Chapter 1

Mécanique Quantique des Systèmes Discrets: principes élémentaires

La physique moderne est fondée sur la Mécanique Quantique. Cette théorie a été élaborée entre 1900 et 1926 environ suite à plusieurs expériences. En 1930 les grands principes physiques de la mécanique quantique étaient essentiellement connus et clairement formulés par les physiciens. Leur formulation mathématique précise et un cadre cohérent fut donné par Paul Dirac et John von Neumann. Leurs livres "Principles of Quantum Mechanics" (Dirac 1930) et "Mathematische Grundlagen der Quantenmechanik" (von Neumann 1932) jouèrent un role absolument fondamental. Aujoud'hui même, les grands principes sont et restent inchangés.

Ici nous donnons un résumé assez élémentaire de ces principes dans le cadre des *systèmes avec degrés de liberté discrets* qui sont d'intéret pour la théorie du calcul quantique. En effet les bits quantiques qui sont les unités de l'information et du calcul quantique sont des analogues des bits classiques (variables binaires usuelles) et décrivent des degrés de liberté discrets (cette desription peut être excate ou approximative selon les cas. Par exemple elle est exacte pour la polarization d'un photon, le spin d'un électron mais approximative pour les niveaux atomiques).

Le cadre général est l'éspace de Hilbert (de dimension finie pour nous). L'espace de Hilbert est essentiellement un espace vectoriel sur le corps des nombres complexes muni d'un produit scalaire. Nous allons donc commencer par donner quelques rappels d'algèbre linéaire sur ces espaces. En même temps ceci est l'occasion d'introduire la notation de Dirac des "bras" et "kets" de facon un peu plus formelle. Ensuite nous formulons 5 postulats qui ensembles forment les grands principes de la MQ.

1.1 Algèbre linéaire en notation de Dirac

Un espace de Hilbert $\mathcal{H}$ est un espace vectoriel sur le corps $\mathbf{C}$, muni d'un produit scalaire. Pour un espace de dimension fini cette définition est suffisante. Pour des espaces de dimension infinie il faut préciser des conditions qui permettent de prendre des limites; mais dans le cadre de ce cours nous resterons en dimension finie comme cela est le plus souvent le cas en information quantique.

Les vecteurs sont notés $|\psi\rangle$ (prononcé "ket psi"). L'hermitien conjugué (transposé et complexe conjugué) est noté $\langle\psi|$ (pronouncé "bra psi"). Le produit scalaire est noté $\langle\phi|\psi\rangle$. C'est le produit scalaire entre les vecteurs $|\phi\rangle$ et $|\psi\rangle$. On appelent aussi $\langle\phi|\psi\rangle$ un "bracket". Le produit scalaire satisfait à:

1. *Positivité*: $\langle\phi|\phi\rangle \geq 0$ avec égalité si et seulement si $|\phi\rangle = 0$.
2. *Linearité*: $\langle\phi|(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha\langle\phi|\psi_1\rangle + \beta\langle\phi|\psi_2\rangle$, $\alpha, \beta \in \mathbf{C}$
3. *Symmetrie*: $\langle\phi|\psi\rangle = \overline{\langle\psi|\phi\rangle}$ ou la barre dénote la conjugaison complexe.

Exemple 1: Bit quantique ou système à deux niveaux. $\mathcal{H} = \mathbf{C}^2 = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \text{ with } \alpha, \beta \in \mathbf{C} \right\}$. Le produit scalaire est $(\overline{\gamma}, \overline{\delta}) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \overline{\gamma}\alpha + \overline{\delta}\beta$. En notation de Dirac

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

où $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. De plus

$$(\bar{\gamma}, \bar{\delta}) = \bar{\gamma}\langle 0| + \bar{\delta}\langle 1|$$

et

$$(\bar{\gamma}\langle 0| + \bar{\delta}\langle 1|)(\alpha|0\rangle + \beta|1\rangle) = \overline{\gamma}\alpha\langle 0|0\rangle + \overline{\gamma}\beta\langle 0|1\rangle + \overline{\delta}\alpha\langle 1|0\rangle + \overline{\delta}\beta\langle 1|1\rangle = \overline{\gamma}\alpha + \overline{\delta}\beta$$

