LECTURE 2
FUNDAMENTALS OF QUANTUM COMPUTING AND QUANTUM INFORMATION

Quantum computer science and applications

Thomas Debris-Alazard

Inria, École Polytechnique

THE OBJECTIVE OF THE DAY

To define more rigorously and deeply what we have seen during Lecture 1

$\longrightarrow$ In particular the concept of measurement!

COURSE OUTLINE

1. Basics of linear algebra: spectral decomposition of normal operators, function operators, etc. . .
2. Postulates of quantum mechanics:
   - State space $\left(\text{Hilbert space}\right)$
   - Evolution $\left(\text{unitary operators}\right)$
   - Measurement $\left(\text{general description, projective measurements, POVM}\right)$
   - Composite systems $\left(\text{tensor products}\right)$
3. Applications: teleportation and its dual superdense coding

LINEAR ALGEBRA: SOME NOTATION

PRE-REQUISITE

You have to be familiar with:

linear spaces, linear operators, basis, dimension, scalar product over Hilbert-spaces

$\longrightarrow$ We will always work in finite dimension

In particular: linear operator $\Longleftrightarrow$ matrix

The vector space of most interest to us is $\mathbb{C}^N$

- Given $z \in \mathbb{C}$, $\bar{z}$ denotes its conjugate. For instance $\overline{(1+i)} = 1 - i$
- Given $\mathbf{A}$ linear operator $\left(i.e.\text{ a matrix}\right)$, $\mathbf{A}^\dagger = \left(\overline{\mathbf{A}}\right)^\top$ denotes its Hermitian conjugate. For instance $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\dagger = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$

The vector space of most interest to us is $\mathbb{C}^N$

Dirac Notation:

- Ket: $|\psi\rangle$ denotes an element of $\mathbb{C}^N$, *i.e.* $|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix}$ where the α_i's are complex

  Convention: for any A linear operator $\mathsf{A}\,|\psi\rangle$ denotes $\mathsf{A}(|\psi\rangle)$

- Bra: $\langle\psi|$ denotes its conjugate transpose, *i.e.* $\langle\psi| = \Big(\,|\psi\rangle\,\Big)^\dagger = \begin{pmatrix} \overline{\alpha_1} & \overline{\alpha_2} & \cdots & \overline{\alpha_N} \end{pmatrix}$

  Convention: for any linear operator $\langle\psi|\,\mathsf{A}^\dagger$ denotes $\Big(\mathsf{A}\,|\psi\rangle\Big)^\dagger$

- Scalar product: $\langle\psi|\varphi\rangle$ scalar-product between $|\psi\rangle$ and $|\varphi\rangle$ is matrix multiplication $\langle\psi| \cdot |\varphi\rangle$

- Inner product and linear operator: $\langle\psi|\,\mathsf{A}\,|\varphi\rangle$ inner product between $|\psi\rangle$ and $\mathsf{A}\,|\varphi\rangle$

- Ket-bra: $|\psi\rangle\langle\varphi|$ is the linear rank 1 operator such that $|\psi\rangle\langle\varphi|\,|\phi\rangle = \langle\varphi|\phi\rangle \cdot |\psi\rangle$

AN IMPORTANT PROPOSITION

Proposition:

Let $(|i\rangle)_{1\leq i\leq N}$ be some orthonormal basis of $\mathbb{C}^N$, then,

$$\sum_{i=1}^{N} |i\rangle\langle i| = \mathbf{Id} \quad \Big(\text{the identity operator}\Big)$$

Proof:

Let $|v\rangle \in \mathbb{C}^N$, as $(|i\rangle)_{1\leq i\leq N}$ basis, $|v\rangle = \sum_{i=1}^{N} v_i\,|i\rangle$ and $v_i = \langle i|v\rangle$, as $(|i\rangle)_{1\leq i\leq N}$ orthonormal basis.

