# LECTURE 1
# INTRODUCTION TO QUANTUM COMPUTING

INF587 Quantum computer science and applications

Thomas Debris-Alazard

Inria, École Polytechnique

**Feynman (1981)**

Can quantum systems be probabilistically simulated by a classical computer?

$\longrightarrow$ The answer is is almost certainly, no!

$\longrightarrow$ Use quantum systems/computers to simulate quantum systems!

(birth of quantum simulation)

**A natural question**

What other problems can quantum computers solve more quickly than classical computer?

**Deutsch (1985)**

Foundation of quantum computing!

$\longrightarrow$ Deutsch-Jozsa algorithm (1992) quantum algorithm faster than any classical algorithm

**Shor (1994)**

Solves the discrete logarithm and factoring problem in polynomial time with a quantum computer!

**Terrible situation**: public-key cryptography currently deployed is broken by using an “efficient” quantum computer

$\longrightarrow$ Crypto community worried about this since many years...

**There exists quantum resistant solutions: post-quantum cryptography (active research topic)**

American’s government (2017) has launched a process to standardized post-quantum primitives

**Grover (1996)**

Find an element in a list of size $n$ in time $O\left(\sqrt{n}\right)$ while any classical algorithm needs a time $\approx n$

**Consequence**: size of keys in symmetric cryptography has to be $\times 2$.

# A BIG ISSUE: DECOHERENCE

Computations are "noisy"

- Quantum bits are very fragile, they quickly interfere with the environment: decoherence
- Quantum architectures are not "ideal"

$\longrightarrow$ Faults in computation can theoretically be "corrected": quantum error correcting codes

**Theorem 1. [Aharonov, Ben-Or, 1997]**

Quantum computation is possible provided the noise is sufficiently low

**Benett-Brassard (1984)**

Quantum protocol for key-exchange

- Already implemented
- If an authenticated canal has been established, unconditional security: relies only on the validity of physic laws and not computational assumptions

$\longrightarrow$ Basics of quantum computing and quantum information theory

- Quantum formalism with density operators, general measures, partial trace, etc...
- Quantum circuit model, quantum algorithms (Deutsch-Josza, Simon, Grover, Quantum Fourier Transform, Shor)
- Basics of quantum error correcting codes and quantum cryptography

References:

- Nielsen and Chuang, *Quantum computation and quantum information*,

  $\longrightarrow$ Nice introduction to quantum computing and quantum information
- de Wolf's lecture notes: `https://arxiv.org/abs/1907.09415`,

  $\longrightarrow$ Nice for advanced quantum algorithms
- Zemor's lecture notes: `https://www.math.u-bordeaux.fr/~gzemor/QuantumCodes.pdf`,

  $\longrightarrow$ Introduction to quantum error correcting codes

1. An exam (3 hours): **an $A3$ sheet allowed**

   → Three exercises seen during the Exercise Sessions will be at the exam.

2. Presentation of a research article or a chapter of some lecture notes (30min).

You are in a course of computer science

Computer science: art of computing

$\longrightarrow$ We don't care that an object "exists", we want to compute it efficiently!

**Using the law of quantum physic: new model of computation**

What does mean quantum computing? What is a quantum algorithm?

$\longrightarrow$ This course is not about the law of physics or about the "technologies" to verify/use them

# CLASSICAL BITS VERSUS QUANTUM BITS

- Classical bit: $b \in \{0,1\}$
- Probabilistic bit: $\begin{pmatrix} p \\ q \end{pmatrix}$ where

$$p \stackrel{\text{def}}{=} \mathbb{P}(b=0)$$
$$q \stackrel{\text{def}}{=} \mathbb{P}(b=1)$$

- Evolution during a computation (a probabilistic bit stays a probabilistic bit):

$$\begin{pmatrix} p \\ q \end{pmatrix} \longrightarrow \begin{pmatrix} p' \\ q' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix} \quad \text{where} \begin{cases} a+c=1 \\ b+d=1 \end{cases} \quad \text{and } a,b,c,d \geq 0.$$

Probabilistic computation: multiplication by a stochastic matrix

**Examples:** $b \to b \oplus b$ **and** $b \mapsto b \oplus 1$

$$\begin{pmatrix} p \\ q \end{pmatrix} \longrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} p \\ q \end{pmatrix} \longrightarrow \begin{pmatrix} q \\ p \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix}$$

*"A superposition of classical states"*

- A qubit $|\psi\rangle$ is an element of $\mathbb{C}^2$ with Euclidean norm 1:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ with } \alpha, \beta \in \mathbb{C} \text{ (called amplitude) and } |\alpha|^2 + |\beta|^2 = 1$$

where $(|0\rangle\,, |1\rangle)$ orthonormal basis of $\mathbb{C}^2$. Usually defined as

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

*"A superposition of classical states"*

- A qubit $|\psi\rangle$ is an element of $\mathbb{C}^2$ with Euclidean norm 1:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ with } \alpha, \beta \in \mathbb{C} \text{ (called amplitude) and } |\alpha|^2 + |\beta|^2 = 1$$

where $(|0\rangle\,, |1\rangle)$ orthonormal basis of $\mathbb{C}^2$. Usually defined as

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

We "cannot see" a superposition, we "can only see" classical states: measure and observe!

- Measurement: probabilistic orthogonal projection. Given $|e_0\rangle\,, |e_1\rangle \in \mathbb{C}^2$ orthonormal basis:

$$\text{Measuring in the basis } (|e_0\rangle\,, |e_1\rangle): \; |\psi\rangle = \alpha\,|e_0\rangle + \beta\,|e_1\rangle \xrightarrow{\textit{measure}} \begin{cases} |e_0\rangle \text{ with prob. } |\alpha|^2 \\ |e_1\rangle \text{ with prob. } |\beta|^2 \end{cases}$$

**Exercise: Computational versus Hadamard basis**

1. Show that $(|+\rangle\,, |-\rangle)$ is an orthonormal basis of $\mathbb{C}^2$ where

$$|+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |-\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

2. Give the outcome distribution when measuring $|0\rangle$, $|-\rangle$, and $\frac{1}{\sqrt{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle$ in the bases $(|0\rangle\,, |1\rangle)$ and $(|+\rangle\,, |-\rangle)$.

- **Qubit**: $|\psi\rangle \in \mathbb{C}^2$ of Hermitian norm 1,
- **Measuring** in the orthonormal basis $(|e_0\rangle, |e_1\rangle)$:

$$|\psi\rangle = \alpha |e_0\rangle + \beta |e_1\rangle \xrightarrow{\text{measure}} \begin{cases} |e_0\rangle \text{ with prob. } |\alpha|^2 \\ |e_1\rangle \text{ with prob. } |\beta|^2 \end{cases}$$

A measurement is a "computation" you have access to

$\longrightarrow$ See Lecture 2 for a precise definition of measurement...

# QUANTUM BIT (QUBIT)

- **Qubit**: $|\psi\rangle \in \mathbb{C}^2$ of Hermitian norm 1,
- **Measuring** in the orthonormal basis $(|e_0\rangle, |e_1\rangle)$:

$$|\psi\rangle = \alpha |e_0\rangle + \beta |e_1\rangle \overset{measure}{\longrightarrow} \begin{cases} |e_0\rangle \text{ with prob. } |\alpha|^2 \\ |e_1\rangle \text{ with prob. } |\beta|^2 \end{cases}$$

A measurement is a "computation" you have access to

$\longrightarrow$ See Lecture 2 for a precise definition of measurement...

Are there other computations over qubits we have access to?

- **Qubit**: $|\psi\rangle \in \mathbb{C}^2$ of Hermitian norm $1$,
- **Measuring** in the orthonormal basis $(|e_0\rangle, |e_1\rangle)$:

$$|\psi\rangle = \alpha |e_0\rangle + \beta |e_1\rangle \xrightarrow{\textit{measure}} \begin{cases} |e_0\rangle \text{ with prob. } |\alpha|^2 \\ |e_1\rangle \text{ with prob. } |\beta|^2 \end{cases}$$

A measurement is a “computation” you have access to

$\longrightarrow$ See Lecture 2 for a precise definition of measurement...

Are there other computations over qubits we have access to?

$\longrightarrow$ Yes! **Unitary evolutions**

- Unitary evolution: $\mathsf{U} \in \mathbb{C}^{2\times 2}$ unitary matrix $\iff \mathsf{U}\mathsf{U}^\dagger = \mathsf{I}_2$

$$|\psi\rangle \longrightarrow \mathsf{U}\,|\psi\rangle$$

Is it true that a qubit is still a qubit after a unitary evolution? Why?

$\longrightarrow$ Yes! Unitary evolutions preserve the Hermitian norm (more generally the inner-product)

**Unitary evolutions are inversible!**

$$|\psi\rangle \xrightarrow{\mathsf{U}} \mathsf{U}\,|\psi\rangle \xrightarrow{\mathsf{U}^\dagger} \mathsf{U}^\dagger\mathsf{U}\,|\psi\rangle = |\psi\rangle$$

- $\mathsf{U} \in \mathbb{C}^{2\times 2}$ unitary over qubits is often called quantum gate

$\longrightarrow$ It exists a small set of gates which is universal

To define a quantum gate: enough to specify the image of an orthonormal basis and then extended it by linearity

But it has to map an orthonormal basis to an orthonormal basis!

**Exercise: Quantum Gates?**

Are the following linear operators over qubits be quantum gates?

1. $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,
2. $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$.

Quantum gates have matrix representations!

For instance: $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$ has the representation: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Only linear operator that maps $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $|1\rangle$ to $|0\rangle$.

- NOT-gate **X**:

| Linear op. | Matrix rep. |
|---|---|
| $\|0\rangle \mapsto \|1\rangle$ <br> $\|1\rangle \mapsto \|0\rangle$ | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ |

- Hadamard-gate **H**:

| Linear op. | Matrix rep. |
|---|---|
| $\|0\rangle \mapsto \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ <br> $\|1\rangle \mapsto \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$ | $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ |

**Exercise:**

1. What is the effect of applying **H** on $|0\rangle$ and measuring it?
2. What is the effect of applying **H** on $|0\rangle$ twice?

Is quantum computation over qubits the same than classical computation over probabilistic bits?

**Exercise:**

Show that there is no stochastic matrix **P** which when applied to 0, *i.e.* to $\begin{pmatrix}1\\0\end{pmatrix}$, simulates the effect of the Hadamard gate

The "−1" gives you a huge power...

# YOUR FIRST QUANTUM ALGORITHM

**Problem**

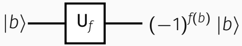
- Input: $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced,
- Output: 0 if and only if $f$ is constant.

Query complexity to $f$:

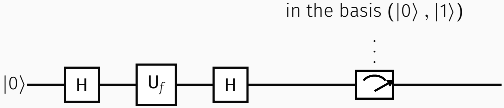
- Classically: $1 + \frac{2^n}{2}$,
- Quantumly: 1.

# THE DEUTSCH-JOSZA ALGORITHM FOR $n = 1$

- Suppose that we have access to the following gate (see exercise session)




- The algorithm




- Analysis

1. Applying $\mathbf{H}$: $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$,
2. Applying $\mathbf{U}_f$:

$$\mathbf{U}_f\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\right) = \frac{1}{\sqrt{2}}\left(\mathbf{U}_f\,|0\rangle + \mathbf{U}_f\,|1\rangle\right) = \frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}}$$

3. Applying $\mathbf{H}$:

$$\begin{aligned}\mathbf{H}\left(\frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}}\right) &= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}\mathbf{H}\,|0\rangle + (-1)^{f(1)}\mathbf{H}\,|1\rangle\right) \\ &= \frac{\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle}{2}\end{aligned}$$

**Before measuring we have computed**

$$|\psi_{\text{out}}\rangle \stackrel{\text{def}}{=} \frac{\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle}{2}$$

- If $f$ constant:
$$|\psi_{\text{out}}\rangle = \pm |0\rangle .$$
- If $f$ balanced, namely $f(0) \neq f(1)$:
$$|\psi_{\text{out}}\rangle = \pm |1\rangle .$$

**Before measuring we have computed**

$$|\psi_{\text{out}}\rangle \stackrel{\text{def}}{=} \frac{\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle}{2}$$

- If $f$ constant:

$$|\psi_{\text{out}}\rangle = \pm |0\rangle \,.$$

- If $f$ balanced, namely $f(0) \neq f(1)$:

$$|\psi_{\text{out}}\rangle = \pm |1\rangle \,.$$

Measuring in the $(|0\rangle\,, |1\rangle)$ basis leads to (with probability one)

$|0\rangle$ if $f$ constant or $|1\rangle$ if $f$ balanced

## $n$ QUBITS SYSTEM

During all this course we will work in finite dimension, think $\mathbb{C}^N$

$\longrightarrow$ Vector spaces have finite dimension, linear operator can be written as matrices, etc...

Given two vector spaces $V$ and $W$, the **tensor product** $\mathbf{v} \otimes \mathbf{w}$ between $\mathbf{v} \in V$ and $\mathbf{w} \in W$ verifies:

(1) for any scalar $z$,

$$z\,(\mathbf{v} \otimes \mathbf{w}) = (z\mathbf{v}) \otimes \mathbf{w} = \mathbf{v} \otimes (z\mathbf{w})$$

(2) for any $\mathbf{v}_1, \mathbf{v}_2 \in V$,

$$(\mathbf{v}_1 + \mathbf{v}_2) \otimes \mathbf{w} = \mathbf{v}_1 \otimes \mathbf{w} + \mathbf{v}_2 \otimes \mathbf{w}$$

(3) for any $\mathbf{w}_1, \mathbf{w}_2 \in W$,

$$\mathbf{v} \otimes (\mathbf{w}_1 + \mathbf{w}_2) = \mathbf{v} \otimes \mathbf{w}_1 + \mathbf{v} \otimes \mathbf{w}_2$$

Think the tensor product $v \otimes w$ as a column/row product:

$$\begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} \begin{pmatrix} w_1 & \cdots & w_{N'} \end{pmatrix}$$

**Tensor Product of Spaces**

$V$ and $W$ be two vector spaces with bases the $\mathbf{v}_i$'s and the $\mathbf{w}_j$ respectively

$$V = \text{Span}\left(\mathbf{v}_1, \ldots, \mathbf{v}_n\right) \quad \text{and} \quad W = \text{Span}\left(\mathbf{w}_1, \ldots, \mathbf{w}_m\right)$$

The vector space $V \otimes W$ is defined as being generated by the $\mathbf{v}_i$'s and the $\mathbf{w}_j$'s

$$V \otimes W \stackrel{\text{def}}{=} \text{Span}\left(\mathbf{v}_i \otimes \mathbf{w}_j \;:\; 1 \leq i \leq n,\; 1 \leq j \leq m\right)$$

- **Dimension**,

$$\mathbf{dim}\, V \otimes W = \mathbf{dim}\, V\, \mathbf{dim}\, W = nm$$

- **Basis**, $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ (*resp.* $(\mathbf{w}_1, \ldots, \mathbf{w}_m)$) be a basis of $V$ (*resp.* $W$)

$$\left(\mathbf{v}_i \otimes \mathbf{w}_j : 1 \leq i \leq n,\; 1 \leq j \leq m\right) \;\text{ is a basis of } V \otimes W$$

- **Characterization**,

$$\mathbf{x} \in V \otimes W \iff \exists \alpha_{i,j} \;:\; \mathbf{x} = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \alpha_{i,j}\, \mathbf{v}_i \otimes \mathbf{w}_j$$

**Classical Error:**

$\mathbf{x} \in V \otimes W$, then there exists $\mathbf{v} \in V$ and $\mathbf{w} \in W$ such that $\mathbf{x} = \mathbf{v} \otimes \mathbf{w}$.

$(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ $\Big($ *resp.* $(\mathbf{w}_1, \ldots, \mathbf{w}_m)$ $\Big)$ be a basis of $V$ (*resp.* $W$).

### Scalar product over tensor product spaces

Suppose that $V$ (*resp.* $W$) is equipped by a scalar product $\langle \cdot, \cdot \rangle_V$ (*resp.* $\langle \cdot, \cdot \rangle_W$). The scalar product over $V \otimes W$ is defined as (and extended by bilinearity) as

$$\langle \mathbf{v}_i \otimes \mathbf{w}_j, \mathbf{v}_k \otimes \mathbf{w}_\ell \rangle_{V \otimes W} \stackrel{\text{def}}{=} \langle \mathbf{v}_i, \mathbf{v}_k \rangle_V \, \langle \mathbf{w}_j, \mathbf{w}_\ell \rangle_W$$

### An important remark

If $\mathbf{v}_1 \perp \mathbf{v}_2$, then for all $\mathbf{w}_1, \mathbf{w}_2$: $\quad \mathbf{v}_1 \otimes \mathbf{w}_1 \perp \mathbf{v}_2 \otimes \mathbf{w}_2$

$(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ $\Big($ *resp.* $(\mathbf{w}_1, \ldots, \mathbf{w}_m)$ $\Big)$ be a basis of $V$ (*resp.* $W$).

**Linear Operator over tensor product of spaces**

Given $\mathbf{A}$, $\mathbf{B}$ be linear operator over $V$, $W$, $\mathbf{A} \otimes \mathbf{B}$ is a linear operator over $V \otimes W$ be defined (and extended by linearity) as

$$\mathbf{A} \otimes \mathbf{B} \left(\mathbf{v}_i \otimes \mathbf{w}_j\right) \stackrel{\text{def}}{=} \mathbf{A}\mathbf{v}_i \otimes \mathbf{B}\mathbf{w}_j$$

- **Characterization**,

$$\mathbf{C} \text{ linear operator over } V \otimes W \iff \exists \alpha_i, \mathbf{A}_i, \mathbf{B}_i \ : \ \mathbf{C} = \sum_i \alpha_i \ \mathbf{A}_i \otimes \mathbf{B}_i$$

**Classical Error:**

$\mathbf{C}$ linear operator over $V \otimes W$, then there exists $\mathbf{A}$, $\mathbf{B}$ linear operators over $V$ and $W$ s.t $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$.

**Tensor product of matrices**

Let $\mathbf{A} \overset{\text{def}}{=} (a_{i,j})_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} \in \mathbb{C}^{n\times m}$ and $\mathbf{B} \in \mathbb{C}^{p\times q}$, then

$$\mathbf{A} \otimes \mathbf{B} \overset{\text{def}}{=} \begin{pmatrix} a_{1,1}\mathbf{B} & a_{1,2}\mathbf{B} & \cdots & a_{1,m}\mathbf{B} \\ a_{2,1}\mathbf{B} & a_{2,2}\mathbf{B} & \cdots & a_{2,m}\mathbf{B} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}\mathbf{B} & a_{n,2}\mathbf{B} & \cdots & a_{n,m}\mathbf{B} \end{pmatrix} \in \mathbb{C}^{np\times mq}$$

**Example:**

1. $\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1\times 2 \\ 1\times 3 \\ 2\times 2 \\ 2\times 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 4 \\ 6 \end{pmatrix}.$

2. $\mathbf{X} \otimes \mathbf{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}$

**Properties: for any $\alpha \in \mathbb{C}$, $A, B \in \mathbb{C}^{m\times n}$ and $C, D \in \mathbb{C}^{p\times q}$**

1. $\alpha\,(A \otimes C) = (\alpha A) \otimes C = A \otimes (\alpha C)$,
2. $(A + B) \otimes C = A \otimes C + B \otimes C$,
3. $C \otimes (A + B) = C \otimes A + C \otimes B$,
4. If we can form matrix products **AC** and **BD**, then
$$(A \otimes B)\ (C \otimes D) = (AC) \otimes (BD)$$
5. If **A**, **B** are invertible, then $$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

**Classical Error:**

$$A \otimes B = B \otimes A.$$

- 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 Euclidean norm 1.

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

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

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

- Notation: for $b_1, \dots, b_n \in \{0,1\}$ and $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle$ be qubits

$$|b_1 b_2 \dots b_n\rangle \stackrel{\text{def}}{=} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \quad \text{and} \quad |\psi_1\rangle |\psi_2\rangle \dots |\psi_n\rangle \stackrel{\text{def}}{=} |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

- Characterization: any register $|\psi\rangle \in \mathbb{C}^{2^n}$ of $n$ qubits can be written as

$$|\psi\rangle = \sum_{\mathbf{x} \in \{0,1\}^n} \alpha_{\mathbf{x}} |\mathbf{x}\rangle \quad \text{where } \alpha_{\mathbf{x}} \in \mathbb{C} \text{ (called amplitude)} \quad \text{and} \quad \sum_{\mathbf{x} \in \{0,1\}^n} |\alpha_{\mathbf{x}}|^2 = 1.$$

- 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 Euclidean 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 $b_1, \ldots, b_n \in \{0,1\}$ and $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ be qubits

$$|b_1 b_2 \ldots b_n\rangle \stackrel{\text{def}}{=} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_n\rangle \quad \text{and} \quad |\psi_1\rangle |\psi_2\rangle \ldots |\psi_n\rangle \stackrel{\text{def}}{=} |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

- Characterization: any register $|\psi\rangle \in \mathbb{C}^{2^n}$ of $n$ qubits can be written as

$$|\psi\rangle = \sum_{\mathbf{x} \in \{0,1\}^n} \alpha_{\mathbf{x}} |\mathbf{x}\rangle \quad \text{where } \alpha_{\mathbf{x}} \in \mathbb{C} \text{ (called amplitude)} \quad \text{and} \quad \sum_{\mathbf{x} \in \{0,1\}^n} |\alpha_{\mathbf{x}}|^2 = 1.$$

**A remark: choose your orthonormal basis!**

From any $(|e_0\rangle, |e_1\rangle)$ orthonormal basis of $\mathbb{C}^2$, then $\left(\left|e_{i_1}\right\rangle \ldots \left|e_{i_n}\right\rangle\right)$ for $i_1, \ldots, i_n \in \{0,1\}^n$ is an orthonormal basis of $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = \mathbb{C}^{2^n}$.

**Exercise:**

1. Compute the scalar product between $|+\rangle\,|1\rangle$, $|00\rangle$ and $|11\rangle$ where $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$.
2. Let $(|e_0\rangle\,, |e_1\rangle)$ be an orthonormal basis of $\mathbb{C}^2$. Show that $\left(\left|e_{i_1}\right\rangle \ldots \left|e_{i_n}\right\rangle\right)$ for $i_1, \ldots, i_n \in \{0,1\}^n$ is an orthonormal basis of $\underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = \mathbb{C}^{2^n}$.
3. Do we have $|00\rangle + |10\rangle = (|0\rangle + |1\rangle) \otimes |0\rangle$?
4. (*) Do there exist two qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ such that
$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = |\psi_1\rangle \otimes |\psi_2\rangle\,.$$
5. Do there exists two qubits $|\psi_1\rangle$ and $|\psi_2\rangle$ such that
$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) = |\psi_1\rangle \otimes |\psi_2\rangle\,.$$

**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

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

$\rightarrow$ Entangled states play a crucial role in quantum computation/information (teleportation, quantum cryptography, ...)

- Measuring in the basis $|e_1\rangle |e_2\rangle \dots |e_n\rangle$:

$$|\psi\rangle = \sum_{i_1,\dots,i_n \in \{0,1\}^n} \alpha_{i_1\dots i_n} \left|e_{i_1}\right\rangle \cdots \left|e_{i_n}\right\rangle \overset{measure}{\longrightarrow} \left|e_{j_1}\right\rangle \dots \left|e_{j_n}\right\rangle \text{ with probability } |\alpha_{j_1\dots j_n}|^2$$

- Measuring the first register in the basis $(|e_0\rangle, |e_1\rangle)$

$$|\psi\rangle = \alpha_0 |e_0\rangle |\psi_0\rangle + \alpha_1 |e_1\rangle |\psi_1\rangle \overset{measure}{\longrightarrow} \begin{cases} |e_0\rangle |\psi_0\rangle \text{ with prob. } |\alpha_0|^2 \\ |e_1\rangle |\psi_1\rangle \text{ with prob. } |\alpha_1|^2 \end{cases}$$

Be careful: necessarily $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

**Exercise:**

Give the outcome distribution of measuring in the basis $(|bb'\rangle : b, b' \in \{0,1\})$ the first registers of the following two-qubits

$$|0\rangle \left(\sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right), \quad \sqrt{\frac{1}{2}}|01\rangle + \sqrt{\frac{1}{3}}|11\rangle + \sqrt{\frac{1}{6}}|10\rangle \quad \text{and} \quad \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

Unitary evolution $\mathbf{U} \in \mathbb{C}^{2^n \times 2^n}$ unitary matrix $\iff$ $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}_{2^n}$.

**Exercise:**

Is the following operator a unitary of $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Describe the image of $|bb'\rangle$ for $b, b' \in \{0, 1\}$.

# BRA-KET AND KET-BRA NOTATION

**Scalar Product:**

Let $|e_1\rangle, \ldots, |e_{2n}\rangle$ be an orthonormal basis, $|\psi\rangle \overset{\text{def}}{=} \sum_i \alpha_i |e_i\rangle$ and $|\varphi\rangle \overset{\text{def}}{=} \sum_i \beta_i |e_i\rangle$. Then

$$\langle\psi|\varphi\rangle \overset{\text{def}}{=} \sum_i \overline{\alpha_i}\beta_i.$$

- **Ket-notation:** $|\psi\rangle$ is called a ket
- **Bra-notation:** a ket $|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{2n} \end{pmatrix}$ is a vector of $\mathbb{C}^{2^n}$,

$$\langle\psi| \overset{\text{def}}{=} (|\psi\rangle)^\dagger = \begin{pmatrix} \overline{\alpha_1} & \ldots & \overline{\alpha_{2n}} \end{pmatrix} \text{ is a bra}$$

**Useful notation:**

$\longrightarrow$ It enables to interpret $\langle\psi|\varphi\rangle$ as $\langle\psi| \cdot |\varphi\rangle$.

| Bra | Ket |
|---|---|
| $\langle\psi\|$ | $\|\psi\rangle$ |

**The $|\varphi\rangle\langle\psi|$ operator**

$$\begin{aligned} |\varphi\rangle\langle\psi| : \left(\mathbb{C}^2\right)^{\otimes n} &\longrightarrow \left(\mathbb{C}^2\right)^{\otimes n} \\ \left|\psi'\right\rangle &\longmapsto |\varphi\rangle\langle\psi| \left|\psi'\right\rangle \overset{\text{def}}{=} \left\langle\psi|\psi'\right\rangle |\varphi\rangle \, . \end{aligned}$$

**Exercise:**

1. Give the image of $|0\rangle$ and $|1\rangle$ by $|0\rangle\langle 1| + |1\rangle\langle 0|$. Give the matrix representation of this operator. Do you recognize a quantum gate?
2. Let $(|i\rangle)$ be an orthonormal basis. Which operator is

$$\sum_i |i\rangle\langle i| \, .$$

**Adjoint of an operator**

$\mathsf{A}^\dagger$ is known as the adjoint of $\mathsf{A}$

**Exercise:**

1. Show that $(\mathsf{A}\,|\varphi\rangle)^\dagger = \langle\varphi|\,\mathsf{A}^\dagger$,
2. Show that $(|\varphi\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\varphi|$.

Be careful with adjoint/dagger over tensor product... (do not reverse the order...)

**Proposition:**

We have

$$(|\varphi\rangle\,|\psi\rangle)^\dagger = \langle\varphi|\,\langle\psi| \quad \text{and} \quad (\mathsf{A}\otimes\mathsf{B})^\dagger = \mathsf{A}^\dagger\otimes\mathsf{B}^\dagger$$

**Proof:**

See exercise session!

# EXERCISE SESSION