Exemple 2: particule dans l'espace à trois dimensions. $\mathcal{H} = L^2(\mathbf{R}^3) = \{f : \mathbf{R}^3 \to \mathbf{C},\ \int d^3\vec{x}|f(\vec{x})|^2 < \infty\}$. Le produit scalaire $\langle f|g\rangle = \int d^3\vec{x}\overline{f(\vec{x})}g(\vec{x})$ et la norme induite $||f||_2 = \langle f|f\rangle^{1/2} = \int d^3\vec{x}|f(\vec{x})|^2$. Cet espace joue un rôle fondamental en MQ mais nous n'en parlerons quasiment plus dans ce cours car nous nous occuperons uniquement de degrés de liberté discrets.

Nous aurons besoin de la notion de produit tensoriel. Soit $\mathcal{H}_1$ et $\mathcal{H}_2$ deux espaces de Hilbert avec deux bases finies. Soit $|i\rangle_1$, $i = 1, ..., n_1$ la première

base de $\dim \mathcal{H}_1 = n_1$ et $|j\rangle_2$, $j = 1, ..., n_2$ celle de $\dim \mathcal{H}_2 = n_2$. Nous pouvons former "l'espace produit"

$$\mathcal{H}_1 \otimes \mathcal{H}_2$$

qui est simplement le nouvel esapce de Hilbert engendré par la base des vecteurs

$$|i\rangle_1 \otimes |j\rangle_2$$

(aussi notés $|i, j\rangle$ or $|i\rangle_1|j\rangle_2$). Il y a $n_1 n_2$ vecteurs dans cette base, donc

$$\dim \mathcal{H}_1 \otimes \mathcal{H}_2 = n_1 n_2$$

Un vecteur général de l'espace produit est

$$|\psi\rangle = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} c_{ij} |i, j\rangle = \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} c_{ij} |i\rangle_1 \otimes |j\rangle_2$$

Le produit scalaire dans l'espace produit est par définition:

$$\langle i', j'|i, j\rangle = (\langle i'|_1 \otimes \langle j'|_2)(|i\rangle_1 \otimes |j\rangle_2) = \langle i'|i\rangle_1 \langle j'|j\rangle_2$$

.

Exemple 3. Pour un bit quantique l'espace de Hilbert est $\mathbf{C}^2$. Nous verrons que l'espace de Hilbert de deux bits quantiques est $\mathbf{C}^2 \otimes \mathbf{C}^2$. Les vecteurs de base de $\mathbf{C}^2 \otimes \mathbf{C}^2$ sont $\{|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle\}$ ou bien $\{|0, 0\rangle$, $|0, 1\rangle$, $|1, 0\rangle$, $|1, 1\rangle\}$. Un état général est

$$|\psi\rangle = \alpha_{00}|0, 0\rangle + \alpha_{01}|0, 0\rangle + \alpha_{10}|0, 0\rangle + \alpha_{11}|1, 1\rangle$$

On a $\dim \mathbf{C}^2 \otimes \mathbf{C}^2 = 4$ et biensur $\mathbf{C}^2 \otimes \mathbf{C}^2$ est isomorphe à $\mathbf{C}^4$. Voici quelques exemples de produits scalaires: $\langle 0, 0|0, 0\rangle = \langle 0|0\rangle\langle 0|0\rangle = 1$, $\langle 0, 1|0, 1\rangle = \langle 0|0\rangle\langle 1|1\rangle = 1$, $\langle 0, 1|1, 1\rangle = \langle 0|1\rangle\langle 1|1\rangle = 0$ etc... A partir de la on peut calculer le produit scalaire de $|\psi\rangle$ and $|\phi\rangle = \overline{\beta}_{00}|0, 0\rangle + \overline{\beta}_{01}|0, 0\rangle + \overline{\beta}_{10}|0, 0\rangle + \overline{\beta}_{11}|1, 1\rangle$. On trouve comme attendu $\langle\phi|\psi\rangle = \overline{\beta}_{00}\alpha_{00} + \overline{\beta}_{01}\alpha_{01} + \overline{\beta}_{10}\alpha_{10} + \overline{\beta}_{11}\alpha_{11}$. Il peut être utile de travailler dans une base canonique de $\mathbf{C}^4$

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

Une fois cette correspondance (conventionnelle) fixée on peut inférer les règles du produit tensoriel en composantes:

$$\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\qquad \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\qquad \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Ces règles se généralisent à $\mathbf{C}^2\otimes\mathbf{C}^2\otimes\mathbf{C}^2$ etc...

