MÉCANIQUE QUANTIQUE

COURS 11 & 12 – INTRODUCTION À L'INFORMATION QUANTIQUE

QUENTIN GLORIEUX

3P001 – UNIVERSITÉ PIERRE ET MARIE CURIE 2015-2016

INTRODUCTION À L'INFORMATION QUANTIQUE

- Notion de qubit
- Etats séparables, états intriqués
- Argument EPR : La mécanique quantique est elle complète ?
- Portes quantiques et théorème de non-clonage
- Applications (cours 12)
  - Codage dense
  - Cryptographie quantique
  - Téléportation quantique

NOTIONS DE QUBIT

On va s'intéresser aujourd'hui aux systèmes à deux niveaux.

On a déjà vu au moins 3 de ces systèmes :

- Un particule de spin 1/2
- La polarisation d'un photon
- L'orientation de la molécule d'ammoniac

Pour chacun de ces systèmes nous connaissons un appareil de mesure et plusieurs bases pour les décrire (respectivement):

- Appareil de Stern et Gerlach : $|+\rangle_z, |-\rangle_z$ ou $|+\rangle_x, |-\rangle_x$
- Polariseur : $|H\rangle, |V\rangle$ ou $|D\rangle, |A\rangle$

NOTIONS DE QUBIT

Un qubit est le vecteur d'état d'un système à deux niveaux :

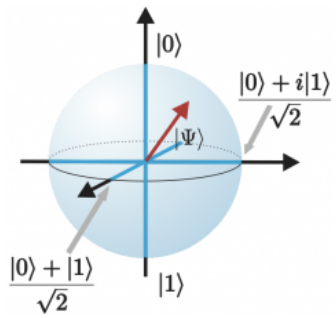
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Cette écriture correspond à une base donnée : base de computation

Un qubit peut se représenter dans la sphère de Bloch

Plus riche qu'un bit classique 0,1 du fait du principe de superposition !

Information quantique = utilisation des qubits pour améliorer des protocoles classiques



PRODUIT TENSORIEL

Comment décrir un système de 2 qubits ?

- On utilise le formalisme du produit tensoriel

Prenons un système quantique (a) dans l'état $|\psi_a\rangle$ de l'espace $\mathcal{E}_a$
Et un système quantique (b) dans l'état $|\psi_b\rangle$ de l'espace $\mathcal{E}_b$

Le système global comprenant le système (a) et le système (b) est noté : $|\psi_a\rangle \otimes |\psi_b\rangle$ ou $|\psi_a\rangle|\psi_b\rangle$ ou même $|\psi_a, \psi_b\rangle$

L'espace vectoriel associé est appelé espace produit tensoriel : $\mathcal{E}_a \otimes \mathcal{E}_b$

- Généralisation :
  On note $|\alpha_m\rangle$ une base de $\mathcal{E}_a$ et $|\beta_n\rangle$ une base de $\mathcal{E}_b$.
  La forme général d'un élément de $\mathcal{E}_b \otimes \mathcal{E}_b$ est :

$$|\phi\rangle = \sum c_{m,n} |\alpha_m\rangle \otimes |\beta_n\rangle$$

DIMENSION ?

QUELQUES PROPRIÉTÉS

- Produit scalaire hermitien dans $\mathcal{E}_H = \mathcal{E}_a \otimes \mathcal{E}_b$
  Si $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$ et $|\psi'\rangle = |\alpha'\rangle \otimes |\beta'\rangle$ alors $\langle\psi|\psi'\rangle = \langle\alpha|\alpha'\rangle\langle\beta|\beta'\rangle$.
- Action des opérateurs dans $\mathcal{E}_H = \mathcal{E}_a \otimes \mathcal{E}_b$
  $\hat{A}$ et $\hat{B}$ agissant respectivement dans $\mathcal{E}_a$ et $\mathcal{E}_b$, on définit $\hat{A} \otimes \hat{B}$
  par $(\hat{A} \otimes \hat{B})|\alpha\rangle \otimes |\beta\rangle = (\hat{A}|\alpha\rangle) \otimes (\hat{B}|\beta\rangle)$.
- Quelques abus de notation très fréquents :
  - $\hat{A} \otimes \hat{I}_b$ est simplement noté $\hat{A}$
  - $\hat{A} \otimes \hat{B}$ est simplement noté $\hat{A}\hat{B}$
  - $|a : \alpha\rangle \otimes |b : \beta\rangle = |\alpha\rangle \otimes |\beta\rangle = |\alpha\rangle|\beta\rangle = |\alpha, \beta\rangle$
- On n'échange pas l'ordre de a et b pour le bra :
  - $\langle a : \alpha| \otimes \langle b : \beta| = \langle\alpha| \otimes \langle\beta| = \langle\alpha|\langle\beta| = \langle\alpha, \beta|$

