Quantum Information Processing

Lecture 1: Quantum Bits, Reversible Operations

Who am I?

- Prof. Luca Barletta
- Email: luca.barletta@polimi.it
- Office: Building 20, 3rd floor
- Research interests:
  - Information Theory
  - Classical and Quantum Coding Theory
  - Communication Theory
- Courses:
  - Informazione e stima (2nd year Bachelor degree)
  - Classical and quantum error correction (Master degree)
  - Quantum Information Theory (with Prof. Magarini, Doctoral degree)
  - Quantum Machine Learning (with Prof. Rini (NCTU, Taiwan), Doctoral degree)

Topics Covered in Quantum Information Processing

Theoretic part:

- Introduction to Quantum Mechanics (31/03 (room 9.0.3) and 04/04 (room T.0.4) - Prof. Barletta)
- Three Quantum Protocols (Prof. Magarini)
- Shor's and Grover's Algorithms (Prof. Magarini)
- Quantum Key Distribution (Prof. Magarini)
- Quantum Error Correction (Prof. Barletta)

Outline

- Motivation
- Introduction to Quantum Mechanics
  - State Preparation
  - Quantum State Evolution

Motivation

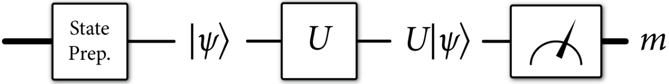
Why to study quantum information processing?

- Quantum computing, quantum cryptography, and quantum communication are expected to have a significant impact on various industries in the next decades
  - Efficient drug design and testing
  - Study of semi- and super-conductors
  - Simulation of fundamental physics
  - Secure communications
  - ...
- As quantum technologies continue to mature, there will be a growing demand for professionals with expertise in this field
- Quantum computing and information processing require to think differently. It challenges traditional binary logic and encourages a quantum mindset, which can enhance problem-solving skills and creativity

Overview of Quantum Information Processing

Quantum Information Processing Steps:

1. State Preparation: The initialization of quantum system to some beginning state
2. Quantum Processing: We perform some quantum operations. This is the stage where we take advantage of quantum effects
3. Measurement: Perform “read out” or measurement (Lecture 2)



Section 1

State Preparation

State Preparation

Physical Examples of a Quantum Object: The spin of an electron, the polarization of a photon, ...

Classical Interfacing: Switching on an attenuated laser that produces a single photon in a given time window

Mathematical Model: Qubit (Quantum bit)

Quantum Bit

Definition

A qubit is a unit-norm vector in $\mathbb{C}^2$. If we denote the basis vectors of this space by

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

then a single qubit $|\psi\rangle$ is a linear combination of $|0\rangle$ and $|1\rangle$, that is

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

- We say that $|\psi\rangle$ is a superposition (linear combination) of $|0\rangle$ and $|1\rangle$.
- We refer to $|\cdot\rangle$ as "ket". This is known as Dirac notation and has some advantages in quantum theory.
- The constraint $|\alpha|^2 + |\beta|^2 = 1$ is needed to guarantee unit norm, but also leads to a probabilistic interpretation of quantum theory (see Born rule in Lecture 2).

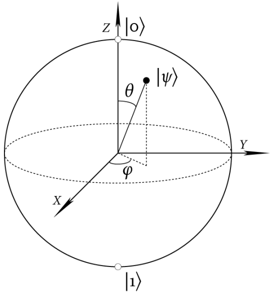
Bloch Sphere

A qubit can be uniquely represented in spherical coordinates: This representation is known as the Bloch sphere.
Specifically, every qubit can be represented as

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$$

where

$$0 \le \theta \le \pi, \text{ and } 0 \le \phi \le 2\pi$$



Bloch Sphere (Derivation)

Consider a qubit

$$\begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ &= r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle \text{ (representation of } \alpha \text{ and } \beta \text{ in polar coordinates)} \end{aligned}$$

Two qubits are physically equivalent up to a global phase (more on this when we study measurement postulates). Thus, we have that

$$\begin{aligned} |\psi\rangle &\equiv e^{-i\phi_0}|\psi\rangle \\ &= r_0\,|0\rangle + r_1 e^{i(\phi_1-\phi_0)}|1\rangle \\ \text{(using that } |r_0|^2 + |r_1|^2 = 1) \quad &= \cos(\theta/2)\,|0\rangle + \sin(\theta/2) e^{i(\phi_1-\phi_0)}|1\rangle \\ &= \cos(\theta/2)\,|0\rangle + \sin(\theta/2) e^{i\phi}|1\rangle \end{aligned}$$

The “bra” and the “ket”

Recall that ket notation $|\phi\rangle$ denotes a column vector in $\mathbb{C}^2$. The Hermitian transpose of $|\phi\rangle$, which is a row vector, is denoted by

$$\langle\phi| = (|\phi\rangle)^\dagger$$

we refer to $\langle\phi|$ as “bra”.