Then,

$$\left(\sum_{i=1}^{N} |i\rangle\langle i|\right)|v\rangle = \sum_{i=1}^{N} \left(|i\rangle\langle i|\,|v\rangle\right) = \sum_{i=1}^{N} \langle i|v\rangle\,|i\rangle = \sum_{i=1}^{N} v_i\,|i\rangle = |v\rangle$$

AN IMPORTANT CONVENTION

When working in $\mathbb{C}^2$ $\left(\text{the qubits space}\right)$

$$|0\rangle \overset{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \overset{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

is an orthonormal basis of $\mathbb{C}^2$

$\longrightarrow$ Don't confuse $|0\rangle$ with $\mathbf{0}$ the zero vector of $\mathbb{C}^2$ $\left(\mathbf{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$

We will often use the following operators $\left(\text{in quantum computing and quantum information}\right)$

Pauli matrices:

$$\sigma_0 = \mathsf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \sigma_x = \mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \sigma_y = \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \sigma_z = \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exercise:

Show that:

$$\mathsf{Id} = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad \mathsf{X} = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad \mathsf{Y} = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1| \quad \text{and} \quad \mathsf{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

The following operator will be at the core of quantum computing

$$\Big(\text{some relation to the Quantum Fourier Transform}\Big)$$

Hadamard matrix:

$$\mathsf{H} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The $\frac{1}{\sqrt{2}}$ factor is here to ensure that H is an isometry!

Exercise:

Show that

$$\mathsf{H}\mathsf{H}^\dagger = \mathsf{H}^\dagger\mathsf{H} = \mathsf{H}^2 = \mathsf{I}_2 \quad \text{and} \quad \mathsf{H} = \frac{(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|}{\sqrt{2}}$$

Spectral decomposition, . . .

- Hermitian: A such that $A^\dagger = A$
- Positive: A Hermitian such that $\forall |v\rangle \neq 0, \langle v| A |v\rangle \geq 0$ $\Big($and > 0 when A strictly positive$\Big)$
- Orthogonal projector: P such that $P^2 = P$ and $\mathrm{Im}(P) \perp \mathrm{Ker}(P)$

Orthogonal projectors $\subseteq$ Hermitian and Strictly Positive $\subseteq$ Positive $\subseteq$ Hermitian

- Unitary: U such that $UU^\dagger = U^\dagger U = Id$
- Normal: A such that $A^\dagger A = AA^\dagger$

Hermitian $\subseteq$ Normal and Unitary $\subseteq$ Normal

$\longrightarrow$ Except some measurements, all the considered operators in this course are normal!

SPECTRAL DECOMPOSITION OF NORMAL OPERATORS

Theorem: spectral decomposition of normal operators

Any normal operator A is diagonal with respect to some orthonormal basis

Conversely, any diagonalizable operator in an orthonormal basis is normal.

In practice:

Let A be a positive, or an Hermitian, or orthogonal projector, or a unitary, or a normal operator.

Then it exists an orthonormal basis $(|i\rangle)_i$ and $(\lambda_i)_i \in \mathbb{C}^N$ such that

$$\mathsf{A} = \sum_i \lambda_i \, |i\rangle\langle i|$$

$\longrightarrow$ Extremely useful in many "theoretical" proofs or to define classes of operators!

Operator functions:

Let $\mathbf{A}$ be a normal operator and $f : \mathbb{C} \to \mathbb{C}$ some function. The operator $f(\mathbf{A})$ is defined as follows:

1. Diagonalize $\mathbf{A}$ in an orthonormal basis: $\mathbf{A} = \sum_i \lambda_i |i\rangle\langle i|$
2. Define $f(\mathbf{A}) \stackrel{\text{def}}{=} \sum_i f(\lambda_i) |i\rangle\langle i|$

Definition possible because spectral decomposition normal operators!

$\Big($you can also verify that $f(\mathbf{A})$ is uniquely defined$\Big)$

Operator functions:

Let $\mathbf{A}$ be a normal operator and $f : \mathbb{C} \to \mathbb{C}$ some function. The operator $f(\mathbf{A})$ is defined as follows:

1. Diagonalize $\mathbf{A}$ in an orthonormal basis: $\mathbf{A} = \sum_i \lambda_i \, |i\rangle\langle i|$
2. Define $f(\mathbf{A}) \stackrel{\text{def}}{=} \sum_i f(\lambda_i) \, |i\rangle\langle i|$

Definition possible because spectral decomposition normal operators!