Inégalités de Cauchy-Schwarz. Comme d'habitude:

$$|\langle\phi|\psi\rangle|\leq\langle\phi|\phi\rangle^{1/2}\langle\psi|\psi\rangle^{1/2}$$

Relation de Fermeture. Soit $|i\rangle$, $i=1,...,n$ une base orthonormée d'un espace de Hilbert à n-dimensions. Un vecteur peut être développé

$$|\phi\rangle=\sum_{i=1}^{n}c_i|i\rangle,\qquad c_i=\langle i|\phi\rangle$$

Les composantes c_i sont obtenues en projetant $|\phi\rangle$ sur les vecteurs de base. Le développement devient

$$|\phi\rangle=\sum_{i=1}^{n}|i\rangle\langle i|\phi\rangle$$

Notez que $|i\rangle\langle i|$ la (matrice du) projecteur sur $|i\rangle$. On peut penser à $\sum_{i=1}^{n}|i\rangle\langle i|$ comme à la matrice identité agissant sur $|\phi\rangle$. On obtient donc la *relation de fermeture*

$$\sum_{i=1}^{n}|i\rangle\langle i|=I$$

Projecteurs en notation de Dirac. L'opération linéaire

$$|i\rangle\langle i|=P_i$$

est un projecteur sur le vecteur de base $|i\rangle$. Si P_i est un projecteur, on a $P_i^\dagger=P_i$ et $P_i^2=P_i$. Voici comment on peut le vérifier en notation de Dirac:

$$P_i^\dagger=(|i\rangle\langle i|)^\dagger=(\langle i|)^\dagger(|i\rangle)^\dagger=|i\rangle\langle i|=P_i$$

$$P_i^2 = (|i\rangle\langle i|)(|i\rangle\langle i|) = |i\rangle\langle i|i\rangle\langle i| = |i\rangle\langle i| = P_i$$

Puisque $|i\rangle$ and $|j\rangle$ sont orthogonaux pour $i \neq j$ on a $P_iP_j = P_jP_i = 0$. En effet

$$P_iP_j(|i\rangle\langle i|)(|j\rangle)(\langle j|) = |i\rangle\langle i|j\rangle\langle j|) = 0$$

$$P_jP_i(|j\rangle\langle j|)(|i\rangle\langle i|) = |j\rangle\langle j|i\rangle\langle i|) = 0$$

Si $|\phi\rangle$ est n'importe quel vecteur sur l'esapce de Hilbert, alors $P_\phi = |\phi\rangle\langle\phi|$ est le projecteur sur $|\phi\rangle$.

Décomposition Spectrale. Les matrices hermitiennes sur l'espace de Hilbert ont une *décomposition spectrale*,

$$A = \sum_n a_n P_n$$

où $a_n \in \mathbf{R}$ sont les valeurs propres et P_n les projecteurs propres de A. Dans le cas non-dégénéré on a

$$P_n = |\phi_n\rangle\langle\phi_n\rangle$$

où $|\phi_n\rangle$ est le vecteur propre associé à la valeur propre a_n:

$$A|\phi_n\rangle = a_n|\phi_n\rangle$$

Les vecteurs propres et projecteurs associés à des valeurs propres différentes sont orthogonaux. De plus ils satisfont à la relation de fermeture

$$I = \sum_n P_n = \sum_n |\phi_n\rangle\langle\phi_n\rangle$$

Nous écrirons souvent la décomposition spectrale sous la forme

$$A = \sum_n a_n|\phi_n\rangle\langle\phi_n\rangle$$

1.2 Principes de la mécanique quantique

Dans ce paragraphe nous introduisons 4 grands principes de la MQ:

- les systèmes isolés sont décrits par *des vecteurs (kets) states d'un espace de Hilbert*,
- le vecteur d'état *évolue dans le temps de facon unitaire*,
- l'opération de mesure est un processus distinct de l'évolution temporelle: c'est une *projection aléatoire*,

- on peut *composer* des systèmes: leur espace d'Hilbert est un espace produit (tensoriel).

