

Cours 1 — 4 janvier

Enseignant : Philippe Grangier – Frédéric Magniez – Alexandre Boulc'h – Thomas Hout

Introduction

La loi de Moore (figure 1.1) conjecture qu'en 2020 la taille des transistors sera à l'échelle atomique. Cette diminution de la taille des transistors pose des problèmes aux scientifiques notamment à cause de l'apparition d'effets quantiques perturbant leur utilisation. L'approche actuelle est de chercher à supprimer ces effets pour pouvoir continuer à construire des ordinateurs de la même façon et essayer de repousser les limites de la loi de Moore.

Mais une autre approche est possible. Au lieu de chercher à éviter les effets quantiques, pourquoi ne pas les utiliser ? De cette manière on pourrait créer un nouveau type d'ordinateur qui aurait des capacités différentes, et parfois meilleures, de l'ordinateur que nous connaissons.

Cette idée a été développée, et le calcul quantique a déjà réussi à accomplir certaines prouesses. En cryptographie [Bennet et Brassard] ont mis en place en 1984 un protocole de distribution de clés secrètes. Ce protocole a pu être testé en 2008 pour échanger des données entre deux points éloignés de 100km. En information quantique le phénomène de « téléportation » a été découvert en 1993 par [Bennet - Brassard - Crépeau - Jozsa - Peres - Wootters] et a été réalisé en 1997. Enfin en algorithmique les algorithmes de [Simon-Shor 1994] et de [Grover 1996] révèlent la puissance des ordinateurs quantiques en proposant des nouvelles méthodes de factorisation.

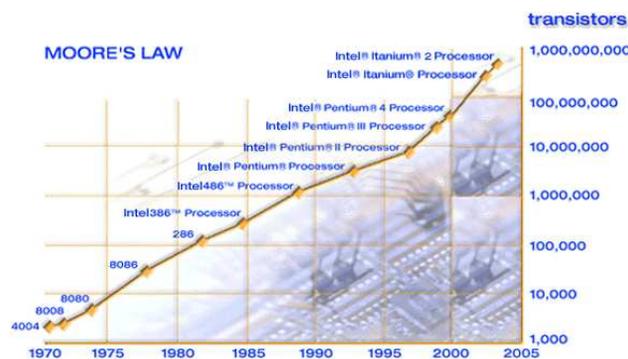


Figure 1.1. Loi de Moore

Table des matières

1	Qubits, produit tensoriel, intrication quantique, inégalités de Bell	3
1.1	Etats quantiques, notations de Dirac	3
1.1.1	Espace des états, notations de Dirac	3
1.1.2	Etats quantiques, valeurs propres et résultats de mesure	4
1.1.3	Exemple d'espaces des états de dimension deux	4
1.1.4	Sphère de Bloch	7
1.1.5	Sphère de Poincaré	9
1.2	Produits tensoriels d'espaces d'états	9
1.2.1	Espace de travail, produit tensoriel	9
1.2.2	Intrication	10
1.2.3	Exemple : particules de spin 1/2	11
1.2.4	« Paradoxe »EPR (Einstein, Podolski et Rosen)	12
1.2.5	Tests expérimentaux des inégalités de Bell	14
2	Matrice densité, description des sous-systèmes	17
2.0.6	Nécessité de généraliser le vecteur d'état	17
2.0.7	L'opérateur densité	17
2.0.8	Sous-systèmes et intrication	21
3	Exercices	23
3.0.9	Exercice 1 : Le paradoxe EPR (Einstein-Podolsky-Rosen) et les inégalités de Bell	23
3.0.10	Exercice 2 : Décomposition de Schmidt et « mise en gage de bit quantique »	26

Chapitre 1

Qubits, produit tensoriel, intrication quantique, inégalités de Bell

1.1 Etats quantiques, notations de Dirac

1.1.1 Espace des états, notations de Dirac

La notation de Dirac a été introduite pour faciliter l'écriture des équations de la mécanique quantique, mais aussi pour souligner l'aspect vectoriel de l'objet représentant un état quantique.

Le nom provient d'un jeu de mots avec le terme *bracket* qui signifie *crochet de parenthèse*, en l'occurrence « \langle » et « \rangle » respectivement appelés « bra » et « ket ».

De cette manière l'état d'un système quantique est décrit mathématiquement par un vecteur $|\psi\rangle$ dans un espace de Hilbert \mathcal{E} (espace vectoriel sur les nombres complexes).

Les quantités physiques sont décrites par des opérateurs linéaires hermitiens \hat{A} (observables) agissant dans \mathcal{E} . Les résultats de mesures sont associés aux valeurs propres réelles de \hat{A} .

◆ On parle bien de valeurs propres réelles et non complexes !

L'espace \mathcal{E} est muni d'un produit scalaire, noté $(\langle \phi |, | \psi \rangle)$ ou plus simplement $\langle \phi | \psi \rangle$. Comme tout produit scalaire complexe, ce produit est sesquilinéaire, c'est-à-dire qu'il est linéaire en $\langle \phi |$:

$$\langle \phi | \lambda \cdot \psi_1 + \mu \cdot \psi_2 \rangle = \lambda \cdot \langle \phi | \psi_1 \rangle + \mu \cdot \langle \phi | \psi_2 \rangle$$

et antilinéaire en $| \phi \rangle$:

$$\langle \lambda \cdot \phi_1 + \mu \cdot \phi_2 | \psi \rangle = \lambda^* \cdot \langle \phi_1 | \psi \rangle + \mu^* \cdot \langle \phi_2 | \psi \rangle$$

où l'expression $*$ signifie que l'on prend le complexe conjugué. Avec la notation de Dirac, on a de même :

$$\text{ket} : \lambda A | \psi \rangle \rightarrow \text{bra} : \langle \psi | A^\dagger \lambda^* = \lambda^* \langle \psi | A^\dagger$$

Exercice : Montrer en utilisant les notations de Dirac qu'un opérateur hermitien a des valeurs propres réelles, et que ses vecteurs propres correspondant à des valeurs propres distinctes sont orthogonaux.

On a :

$$\begin{aligned} A|\psi\rangle &= \lambda|\psi\rangle \\ \langle\psi|A^\dagger &= \bar{\lambda}\langle\psi| \\ \langle\psi|A|\psi\rangle &= \lambda|\psi|^2 \\ &= \bar{\lambda}|\psi|^2 \end{aligned}$$

car A est hermitien, donc $A^\dagger = A$. D'où $\lambda = \bar{\lambda}$. Un opérateur hermitien a donc des valeurs propres réelles.