DEUX EXEMPLES

- Une particule de spin ½ et sa fonction d'onde :
  - Si on prend en compte la fonction d'onde d'une particule de spin ½ l'état global du système est : $|\psi\rangle \otimes |s\rangle$
  - L'espace produit tensoriel est : $\mathcal{L}^2(R)^3 \otimes \mathcal{E}_{spin}$

- Deux particules de spin ½ (sans prendre en compte les degrés de liberté externe : la fonction d'onde) :
  - Produit tensoriel de deux espaces de dimensions 2
    Espace de dimension 4
    Ecriture générale : (ne pas oublier la normalisation)

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

INTRICATION

La forme générale d'un état de 2 qubits est :

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

Il existe deux types d'états : séparables ou intriqués.

- Etats séparables :
  On dit qu'un état de $\mathcal{E}_a \otimes \mathcal{E}_b$ est séparable (ou factorisable) s'il peut se mettre sous la forme : $|\alpha\rangle \otimes |\beta\rangle$
  avec $|\alpha\rangle$ dans $\mathcal{E}_a$ et $|\beta\rangle$ dans $\mathcal{E}_b$
  - De façon générale $|\phi\rangle = \sum c_{m,n}|\alpha_m\rangle \otimes |\beta_n\rangle$ est factorisable ssi $c_{m,n} = a_m b_n$

- Un état intriqué est un état non-factorisable !
  - en anglais : *entangled*

QUIZZ INTRICATION

COMMENT COMPRENDRE L'INTRICATION ?

Prenons l'état $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

Il s'agit d'un état intriqué (non factorisable)

Donnons le premier qubit à Alice et le second à Bob :

- Avant la mesure Alice et Bob ont 50/50 de trouver le résultat 0 ou 1.
- Si lors d'une mesure Alice trouve l'état 0, cela force Bob à trouver le résultat 1 (et réciproquement).

Pour cette situation il est possible de trouver un « équivalent » classique

Que se passe-t-il lors d'une mesure dans une autre base ?

- Exemple de la mesure du spin

ARGUMENT EPR

Un article de 1935 de Einstein, Podolsky et Rosen (EPR) pose la question suivante :

- *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*

Einstein était choqué par l'intrication et ses conséquences et il propose en 1935 que la théorie quantique est incomplète, il nous manque un 'élément de réalité' : une variable cachée

Bohr pulie la même année un article :

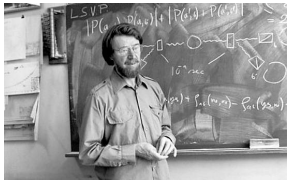
- *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*

où il assure que la mécanique quantique est complète : pas de variables cachées !

INÉGALITÉS DE BELL & EXPÉRIENCES D'ORSAY

Il est possible de répondre à cette question par l'expérience !

- John Bell a écrit un article mathématique en 1964 qui donne une inégalité lors de la mesure d'une grandeur physique que toutes théories incluant des variables cachées doit satisfaire



- En 1982, Alain Aspect, Philippe Grangier et Jean Dalibard réalisent une expérience qui mesure cette grandeur physique et donne une réponse définitive à la controverse de presque 50 ans entre Eisntein et Bohr !
- SUSPENSE MAXIMAL ! Réponse au TD 14

INTRODUCTION À L'INFORMATION QUANTIQUE

- Notion de qubit
- Etats séparables, états intriqués
- Argument EPR : La mécanique quantique est elle complète ?
- **Portes quantiques et théorème de non-clonage**
- Applications (cours 12)
  - Codage dense
  - Cryptographie quantique
  - Téléportation quantique

PORTES QUANTIQUES

Une porte est une opération unitaire de l'espace dans lequel est définit le système.

On s'intéresse tout d'abord aux portes à 1 qubit : dans ce cas une porte est une matrice 2x2 tq U*U=UU*=I

Exemples :

- Porte Pauli X : échange $|0\rangle$ et $|1\rangle$ - Matrice : $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- Porte Pauli Z : échange le signe de $|1\rangle$ - Matrice : $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Porte Hadamard : $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Quel est l'effet de la porte Hadamard ?

