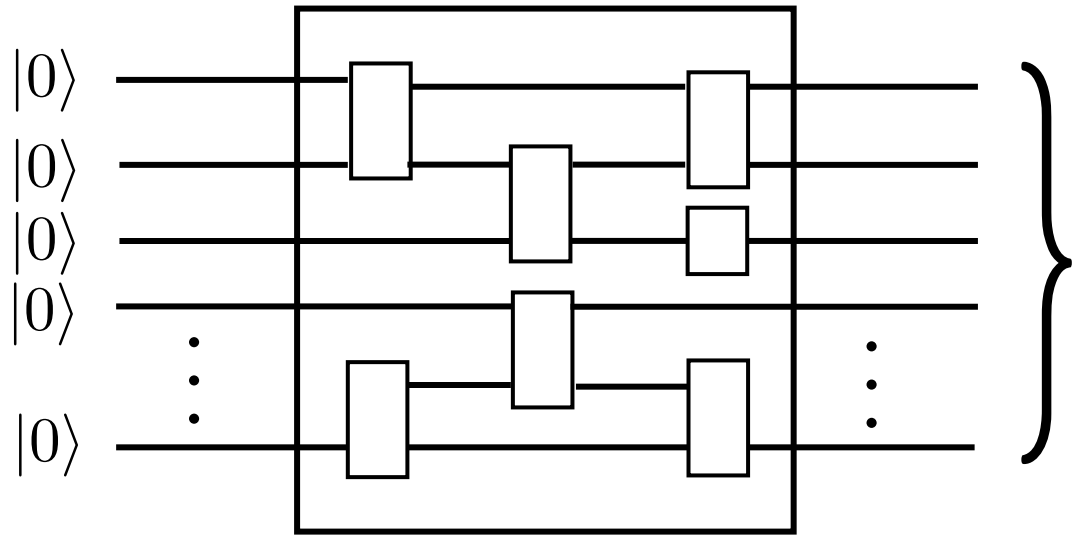
Quantum Circuit Model

- Quantum circuits implement unitaries, $U : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$



Quantum Circuit Model

- Quantum circuits implement unitaries, $U : \mathcal{H}^{\otimes n} \to \mathcal{H}^{\otimes n}$

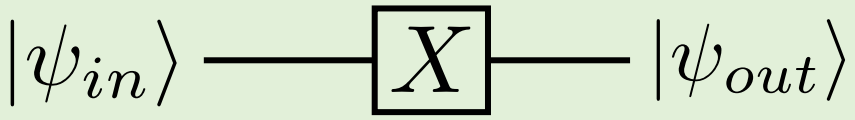


$$|\psi\rangle = U|0^n\rangle$$

- $\exists$ sets of 1 and 2 qubit gates that are UNIVERSAL
- (Ideal) quantum circuits are reversible.
- Resource count: # gates, depth of circuit (# layers of gates).
- Most unitaries need exponential number of gates.

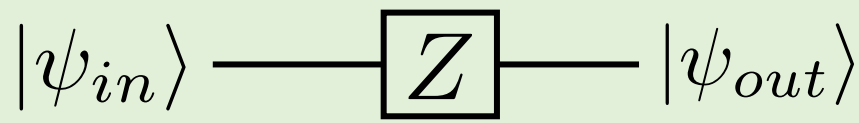
1-qubit gates

NOT gate



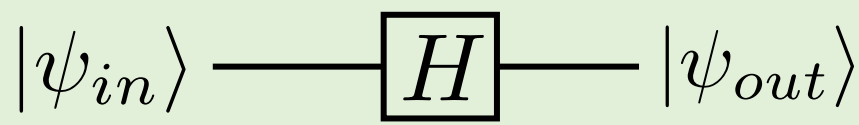
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Z gate