Ensuite si on associe λ à $|\psi\rangle$ et μ à $|\phi\rangle$, on a :

$$\begin{aligned} \langle\phi|A|\psi\rangle &= \lambda\langle\phi|\psi\rangle \\ \langle\psi|A|\phi\rangle &= \mu\langle\psi|\phi\rangle \\ \langle\phi|A^\dagger|\psi\rangle &= \bar{\mu}\langle\phi|\psi\rangle \\ \lambda\langle\phi|\psi\rangle &= \bar{\mu}\langle\phi|\psi\rangle \end{aligned}$$

Or comme $\lambda \neq \mu$ (et $\mu = \bar{\mu}$) on a nécessairement $\langle\phi|\psi\rangle = 0$. Les vecteurs propres correspondant à des valeurs propres distinctes sont donc orthogonaux.

1.1.2 Etats quantiques, valeurs propres et résultats de mesure

Physiquement, la donnée d'un état quantique est équivalente à la donnée des valeurs d'un ensemble de propriétés physiques, qui sont prédictibles avec certitude, et peuvent être mesurées de manière répétée sans perturber l'état.

Ceci s'exprime mathématiquement par le fait qu'un état $|\psi\rangle$ est état propre commun d'un ensemble d'observables $\hat{A}, \hat{B}, \hat{C} \dots$ qui commutent entre elles :

$$\hat{A}|\psi\rangle = a|\psi\rangle, \hat{B}|\psi\rangle = b|\psi\rangle, \hat{C}|\psi\rangle = c|\psi\rangle \dots$$

L'état $|\psi\rangle$ peut donc être repéré par le multiplet de valeurs propres (a, b, c, \dots) . Si ce multiplet spécifie l'état de manière univoque, l'ensemble $\hat{A}, \hat{B}, \hat{C} \dots$ forme une « ECOC » (Ensemble Complet d'Observables qui Commutent). On utilise alors souvent le multiplet pour désigner l'état, en notant : $|\psi\rangle = |a, b, c, \dots\rangle$.

1.1.3 Exemple d'espaces des états de dimension deux

Particule de spin 1/2

Définition 1.1. Spin : moment cinétique multiple demi-entier de \hbar . Le spin est un concept entièrement quantique.

Un spin $\frac{1}{2}$ correspond à un espace des états de dimension 2. Dans cet espace l'opérateur moment cinétique $\vec{S} = (S_x, S_y, S_z)$ est donné par :

$$\vec{S} = \frac{\hbar}{2} \vec{\sigma}$$

avec $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ où $\sigma_x, \sigma_y, \sigma_z$ sont les matrices de Pauli :

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Ces matrices ont toutes pour valeur propre 1 ou -1 .

On choisit souvent comme base les états propres $|\pm\rangle_z$ de σ_z , qui vérifient :

$$\sigma_z |\pm\rangle_z = \pm |\pm\rangle_z$$

Il existe d'autres particules de spin $\frac{1}{2}$:

- Electron
- Proton
- Neutron

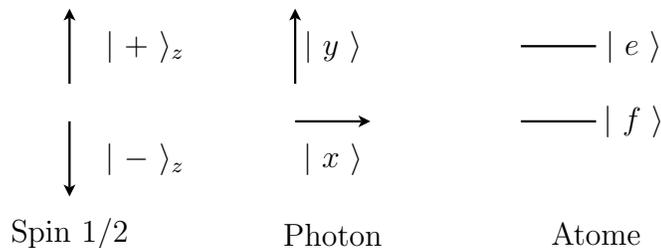
A un spin est associé un moment magnétique : on peut contrôler facilement l'état d'un spin $\frac{1}{2}$ en le faisant « précesser » dans un champ magnétique imposé.

Photon polarisé

On peut utiliser des états de polarisation linéaires ou circulaires. La structure mathématique est très proche de celle du spin $\frac{1}{2}$.

Atome « à deux niveaux »

On peut également utiliser des atomes « à deux niveaux ». Il faut faire cependant faire attention à l'émission spontanée lors de l'utilisation d'atomes de ce genre.



La notion de « bit quantique » ou qubit

Tous ces systèmes sont des réalisations de la notion de « bit quantique » que l'on appelle de façon raccourcie un « qubit ». En effet grâce à ce genre de système il est possible de former de façon distincte les états logiques 0 ou 1, que l'on écrit respectivement $|0\rangle$ et $|1\rangle$.

Considérons un état pur $|\psi\rangle$ d'un système à deux niveaux. En toute généralité, on peut le décomposer sur les états propres de l'espace $|0\rangle$ et $|1\rangle$ par :

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

avec $\alpha^2 + \beta^2 = 1$ et $(\alpha, \beta) \in \mathbb{C}^2$. De plus, puisque les facteurs de phase n'affectent pas l'état physique d'un système, nous pouvons sans perte de généralité supposer α réel positif, et réécrire :

$$|\psi\rangle = \cos\theta'|0\rangle + e^{i\phi}\sin\theta'|1\rangle$$

avec

$$0 \leq \theta' < \frac{\pi}{2}, 0 \leq \phi < 2\pi$$

Cette représentation décrit ψ sans ambiguïté, sauf dans les cas où il est dans un état propre. Les paramètres ϕ et θ spécifient de manière unique un point sur la sphère unité de \mathbb{R}^3 ayant pour coordonnées cartésiennes :

$$\begin{cases} x = \sin 2\theta' \cos \phi \\ y = \sin 2\theta' \sin \phi \\ z = \cos 2\theta' \end{cases}$$

Dans cette représentation :

$$\begin{cases} |0\rangle \sim (0, 0, 1) \\ |1\rangle \sim (0, 0, -1) \end{cases}$$

On en reparlera en 1.1.4.

Exercice : On considère un qubit dans l'état quantique :

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

qui est la superposition des deux états logiques $|0\rangle$ et $|1\rangle$.

Suivant le système utilisé (spin $\frac{1}{2}$, photon, atome...) on aura par exemple :

$$|1\rangle = |+\rangle_z = |x\rangle = |e\rangle\dots$$

$$|0\rangle = |-\rangle_z = |y\rangle = |g\rangle\dots$$

1. Que peut-on trouver si on mesure l'état logique du qubit ?
2. Avec quelles probabilités ?
3. Qu'est-ce qui distingue le qubit d'un « bit aléatoire classique » auquel on attribuerait les mêmes probabilités de trouver 0 et 1 ?

1. Si l'on mesure l'état logique d'un qubit on trouve pour valeurs 0 ou 1.
2. Les probabilités de trouver chacune de ces valeurs sont respectivement α^2 et β^2
3. Ce qui distingue le qubit d'un bit aléatoire classique est que si on mesure une quantité ϕ dont ψ est état propre, on trouve à coup sûr $|\psi\rangle$. Ce résultat est certain !