PORTE À 2 QUBITS

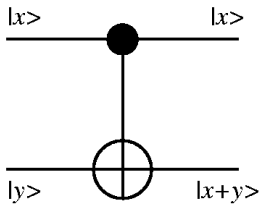
On peut construire des portes plus complexes qui impliquent plusieurs qubits.

Pour une porte à deux qubits, l'espace de Hilbert est de dimension 4, on a donc des matrices unitaires de taille 4x4.

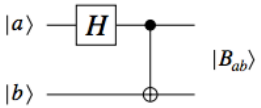
Exemple : la porte control-not $\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Que fait-elle ?

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$



QUIZZ HADAMARD+C-NOT



MESURE SUR UN ESPACE PRODUIT TENSORIEL

Nous avons vu des opérations unitaires.

La mesure en mécanique quantique n'est pas unitaire, comment décrire la mesure en information quantique ?

Soit une grandeur physique A associée à l'observable $\hat{A}$ agissant sur $\mathcal{E}_a$

On a définit valeurs propres et vecteurs propres : $\hat{A}|\psi_n\rangle = a_n|\psi_n\rangle$

Prenons un système composé de deux sous-système (a) et (b)

- Les seuls résultats possibles d'une mesure de A sur le sous-systéme (a) sont les a_n
- Si on mesure a_n alors le nouvel état du système global est :

$$|\Psi'\rangle = \left(|\psi_n\rangle\langle\psi_n| \otimes \hat{I}_b\right)|\Psi\rangle$$ Ne pas oublier la normalisation

- La probabilité de trouver a_n est $\mathcal{P}(a_n) = \||\Psi'\rangle\|^2$

EXEMPLE DE MESURE

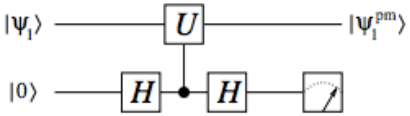
Un exemple simple :

- On part de l'état général : $|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$
- On effectue une mesure sur le premier qubit et on obtient la valeur propre associée à l'état $|0\rangle$ (on dit que l'on mesure le qubit dans $|0\rangle$)
- Le nouvel état du système est alors : $(|0\rangle\langle 0| \otimes \hat{I})|\psi\rangle$

Soit : $\dfrac{c_{00}|00\rangle + c_{01}|01\rangle}{\sqrt{|c_{00}|^2 + |c_{01}|^2}}$ ou encore $|0\rangle \otimes \dfrac{c_{00}|0\rangle + c_{01}|1\rangle}{\sqrt{|c_{00}|^2 + |c_{01}|^2}}$

On voit que faire une mesure peut détruire l'intrication !

Un exemple plus compliqué:



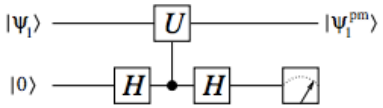
MESURE PROJECTIVE

On veut mesurer un observable U qui agit sur le qubit $|\psi_1\rangle$ pour donner les résultats +/- 1

On note $|\psi_+\rangle, |\psi_-\rangle$ les deux vecteurs propres associées à ces résultats.

De manière générale on peut écrire $|\psi_1\rangle = c_+|\psi_+\rangle + c_-|\psi_-\rangle$

Quel est l'effet de :



$$\begin{aligned}
|\psi_1\rangle|0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}|\psi_1\rangle(|0\rangle + |1\rangle) \xrightarrow{W_{CU}} \frac{1}{\sqrt{2}}(|\psi_1\rangle|0\rangle + U|\psi_1\rangle|1\rangle) \\
&= \frac{1}{\sqrt{2}}[(c_+|\psi_+\rangle + c_-|\psi_-\rangle)|0\rangle + (c_+|\psi_+\rangle - c_-|\psi_-\rangle)|1\rangle] \\
&\xrightarrow{H} c_+|\psi_+\rangle|0\rangle + c_-|\psi_-\rangle|1\rangle .
\end{aligned}$$

CLONAGE D'UN QUBIT

Peut on cloner un état quantique (un qubit) inconnu ?

- Il semble que la porte CNOT fasse cette opération :

$$\mathrm{CNOT}\,|0\rangle|0\rangle \to |0\rangle|0\rangle$$
$$\mathrm{CNOT}\,|1\rangle|0\rangle \to |1\rangle|1\rangle$$

L'état du premier qubit 1 est copié sur le deuxième qubit.

- Ce n'est pas vrai de manière générale :

$$W_{\mathrm{CNOT}}(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle \to \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle \neq (\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha\,|0\rangle + \beta\,|1\rangle)$$

- Si le qubit est connu, on peut le copier autant de fois que l'on souhaite (préparation d'états quantiques cf RMN).