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

Hadamard gate



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

Phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

T gate

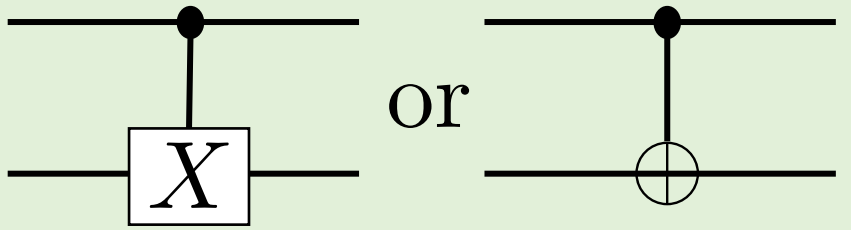
$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Gates: 2-qubit

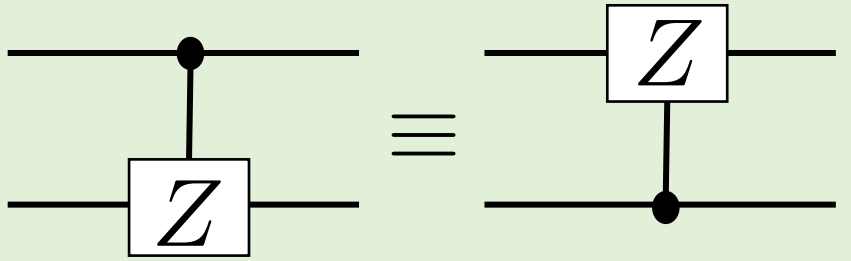
Controlled-not gate (cnot gate):

$$U_{\wedge X} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$



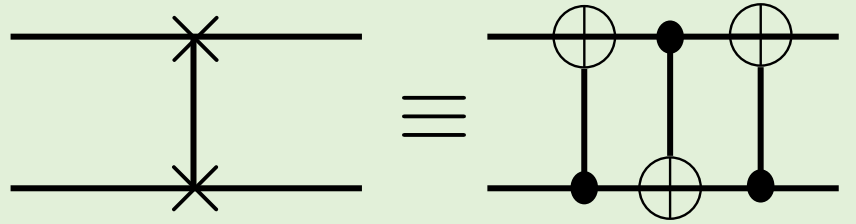
Controlled-Z gate:

$$U_{\wedge Z} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z = \mathrm{diag}(1, 1, 1, -1)$$



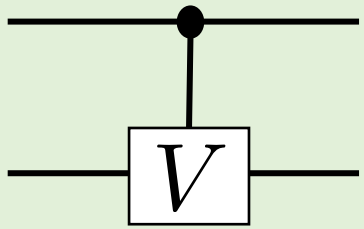
SWAP (permutation) gate

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



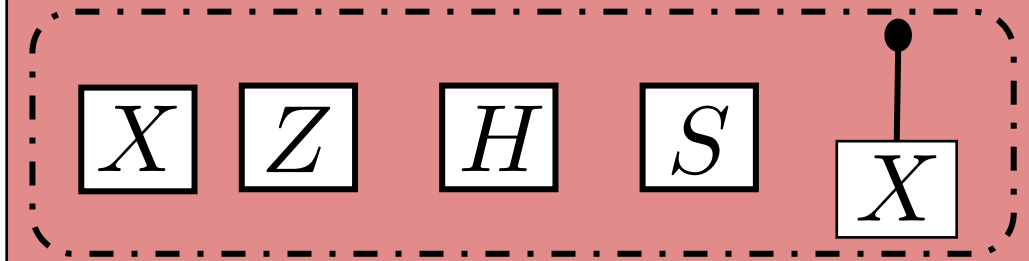
Controlled-V gate:

$$U_{\wedge V} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes V$$



Universal sets of gates

Clifford Gates

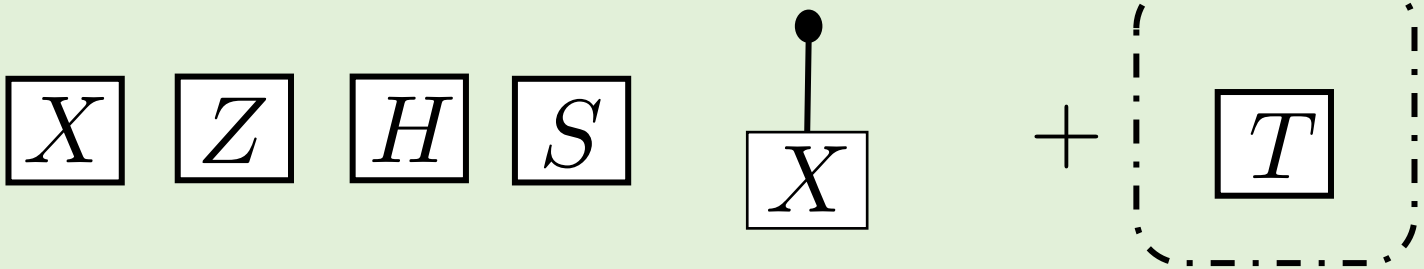


Very important role in QC: QEC
(Quantum Error Correction)

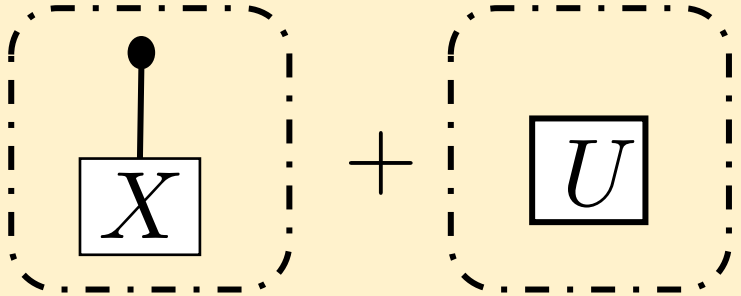
Map chain of Pauli to another

Can be classically simulated! (Gottesman-Knill Th)

Clifford gates + T



CNOT + Almost any 1-qubit gate



Almost any 2-qubit gate

Certainly not practical!

Hardness of General U

Shannon: almost all Boolean function require $\approx 2^n$ gates.