1.1.4 Sphère de Bloch

La sphère de Bloch, du nom du physicien et mathématicien Félix Bloch, est une représentation géométrique d'un état pur d'un système quantique à deux niveaux ; c'est donc, entre autres, une représentation d'un qubit.

Sur la figure 1.1 le vecteur unitaire \vec{u} vaut :

$$\begin{cases} u_x = \sin \theta \cos \phi \\ u_y = \sin \theta \sin \phi \\ u_z = \cos \theta \end{cases}$$

Avec $\vec{S} \cdot \vec{u} = \frac{\hbar}{2} \vec{\sigma} \cdot \vec{u}$ où :

$$\vec{\sigma} \cdot \vec{u} = \begin{pmatrix} \cos \theta & \sin \theta e^{-i\phi} \\ \sin \theta e^{i\phi} & -\cos \theta \end{pmatrix}$$

Les valeurs propres de $\vec{\sigma} \cdot \vec{u}$ sont ± 1 et les états propres de $\vec{S} \cdot \vec{u}$ sont les états propres de $\vec{\sigma} \cdot \vec{u}$:

$$\begin{aligned} |+\vec{u}\rangle &= \cos \frac{\theta}{2} e^{-i\theta/2} |+_z\rangle + \sin \frac{\theta}{2} e^{i\phi/2} | -_z\rangle \\ |-\vec{u}\rangle &= -\sin \frac{\theta}{2} e^{-i\theta/2} |+_z\rangle + \cos \frac{\theta}{2} e^{i\phi/2} | -_z\rangle \end{aligned}$$

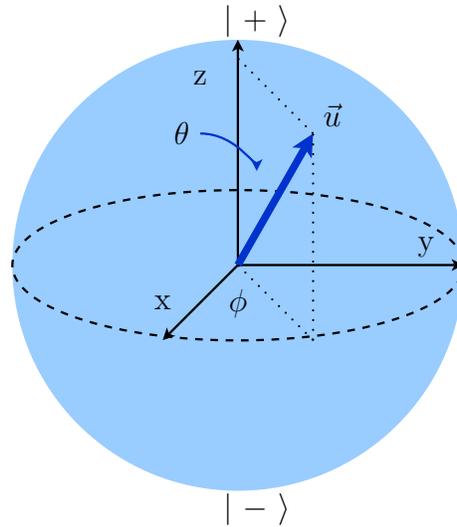


Figure 1.1. Sphère de Bloch (spin $\frac{1}{2}$). Repère l'état propre suivant la direction $\vec{u}(\theta, \phi)$.

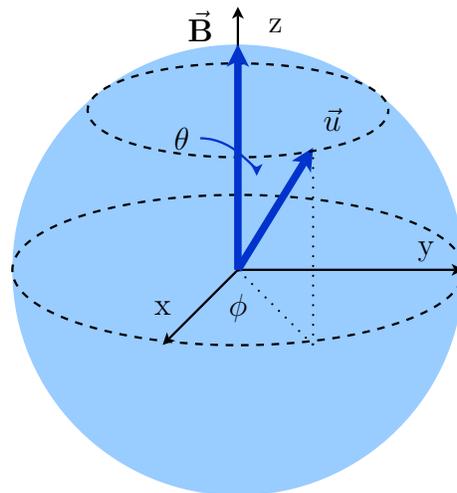


Figure 1.2. Sphère de Bloch (spin $\frac{1}{2}$). Précession de $\vec{u}(\theta, \phi)$ autour du champ $\vec{B} // O_z$.

Champ magnétique suivant O_z

Dans le cas d'un champ magnétique suivant O_z défini par :

$$H_z = \frac{\hbar g}{2} \sigma_z$$

$$|\psi(0)\rangle = \alpha |+_z\rangle + \beta |-_z\rangle$$

$$|\psi(t)\rangle = \alpha e^{-igt/2} |+_z\rangle + \beta e^{igt/2} |-_z\rangle$$

On peut utiliser la Sphère de Bloch comme sur la figure 1.2

L'évolution au cours du temps de \vec{u} qui précesse autour de \vec{B} est alors caractérisée par :

$$|\psi(0)\rangle = |_{+\vec{u}}\rangle = \cos \frac{\theta}{2} e^{-i\phi/2} |+_z\rangle + \sin \frac{\theta}{2} e^{i\phi/2} |-_z\rangle$$

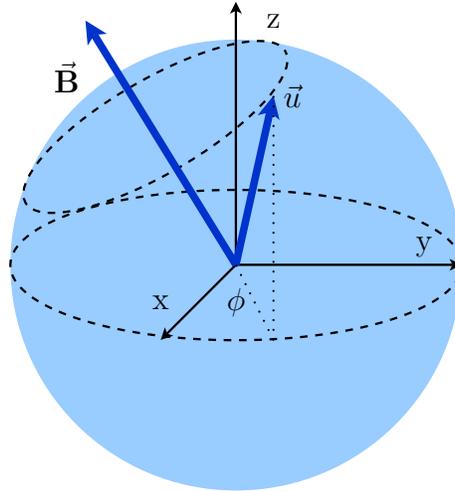


Figure 1.3. Sphère de Bloch (spin $\frac{1}{2}$). Précession de $\vec{u}(\theta, \phi)$ autour du champ \vec{B} quelconque.

$$|\psi(t)\rangle = \cos\frac{\theta}{2}e^{-i(\phi+gt)/2}|+_z\rangle + \sin\frac{\theta}{2}e^{i(\phi+gt)/2}|-_z\rangle$$

Champ magnétique quelconque

Dans le cas d'un champ magnétique quelconque nous avons la figure 1.3.

Où le champ magnétique quelconque est défini par :

$$H_z = \frac{\hbar g}{2}\sigma_z \cdot \frac{\vec{B}}{B}$$

1.1.5 Sphère de Poincaré

Si on a des photons polarisés au lieu de spins $\frac{1}{2}$, la Sphère de Bloch est remplacée par la sphère de Poincaré dessinée sur la figure 1.4. Les phénomènes sont très similaires et on parle toujours de qubits. En fait, en doublant les angles de polarisation des photos sur la représentation de la sphère, on peut se ramener à des états orthogonaux qui sont parallèles : un orienté vers le haut \uparrow l'autre vers le bas \downarrow . Au lieu d'avoir des états orthogonaux \uparrow et \rightarrow pour un photon. On utilise ainsi toute la sphère.

1.2 Produits tensoriels d'espaces d'états

1.2.1 Espace de travail, produit tensoriel

Pour décrire un système à plusieurs espaces d'états, l'outil mathématique approprié est le produit tensoriel des espaces d'états. Le principe est de décrire chaque l'état de chaque espace, et de considérer l'état total comme la combinaison des états des sous espaces.