Il exsite en fait un principe supplémentaire concernant la représentation des quantitś mesurables (observables) qui ne sera pas utilisé explicitement. Celui est énoncé dans le complément facultatif à la fin du chapitre.

Principe 1: vecteurs détats. L'état dun système - isolé du reste de l' univers - est *completement* specifié par un vecteur de l'espace de Hilbert. Le vecteur $|\psi\rangle \in \mathcal{H}$ doit être normalisé $\langle\psi|\psi\rangle = 1$.

Example 4.

- La polarization du photon est décrite par $\mathcal{H} = \mathbf{C}^2$. Les vecteurs détat de $\mathbf{C}^2$ sont $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. Un état de polarisation linéaire $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, un état de polarisation circulaire $|\tilde{\theta}\rangle = \cos\theta|0\rangle + i\sin\theta|1\rangle$, et un état général

$$\cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$$

  .

- Le spin $\frac{1}{2}$ (de l'électron par exemple) est décrit par le même espace d'Hilbert. La paramétrisation naturelle est

$$\cos\frac{\theta}{2}|0\rangle + e^{i\delta}\sin\frac{\theta}{2}|1\rangle$$

  (La sphère de Bloch est une représentation géométrique naturelle de l'espace de Hilbert de ces états.)

- Pour une particule dans $\mathbf{R}^3$ on a $\mathcal{H} = L^2(\mathbf{R}^3)$. Les vecteurs d'états sont les fonctions d'ondes normalisées $\int d^3\vec{x}|\psi(\vec{x})|^2 = 1$.

Principe 2: évolution temporelle. Un système isolé évolue (au cours du temps) de facon unitaire. Cela signifie que si $|\psi\rangle$ est l'état au temps 0, l'état au temps t est de la forme $U_t|\psi\rangle$ où U_t est une matrice unitaire de $\mathcal{H} \to \mathcal{H}$. Ici unitaire signifie que $U_t^\dagger U_t = U_t U_t^\dagger = 1$ ou bien de facon équivalente $U_t^{-1} = U_t^\dagger$.

L'évolution unitaire forme un groupe (ou plutot la représentation du groupe des translations temporelles) au sens suivant:

$$U_{t=0} = I, \qquad U_{t_1}U_{t_2} = U_{t_1+t_2}$$

La MQ nous indique comment calculer U_t pour un système donné: il faut résoudre *l'équation de Schroedinger*.

En information quantique nous ne nous interessons pas (en général) à cette équation. On suppose (de facon optimiste) qu'un ingénieur ou un physicien saura construire un appareil (appelé circuit quantique) qui réalise l'opération unitaire U_t voulue. Ces opérations (matrices) unitaires seront pour nous une généralization des portes logiques quantiques, et seront spécifiées par l'algorithme quantique. Notez aussi que pour nous il ne sera pas important d'expliciter la dépendance temporelle et nous laisserons complètement tomber l'indice t. Nous reviendrons sur ces point plus tard dans le cours.