(you can also verify that $f(\mathbf{A})$ is uniquely defined)

An example:

$$\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{then } \exp(\theta \mathbf{Z}) = \begin{pmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{pmatrix}$$

Exercise:

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{then } \exp(\theta \mathbf{X}) = e^{\theta} \, |+\rangle\langle +| + e^{-\theta} \, |-\rangle\langle -| = \frac{1}{2} \begin{pmatrix} e^{\theta} + e^{-\theta} & e^{\theta} - e^{-\theta} \\ e^{\theta} - e^{-\theta} & e^{\theta} + e^{-\theta} \end{pmatrix}$$

Trace:

Given some operator $\mathbf{A} = (A_{ij})_{i,j}$, its trace is defined as the sum of its diagonal elements:

$$\mathbf{tr}(\mathbf{A}) = \sum_j A_{j,j}$$

$\longrightarrow$ Independent of the choice of bases in which $\mathbf{A}$ is written.

Properties:

1. Cyclicity: $\mathbf{tr}(\mathbf{AB}) = \mathbf{tr}(\mathbf{BA})$
2. Linearity: $\mathbf{A} \mapsto \mathbf{tr}(\mathbf{A})$ is linear
3. Decomposition: let $(|i\rangle)$ be an orthonormal basis, then $\mathbf{tr}(\mathbf{A}) = \sum_i \langle i| \mathbf{A} |i\rangle$

Trace:

Given some operator $\mathbf{A} = (A_{ij})_{i,j}$, its trace is defined as the sum of its diagonal elements:

$$\mathbf{tr}(\mathbf{A}) = \sum_j A_{j,j}$$

$\longrightarrow$ Independent of the choice of bases in which $\mathbf{A}$ is written.

Properties:

1. Cyclicity: $\mathbf{tr}(\mathbf{AB}) = \mathbf{tr}(\mathbf{BA})$
2. Linearity: $\mathbf{A} \mapsto \mathbf{tr}(\mathbf{A})$ is linear
3. Decomposition: let $(|i\rangle)$ be an orthonormal basis, then $\mathbf{tr}(\mathbf{A}) = \sum_i \langle i| \mathbf{A} |i\rangle$

Proof of Item 3:

Write $\mathbf{A} = (A_{i,j})$ in the basis $(|i\rangle)$. By definition $\mathbf{A}|j\rangle = \sum_i A_{i,j} |i\rangle$. Notice:

$$\langle j| \mathbf{A} |j\rangle = \langle j| \left(\sum_i A_{i,j} |i\rangle \right) = \sum_i A_{i,j} \langle j|i\rangle = A_{j,j}$$

where in the last equality we used the orthonormality. To conclude: $\mathbf{tr}(\mathbf{A})$ independent of the basis in which $\mathbf{A}$ is written

Proposition:

For any unitary $|\psi\rangle$,

$$\mathrm{tr}\left(\mathsf{A}\,|\psi\rangle\langle\psi|\right) = \langle\psi|\,\mathsf{A}\,|\psi\rangle$$

Proof: as usual, use a well chosen orthonormal basis

As $|\psi\rangle$ is unitary, let $(|i\rangle)$ be an orthonormal basis such that its first element is $|\psi\rangle$. Therefore

$$\mathrm{tr}\left(\mathsf{A}\,|\psi\rangle\langle\psi|\right) = \sum_i \langle i|\left(\mathsf{A}\,|\psi\rangle\langle\psi|\right)|i\rangle = \sum_i \langle i|\,\mathsf{A}\,|\psi\rangle\,\langle\psi|i\rangle = \langle\psi|\,\mathsf{A}\,|\psi\rangle$$

where in the last inequality we used that $\langle\psi|i\rangle = 0$ as soon as $|\psi\rangle \neq |i\rangle$ and $\langle\psi|\psi\rangle = 1$

$\longrightarrow$ You can also prove this theorem with the vector notation $\Big($we are in finite dimension$\Big)$

- Positive $\mathbf{A}$ Hermitian such that $\forall\, |v\rangle \neq 0$, $\langle v|\, \mathbf{A}\, |v\rangle \geq 0 \iff \mathbf{A}$ Hermitian + Eigenvalues ≥ 0

- Unitary: $\mathbf{U}$ such that $\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{Id} \iff \forall\, |v\rangle\,, |w\rangle$: $\langle \mathbf{U}\, |w\rangle\,, \mathbf{U}\, |v\rangle\rangle = \langle w|\, \mathbf{U}^\dagger\mathbf{U}\, |v\rangle = \langle w|v\rangle$