Définition 1.2. *Produit tensoriel des espaces des états : on appelle espace produit tensoriel des espaces E_1, E_2 l'espace E noté $E_1 \otimes E_2$ engendré par « juxtaposition » des vecteurs de*

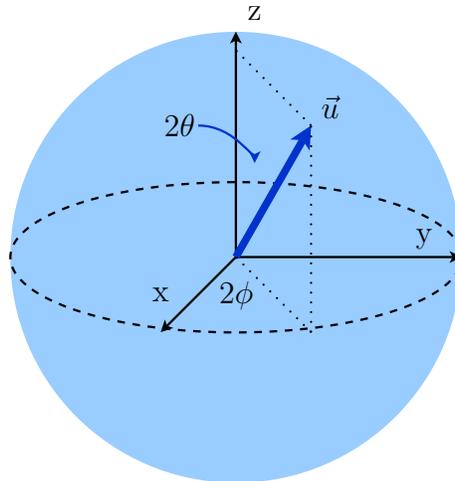


Figure 1.4. Sphère de Poncaré (photon polarisé) avec $\cos \varphi | x \rangle + e^{i(2\theta - \pi/2)} \sin \varphi | y \rangle$. Les points opposés ont des polarisation orthogonales. Le plan (x, y) représente les polarisation linéaires. Enfin les pôles représentent les polarisations circulaires.

base $|\phi_n^{(1)}\rangle$ et $|\phi_p^{(2)}\rangle$. Ainsi les vecteurs de base de E sont de la forme :

$$|\phi_{n,p}\rangle = |\phi_n^{(1)}\rangle \otimes |\phi_p^{(2)}\rangle$$

Les propriétés de l'espace ainsi défini sont les suivantes :

– Dimension de l'espace

$$\dim(E) = \dim(E_1) \times \dim(E_2) \quad (1.1)$$

– Produit scalaire dans E

Si $|\mu\rangle = |\mu_1\rangle \otimes |\mu_2\rangle$ et $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ alors

$$\langle \mu | \phi \rangle = \langle \mu_1 | \phi_1 \rangle \langle \mu_2 | \phi_2 \rangle$$

– Opérateurs dans E

Soit A_1 un opérateur sur E_1 et A_2 un opérateur sur E_2 . On définit alors $A = A_1 \otimes A_2$ par :

$$A(|\phi_{n,1}\rangle \otimes |\phi_{n,2}\rangle) = (A_1|\phi_{n,1}\rangle) \otimes (A_2|\phi_{n,2}\rangle)$$

– Abus de notation courants

– $A = A_1 \otimes I_2$ est souvent noté A_1

– $|\phi_1\rangle \otimes |\phi_2\rangle$ est souvent noté $|\phi_1\rangle|\phi_2\rangle$ ou même $|\phi_1, \phi_2\rangle$

⚠ Il faut noter les différence avec le produit cartésien noté $E_1 \times E_2$ défini par l'ensemble des doublets dont la première coordonnée est dans E_1 et la seconde dans E_2 (la dimension de l'espace produit est $\dim(E) = \dim(E_1) + \dim(E_2)$).

1.2.2 Intrication

Etats factorisables

Définition 1.3. Un état factorisable de E est un vecteur $|\psi\rangle$ pouvant s'écrire sous la forme :

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \quad (1.2)$$

Avec $|\psi_1\rangle \in E_1$ et $|\psi_2\rangle \in E_2$.

Factorisation et intrication

Soient de vecteurs $|\psi_1\rangle \in E_1$ et $|\psi_2\rangle \in E_2$ avec : $|\psi_1\rangle = \sum_n a_n |\phi_n^{(1)}\rangle$ et $|\psi_2\rangle = \sum_p b_p |\phi_p^{(2)}\rangle$

Alors :

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \sum_{n,p} a_n b_p |\phi_n^{(1)}\rangle \otimes |\phi_p^{(2)}\rangle$$

est un élément de E .



La Réciproque est fausse.

Théorème 1.4. *Il existe des vecteurs « intriqués » (ou non factorisables, entangle) de E ; ils ne peuvent pas s'écrire sous la forme $|\psi_1\rangle \otimes |\psi_2\rangle$.*

Preuve: Soit $|\psi\rangle = \sum_{n,p} c_{n,p} |\phi_n^{(1)}\rangle \otimes |\phi_p^{(2)}\rangle$, nous allons montrer que celui-ci n'est pas forcément factorisable.

On suppose que $|\psi\rangle$ est factorisable, on note N_1 et N_2 les dimensions respectives de E_1 et E_2 .

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \sum_{n,p} a_n b_p |\phi_n^{(1)}\rangle \otimes |\phi_p^{(2)}\rangle$$

On a donc $N_1 \times N_2$ équations du type $c_{n,p} = a_n b_p$. Les inconnues du système (les a_n et b_p) sont au nombre de $N_1 + N_2$. Le système est donc surcontraint et n'a donc pas forcément de solution. \square

1.2.3 Exemple : particules de spin 1/2

A titre d'illustration de ce qui précède, nous allons étudier deux particules de spin 1/2 pouvant se déplacer dans l'espace. On considère l'espace des états $\mathcal{E} = \mathcal{E}_r \otimes \mathcal{E}_s$.

Une base de \mathcal{E} est donnée par $\{|\mathbf{r}\rangle \otimes |\epsilon\rangle, \mathbf{r} = (x, y, z), \epsilon = \pm 1\}$ avec $S_z |\epsilon\rangle = \epsilon \frac{\hbar}{2} |\epsilon\rangle$. La fonction d'onde quant à elle est donnée par $\psi_\epsilon = (\psi_+(\mathbf{r}), \psi_-(\mathbf{r}))$.

Dans la suite on considère les états dans la base $\{|+\rangle, |-\rangle\}$ des états propres suivant z .

1. Donner une base de l'espace produit tensoriel

En appliquant la formule donnant la base de l'espace produit tensoriel, on obtient une base de dimension 4 :

$$\{|+, +\rangle, |+, -\rangle, |-, +\rangle, |-, -\rangle\}$$

2. Effectuer un changement de base pour que chaque vecteur de base devienne soit symétrique, soit antisymétrique par permutation des deux spins.

On remarque que $|+, +\rangle$ et $|-, -\rangle$ sont déjà symétriques. Comme les deux autres états sont des états opposés par permutation des spins : il vient que $\frac{1}{\sqrt{2}}(|+, -\rangle + |-, +\rangle)$

et $\frac{1}{\sqrt{2}}(|+, -\rangle - |-, +\rangle)$ sont respectivement symétrique et anti-symétrique. De plus la matrice :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

est bien une matrice de changement de base.