Few comments:

- Example: for $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\langle\phi| = \langle 0|\alpha^\star + \langle 1|\beta^\star$$

  where * denotes complex conjugate
- bras do not represent quantum states but are only helpful tools

From “bra” and “ket” to “braket”

Bras can be used to compute the amplitudes

$$\begin{aligned}\langle 0||\psi\rangle &= \langle 0|\left(\alpha|0\rangle + \beta|1\rangle\right)\\ &= \alpha\langle 0||0\rangle + \beta\langle 0||1\rangle\\ &= \alpha 1 + \beta 0 = \alpha\end{aligned}$$

The notation $\langle 0||\psi\rangle$ is so common that we use the shorthand

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

Note: $\langle 0|\psi\rangle$ is simply an inner product (dot product).

From “bra” and “ket” to “braket” (Con’t)

Exercise

$$
\begin{aligned}
\langle\psi|\psi\rangle &= (\langle 0|\alpha^{\star} + \langle 1|\beta^{\star})\,(\alpha|0\rangle + \beta|1\rangle) \\
&= \alpha^{\star}\alpha\langle 0|0\rangle + \beta^{\star}\alpha\langle 1|0\rangle + \beta\alpha^{\star}\langle 0|1\rangle + \beta\beta^{\star}\langle 1|1\rangle \\
&= |\alpha|^2 + |\beta|^2 \\
&= 1
\end{aligned}
$$

We can express this result in terms of the Euclidean norm

$$\||\psi\rangle\|_2 = \sqrt{\langle\psi|\psi\rangle} = 1$$

Remark: Note that $\langle\psi|\psi\rangle$ is an inner product which induced a norm. This property implies that $\mathbb{C}^2$ together with $\langle\psi|\psi\rangle$ form what is known as the Hilbert space (i.e., a vector space endowed with an inner product).

Hadamard Basis

The states $|0\rangle$ and $|1\rangle$ form a particular basis for a qubit, which we call computational basis (or "$0/1$" basis). Other bases are important too. For example,

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ and } |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

This basis is known as "$+/-$" basis or the Hadamard basis.

The Hadamard basis can be expressed in terms of computational basis as follows:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Hadamard Basis (Exercise)

Exercise: Calculate the amplitudes $\langle +|\psi\rangle$ and $\langle -|\psi\rangle$

$$\langle +|\psi\rangle = \langle +| \left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha\langle +|0\rangle + \beta\langle +|1\rangle$$

Now,

$$\langle +|0\rangle = \frac{\langle 0|0\rangle + \langle 1|0\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}, \text{ and } \langle +|1\rangle = \frac{\langle 0|1\rangle + \langle 1|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}.$$

Therefore,

$$\langle +|\psi\rangle = \frac{\alpha + \beta}{\sqrt{2}}.$$

Using similar steps we have that $\langle -|\psi\rangle = \frac{\alpha-\beta}{\sqrt{2}}$.
This computation is significant and allows us to represent qubits in the $+/-$ basis

$$\begin{aligned} |\psi\rangle &= \langle +|\psi\rangle\, |+\rangle + \langle -|\psi\rangle\, |-\rangle \\ &= \left(\frac{\alpha + \beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|-\rangle \end{aligned}$$

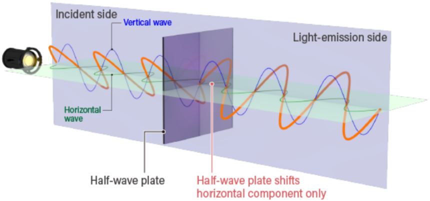
Section 2

Quantum State Evolution

Quantum System Manipulation

Physical Quantum Operation: Changing the state of polarization of the photon

Classical Interfacing: Use a half-wave plate in the optical path of the laser, that acts rotating the polarization direction



Mathematical Model: Unitary matrix

Reversibility of Quantum Operations

- Physical systems evolve over time
- There is only a couple of ways in which physical systems change
- The Schroedinger equation governs the evolution of closed quantum system
- Reversible Operation Postulate: The evolution of the closed quantum system is reversible if we do not learn anything about the state of the system (that is, we do not measure it)
- Reversibility implies that we can determine the input of the system given the output
- In general, a closed quantum system evolves according to a unitary matrix U

$$U : \; |\psi_{\text{initial}}\rangle \mapsto |\psi_{\text{final}}\rangle = U|\psi_{\text{initial}}\rangle$$