  $\longrightarrow$ *An operator* $\mathbf{U}$ *is unitary if and only if it preserves the scalar product between vectors*

- Orthogonal projector: let $V \subseteq \mathbb{C}^N$ subspace of dimension K and $(|1\rangle\,, \ldots, |K\rangle)$ be an orthonormal basis such that$(|1\rangle\,, \ldots, |N\rangle)$ orthonormal basis of $\mathbb{C}^N$

$$\mathbf{P} = \sum_{i=1}^{K} |i\rangle\langle i| \text{ is an orthogonal projector onto } V$$

  Reciprocally, given $\mathbf{P}$ orthogonal projector, if $(|i\rangle)$ orthonormal basis of $\mathbf{Im(P)}$, then $\mathbf{P} = \sum_i |i\rangle\langle i|$

Postulates of Quantum Mechanics

Postulate 1: State Space

Associated to any isolated physical system is an Hilbert space known as the state space of the system. The system is completely described by its state vectors, which are unit vectors in the system's state space

- Our considered Hilbert spaces will be often $\mathbb{C}^{2^n}$ for some $n \in \mathbb{N}$ $\left(n \text{ register qubits}\right)$
- Be careful, state vector/quantum states $|\psi\rangle$ are such that $\langle\psi|\psi\rangle = 1$

During this course: we will mainly consider the qubit space $\mathbb{C}^2$

Computational basis for qubits:

$$|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

A qubit:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1$$

Postulate 2: Evolution

The evolution of a closed quantum system is described by a unitary operator

The following operators over qubits are all unitaries:

$$\sigma_1 = \sigma_x = \mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \sigma_y = \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \sigma_z = \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

$\longrightarrow$ They will be fundamental for quantum computing/information theory!

Postulate 3: Quantum measurement

Quantum measurements are described by a collection $(\mathbf{M}_m)_m$ of measurement operators which are operators acting on the state space with the following rules and relation,

- m: measurement outcome that may occur during the experiment
- Given $|\psi\rangle$, the probability to measure m is

$$p(m) \overset{\text{def}}{=} \langle\psi|\, \mathbf{M}_m^\dagger \mathbf{M}_m\, |\psi\rangle = \mathrm{tr}\left(\mathbf{M}_m^\dagger \mathbf{M}_m\, |\psi\rangle\langle\psi|\right)$$

- Given $|\psi\rangle$, after measuring m, $|\psi\rangle$ becomes

$$\frac{\mathbf{M}_m\, |\psi\rangle}{\sqrt{\langle\psi|\, \mathbf{M}_m^\dagger \mathbf{M}_m\, |\psi\rangle}} = \frac{\mathbf{M}_m\, |\psi\rangle}{\sqrt{\mathrm{tr}\left(\mathbf{M}_m^\dagger \mathbf{M}_m\, |\psi\rangle\langle\psi|\right)}}$$

- Completeness relation

$$\sum_m \mathbf{M}_m^\dagger \mathbf{M}_m = \mathrm{Id}$$

The completeness relations ensures that:

$$1 = \sum_m p(m) = \sum_m \langle\psi|\, \mathbf{M}_m^\dagger \mathbf{M}_m\, |\psi\rangle = \langle\psi|\left(\sum_m \mathbf{M}_m^\dagger \mathbf{M}_m\right)|\psi\rangle = \langle\psi|\psi\rangle$$

We have seen during Lecture 1:

Measuring in the basis $(|0\rangle, |1\rangle)$: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{measure} \begin{cases} |0\rangle & \text{with probability } |\alpha|^2 \\ |1\rangle & \text{with probability } |\beta|^2 \end{cases}$

With the measurement formalism:

$$\mathbf{M}_0 = |0\rangle\langle 0| \quad \text{and} \quad \mathbf{M}_1 = |1\rangle\langle 1|$$

Probability to measure:

- 0: $p(0) = \langle\psi|\,\mathbf{M}_0^\dagger \mathbf{M}_0\,|\psi\rangle = \overline{\alpha}\alpha = |\alpha|^2$
- 1: $p(1) = \langle\psi|\,\mathbf{M}_1^\dagger \mathbf{M}_1\,|\psi\rangle = \overline{\beta}\beta = |\beta|^2$

After measuring:

- 0: $\frac{\mathbf{M}_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle$
- 1: $\frac{\mathbf{M}_1|\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|}|1\rangle$

$\longrightarrow$ More rigorous but many times useless $\Big($unnecessarily complicated$\Big)$ when studying quantum algorithms!