Example 5. Un mirroir semi-transparent decompose un rayon (photon) incident en rayon réfléchi et rayon transmis. Soit $\mathcal{H} = \mathbf{C}^2$ l'espace de Hilbert avec la base $|T\rangle$, $|R\rangle$ qui représentent les états transmis et réfléchis du rayon (photon). Le mirroir semi-transparent agit de facon unitaire

$$|T\rangle \rightarrow \boxed{\text{H}} \rightarrow H|T\rangle = \frac{1}{\sqrt{2}}(|T\rangle + |R\rangle)$$

$$|R\rangle \rightarrow \boxed{\text{H}} \rightarrow H|R\rangle = \frac{1}{\sqrt{2}}(|T\rangle - |R\rangle)$$

La matrice unitaire H s'appele matrice de Hadamard ou "porte logique de Hadamard"

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

Principe 3: postulat de la mesure. Soit un système préparé dans l'état $|\psi\rangle$. On veut mesurer une observable du système grâce â un appareil. L'appareil est modélisé par un ensemble de projecteur orthogonaux $\{P_n\}$ satisfaisant $\sum_n P_n = I$. Une mesure *projette*[1] l'état ψ du système qui devient juste après la mesure

$$|\phi_n\rangle = \frac{P_n|\psi\rangle}{||P_n|\psi\rangle||} = \frac{P_n|\psi\rangle}{\langle\psi|P_n|\psi\rangle^{1/2}}$$

Pour une mesure unique *il n'y a pas moyen de prédire* l'état résultant $|\phi_n\rangle$: celui-ci est aléatoire. Si l'expérience de mesure est répétée plusieurs fois la probabilité (interprétation fréquentiste de la probabilité) d'observer n est

$$\text{Prob(resultat } n) = |\langle\phi_n|\psi\rangle|^2 = \langle\psi|P_n|\psi\rangle$$

Remarque 1. Puisque $\sum_j P_j = I$ et $|\psi\rangle$ sont normalisés on a

$$\sum_j \text{Prob(resultat } j) = 1$$

[1] les physiciens disent que l'état ou la fonction d'onde est "réduit(e)"

Remarque 2. Avec $P_j = |j\rangle\langle j|$ la probabilité de l'état résultant j est

$$\text{Prob(resultat } j) = \langle\psi|P_j|\psi\rangle = |\langle j|\psi\rangle|^2$$

et l'état juste après la mesure est $|j\rangle$.

Principe 4: sytèmes quantiques composés. Prenons deux systèmes $\mathcal{A}$ et $\mathcal{B}$ avec espaces de Hilbert $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$. L'espace de Hilbert du système composé $\mathcal{AB}$ est donné par le produit tensoriel

$$\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$$

Les états de $\mathcal{AB}$ sont les vecteurs $|\psi\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. Les postulats précédents s'appliquent aux systèmes composés.

Ce postulat est en fait non trivial et nous étudierons quelques conséquences. En particulier Einstein, Podolsky et Rosen ainsi que Schroedinger furent les premiers a analyser la significaction de ce postulat. Ces études menŕent aux inégalités de Bell, à la téléportation et au dense coding qui jouent aujourd'hui un role important en information quantique.

Eeample 8. Deux photons avec degrés de liberté de polarisation ou deux bits quantiques. L'espace de Hilbert est $\mathbf{C}^2 \otimes \mathbf{C}^2$. Exemples d'états $|x\rangle_\mathcal{A} \otimes |y\rangle_\mathcal{B}$ ou $|x\rangle_\mathcal{A} \otimes |y\rangle_\mathcal{B} + |\theta\rangle_\mathcal{A} \otimes |\theta\rangle_\mathcal{B}$. N bits quantiques possèdent l'espace de Hilbert

$$\underbrace{\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes ... \otimes \mathbf{C}^2}_{N \text{ copies}}$$

Si $|0\rangle, |1\rangle$ est une base pour $\mathbf{C}^2$, une base du système composé est donnée par

$$|b_1\rangle \otimes |b_2\rangle ... \otimes |b_N\rangle = |b_1, ..., b_N\rangle$$

où $b_i = \{0, 1\}$. Il y a 2^N états de base en correspondance avec 2^N suites de longueur N de bits classiques. Un état de N bits quantiques est une superposition des états de base:

$$|\psi\rangle = \sum_{b_1,...,b_N} c_{b_1,...,b_N} |b_1, ..., b_N\rangle$$

ou les coefficients $c_{b_1...b_N}$ satisfont

$$\sum_{b_1,...,b_N} |c_{b_1,...,b_N}|^2$$

1.3 Etats produit et état intriqués

Les états d'un système composé $\mathcal{AB}$ appartiennent à $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. Un état est de type produit si il peut être reprśenté comme

$$|\psi\rangle = |\phi\rangle_\mathcal{A} \otimes |\phi\rangle_\mathcal{B}$$

Un état intriqué $|\psi\rangle \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ est un état pour lequel il est impossible de trouver $|\phi\rangle_\mathcal{A} \in \mathcal{H}_\mathcal{A}$ et $|\phi\rangle_\mathcal{B} \in \mathcal{H}_\mathcal{B}$ telle que ψ soit de la forme produit.