3. *Montrer qu'il y a trois états symétriques (états « triplets ») et un état anti-symétrique (état « singulet »).*

On reprend la base obtenue à la question précédente :

$|+, +\rangle, |-, -\rangle$ et $\frac{1}{\sqrt{2}}(|+, -\rangle + |-, +\rangle)$ sont des états symétriques.

$\frac{1}{\sqrt{2}}(|+, -\rangle - |-, +\rangle)$ est un état anti-symétrique.

4. *Montrer que l'état singulet est non séparable.*

On suppose que l'état $\frac{1}{\sqrt{2}}(|+, -\rangle - |-, +\rangle)$ est factorisable :

$$\begin{aligned} \frac{1}{\sqrt{2}}(|+, -\rangle - |-, +\rangle) &= (\alpha|+\rangle + \beta|-\rangle) \otimes (\gamma|+\rangle + \delta|-\rangle) \\ &= \alpha\gamma|+, +\rangle + \alpha\delta|+, -\rangle + \beta\delta|-, +\rangle + \beta\delta|-, -\rangle \end{aligned}$$

On obtient donc le système suivant :

$$\begin{cases} \alpha\gamma &= 0 \\ \beta\delta &= 0 \\ \alpha\delta &= \frac{1}{\sqrt{2}} \\ -\beta\gamma &= \frac{1}{\sqrt{2}} \end{cases}$$

qui n'a pas de solution. L'état singulet est donc intriqué.

1.2.4 « Paradoxe »EPR (Einstein, Podolski et Rosen)

Le paradoxe EPR est une expérience imaginée par Einstein, Podolski et Rosen qui vise tend à pourver que l'une des trois hypothèses suivantes est erronée pour la mécanique quantique :

- impossibilité pour un signal de dépasser la vitesse c (causalité relativiste) ;
- la mécanique quantique est complète et décrit entièrement la réalité (pas de variable cachée locale) ;
- les deux particules éloignées forment deux entités pouvant être considérées indépendamment l'une de l'autre, chacune étant localisée dans l'espace-temps (localité).

Le principe est de produire un système à deux particules (des photons sur la figure 1.2.4) dans un état intriqué. La mesure sur l'une des particules dans détermine avec une probabilité 1 l'état de l'autre particule spatialement séparée de la première et ce quelque soit la distance entre les deux particules.

Le point de vue de Niels Bohr est que rien ne détermine à priori l'état de la paire de particule avant la mesure. C'est la mesure qui détermine l'état de la première particule ce qui place la seconde dans le même état.

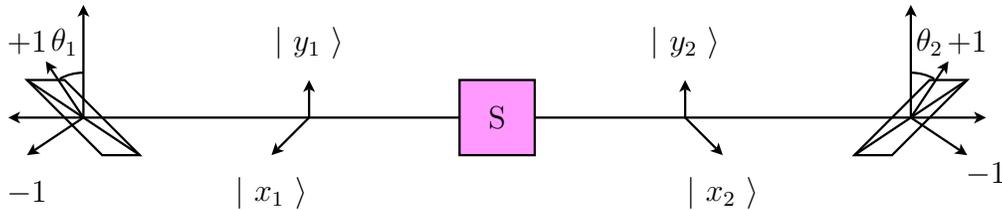


Figure 1.5. Paradoxe EPR

Principe de l'expérience

Si les deux mesures se font dans un intervalle de temps tel que la lumière n'a pas eu le temps de se propager entre les deux particules, aucune information n'a pu être transmise entre les deux particules. La théorie de Bohr est ainsi invalidée car une telle possibilité conduirait à une violation des inégalités de Heisenberg.

Cette hypothèse amène Einstein à vouloir compléter la mécanique quantique en y introduisant une variable cachée qui déterminerait à priori l'état du système.

Les inégalités de Bell et violations

On considère un système à « variables cachées » ou « paramètres supplémentaires » notés λ avec une distribution statistique $\rho(\lambda)$ normée : $\int d\lambda \rho(\lambda) = 1$

On introduit les fonctions $\epsilon_1(\lambda, \theta_1)$ et $\epsilon_2(\lambda, \theta_2)$ qui sont les fonctions statistiques donnant le résultat de la mesure par 1 et 2 en fonction de λ la variable cachée et θ l'angle de mesure.

On considère aussi la fonction de corrélation E qui lie les mesures des deux côtés :

$$E(\theta_1, \theta_2) = \int d\lambda \epsilon_1(\lambda, \theta_1) \epsilon_2(\lambda, \theta_2)$$

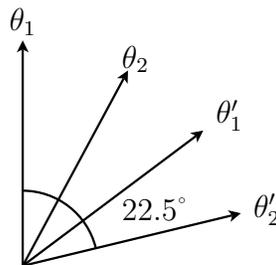
Pour deux directions de mesures de chaque côté $\theta_1, \theta'_1, \theta_2, \theta'_2$, alors pour :

$$S = E(\theta_1, \theta_2) + E(\theta'_1, \theta_2) + E(\theta_1, \theta'_2) - E(\theta'_1, \theta'_2)$$

et

$$|S| \leq 2$$

Pour les angles correspondants à la figure suivante :



On a une violation des inégalités de Bell ($S = 2\sqrt{2}$). Il n'y a donc pas de variable locale cachée en mécanique quantique, la théorie d'Einstein est donc réfutée. (La démonstration est effectuée en exercice)

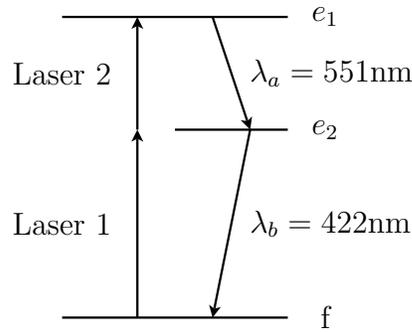


Figure 1.6. Schéma des niveaux de l'atome de calcium utilisés pour produire les paires de photons corrélés en polarisation.

Il est faut donc considérer que les deux particules une fois émises formes un système intriqué non local. Même si elles sont spatialement séparées, elles forment toujours un système unique. Pour en revenir aux trois règles qui pouvaient être violée par la mécanique quantique pour expliquer le paradoxe EPR, c'est donc la troisième qui ne s'applique pas (« les deux particules éloignées forment deux entités pouvant être considérées indépendamment l'une de l'autre, chacune étant localisée dans l'espace-temps (localité) »).

1.2.5 Tests expérimentaux des inégalités de Bell

Les premières expériences de test des inégalités de Bell ont été réalisées pour la première fois au début des années 1970. Ces expériences cherchaient à violer les inégalités de Bell en utilisant des photons (il est plus simple de fabriquer expérimentalement un état intriqué avec des photons). L'expérience proposée par Alain Aspect en 1976 qui utilise des polariseurs variables, a mis en évidence pour la première fois une violation claire des inégalités de Bell.