Projective measurement:

Observable $\mathbf{M}$: Hermitian operator which has the spectral decomposition

$$\sum_m m\mathbf{P}_m$$

where $\mathbf{P}_m$ orthogonal projection onto the eigenspace of $\mathbf{M}$ with eigenvalue m

$(\mathbf{P}_m)_m$ defines the associated quantum measurement to $\mathbf{M}$. In particular, the possible outcomes correspond to the eigenvalues m

Proposition (exercise):

Given an observable $\mathbf{M}$, then $(\mathbf{P}_m)_m$ defines a measurement. In particular (by using that $\mathbf{P}_m^\dagger \mathbf{P}_m = \mathbf{P}_m$), given the quantum state $|\psi\rangle$

- probability to measure m: $p(m) = \langle\psi| \mathbf{P}_m |\psi\rangle = \mathrm{tr}\left(\mathbf{P}_m |\psi\rangle\langle\psi|\right)$
- given that m occurred, $|\psi\rangle$ becomes:

$$\frac{\mathbf{P}_m |\psi\rangle}{\sqrt{\langle\psi| \mathbf{P}_m |\psi\rangle}} = \frac{\mathbf{P}_m |\psi\rangle}{\sqrt{\mathrm{tr}\left(\mathbf{P}_m |\psi\rangle\langle\psi|\right)}}$$

Given $|\psi\rangle$ what is the average outcome when given the observable $\mathbf{M}$?

Proposition:

Given $|\psi\rangle$, the average outcome for the observable $\mathbf{M}$ is given by,

$$\langle \mathbf{M} \rangle \stackrel{\text{def}}{=} \langle \psi | \, \mathbf{M} \, | \psi \rangle$$

Proof:

$$\mathbb{E}(\mathbf{M}) = \sum_m m p(m) = \sum_m m \, \langle \psi | \, \mathbf{P}_m \, | \psi \rangle = \langle \psi | \left(\sum_m m \mathbf{P}_m \right) | \psi \rangle = \langle \psi | \, \mathbf{M} \, | \psi \rangle = \langle \mathbf{M} \rangle$$

Given $|\psi\rangle$ what is the typical spread of the observed values upon measurement of $\mathbf{M}$?

Standard deviation of the outcomes for the measurable $\mathbf{M}$ given $|\psi\rangle$:

$$\Delta(\mathbf{M}) \stackrel{\text{def}}{=} \sqrt{\langle \mathbf{M}^2 \rangle - \langle \mathbf{M} \rangle^2}$$

During the Exercise Session we will prove:

$$\text{Measurements} \iff \text{Projective measurements}$$

For now:

If we can perform quantum measurements, then we can perform projective measurements. The reciprocal is not clear

$$\left(\left\{\text{projective measurements}\right\} \subseteq \left\{\text{quantum measurements}\right\}\right)$$

Quantum measurement:

- Distribution of the outcomes
- Rules describing the post-measurement quantum sate

What happens if we only care of the distribution of the outcomes or if we don't care of the post-measurement quantum sates?

$\longrightarrow$ Positive Operator-Valued Measure (POVM) formalism!

POVM:

Any set of operators $(\mathbf{E}_m)_m$ be such that

1. $\forall m$, $\mathbf{E}_m$ is positive $\left(\iff \text{Hermitian with eigenvalues} \geq 0 \right)$
2. Completeness relation: $\sum_m \mathbf{E}_m = \mathbf{Id}$
3. Given $|\psi\rangle$: $p(m) = \langle\psi| \mathbf{E}_m |\psi\rangle$ is the probability to measure $\mathbf{m}$

Proposition:

For any POVM there exists an associated quantum measurement and reciprocally

Proof:

- Let $(\mathbf{E}_m)_m$ be a POVM. Define $\mathbf{M}_m \overset{\text{def}}{=} \sqrt{E_m}$ $\left(\mathbf{E}_m \text{ positive}\right)$. Then $\sum_m \mathbf{M}_m^\dagger \mathbf{M}_m = \sum_m \mathbf{E}_m = \mathbf{Id}$
- Let $(\mathbf{M}_m)_m$ be a quantum measurement. Define $\mathbf{E}_m \overset{\text{def}}{=} \mathbf{M}_m^\dagger \mathbf{M}_m$. It is a positive operator that satisfies the completeness relation

Let's play together to the following game:

1. Let $\left\{ |\psi_1\rangle , \ldots , |\psi_M\rangle \right\}$ be a set of quantum states that we know
2. I choose one state, let's say $|\psi_i\rangle$ and I give it to you
3. Your goal is to recover i and you have the right to use your favourite measurement

There are three types of measurement:

- Find each time the right answer with probability one 1 $\left(\text{the best expected measurement}\right)$
- Never make mistake but sometimes answer "I don't know" $\left(\text{unambiguous measurement}\right)$
- Can make mistakes $\left(\text{ambiguous measurement}\right)$

$\longrightarrow$ Sometimes the best expected measurement cannot exist. . .

We don't require the proposed measurement to be efficiently computable!

Orthogonal quantum states $\left\{ |\psi_1\rangle, \ldots, |\psi_M\rangle \right\}$ can be easily distinguished!

$\longrightarrow$ Define the projective measurements $\mathbf{P}_i \stackrel{\text{def}}{=} |\psi_i\rangle\langle\psi_i|$ and $\mathbf{P}_0 = \mathbf{Id} - \sum_{i \neq 0} \mathbf{P}_i$

Theorem:

No quantum measurement are capable of distinguishing non-orthogonal states

Exercise: during Exercise Session

1. Prove the theorem
2. Give a POVM $(\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3)$ that never makes error to distinguish the following quantum states:

$$|\psi_1\rangle = |0\rangle \quad \text{and} \quad |\psi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

Two papers about this topic (to be presented at the end of the course):

- *Optimum Unambiguous Discrimination Between Linearly Independent Symmetric States*, A. Chefles and S. M. Barnett.

  https://arxiv.org/abs/quant-ph/9807023

- *On the distinguishability of random quantum states*, A. Montanaro

  https://arxiv.org/abs/quant-ph/0607011

Given a quantum state $|\psi\rangle$, then $e^{i\theta}\,|\psi\rangle$ is also a quantum state

$\longrightarrow$ $e^{i\theta}\,|\psi\rangle$ is said to be equal to $|\psi\rangle$ up to the global phase θ

In quantum computation, two states equal up to some global phase can be considered as equal!

The reason:

For any measurement $\mathbf{M}_m$:

$$\langle\psi|\,\mathbf{M}_m^\dagger\mathbf{M}_m\,|\psi\rangle = \langle\psi|\,e^{-i\theta}\mathbf{M}_m^\dagger\mathbf{M}_m e^{i\theta}\,|\psi\rangle$$

$\longrightarrow$ Both quantum states have the same statistics of measurement!

Postulate 4: Composite system

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems

Furthermore, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$

$\longrightarrow$ The state space of a composite system:

$$\text{Span}\Big(|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \ : \ |\psi_i\rangle \text{'s states} \Big) = \left\{ \sum_{i_1,\ldots,i_n} \lambda_{i_1,\ldots,i_n} \left|\psi_{i_1}\right\rangle \otimes \left|\psi_{i_2}\right\rangle \otimes \cdots \otimes \left|\psi_{i_n}\right\rangle \right\}$$

.

Be careful:

1. $\Big(|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \Big)^\dagger = \langle\psi_1| \otimes \langle\psi_2| \otimes \cdots \otimes \langle\psi_n| \quad \Big(\text{do not reverse the order}\Big)$
2. It exists quantum states that cannot be written as $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$

Scalar product for composite system:

Let $|\psi\rangle \stackrel{\text{def}}{=} |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ and $|\varphi\rangle \stackrel{\text{def}}{=} |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_n\rangle$. We have,

$$\langle \psi | \varphi \rangle = \langle \psi_1 | \varphi_1 \rangle \cdot \langle \psi_2 | \varphi_2 \rangle \cdots \langle \psi_n | \varphi_n \rangle$$