Les états intriqués engendrent des corrélations très spéciales entre les parties $\mathcal{A}$ et $\mathcal{B}$. Nous verrons que ces corrélations n'ont aucunne contrepartie classique (et jouent un role imporatnt dans la téléporation par exemple).

Exemple 9. Deux bits quantiques avec $\mathcal{A} \otimes \mathcal{B} = \mathbf{C}^2 \otimes \mathbf{C}^2$. Quelques états produit : $|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} = |0,0\rangle$, $|0\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B} = |0,1\rangle$, $|1\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} = |1,0\rangle$, $|1\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B} = |1,1\rangle$. Des états produits moins évidents

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} + |1\rangle_\mathcal{B}) \otimes |0\rangle_\mathcal{B} = \frac{1}{2}(|0,0\rangle + |1,0\rangle)$$

et

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} + |1\rangle_\mathcal{B}) \otimes \frac{1}{\sqrt{2}}(|0\rangle_\mathcal{B} - |1\rangle_\mathcal{B}) = \frac{1}{2}(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle)$$

Il existe des états intriqués qui ne peuvent pas se mettre sous forme produit. Par exemple,

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} + |1\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} - |1\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|0,0\rangle - |1,1\rangle)$$

$$\frac{1}{\sqrt{2}}(|1\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} + |0\rangle_\mathcal{A} \otimes |1\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|1,0\rangle + |0,1\rangle)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B} - |1\rangle_\mathcal{A} \otimes |0\rangle_\mathcal{B}) = \frac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle)$$

Ces quatres états jouent un role particulier et s'appelent états de Bell.

Production d'états intriqués. Soit un système composé avec état initial $|\phi\rangle_\mathcal{A} \otimes |\chi\rangle_\mathcal{B}$. Ce pourrait être par exemple deux électrons dans létat de spin $|\uparrow\rangle \otimes |\downarrow\rangle$. Si on les laisse évoluer séparément sans interaction, l'opérateur dévolution unitaire est de la forme $U_\mathcal{A} \otimes U_\mathcal{B}$ et

$$U_\mathcal{A} \otimes U_\mathcal{B}(|\uparrow\rangle \otimes |\downarrow\rangle) = U_\mathcal{A}|\uparrow\rangle \otimes U_\mathcal{B}|\downarrow\rangle$$

si bien que l'état reste dans un état produit.

Pour produire des états intriqués $\mathcal{A}$ and $\mathcal{B}$ doivent interagir pendant l'evolution temporelle, pour que $U_{\mathcal{AB}} \neq U_{\mathcal{A}} \otimes U_{\mathcal{B}}$. Toutes les interactions physiques connues sont locales dans l'espace et le temps: deux systèmes dans un état intriqué ont nécessairement été en contact dans le passé.

1.4 Impossibilité de "cloner" un état quantique

Les bits classiques peuvent être copiés. Par exemple un texte peut être dupliqué ou copié avec une machine à photocopier "universelle": la même machine peut copier tous les textes.