L'expérience proposée par Alain Aspect utilise des paires de photons émises dans une cascade atomique d'atomes de calcium (figure 1.6). Au moyen de lasers, ces atomes de calcium sont portés dans un niveau atomique excité e_1 . Celui-ci se désexcite vers un niveau excité e_2 en émettant un photon a de longueur d'onde $\lambda_a = 551\text{nm}$. Ce niveau e_2 se désexcite lui-même vers le niveau fondamental f en émettant un deuxième photon b de longueur d'onde $\lambda_b = 422\text{nm}$. Le niveau initial e_1 et le niveau final f sont de moment cinétique nul, alors que le niveau intermédiaire e_2 est de moment cinétique 1. Dans ces conditions, on peut montrer que l'état de polarisation de la paire de photons émises est :

$$|\Psi_p\rangle = \frac{1}{\sqrt{2}}(|a:\uparrow; b:\uparrow\rangle + |a:\rightarrow; b:\rightarrow\rangle)$$

Le dispositif expérimental proposé par Alain Aspect est présenté sur la figure 1.7. Le problème est qu'il faut modifier l'orientation des polariseurs plus vite que le temps de propagation de la lumière entre les deux polariseurs (40 nanosecondes pour $L = 12\text{m}$). Ceci est irréaliste avec des polariseurs massifs, mais devient possible avec des commutateurs optiques.

La première expérience mettant en évidence de façon claire une violation des inégalités de Bell à été faite à Orsay en 1982 (Aspect, Dalibar, Grangier, Roger) avec les caractéristiques suivantes :

- distance entre les polariseurs : $15\text{m} \rightarrow \frac{L}{c} = 50\text{ns}$

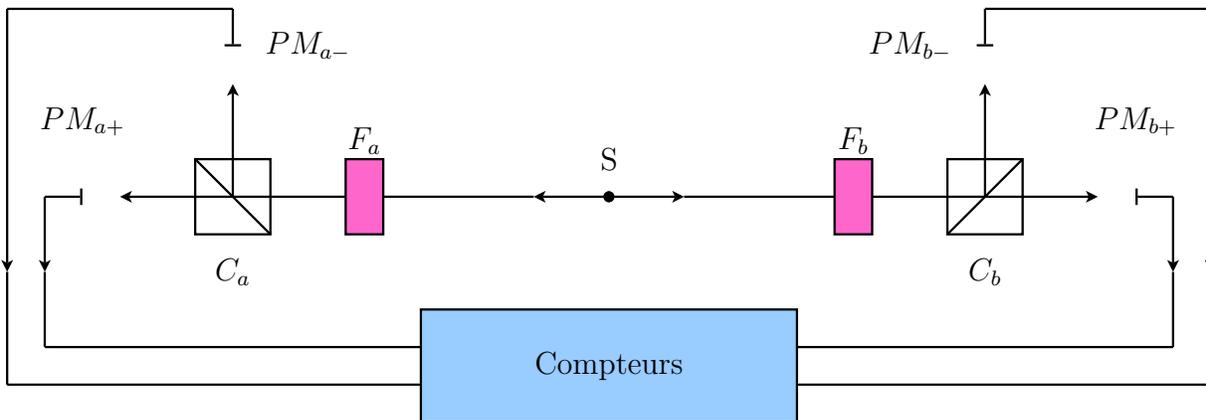


Figure 1.7. Les photons a et b sont filtrés en fréquence (F_a transmet les photons a et bloque les photons b , et vice versa pour F_b), puis détectés sur des photomultiplicateurs PM_{a+} , PM_{a-} , PM_{b+} et PM_{b-} . Les cubes polariseurs C_b et C_a transmettent soit vers PM_{b+} , soit vers PM_{b-} (et respectivement pour C_a). (Polariseur basculant).

- temps de commutation : 20ns
- violation des inégalités de Bell par 6 écarts-types (15h de comptage)
- excellent accord avec les prédictions quantiques

Puis à Innsbruck en 1998 Zeilinger, Weinfürter et collaborateurs ont reproduit cette expérience avec :

- distance entre les polariseurs : 400m (fibres optiques) $\rightarrow \frac{L}{c} = 1.3\mu\text{s}$
- commutations indépendantes et parfaitement aléatoires
- violation des inégalités de Bell par 30 écarts-types (10s de comptage)

Test expérimental des inégalités de Bell « à faire soi-même »

Il est possible aujourd'hui de faire plus facilement le test de violation des inégalités de Bell grâce au dispositif expérimental présenté sur la figure 1.8.

La source de photons intriqués en polarisation est constituée par une diode laser violette à 405nm focalisée sur deux cristaux non linéaire (BBO). Dans ces cristaux, un processus de conversion paramétrique peut se produire : un photon violet est alors transformé en une paire de photons jumeaux infrarouges à 810nm. L'un des cristaux peut donner des paires de photons de polarisation verticale, tandis que le second peut donner des paires de photons de polarisation horizontale. Ces photons sont émis symétriquement par rapport au faisceau de pompe dans un cône d'angle au sommet de 3 degrés environ.

Une lame $\frac{\lambda}{2}$ à 405nm et un compensateur de Babinet permettent d'ajuster l'état de polarisation des photons pompes (la diode est polarisée linéairement, quasi-verticale).

Sur chaque bras est disposé :

- Un diaphragme à iris
- un analyseur de polarisation constitué d'une lame $\frac{\lambda}{2}$ à 810nm et d'un cube séparateur de polarisation.
- une lentille pour focaliser le flux de photons sur les détecteurs
- un filtre interférentiel à 810nm de largeur 10nm.
- une photodiode à avalanche en mode comptage de photons