$\longrightarrow$ In particular: if $|\psi_j\rangle \perp |\varphi_j\rangle$ for at least one j, then $|\psi\rangle \perp |\varphi\rangle$

A PARTICULAR CASE: n QUBITS SPACE

As we have seen during Lecture 1:

- A qubit $|\psi\rangle$ is an element of $\mathbb{C}^2$ with Hermitian norm 1
- A register of n qubits $|\psi\rangle$ is an element of $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = \mathbb{C}^{2^n}$ with Hermitian norm 1

Let $(|0\rangle, |1\rangle)$ be an orthonormal basis of $\mathbb{C}^2$. Then,

$$(|b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \ : \ b_1, \ldots, b_n \in \{0,1\})$$

is an orthonormal basis of $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = \mathbb{C}^{2^n}$

- Notation: for $\mathbf{b} \stackrel{\text{def}}{=} (b_1, \ldots, b_n) \in \{0,1\}$,

$$|\mathbf{b}\rangle = |b_1 b_2 \ldots b_n\rangle \stackrel{\text{def}}{=} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle$$

Separable versus entangled states:

A n-qubit system $|\psi\rangle$ that can be decomposed as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ is called separable

When there is no such decomposition, the state is called entangled

Example:

1. Separable states

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

2. Entangled state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$\longrightarrow$ Entangled states play a crucial role in quantum computation/information

$\left(\text{teleportation, quantum cryptography, etc. . .}\right)$

Operators over composite systems:

Given $A_1, \ldots, A_n$, the operator $A_1 \otimes A_2 \otimes \cdots \otimes A_n$ over the composite system is defined as:

$$A_1 \otimes A_2 \otimes \cdots \otimes A_n \, |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \stackrel{\text{def}}{=} A_1 \, |\psi_1\rangle \otimes A_2 \, |\psi_2\rangle \otimes \cdots \otimes A_n \, |\psi_n\rangle$$

$\longrightarrow$ The set of operators over a composite system is

$$\text{Span}\,(A_1 \otimes A_2 \otimes \cdots \otimes A_n : A_i\text{'s operators}) = \left\{ \sum_{i_1,\ldots,i_n} \lambda_{i_1,\ldots,i_n} \, A_{i_1} \otimes A_{i_2} \otimes \cdots \otimes A_{i_n} \right\}$$

Be careful:

1. $\left(A_1 \otimes A_2 \otimes \cdots \otimes A_n\right)^\dagger = A_1^\dagger \otimes A_2^\dagger \otimes \cdots \otimes A_n^\dagger$ $\left(\text{do not reverse the order}\right)$
2. It exists operators that cannot be written as: $A_1 \otimes A_2 \otimes \cdots \otimes A_n$

Products of operators:

Let $A \stackrel{\text{def}}{=} A_1 \otimes A_2 \otimes \cdots \otimes A_n$ and $B \stackrel{\text{def}}{=} B_1 \otimes B_2 \otimes \cdots \otimes B_n$. We have,

$$AB = A_1B_1 \otimes A_2B_2 \otimes \cdots \otimes A_nB_n$$

An application: teleportation

Aim:

Alice has a state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ that she does not know $\Big($*i.e.* α and β are unknown$\Big)$

$\longrightarrow$ Alice's goal: send $|\psi\rangle$ to her friend Bob!

How to proceed?

$\longrightarrow$ Little crooks: a "quantum" channel is not allowed!

Aim:

Alice has a state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ that she does not know $\Big($*i.e.* α and β are unknown$\Big)$

$\longrightarrow$ Alice's goal: send $|\psi\rangle$ to her friend Bob!

How to proceed?

$\longrightarrow$ Little crooks: a "quantum" channel is not allowed!

Achievable:

1. Alice can send only two bits $\Big($"classical" information$\Big)$ to Bob
2. Alice and Bob previously shared an EPR-pair

$\longrightarrow$ Entanglement offers a huge power. . .