THÉORÈME DE NON-CLONAGE

- Théorème : Pour un état quantique inconnu quelconque, il n'est pas possible de faire une copie parfaite de cet état (sans détruire l'état initial)
- Preuve :
  - On fait un démonstration par l'absurde.
  - Supposons qu'il existe une transformation unitaire $\mathcal{U}_{clone}$ qui clone un système dans un état inconnu.
  - Pour deux états $|\psi\rangle, |\phi\rangle$ on a : $\mathcal{U}_{\mathrm{clone}}\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$
    $\mathcal{U}_{\mathrm{clone}}\,|\phi\rangle\,|0\rangle = |\phi\rangle\,|\phi\rangle$
  - Que se passe t'il pour l'état $|\sigma\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$?

$$\mathcal{U}_{\mathrm{clone}}\,|\sigma\rangle\,|0\rangle = \mathcal{U}_{\mathrm{clone}}\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle\,|\psi\rangle + |\phi\rangle\,|\phi\rangle)$$
$$\neq |\sigma\rangle\,|\sigma\rangle = \frac{1}{2}(|\psi\rangle\,|\psi\rangle + |\psi\rangle\,|\phi\rangle + |\phi\rangle\,|\psi\rangle + |\phi\rangle\,|\phi\rangle)$$

CODAGE DENSE

Combien de bits d'information classique peut on envoyer avec un qubit ?

- Principe du codage dense :
  - Alice et Bob partagent une paire de qubits intriqués prenons par exemple : $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
  - Alice peut faire 4 opérations différentes sur son qubit : I, X, Z, XZ
  - Les 4 états obtenus sont :

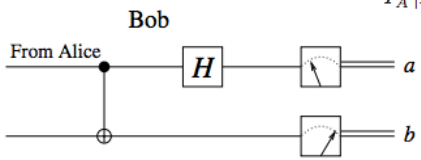
$$I_A\,|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = |B_{00}\rangle\,,$$
$$X_A\,|B_{00}\rangle = \frac{1}{\sqrt{2}}(|1^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |0^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = |B_{01}\rangle\,,$$
$$Z_A\,|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle - |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = |B_{10}\rangle\,,$$
$$Y_A\,|B_{00}\rangle = \frac{\mathrm{i}}{\sqrt{2}}(|1^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle - |0^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = \mathrm{i}\,|B_{11}\rangle$$

CODAGE DENSE

Ces 4 états sont orthogonaux.

On peut les distinguer avec certitude.

$$I_A\,|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = |B_{00}\rangle\,,$$
$$X_A\,|B_{00}\rangle = \frac{1}{\sqrt{2}}(|1^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle + |0^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = |B_{01}\rangle\,,$$
$$Z_A\,|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle - |1^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = |B_{10}\rangle\,,$$
$$Y_A\,|B_{00}\rangle = \frac{\mathrm{i}}{\sqrt{2}}(|1^{\mathrm{A}}\rangle\,|0^{\mathrm{B}}\rangle - |0^{\mathrm{A}}\rangle\,|1^{\mathrm{B}}\rangle) = \mathrm{i}\,|B_{11}\rangle$$



$$|B_{00}\rangle \xrightarrow{\mathrm{CNOT}} \frac{1}{\sqrt{2}}(|00^{\mathrm{B}}\rangle + |10^{\mathrm{B}}\rangle) \xrightarrow{H} |00^{\mathrm{B}}\rangle\,,$$
$$|B_{01}\rangle \xrightarrow{\mathrm{CNOT}} \frac{1}{\sqrt{2}}(|11^{\mathrm{B}}\rangle + |01^{\mathrm{B}}\rangle) \xrightarrow{H} |01^{\mathrm{B}}\rangle$$
$$|B_{10}\rangle \xrightarrow{\mathrm{CNOT}} \frac{1}{\sqrt{2}}(|00^{\mathrm{B}}\rangle - |10^{\mathrm{B}}\rangle) \xrightarrow{H} |10^{\mathrm{B}}\rangle\,,$$
$$\mathrm{i}\,|B_{11}\rangle \xrightarrow{\mathrm{CNOT}} \frac{\mathrm{i}}{\sqrt{2}}(|11^{\mathrm{B}}\rangle - |01^{\mathrm{B}}\rangle) \xrightarrow{H} -\mathrm{i}\,|11^{\mathrm{B}}\rangle$$