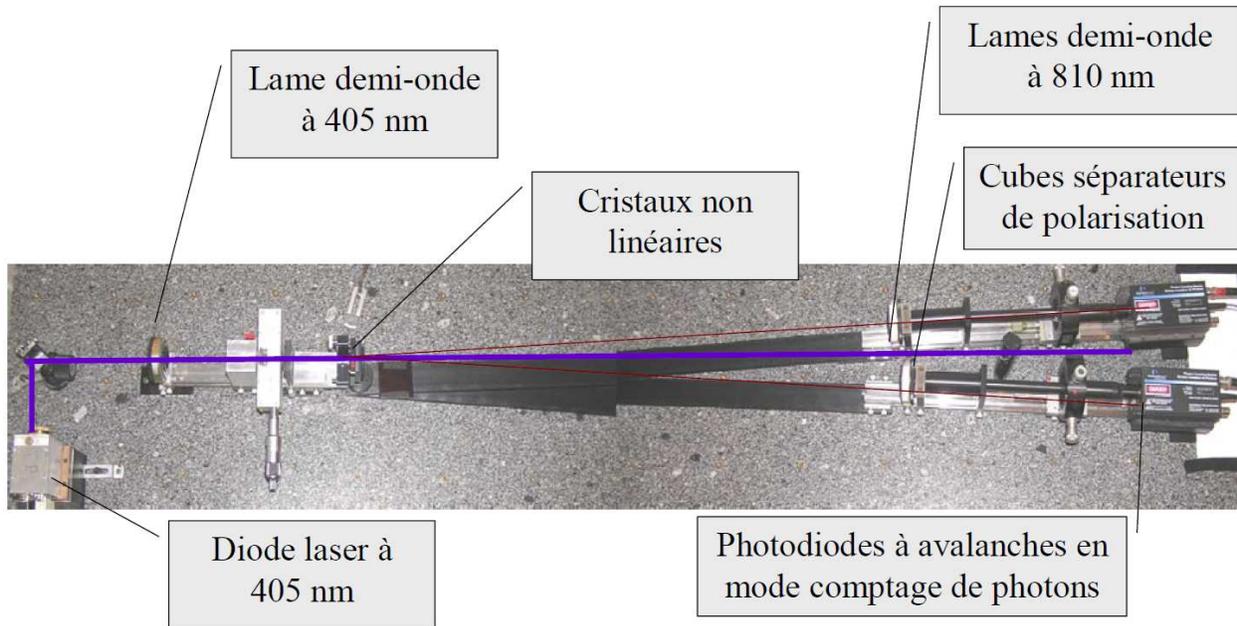


Figure 1.8.

Un détecteur de coïncidences permet de repérer les arrivées simultanées (à une fenêtre temporelle τ près) des paires de photons sur les deux compteurs de photons. Les nombres d'événements individuels et de coïncidences sont mesurés par 3 compteurs.

Quelques considérations sur les systèmes intriqués

En physique classique, on décrit les corrélations entre des mesures effectuées sur des sous-systèmes séparés en attribuant à chaque sous système des propriétés corrélées à celles de l'autre. si on veut reproduire les corrélations quantiques par un tel modèle, les inégalités de Bell montrent que ces propriétés devraient être non-locales (violer la causalité relativiste), ce qui est inacceptable.

La mécanique quantique reste en parfait accord avec la causalité relativiste. Mais ceci a un prix : il est impossible d'attribuer une « réalité physique locale » à l'état de chaque sous-système.

⚡ « Paradoxe EPR » (Einstein Podolsky Rosen) : « Non-séparabilité quantique »

Nous allons voir que l'intrication joue un rôle essentiel en mécanique quantique en général, et en information quantique en particulier...

Chapitre 2

Matrice densité, description des sous-systèmes

2.0.6 Nécessité de généraliser le vecteur d'état

Pour montrer que le vecteur d'état ne suffit pas, considérons une assemblée d'atomes d'argent (ils ont des spins 1/2) issus d'une expérience de Stern et Gerlach. Ces atomes ne sont pas polarisés, c'est-à-dire qu'on a autant de chance de trouver $\hbar/2$ et $-\hbar/2$ lors d'une mesure de S selon \vec{u} .

Si on se place dans la même description que précédemment, on obtient $|\psi\rangle = \frac{1}{\sqrt{2}}(|+_z\rangle + e^{i\theta}|-_z\rangle)$, mais cette description pour les mesures selon l'axe z ne marche que lorsque l'atome à un spin polarisé selon : $\vec{u} = \cos\phi\vec{e}_x + \sin\phi\vec{e}_y$, or on ne connaît pas à l'avance la polarisation du spin de l'atome, les prédictions de mesures sont erronées.

De même si on isole un spin d'un état singulet (intriqué) on ne peut pas lui attribuer un état défini.

Ces deux exemples suffisent à montrer que le vecteur d'état n'est pas suffisant pour décrire correctement l'état d'une particule ou d'un système. C'est pourquoi il est nécessaire d'introduire une notion plus générale : **l'opérateur (matrice) densité**.

2.0.7 L'opérateur densité

Pour toute cette partie, on pourra se référer à l'appendice D, consacré à l'opérateur densité, du livre « Mécanique Quantique » de Jean-Louis Basdevant et Jean Dalibard.

Intuition de l'opérateur

Soit le système se trouvant dans l'état $|\psi_i\rangle$ avec une probabilité Π_i (on travaille ici avec les statistiques classiques). La moyenne statistique lorsqu'on applique l'opérateur A est :

$$\langle A \rangle_{\text{stat}} = \sum_i (\Pi_i \langle \psi_i | \hat{A} | \psi_i \rangle)$$

Si maintenant on définit l'opérateur :

$$\hat{\rho} = \sum_i \Pi_i |\psi_i\rangle\langle\psi_i|$$

associé aux probabilités $0 \leq \Pi_i \leq 1$, on remarque que :

$$\text{Tr}(\hat{\rho}\hat{A}) = \sum_i \Pi_i \text{Tr}(|\psi_i\rangle\langle\psi_i|\hat{A}) = \sum_i (\Pi_i \langle\psi_i|\hat{A}|\psi_i\rangle)$$

L'opérateur densité pour les cas purs

Définition 2.1. Pour un système quantique décrit par $|\psi\rangle$ on pose :

$$\hat{\rho} = |\psi\rangle\langle\psi|$$

$\hat{\rho}$ est l'opérateur densité pour le système décrit par $|\psi\rangle$.

Il est possible de redéfinir la mécanique quantique par $\hat{\rho}$ à la place de $|\psi\rangle$.

- $\hat{\rho}$ est hermitien et sa trace vaut 1 ($\hat{\rho}$ est le projecteur sur l'état $|\psi\rangle$, toutes ces valeurs propres sont nulles hormis une qui vaut 1, pour celle-ci le vecteur propre est $|\psi\rangle$)
- Dans une mesure d'une quantité physique A décrite par l'observable \hat{A} , la probabilité de trouver la valeur propre a_α associée à l'état propre $|\phi_\alpha\rangle$ est :

$$\mathcal{P}(a_\alpha) = |\langle\phi_\alpha|\psi\rangle|^2 = \langle\psi|\phi_\alpha\rangle = \sum_{\beta} \langle\phi_\beta|\hat{\rho}\hat{P}_\alpha|\phi_\beta\rangle = \text{Tr}(\hat{\rho}\hat{P}_\alpha)$$

où $\hat{P}_\alpha = |\phi_\alpha\rangle\langle\phi_\alpha|$ (c'est le projecteur sur $|\phi_\alpha\rangle$). Il vient que :

$$\hat{P}_\alpha = \text{Tr}(\hat{\rho}\hat{P}_\alpha)$$

- Si maintenant $\hat{A} = \sum_\alpha a_\alpha \hat{P}_\alpha$, il vient :

$$\langle A \rangle = \text{Tr}(\hat{\rho}\hat{A})$$

- L'évolution de $\hat{\rho}$ est régie par l'équation de Schrödinger :

$$i\hbar \frac{d\hat{\rho}}{dt} = [\hat{H}(t), \hat{\rho}(t)]$$

Généralisation

On suppose que tout système peut être décrit par un opérateur densité $\hat{\rho}$. Les conditions sur $\hat{\rho}$ sont :