TELEPORTATION: THE PROTOCOL (I)

Alice and Bob have shared an EPR-pair: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$; first qubit to Alice, second qubit to Bob

Alice has access to the first two qubits of:

$$|\psi\rangle \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

1. Alice sends her qubits through the CNOT-gate $\left(|b\rangle\,|b'\rangle \mapsto |b\rangle\,|b' + b\rangle\right)$, the state becomes:

$$\frac{1}{\sqrt{2}}\left(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\right)$$

2. Alice send her first qubit trough the Hadamard gate **H**, the state becomes:

$$\frac{1}{2}\left(\alpha\,(|0\rangle + |1\rangle)\,(|00\rangle + |11\rangle) + \beta\,(|0\rangle - |1\rangle)\,(|10\rangle + |01\rangle)\right)$$

Well, what to do next?

TELEPORTATION: THE PROTOCOL (II)

Up to now, the quantum state is (Alice owes the first two qubits):

$$\frac{1}{2}\left(\alpha\left(|0\rangle+|1\rangle\right)\left(|00\rangle+|11\rangle\right)+\beta\left(|0\rangle-|1\rangle\right)\left(|10\rangle+|01\rangle\right)\right)$$

which is equal to:

$$\frac{1}{2}\Big(\,|00\rangle\otimes(\alpha\,|0\rangle+\beta\,|1\rangle)+|10\rangle\otimes(\alpha\,|0\rangle-\beta\,|1\rangle)+|01\rangle\otimes(\alpha\,|1\rangle+\beta\,|0\rangle)+|11\rangle\otimes(\alpha\,|1\rangle-\beta\,|0\rangle)\,\Big)$$

Alice measures the first two qubits (in the basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$) and Bob's quantum state becomes:

$$\begin{aligned}
00 &\longrightarrow \alpha\,|0\rangle+\beta\,|1\rangle\\
10 &\longrightarrow \alpha\,|0\rangle-\beta\,|1\rangle\\
01 &\longrightarrow \alpha\,|1\rangle+\beta\,|0\rangle\\
11 &\longrightarrow \alpha\,|1\rangle-\beta\,|0\rangle
\end{aligned}$$

To achieve the teleportation:

1. Alice sends to Bob her measurement: $bb' \in \{0,1\}^2$
2. Bob applies $Z^b X^{b'}$ $\Big($for instance: $Z^1X^1\left(\alpha\,|1\rangle-\beta\,|0\rangle\right)=\alpha\,|0\rangle+\beta\,|1\rangle\Big)$

FASTER THAN LIGHT?

Suppose that Alice has measured 00

$\longrightarrow$ Bob has instantaneously the quantum state $\alpha\,|0\rangle + \beta\,|1\rangle$

It seems that Alice has sent $|\psi\rangle$ to Bob faster than light. . .

Suppose that Alice has measured 00

$\longrightarrow$ Bob has instantaneously the quantum state $\alpha\,|0\rangle + \beta\,|1\rangle$

It seems that Alice has sent $|\psi\rangle$ to Bob faster than light. . .

The answer is no:

- Intuitively: Bob needs to know Alice's measurement to recover $|\psi\rangle$, otherwise there is no information about $|\psi\rangle$ in his qubit
- Rigorously: come at Lecture 3!

SUPERDENSE CODING

OUR AIM:

Alice wishes to send classical bits to Bob

Alice is allowed to use a quantum channel, i.e., to send qubits to Bob

The goal is dual to teleportation!

Aim:

Alice has two bits $bb' \in \{0,1\}^2$ and her goal is to send them to her friend Bob!

$\longrightarrow$ A quantum channel is allowed but not a classical one!

Achievable:

1. Alice can send a qubit $\Big($"quantum" information$\Big)$ to Bob
2. Alice and Bob previously shared an EPR-pair

Alice and Bob have shared an EPR-pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$: first qubit to Alice, second qubit to Bob

1. Alice applies, on her qubit, one of the following unitary according to $bb' \in \{0,1\}^2$ that she wants to send,

$$00 \longrightarrow \text{nothing} \qquad 10 \longrightarrow \mathsf{X}$$
$$01 \longrightarrow \mathsf{Z} \qquad 11 \longrightarrow i\mathsf{Y}$$

2. Alice sends her qubit to Bob which gets one of the following qubits,

$$00 \longrightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad 10 \longrightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$01 \longrightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad 11 \longrightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

These four quantum states (known as Bell states) are orthonormal: Bob can perfectly distinguish them to recover the bits Alice wanted to send

EXERCISE SESSION