Soit un ensemble d'états quantiques $|\psi\rangle \in \mathcal{H}$ et supposons que nous voulions construire une "machine universelle" qui "copie" tout $|\psi\rangle \in \mathcal{H}$. cette machine quantique devrait être décrite par un opérateur ou matrice unitaire U (ceci est vrai pour tout processus physique sauf pour celui de la mesure). L'espace d'Hilbert est $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ ou $\mathcal{A}$ est l'espace des états que l'on désire copier et $\mathcal{B}$ celui des copies. On commence par l'état initial

$$|\psi\rangle \otimes |\text{blank}\rangle$$

La machine produit la sortie:

$$|\psi\rangle \otimes |\text{blank}\rangle \rightarrow \boxed{\text{U}} \rightarrow |\psi\rangle \otimes |\psi\rangle$$

En termes mathématiques la question est: peut-on trouver un opérateur unitaire tel que pour un ensemble raisonnablement large d'états ψ

$$U(|\psi\rangle \otimes |\text{blank}\rangle) = |\psi\rangle \otimes |\psi\rangle$$

La réponse est non. Ce fait s'appelle parfois le "no cloning theorem". Par contre il est possible de cloner/copier un ensemble d'états orthogonaux avec un U approprié (qui dépend de l'ensemble spécifique en question).

Preuve du théorème de non-clonage. Supposons qu'il existe U tel que $U^\dagger U = UU^\dagger = 1$ avec

$$U(|\phi_1\rangle \otimes |\text{blank}\rangle) = |\phi_1\rangle \otimes |\phi_1\rangle$$

$$U(|\phi_2\rangle \otimes |\text{blank}\rangle) = |\phi_2\rangle \otimes |\phi_2\rangle$$

En prenant l'hermitien conjugué de la deuxième équation

$$(\langle\phi_2| \otimes \langle\text{blank}|)U^\dagger = \langle\phi_2| \otimes \langle\phi_2|$$

En prenant le produit scalaire avec la première équation

$$\langle\phi_2| \otimes \langle \text{blank}|U^\dagger U|\phi_1\rangle \otimes |\text{blank}\rangle = (\phi_2| \otimes \langle\phi_2|)(|\phi_1\rangle \otimes |\phi_1\rangle)$$

ce qui implique

$$\langle\phi_2|\phi_1\rangle\langle \text{blank}|\text{blank}\rangle = \langle\phi_2|\phi_1\rangle^2$$

donc

$$\langle\phi_2|\phi_1\rangle = 0 \text{ or } \langle\phi_2|\phi_1\rangle = 1$$

Nous concluons qu'il n'est pas possible de copier $|\phi_1\rangle$ and $|\phi_2\rangle$ qui ne sont sont identiques ou bien pas orthogonaux, avec le même U. En fait il est possible de copier une base orthogonale ou des états orthogonaux.

Les états non-orthogonaux ne peuvent pas être parfaitement distingués.

Il existe plusieurs variantes et rafinements du no-cloning theorem. Ici nous discutons une de ces variantes. Donnons nous deux états $|\psi\rangle$ et $|\phi\rangle$ et essayons de construire une machine (unitaire) qui permet de les distinguer. Mathématiquement on cherche une matrice unitaire U telle que

$$U|\psi\rangle \otimes |a\rangle = |\psi\rangle \otimes |v\rangle$$

$$U|\phi\rangle \otimes |a\rangle = |\phi\rangle \otimes |v'\rangle$$

où les sorties $|v\rangle$ et $|v'\rangle$ sont différents. Le produit scalaire entre ces deux équations donne

$$\langle\phi| \otimes \langle a|U^\dagger U|\psi\rangle \otimes |a\rangle = (\langle\phi| \otimes \langle v'|)(|\psi\rangle\rangle \otimes |v\rangle)$$

ceci implique

$$\langle\phi|\psi\rangle\langle a|a\rangle = \langle\phi|\psi\rangle\langle v'|v\rangle$$

Si $|\phi\rangle$ n'est pas orthogonal à $|\psi\rangle$ nous avons $\langle\phi|\psi\rangle \neq 0$ donc

$$\langle v'|v\rangle = \langle a|a\rangle = 1$$

Ainsi $|v\rangle = |v'\rangle$ et il n'y a pas d'information dans $|v\rangle$ et $|v'\rangle$ qui permet de distinguer $|\psi\rangle$ et $|\phi\rangle$.

1.5 Appendice: observables en MQ

Il existe un postulat supplémentaire que nous n'utiliserons pas de facon explicite dans le cours. Nous l'exposons ici par souci de complétude. Celui-ci concerne la rprésentation des quantités observables en MQ.

