LECTURE 2
FUNDAMENTALS OF QUANTUM COMPUTING AND QUANTUM INFORMATION

INF587 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!

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

BASICS OF LINEAR ALGEBRA: SOME NOTATION

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 $\iff$ 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 A linear operator (*i.e.* a matrix), $\mathsf{A}^\dagger = (\overline{\mathsf{A}})^\top$ 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 $\mathbb{C}^N$: $|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix}$ 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: $\langle\psi| = (|\psi\rangle)^\dagger = \begin{pmatrix} \overline{\alpha_1} & \overline{\alpha_2} & \cdots & \overline{\alpha_N} \end{pmatrix}$.

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

- **Inner product**: $\langle\psi|\varphi\rangle$ inner-product between $|\psi\rangle$ and $|\varphi\rangle$: 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 operator s.t $|\psi\rangle\langle\varphi|\,|\phi\rangle = \langle\varphi|\phi\rangle\,|\psi\rangle$.

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

$$\sum_{i\in\mathcal{I}} |i\rangle\langle i| = \mathrm{I}_N \quad \text{(the identity operator)}$$

Proof:

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

$$\left(\sum_{i\in\mathcal{I}} |i\rangle\langle i|\right)|v\rangle = \sum_{i\in\mathcal{I}} \left(|i\rangle\langle i|\,|v\rangle\right) = \sum_{i\in\mathcal{I}} \langle i|v\rangle\,|i\rangle = \sum_{i\in\mathcal{I}} v_i\,|i\rangle = |v\rangle$$

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

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

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

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

We will often use the following operators (in quantum computing and quantum information)

Pauli matrices:

$$\sigma_0 = \mathrm{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_1 = \sigma_x = \mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (\textit{bit flip})$$

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

Exercise:

Show that:

$$\mathrm{I}_2 = |0\rangle\langle 0| + |1\rangle\langle 1|\,, \quad \mathrm{X} = |1\rangle\langle 0| + |0\rangle\langle 1|\,, \quad \mathrm{Y} = i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1| \quad \text{and} \quad \mathrm{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|\,.$$

The following operator will be at the core of quantum computing

(some relation to the Quantum Fourier Transform)

Hadamard matrix:

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

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

Exercise:

Show that

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

LINEAR ALGEBRA: SPECTRAL DECOMPOSITION, . . .

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

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

- **Unitary**: U s.t. $UU^\dagger = U^\dagger U = I_N$
- **Normal**: A s.t. $A^\dagger A = AA^\dagger$

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

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

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 $(|i\rangle)$ and $(\lambda_i) \in \mathbb{C}^N$ s.t

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

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

Operator functions:

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

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

Definition possible because spectral decomposition normal operators!

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

Operator functions:

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

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

Definition possible because spectral decomposition normal operators!

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

An example:

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

Exercise:

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

Trace:

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

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

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

Properties:

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

Trace:

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

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

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

Properties:

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

Proof of Item 3:

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

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

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

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 (we are in finite dimension)

- **Positive** $\mathbf{A}$ **Hermitian** s.t. $\forall \left|v\right\rangle \neq 0$, $\left\langle v\right| \mathbf{A} \left|v\right\rangle \geq 0 \iff \mathbf{A}$ Hermitian + Eigenvalues $\in \mathbb{R}_+$

- **Unitary**: $\mathbf{U}$ s.t. $\mathbf{U}\mathbf{U}^\dagger = \mathbf{U}^\dagger\mathbf{U} \iff \forall \left|v\right\rangle, \left|w\right\rangle$: $\langle \mathbf{U}\left|w\right\rangle, \mathbf{U}\left|v\right\rangle\rangle = \left\langle w\right| \mathbf{U}^\dagger\mathbf{U} \left|v\right\rangle = \langle w|v\rangle$

  $\longrightarrow$ *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 $(\left|1\right\rangle, \dots, \left|K\right\rangle)$ be an orthonormal basis s.t $(\left|1\right\rangle, \dots, \left|N\right\rangle)$ 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 $(\left|i\right\rangle)$ orthonormal basis of $\mathbf{Im}(\mathbf{P})$, 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 $\mathbb{C}^{2^n}$ for some $n \in \mathbb{N}$ (n register qubits)
- 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 $(\mathsf{M}_m)_m$ of **measurement operators** which are operators acting on the state space.

- *m*: **measurement outcome** that may occur during the experiment
- Given $|\psi\rangle$, **the probability to measure m** is
$$p(m) \stackrel{\text{def}}{=} \langle\psi| \mathsf{M}_m^\dagger \mathsf{M}_m |\psi\rangle = \mathbf{tr}\left(\mathsf{M}_m^\dagger \mathsf{M}_m |\psi\rangle\langle\psi|\right)$$
- Given $|\psi\rangle$, **after measuring m**, $|\psi\rangle$ becomes
$$\frac{\mathsf{M}_m |\psi\rangle}{\sqrt{\langle\psi| \mathsf{M}_m^\dagger \mathsf{M}_m |\psi\rangle}} = \frac{\mathsf{M}_m |\psi\rangle}{\sqrt{\mathbf{tr}\left(\mathsf{M}_m^\dagger \mathsf{M}_m |\psi\rangle\langle\psi|\right)}}$$
- **Completeness relation**
$$\sum_m \mathsf{M}_m^\dagger \mathsf{M}_m = \mathsf{I}_d$$

The completeness relations ensures that:

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

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:

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

Probability to measure:

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

After measuring:

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

$\longrightarrow$ More rigorous but many times useless (unnecessarily complicated) 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.

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

Exercise:

Given an observable $\mathbf{M}$, show that $(\mathbf{P}_m)$ defines a measurement. In particular

- 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 M?

Average outcome for the observable M given $|\psi\rangle$:

$$\langle \mathsf{M} \rangle = \langle \psi | \, \mathsf{M} \, | \psi \rangle$$

Proof:

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

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

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

$$\Delta(\mathsf{M}) = \sqrt{\langle \mathsf{M}^2 \rangle - \langle \mathsf{M} \rangle^2}$$

During the exercise session we will prove:

Measurement $\Longleftrightarrow$ Projective measurements

For now:

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

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 ($\iff$ Hermitian with eigenvalues ≥ 0)
2. Completeness relation: $\sum_m \mathbf{E}_m = \mathbf{I}_d$
3. Given $|\psi\rangle$: $p(m) = \langle\psi| \mathbf{E}_m |\psi\rangle$ is the probability to measure **m**

Proposition:

For any POVM there exists an associated quantum measurement and reciprocally

Proof:

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

How is defined $\sqrt{\mathbf{E}_m}$?

Let's play together to the following game:

1. Let $(|\psi_1\rangle, \ldots, |\psi_M\rangle)$ 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 (the best expected measurement)
- Never make mistake but sometimes answer "I don't know" (unambiguous measurement)
- Can make mistakes (ambiguous measurement)

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

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

Orthogonal states $|\psi_1\rangle, \ldots, |\psi_M\rangle$ can be easily distinguished!

$\longrightarrow$ Define the projective measurements $\mathsf{P}_i \overset{\text{def}}{=} |\psi_i\rangle\langle\psi_i|$ and $\mathsf{P}_0 = \mathsf{I}_d - \sum_{i\neq 0} \mathsf{P}_i$

Orthogonal states $|\psi_1\rangle, \ldots, |\psi_M\rangle$ can be easily distinguished!

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

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 M_m:

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

$\longrightarrow$ 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:

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

Be careful:

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

Inner product for composite system:

Let $|\mathrm{x}\rangle \stackrel{\text{def}}{=} |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ and $|\mathrm{y}\rangle \stackrel{\text{def}}{=} |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_n\rangle$

$$\langle \mathrm{x}|\mathrm{y}\rangle = \langle\psi_1|\varphi_1\rangle \langle\psi_2|\varphi_2\rangle \cdots \langle\psi_n|\varphi_n\rangle$$

$\longrightarrow$ In particular: if $\left|\psi_j\right\rangle \perp \left|\varphi_j\right\rangle$ for at least one j, then $|\mathrm{x}\rangle \perp |\mathrm{y}\rangle$.

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,

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

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

- Notation: for $b_1, \ldots, b_n \in \{0,1\}$

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

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

(teleportation, quantum cryptography, etc. . .)

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

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

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

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

Be careful:

1. $(A_1 \otimes A_2 \otimes \cdots \otimes A_n)^\dagger = A_1^\dagger \otimes A_2^\dagger \otimes \cdots \otimes A_n^\dagger$ (do not reverse the order)
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 $B \stackrel{\text{def}}{=} B_1 \otimes B_2 \otimes \cdots \otimes B_n$.

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

AN APPLICATION: TELEPORTATION

Aim:

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

$\longrightarrow$ 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 (i.e., α and β are unknown).

$\longrightarrow$ 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 ("classical" information) to Bob,
2. Alice and Bob previously shared an EPR-pair.

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

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:

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

$\longrightarrow$ Well, what to do next?

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 $Z^b X^{b'}$ (for instance: $Z^1X^1\left(\alpha|1\rangle - \beta|0\rangle\right) = \alpha|0\rangle + \beta|1\rangle$)

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

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 ("quantum" information) 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