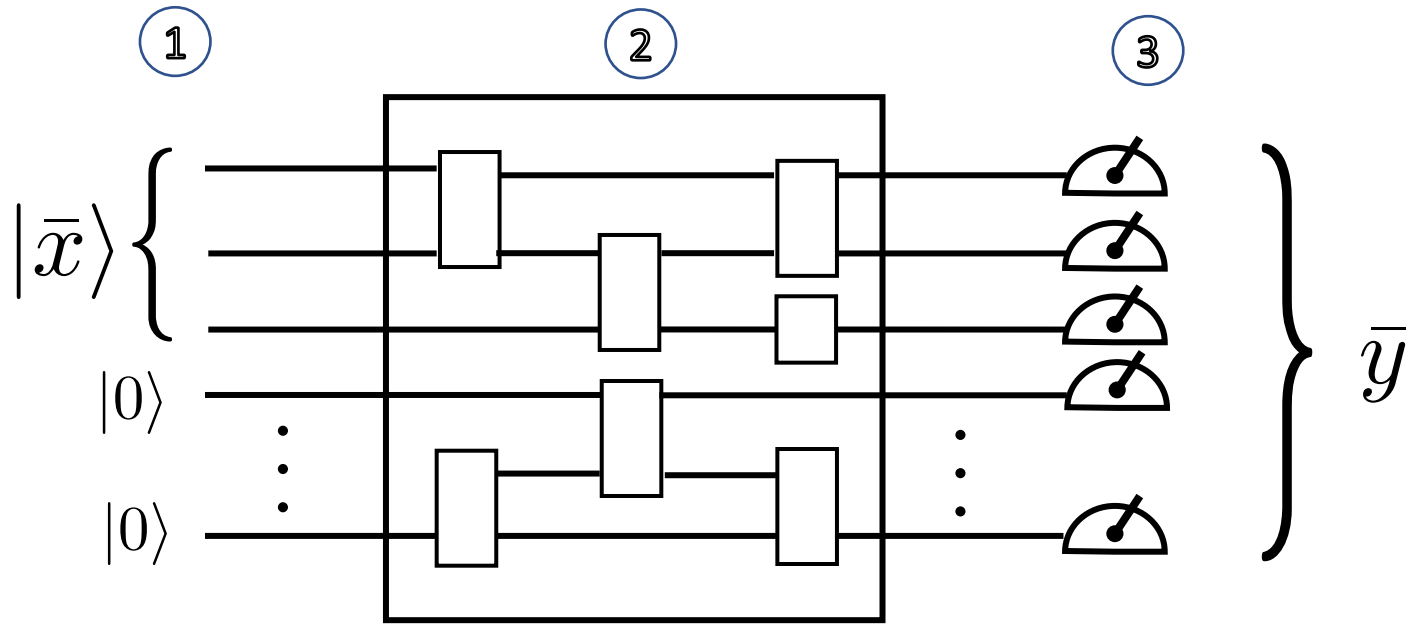
Solovay-Kitaev Theorem

$\exists$quantum circuits that require $\Omega(2^n \log(1/\epsilon)/\log(n))$ gates.

We will be interested in those

that can be generated with poly(n) gates.

Quantum Algorithms



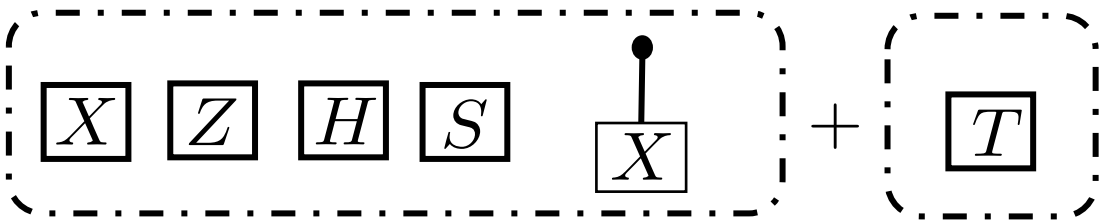
1. Preparation of an n qubit computational state
2. Quantum circuit from a universal set of gates
3. Measurement in the computational basis

Efficient if #gates is $O(\text{poly}(n))$.

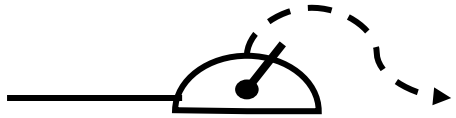
DiVincenzo criteria for Quantum Computation

- Well-defined qubits

- Initialization to a pure state $|000...0\rangle$
- Long coherence times $\frac{1}{\sqrt{2}}(|000...0\rangle + |111...1\rangle)$
- Universal set of gates



- Single qubit measurements



References

This lecture is supposed to be self-contained and there is no associate reading to it. Nonetheless, we provide references for those wanting to explore further the topic.

Further references

1. Quantum circuit model NC 4.2-4.4
2. Universal quantum gates NC 4.5; David Deutsch, Adriano Barenco, and Artur Ekert, Universality in quantum computation, Proc. R. Soc. London A, 449:669–677, 1995.
3. Principle of deferred measurement NC page 186 + Exercise 4.35
4. DiVincenzo criteria for QC: D. P. Divincenzo, Mesoscopic Electron Transport, chapter Topics in Quantum Computers, pages 657–677 (1997), arXiv:cond-mat/9612126.
5. For QMA start with Wikipedia
    1. Quantum NP - A Survey, Dorit Aharonov and Tomer Naveh, arXiv:quant-ph/0210077v1
    2. Watrous, John (2009). "Quantum Computational Complexity", arXiv:0804.3401.

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