En MQ les observables ("quantités mesurables") sont représentées par des matrices hermitiennes agissant sur $\mathcal{H}$. Rappelons quelques propriétés importantes.

L'application $A : \mathcal{H} \to \mathcal{H}$, $|\psi\rangle \to A|\psi\rangle$ est linéaire si

$$A(\alpha|\phi_1\rangle + \beta|\phi_2\rangle) = \alpha(A|\phi_1\rangle) + \beta(A|\phi_2\rangle)$$

une application linéaire peut être représentée par une matrice aussi notée A.

Les éléments de matrice de A dans la base orthonormée $\{|i\rangle, i = 1, ..., n\}$ de $\mathcal{H}$ sont notés $\langle i|A|j\rangle$ or A_{ij}. Etant donné A, *l'adjoint* de A est noté $A^\dagger$ et défini par

$$\langle\phi|A^\dagger|\psi\rangle = \overline{\langle\psi|A|\phi\rangle}$$

Donc l'adjoint (où l'hermitien conjugué) est l'application linéaire avec la matrice transposée et complexe conjuguée. On a pour les éléments de matrice

$$\langle i|A^\dagger|j\rangle = \overline{\langle j|A|i\rangle}, \qquad (A^\dagger)_{ij} = \overline{A_{ij}}$$

On dit que A est hermitienne si $A = A^\dagger$. On peut vérifier que $(A+B)^\dagger = A^\dagger + B^\dagger$ and $(AB)^\dagger = B^\dagger A^\dagger$.

Principe: quantités observables. En mécanique quantique une quantité observable (énergie, moment magnétique moment, position, impulsion, vitesse,...) est représentée par une matrice hermitienne.

Il n'est pas forcément évident de savoir comment choisir la matrice (ou opérateur). Il existe un "principe de correspondence" (voir chap 1, compléments) qui est une sorte de règle pratique pour construire l'opérateur à partir de la quantité classique. En fait cette règle est parfois ambigue car les matrices sont des objets qui ne commutent pas. D'autrepart il existe des observables (comme le spin qui n'ont pas d'analogue classique).

Example 6.

- Position x, impulsion $p = \frac{\hbar}{i}\frac{\partial}{\partial x}$, energie ou Hamiltonien $\frac{p^2}{2m} + V(x)$. dans ce cours nous n'aurons pas besoin de ces observables.
- Polarisation du photon. On envoie un photon à travers une lame biréfringente (voir chapitre 1). Si D_y clique on enregistre -1 alors que si D_x clique on enregistre $+1$. Les observations sont décrites par l'observable

  $$\mathcal{P} = (+1)|x\rangle\langle x| + (-1)|y\rangle\langle y|$$

  cette observable est la matrice hermitienne $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (dans la base $|x\rangle$, $|y\rangle$).

- Toute observable (matrice hermitienne) de $\mathcal{H} = \mathbf{C}^2$ peut être représentée par une matrice 2×2

$$A = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \gamma \end{pmatrix}$$

ou en notation de Dirac

$$A = \alpha|0\rangle\langle 0| + \beta|0\rangle\langle 1| + \overline{\beta}|1\rangle\langle 0| + \gamma|1\rangle\langle 1|$$

Toutes ces matrices peuvent être représentées par une combinaison linéaire des matrices (exercices)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

Les matrices hermitiennes X, Y, Z sont appelées les matrices de Pauli.

Les matrices de Pauli servent entre autres à décrire le spin $\frac{1}{2}$: il s'agit d'un vecteur à 3 components $\Sigma = (X, Y, Z)$. Dans la littérature physique $\Sigma = (\sigma_x, \sigma_y, \sigma_z)$. Les propriétés importantes de ces matrices sont (exercices)

$$X^2 = Y^2 = Z^2 = I,\ XY = -YX,\ XZ = -ZX,\ YZ = -ZY$$

et

$$[X, Y] = 2iZ,\ [Y, Z] = 2iX,\ [Z, X] = 2iY$$