- Unitary matrices always possess an inverse - its inverse is merely $U^\dagger$, that is

$$UU^\dagger = I$$

Unitary Operators

In general, a closed quantum system evolves according to a unitary operation U. Unitary operators have the following properties:

- Unitary operators always possess an inverse - the inverse is just $U^\dagger$, the conjugate transpose of U, that is
$$UU^\dagger = I$$
- Unitary operators preserves the norm: Consider $U|\psi\rangle$
$$\begin{aligned} \| U|\psi\rangle \|^2 &= \langle\psi|U^\dagger U|\psi\rangle \\ &= \langle\psi|I|\psi\rangle \\ &= \langle\psi|\psi\rangle = 1 \end{aligned}$$

Quantum NOT Gate

We define the quantum NOT gate as an operator such that:

$$X : \begin{cases} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{cases}$$

or, in short

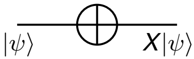
$$X|i\rangle = |i \oplus 1\rangle, \qquad i \in \{0, 1\},$$

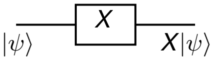
where $\oplus$ denotes binary addition.

Example: Effect of the NOT gate on the superposition state

$$\begin{aligned} X\left(\alpha|0\rangle + \beta|1\rangle\right) &= \alpha X|0\rangle + \beta X|1\rangle \\ &= \alpha|1\rangle + \beta|0\rangle \end{aligned}$$

Block diagram representation:





Matrix Representation of the Quantum NOT Gate

The matrix representation of the NOT gate is

$$
\begin{aligned}
X &= \begin{bmatrix} \langle 0|X|0\rangle & \langle 0|X|1\rangle \\ \langle 1|X|0\rangle & \langle 1|X|1\rangle \end{bmatrix} \\
&= \begin{bmatrix} \langle 0|1\rangle & \langle 0|0\rangle \\ \langle 1|1\rangle & \langle 1|0\rangle \end{bmatrix} \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}
\end{aligned}
$$

Note that the rows represent the bra (output space) and the columns represent the ket (input space).

Action of the Quantum NOT Gate on $+/-$ Basis

$$X|+\rangle = X\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|1\rangle + |0\rangle}{\sqrt{2}} = |+\rangle$$
$$X|-\rangle = X\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|-\rangle$$

Comments:

- This shows that $|+\rangle$ is the eigenstate of X with eigenvalue 1
- Also, $|-\rangle$ is the eigenstate of X with eigenvalue -1
- The matrix representation of the X operator in $+/-$ basis is

$$X = \begin{bmatrix} \langle +|X|+\rangle & \langle +|X|-\rangle \\ \langle -|X|+\rangle & \langle -|X|-\rangle \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

This shows that X operator is diagonal in $+/-$ basis. Therefore, the $+/-$ basis is an eigenbasis for the operator X.

Phase Flip Operator

Let Z be the operator that flips the states of the $+/-$ basis:

$$Z : \begin{cases} |+\rangle \mapsto |-\rangle \\ |-\rangle \mapsto |+\rangle \end{cases}$$

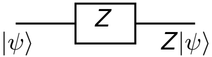
The matrix representation of Z (in $+/-$ basis) is given by

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

and in computational basis is given by

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

Thus, the computational basis is the eigenbasis for the Z operator.
Block diagram representation:



The Pauli Matrices

The matrices (in computational basis)

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

are known as the Pauli matrices.

Properties:

- They are self-inverse, i.e., $X^2 = I$, $Y^2 = I$, $Z^2 = I$
- They anti-commute, i.e., $XY = -YX$, $YZ = -ZY$, $ZX = -XZ$
- Any 2×2 complex-valued matrix can be expressed as a linear combination of the Pauli matrices and the identity matrix I

Exercise: Show that $Y = iXZ$. For this reason, we think of Y as the operator that combines bit flip and phase flip.

Hadamard Gate

Another important unitary operator is the Hadamard gate

$$H : \begin{cases} |0\rangle \mapsto |+\rangle \\ |1\rangle \mapsto |-\rangle \end{cases}$$

Using the above mapping, we have the following operator representation of H:

$$H = |+\rangle\langle 0| + |-\rangle\langle 1|.$$

- The Hadamard operator has the following representation in the computational basis:

$$H = \begin{bmatrix} \langle 0|H|0\rangle & \langle 0|H|1\rangle \\ \langle 1|H|0\rangle & \langle 1|H|1\rangle \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

- The Hadamard operator is also its own inverse.

Block diagram representation: