Le monde quantique

ADRIAN TANASĂ

LABRI, équipe Combinatoire

Talence

Plan du cours

1. Introduction - idée de base (les quantas)
2. Formulation mathématique
3. Postulats de la mécanique quantique
4. Le qubit
5. Cryptographie quantique

"The most incomprehensible thing about the world is that it is comprehensible"
Albert Einstein

Mécanique quantique

La mécanique quantique étudie et décrit les phénomènes fondamentaux à l'œuvre dans les systèmes physiques de petite échelle, comme par exemple l'échelle atomique et subatomique.

profondes difficultés conceptuelles :

- la *dualité onde corpuscule*,
  longueur d'onde de de Broglie :

$$\lambda = \frac{h}{p}$$

  $h = 6,626^{-34} J \cdot s$ - constante de Planck
- la *superposition quantique*,
- l'*intrication quantique* (cours prochain)
- *etc.*

Physique quantique

L'expression *physique quantique* désigne le corpus théorique plus étendu qui s'appuie sur la mécanique quantique pour décrire certains phénomènes, dont les interactions fondamentales.

physique de particules élémentaire *etc.*

Idée centrale - quantas

existence de grandeurs physiques ne pouvant se manifester que par multiples de quantités fixes, appelés quanta, qui donnent leur nom à la théorie.

exemple de quanta : les photons
Ces grandeurs physiques sont par exemple l'énergie ou le moment cinétique des particules.

illustration : la structure de l'atome - organisation des électrons autour du noyau.
les électrons se répartissent en occupant les places laissées libres par les valeurs possibles des nombres quantiques liés à leur énergie et leur moment cinétique.
Cette organisation permet d'expliquer le comportement chimique et spectroscopique des éléments naturels.

Produit scalaire

Soit $\mathcal{H}$ un espace vectoriel sur le corps des nombres complexes $\mathbb{C}$. On appelle "produit scalaire" sur $\mathcal{H}$ toute application de $\mathcal{H} \times \mathcal{H}$ dans $\mathbb{C}$, notée :

$$(u, v) \mapsto (u|v)$$

qui vérifie les propriétés suivantes :

Produit scalaire

linéarité à droite :pour tous $u, v_1, v_2 \in \mathcal{H}, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(u|\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (u|v_1) + \lambda_2 (u|v_2) \tag{1}$$

anti-linéarité à gauche :pour tous $u_1, u_2, v \in \mathcal{H}, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(\lambda_1 u_1 + \lambda_2 u_2|v) = \overline{\lambda_1}(u_1|v) + \overline{\lambda_2}(u_2|v) \tag{2}$$

symétrie hermitienne :pour tous $u, v \in \mathcal{H}$

$$(u|v) = \overline{(v|u)} \tag{3}$$

Remarquons que :
(1) et (3) entrainent (2) ; (3) entraine que $(u|u)$ est un nombre réel.

positivité :pour tout $u \in \mathcal{H}$

$$(u|u) \geq 0 \tag{4}$$

non-dégénérescence :pour tout $u \in \mathcal{H}$

$$\forall v \in \mathcal{H}, (u|v) = 0 \Rightarrow u = 0 \tag{5}$$

Produit scalaire

Cette dernière propriété, sachant que $(*|*)$ est positif, revient à énoncer que

$$\forall u \in \mathcal{H}, (u|u) = 0 \Rightarrow u = 0. \tag{6}$$

Espace pré-hilbertien et espace de Hilbert

On appelle *espace pré-hilbertien* tout espace vectoriel $\mathcal{H}$ sur $\mathbb{C}$ muni d'un produit scalaire $(*|*)$ vérifiant les propriétés ci-dessus.

Lorsque $\mathcal{H}$ est de dimension finie, il s'agit d'un espace *de Hilbert* (cette notion est en fait plus générale : un espace de Hilbert est, par définition, un espace pré-Hilbertien, qui est complet et qui admet une partie dénombrable dense).

On fixe un espace de Hilbert de dimension finie $\mathcal{H}$.

quand on travaille avec des espaces de Hilbert de dimensions infinie, on fait de la

théorie quantique de champs (2ème quantification)

Formes linéaires sur un espace de Hilbert - espace dual

$\mathcal{H}^*$, le dual de $\mathcal{H}$, est l'espace des formes linéaires sur $\mathcal{H}$:
$\mathcal{H}^* := \mathcal{L}(\mathcal{H}, \mathbb{C})$.

$\mathcal{H}$ admet au moins une base orthonormée i.e. une famille de vecteurs $e_1, e_2, \ldots, e_n$ qui est une base t. q.

$$\forall i, j \in [1, n], (e_i | e_j) = \delta_i^j$$

Fixons une base orthonormée de $\mathcal{H}$. Si les vecteurs u, v ont pour coordonnées respectives $X, Y \in \mathbb{M}_{n,1}(\mathbb{C})$ dans cette base, alors leur produit scalaire vaut le produit matriciel

$$(u, v) = X^\dagger \cdot Y.$$

Autrement écrit : si

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_k \\ \vdots \\ k_n \end{pmatrix}$$

alors

$$X^\dagger = \begin{pmatrix} \bar{x}_1 & \dots & \bar{x}_k & \dots & \bar{x}_n \end{pmatrix}$$

$$(u, v) = \sum_{k=1}^{n} \bar{x}_k \cdot y_k.$$

Application adjointe sur un espace de Hilbert

Considérons une application linéaire $L : \mathcal{H} \to \mathcal{H}$.
L'application adjointe, L^* est définie par :

$$\forall u, v \in \mathcal{H}, (u, Lv) = (L^* u, v). \tag{7}$$

On vérifie que si M est la matrice de L dans une bases orthonormée $\mathcal{E}$, alors la matrice de L^* dans la même base est $M^\dagger$ définie par

$$M = (m_{i,j})_{i,j\in[1,n]}, \quad M^\dagger := (\bar{m}_{j,i})_{i,j\in[1,n]}.$$

Applications hermitiens et unitaires

1. L est *hermitien* ssi

$$\forall u, v \in \mathcal{H}, (u, Lv) = (Lu, v)$$

ce qui revient à $L = L^*$ ou encore au fait que sa matrice M (dans une base orthonormée) vérifie $M = M^\dagger$.

2. L est *unitaire* ssi

$$\forall u, v \in \mathcal{H}, (Lu, Lv) = (u, v)$$

ce qui revient à

$$L^* L = \mathrm{Id}_{\mathcal{H}},$$

ou encore au fait que sa matrice M (dans une base orthonormée) vérifie

$$M \cdot M^\dagger = \mathrm{I}_n.$$

Notation de Dirac

universellement utilisée dans les ouvrages de mécanique quantique.
Décidons de noter

$$|u\rangle, |v\rangle, |w\rangle, |0\rangle, |1\rangle, \ldots$$

les vecteurs de $\mathcal{H}$, puis de noter

$$\langle u|, \langle v|, \langle w|, \langle 0|, \langle 1|, \ldots$$

leurs images par G.
Autrement dit, nous utilisons maintenant un alphabet *typé* où chaque lettre de la forme $|\ldots\rangle$ est un élément de $\mathcal{H}$ et chaque lettre de la forme $\langle\ldots|$ est un élément de $\mathcal{H}^*$ et enfin les deux alphabets sont liés par une bijection $|u\rangle \mapsto \langle u|$.

$$(u|v) = \langle u|v\rangle$$

Notation de Dirac

Soit $L \in \mathcal{L}(\mathcal{H}, \mathcal{H})$.

La notation

$$\langle u| L |v\rangle \tag{8}$$

signifie : la forme $\langle u|$ appliquée à l'argument $L(|v\rangle)$

Mais si nous déplaçons les parenthèses d'un cran vers la gauche, la notation devient

$$(\langle u| L)\, |v\rangle$$

qui signifie : la forme $\langle u|\, L$ appliquée à l'argument $|v\rangle$

résultat identique à celui du premier parenthésage.

Notation de Dirac

la traduction sous forme matricielle du produit $\langle u| L |v\rangle$ donne

$$X^\dagger \cdot M \cdot Y$$

que l'on utilise le premier ou le second parenthésage (car la matrice de L^* est $M^\dagger$ ce qui fait que $(M^\dagger X)^\dagger = X^\dagger \cdot M$).

l'oubli de parenthèses dans les expressions à trois arguments $\langle u| L |v\rangle$ n'induit pas d'ambiguité (i.e. cette notation ne désigne bien qu'un seul nombre complexe).

Notation de Dirac - opérateurs (applications linéaires)

$$|v\rangle \langle u| \tag{9}$$

opérateur (application linéaire) :

$$|w\rangle \mapsto |v\rangle \langle u| |w\rangle = |v\rangle (\langle u|w\rangle)$$

(9) désigne l'application linéaire :

$$|w\rangle \mapsto \langle u|w\rangle |v\rangle$$

Notation de Dirac - décompositions d'opérateurs

Si $|u_1\rangle, \ldots, |u_k\rangle, \ldots, |u_n\rangle$ est une base orthonormée de vecteurs propres de L, avec

$$L|u_k\rangle = \lambda_k |u_k\rangle$$

alors

$$L = \sum_{k=1}^{n} \lambda_k |u_k\rangle \langle u_k| \tag{10}$$

Produit tensoriel

la forme associée au vecteur $|u\rangle \otimes |v\rangle$ est $\langle u| \hat{\otimes} \langle v|$

ou

$$\langle u \otimes v| = \langle u| \hat{\otimes} \langle v|$$

puis,

$$\langle u \otimes v| = \langle u| \otimes \langle v| . \tag{11}$$

Produit tensoriel - exo

Soit e_1, e_2 une base de l'espace vectoriel E_2 et soit deux vecteurs de E_2 :

$$X = 2e_1 + 4e_2, \;\; Y = 5e_1 + 3e_2$$

Soit $e_i \otimes e_j$ les vecteurs de la base de l'espace $E_2 \otimes E_2$.

$$X \otimes Y = (2e_1 + 4e_2) \otimes (5e_1 + 3e_2) \tag{12}$$

$$= 10e_1 \otimes e_1 + 6e_1 \otimes e_2 + 20e_2 \otimes e_1 + 12e_2 \otimes e_2 \tag{13}$$

Postulats de la mécanique quantique

1. Principe de superposition
L'état d'un système quantique est défini par un vecteur (un ket) qui est une combinaison linéaire, avec des coefficients complexes, d'états de base.
exemple : états de base : $|0>$ et $|1>$,
état quantique : $|\psi>= c_0|0> + c_1|1>$
N états de base : $|0>, |1>, \ldots, |N-1>$
$|\psi>= c_0|0> + c_1|1> + \ldots + c_{N-1}|N-1>$

$$|\psi>= \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{N-1} \end{pmatrix}$$

2. Principe de correspondance

Les observables physiques (c'est-à-dire les "choses qu'on mesure") sont représentées par des opérateurs mathématiques, appelés observables.

$$\hat{\mathcal{O}}$$

3. Principe de quantification

Les mesures ne peuvent pas donner d'autres résultats que ceux qui correspondent à des valeurs propres de ces opérateurs mathématiques. Les vecteurs propres qui correspondent à ces valeurs propres forment une base de l'espace des états du système.

$$\hat{\mathcal{O}}|\alpha_n >= \alpha_n|\alpha_n >$$

$\hat{\mathcal{O}}$ - l'observable
$|\alpha_n >$ - vecteur propre
α_n - valeur propre

4. Règle de Born - principe de décomposition spectrale

Les calculs mathématiques fournissent la probabilité d'observer tel ou tel résultat de mesure.
La mesure d'une grandeur physique représentée par l'observable $\hat{\mathcal{O}}$, effectuée sur l'état quantique $|\psi(t)\rangle$, donne le résultat a_n, avec la probabilité $P_n = |c_n|^2$.

5. Principe de réduction du paquet d'onde

La mesure modifie l'état du système quantique mesuré de manière à faire disparaître les probabilités qui ne se sont pas réalisées.

Postulat VI - equation de Schrödinger

$$i\hbar\frac{d\Psi(x,t)}{dt} = H\Psi(x,t)$$

Erwin Schrödinger
Nobel Prize, 1933

Erwin Schrödinger (1887 - 1961) : physicien et philosophe autrichien.

Postulat VI

L'évolution dans le temps du système quantique est donnée par l'équation de Schrödinger :
l'état $|\psi(t)\rangle$ de tout système quantique est une solution de l'équation de Schrödinger dépendante du temps :

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = \hat{\mathcal{H}}|\psi(t)\rangle \tag{14}$$

où $\mathcal{H}$ est l'Hamiltonien du système

Retour sur le qubit

Le qubit

La différence essentielle avec l'état classique $0/1$ est que le qubit peut se trouver dans d'autres états (une infinité) que les états $|0\rangle$ ou $|1\rangle$. Tout état de la forme

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

où α et β sont deux nombres complexes ($|\alpha|^2 + |\beta|^2 = 1$, , est accessible au qubit.

l'état du qubit est un vecteur d'un espace vectoriel complexe de dimension 2 dans lequel les éléments $|0\rangle$ et $|1\rangle$ forment une base

Et si on mesure un qubit ?

Que trouve-t-on si on cherche à lire le contenu du qubit, si on le *mesure* ? On trouvera 0 s'il est dans l'état $|0\rangle$ et 1 s'il est dans l'état $|1\rangle$.

s'il est dans l'état $|\psi\rangle$? On trouvera 0 ou 1 mais de façon aléatoire. En fait on aura 0 avec la probabilité $|\alpha|^2$ ou 1 avec la probabilité $|\beta|^2$
On ne peut donc pas observer directement l'état de superposition $|\psi\rangle$ du qubit !

Et si on mesure un qubit ?

De plus, une fois qu'il a été mesuré, l'état du qubit est projeté dans l'état correspondant au résultat de la mesure.

exemple : si le qubit, originellement dans l'état $|\psi\rangle$, est mesuré et que le résultat est 1, le qubit se trouvera alors projeté dans l'état $|1\rangle$ et toute nouvelle mesure donnera immanquablement le résultat 1.

Base du calcul quantique

Ce qui constitue la base du *calcul quantique* c'est de modifier l'état du qubit, en lui appliquant des portes logiques ou en l'associant à un ou plusieurs autres qubits, sans le mesurer, c'est à dire sans le projeter sur les états $|0\rangle$ | ou $|1\rangle$.

C'est seulement à la fin du calcul que le qubit est lu et si l'algorithme est bien choisi le processus de projection que réalise la mesure finale du qubit permet d'extraire l'information recherchée.

Réalisation d'un qubit - états internes d'un atome

on considère deux niveaux de l'atome :

1. le niveau fondamental : c'est celui de plus basse énergie ; l'état quantique de l'atome est noté $|g\rangle$ (ground state) et son énergie E_g.
2. le premier niveau excité ; l'état atomique est noté $|e\rangle$ et son énergie E_e.

Réalisation d'un qubit - états internes d'un atome

Si on envoit sur l'atome dans son état fondamental un photon d'énergie exactement $E_e - E_g$ le photon est absorbé par l'atome qui passe dans le niveau excité :

$$|g\rangle \rightarrow |e\rangle$$

Les énergies mises en jeu à l'échelle atomique sont de l'ordre de l'électron-volt (1.6×10^{-19} J) ; le rayonnement lumineux associé au photon a une longueur d'onde $\lambda = \frac{c}{\nu} = \frac{hc}{E_e - E_g}$ où c est la vitesse de la lumière (3×10^8 ms^{-1}) et h la constante de Planck (6.6×10^{-34} Js) ; l'ordre de grandeur des longueurs d'onde correspondant aux énergies atomiques de l'ordre d'un eV est entre 0.4 et 1 μm ; c'est le domaine de la lumière visible.

Réalisation d'un qubit - états internes d'un atome

L'atome revient dans son état fondamental au bout d'un temps moyen appelé *durée de vie du niveau excité*, en émettant un photon de même énergie $E_e - E_g$ (émission spontanée). La durée de vie d'un niveau atomique varie de quelques nanosecondes à la seconde.

Réalisation d'un qubit - états internes d'un atome

Si on envoit un photon d'énergie $E_e - E_g$ sur l'atome quand il est encore dans l'état excité l'atome va se désexciter en émettant un photon à la même énergie - émission induite

Supposons qu'on éclaire continuellement l'atome avec cette radiation lumineuse composée de photons d'énergie $E_e - E_g$ (radiation résonante), l'atome va osciller entre l'état $|g\rangle$ à l'état $|e\rangle$. A l'instant t il sera dans un état de superposition

$$|\psi\rangle = \cos(\omega t/2)\,|g\rangle + \sin(\omega t/2)e^{i\phi}\,|e\rangle \tag{15}$$

l'atome est un qubit : on associe à l'état $|g\rangle$ l'état $|0\rangle$ et à l'état $|e\rangle$ l'état $|1\rangle$

Réalisation d'un qubit - états internes d'un atome (mesure)

Pour mesurer l'état de l'atome à un moment donné on envoie sur celui-ci une impulsion laser "accordée" sur une transition $|g\rangle \rightarrow |a\rangle$ qui n'a pas d'équivalent à partir de l'état $|e\rangle$.

Si le photon est absorbé c'est que le système est dans l'état $|g\rangle$ sinon il est dans l'état $|e\rangle$.

Réalisation d'un qubit - polarisation d'un photon

Une onde électromagnétique, la lumière par exemple, peut être représentée mathématiquement par un champs vectoriel transverse, i.e. orthogonal à la direction de propagation. Dans un référentiel $(O, \hat{e_x}, \hat{e_y}, \hat{e_z})$, de coordonnés (x, y, z), choisi tel que l'onde se propage selon l'axe des z , le champ électrique est décrit par

$$\overline{E}(t, z) = \overline{E}_0 e^{i(\omega t - kz)}$$

où $\overline{E}_0 = E_{0x}\hat{e_x} + E_{0y}\hat{e_y}$. Le vecteur $\overline{E}_0$, vu comme un nombre complexe, définit la *polarisation* de l'onde. L'intensité de l'onde est proportionnelle au module au carré de $\overline{E}_0$: $\|\overline{E}_0\|^2$.

Réalisation d'un qubit - polarisation d'un photon

La polarisation peut être mise en évidence à l'aide de cristaux ayant une propriété optique particulière : la biréfringence. Si nous envoyons sur une lame biréfringente un faisceau d'intensité I, polarisé linéairement suivant une direction qui fait un angle θ avec l'axe ordinaire du cristal qu'on prend comme axe Ox : le faisceau est séparé en un faisceau polarisé suivant Ox d'intensité $I\cos^2\theta$ et un autre faisceau polarisé suivant Oy d'intensité $I\sin^2\theta$.

Réalisation d'un qubit - polarisation d'un photon

Planck et Einstein ont suggéré au début du XXème siècle que la lumière puisse aussi être décrite en termes de flot de *photons* (les quantas de l'électromagnetisme).

Les sources de lumière "classiques" émettent des grandes quantités de photons même pour des faibles intensités (plusieurs milliards de milliards de photon à la seconde pour une lampe de 1W) ce qui fait que l'aspect "corpusculaire" de la lumière est difficile à mettre en évidence.

L'avènement récent de l'optique quantique et des nanotechnologies a permis de développer des sources qui émettent des photons "un par un", c'est à dire séparés par des intervalles de temps mesurables avec la technologie actuelle (nanoseconde).

Réalisation d'un qubit - polarisation d'un photon

le photon est un "objet quantique" ; on associe un état quantique à chaque vecteur de base de polarisation de l'onde : $|x\rangle$ pour l'état de polarisation suivant l'axe Ox et $|y\rangle$ pour l'état de polarisation suivant l'axe Oy.

À l'orientation θ de la polarisation on associe l'état

$$|\theta\rangle = \cos\theta\ |x\rangle + \sin\theta\ |y\rangle \tag{16}$$

Réalisation d'un qubit - polarisation d'un photon

Quelle trajectoire va suivre le photon qui se trouve dans cet état ? La réponse de la mécanique quantique est qu'*on ne peut pas le savoir*. Mais ce qu'on peut connaitre (postulat de la mesure) c'est la probabilité que le photon sorte polarisé suivant x et qui est donnée par $\cos^2\theta$ et la probabilité complémentaire qu'il sorte polarisé suivant y, donnée par $\sin^2\theta$. Donc, en moyenne, si N est le nombre total de photons qui traversent la lame, on en trouvera $N\cos^2\theta$ sortant avec la polarisation Ox et $N\sin^2\theta$ sortant avec la polarisation Oy. Les coefficients $\cos\theta$ et $\sin\theta$ sont en fait des *amplitudes de probabilité* de trouver le photon dans l'état $|x\rangle$ ou $|y\rangle$ respectivement.

Réalisation d'un qubit - polarisation d'un photon

On peut associer un qubit à chacun des deux états de polarisation du photon, par exemple

$$\begin{aligned} |x\rangle &\rightarrow |0\rangle \\ |y\rangle &\rightarrow |1\rangle \end{aligned}$$

En jouant sur l'orientation du polariseur et sur le type de polarisation (linéaire, circulaire, elliptique) on peut construire là aussi un état quelconque de superposition $\alpha |0\rangle + \beta |1\rangle$.

Qubits et mécanique quantique

Les états du systéme quantique associé à un qubit sont les éléments d'un espace à deux dimensions, engendrés par les états de la base $|0\rangle$ et $|1\rangle$ Tout état sera donc de la forme

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{17}$$

On retrouve donc là la spécificité des qubits de pouvoir se trouver dans un état de superposition.

les coefficients α et β sont en fait des amplitudes de probabilités et doivent satisfaire

$$|\alpha|^2 + |\beta|^2 = 1.$$

Représentations d'un état

1. par une fonction $\psi(\mathbf{r}, t)$ (formalisme des fonctions d'ondes et de la mécanique ondulatoire)
2. par une matrice (notamment dans le cas d'espaces de dimensions finies)

Représentation matricielle d'un espace à 2 dimensions

$$|0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad |1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{18}$$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{19}$$

Qubits et observables

les états $|0\rangle$ et $|1\rangle$ sont les états propres d'une grandeur observable. Si le système physique est un atome l'observable est l'énergie de l'atome et les états $|0\rangle$ et $|1\rangle$ correspondent aux états $|g\rangle$ et $|e\rangle$ (état fondamental et premier état excité) de l'atome. Dans le cas où le système quantique est le photon l'observable est la polarisation qui peut prendre les deux état $|x\rangle$ et $|y\rangle$. Comme ces états forment une base dans l'espace des états du qubit, on a $\forall\, |\psi\rangle \in \mathcal{E} \quad |\psi\rangle = \alpha\, |0\rangle + \beta\, |1\rangle\,.$

Qubits et mesure

si le système est dans l'état

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

le résultat de la mesure sera obtenu avec une probabilité dont *l'amplitude* est définie par

$$\begin{aligned} \alpha &= \langle 0\,|\psi\rangle \quad && \text{amplitude de probabilité d'obtenir l'état } |0\rangle \\ \beta &= \langle 1\,|\psi\rangle \quad && \text{amplitude de probabilité d'obtenir l'état } |1\rangle \end{aligned}$$

Manipulations de qubits

la mesure altère en général l'état d'un qubit puisqu'il en sort nécessairement dans un état propre de l'observable mesuré.

Par contre l'environnement peut agir sur le qubit pour faire évoluer son état tant qu'aucune mesure (aucune "prise d'information") n'est réalisée.

Opérations logiques sur un qubit

Nous allons associer à l'évolution de l'état du qubit les opérations logiques nécessaires à la mise en oeuvre d'algorithmes.

Portes logiques classiques

Par exemple les portes logiques classiques agissant sur un bit sont résumées dans le tableau ci-dessous

Porte logique $\backslash$ b_{in}	0	1
EFFACE	0	0
IDENTITE	0	1
NON	1	0
SET	1	1

Portes logiques et qubits

toute matrice unitaire est susceptible de représenter une porte logique à un qubit.

différence avec les bits classiques -
pour les qubits il existe donc une famille *continue* de transformations qui sont représentées par les matrices unitaires.

Exemples - l'opérateur NOT

l'opérateur *NON* est représenté par la matrice carrée

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

On peut vérifier que cette matrice est bien unitaire :

Exemples - l'opérateur NOT

l'opérateur *NON* est représenté par la matrice carrée

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

On peut vérifier que cette matrice est bien unitaire :

$$X \cdot X^{\dagger} = X^{\dagger} \cdot X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et on peut vérifier que $X|0\rangle = |1\rangle$ et que $X|1\rangle = |0\rangle$

Exemples - l'opérateur NOT

l'opérateur *NON* est représenté par la matrice carrée

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

On peut vérifier que cette matrice est bien unitaire :

$$X \cdot X^{\dagger} = X^{\dagger} \cdot X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et on peut vérifier que $X|0\rangle = |1\rangle$ et que $X|1\rangle = |0\rangle$

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Exemples - la porte Y

la porte Y définie par la matrice

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

On a :

$$\begin{aligned} |0\rangle &\rightarrow i\,|1\rangle \\ |1\rangle &\rightarrow -i\,|0\rangle \end{aligned}$$

Exemples - la porte Z (opérateur de flip)

la porte Z définie par la matrice $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

On a :

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow -|1\rangle \end{aligned}$$

Exemples - la porte ϕ

La porte ϕ définie par la matrice $R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{\imath\phi} \end{pmatrix}$

effet : rotation de la phase du vecteur $|1>$ par un angle ϕ :

$$\begin{aligned} R_\phi|0> &= |0>, \\ R_\phi|1> &= e^{\imath\phi}|1> . \end{aligned} \tag{20}$$

Remarque. $Z = R_\pi$, car $e^{\imath\pi} = -1$.

Exemples - la porte de Hadamard

porte particulièrement importante en info quantique
La porte de *Hadamard* définie par la matrice

$$H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

On a :

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Si on applique H à l'état initial $|0\rangle$ ou à l'état initial $|1\rangle$ et puis on mesure, on a des probabilités égales pour trouver $|0\rangle$ ou $|1\rangle$.

Interférence et porte de Hadamard

$$H\left(\frac{1}{\sqrt{2}}(|0>+|1>)\right)=\frac{1}{\sqrt{2}}H|0>+\frac{1}{\sqrt{2}}H|1>=|0> \qquad (21)$$

effet analogue à l'interférence des ondes

Exo

Exo.
Vérifiez que tous ces matrices correspondent à des opérateurs unitaires.