- $\hat{\rho}$ est hermitien et de trace 1 (lorsque l'état n'est pas pur $\hat{\rho}$ n'est pas forcément un projecteur).
- Toutes ses valeurs propres sont positives ou nulles.
- L'évolution hamiltonienne et les probabilités de mesure restent les mêmes que pour un cas pur :

$$\hat{P}_\alpha = \text{Tr}(\hat{\rho}\hat{P}_\alpha)$$

$$\langle A \rangle = \text{Tr}(\hat{\rho}\hat{A})$$

$$i\hbar \frac{d\hat{\rho}}{dt} = [\hat{H}(t), \hat{\rho}(t)]$$

Par définition comme $\hat{\rho}$ est hermitien, il est orthogonalement diagonalisable. Ainsi :

$$\hat{\rho} = \sum_i (\Pi_i |\psi_i\rangle\langle\psi_i|)$$

Remarque : On retrouve le cas pur quand un seul Π_i est non nul.

Mesure sur un mélange statistique

La valeur moyenne d'une grandeur physique A est donnée par :

$$\langle A \rangle = \text{Tr}(\hat{\rho}\hat{A}) = \sum_i \Pi_i \langle \psi_i | \hat{A} | \psi_i \rangle$$

On a donc bien correspondance entre **une loi de probabilité classique** et la moyenne au sens de $\hat{\rho}$.

Explications : On effectue une mesure sur un atome du mélange, on trouve $|\psi_j\rangle$ (avec une probabilité Π_j) parmi les $|\psi_i\rangle$. On considère le résultat de cette mesure comme acquis et on réitère le procédé sur un autre atome du mélange.

Le grand nombre de mesure ainsi effectué donne un résultat total moyenné par les probabilités Π_i (qui sont les probabilités de trouver $|\psi_j\rangle$ lors d'une mesure).

Exemple

Spin 1/2 dépolarisé Un spin est un système à deux états $|+\rangle$ et $|-\rangle$. L'état dépolarisé correspond à une incertitude totale suivant tout \vec{u} servant pour la mesure.

L'opérateur densité est :

$$\hat{\rho}_{\text{nonpol}} = \frac{1}{2} |+\rangle\langle+| + \frac{1}{2} |-\rangle\langle-| = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \hat{I}$$

Que l'on peut opposer à l'état pur $\frac{|+\rangle+|-\rangle}{\sqrt{2}}$, qui correspond en fait à un état polarisé selon une direction \vec{u} :

$$\hat{\rho}_{\text{pol } \vec{u}} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Qubit : système à deux états On cherche la matrice densité générale pour un système à deux états :

De manière générale, une matrice hermitienne de dimension 2 s'écrit :

$$\hat{M} = \alpha \hat{I} + \beta \hat{\sigma}_x + \gamma \hat{\sigma}_y + \delta \hat{\sigma}_z$$

où les matrices $\hat{\sigma}_x$, $\hat{\sigma}_y$ et $\hat{\sigma}_z$ sont les matrices de Pauli :

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\sigma}_y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

De plus la condition de trace égale à 1 impose que $\alpha = \frac{1}{2}$.

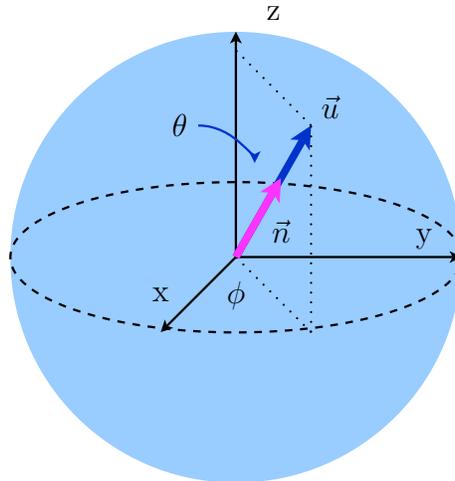


Figure 2.1. Généralisation de la sphère de Bloch : la « Boule de Bloch »

On peut donc écrire la matrice densité de la forme :

$$\hat{\rho} = \frac{1}{2}(\hat{I} + n_x\hat{\sigma}_x + n_y\hat{\sigma}_y + n_z\hat{\sigma}_z) = \frac{1}{2}(\hat{I} + \vec{n} \cdot \vec{\sigma})$$

où $\vec{n} = (n_x, n_y, n_z)$ et $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$.

Les valeurs propres de $\hat{\rho}$ sont égales à $\frac{1}{2}(1 \pm |\vec{n}|)$.

Généralisation de la sphère de Bloch

De manière générale on a :

$$\hat{\rho} = \frac{1}{2}(\hat{I} + n_x\hat{\sigma}_x + n_y\hat{\sigma}_y + n_z\hat{\sigma}_z) = \frac{1}{2}(\hat{I} + \vec{n} \cdot \vec{\sigma})$$

et les valeurs propres sont $\frac{1}{2}(1 \pm |\vec{n}|)$.

En utilisant le fait que $\text{Tr}(\sigma_i) = 0$, $\text{Tr}(\sigma_i\sigma_j) = 0$ et $\sigma_i^2 = \hat{I}_2$ où $i \in \{x, y, z\}$:

$$\begin{aligned} \langle \vec{\sigma} \rangle &= \text{Tr}(\hat{\rho}\vec{\sigma}) \\ &= \text{Tr}((\hat{I} + n_x\hat{\sigma}_x + n_y\hat{\sigma}_y + n_z\hat{\sigma}_z)\vec{\sigma}) \\ &= \begin{pmatrix} \text{Tr}(\sigma_x + n_x\hat{I}_2 + n_y\sigma_x\sigma_y + n_z\sigma_x\sigma_z) \\ \text{Tr}(\sigma_y + n_x\sigma_y\sigma_x + n_y\hat{I}_2 + n_z\sigma_y\sigma_z) \\ \text{Tr}(\sigma_z + n_x\sigma_z\sigma_x + n_y\sigma_z\sigma_y + n_z\hat{I}_2) \end{pmatrix} \\ &= \vec{n} \end{aligned}$$

En regardant sur la boule de Bloch, on remarque :

- si $|\vec{n}| = 1$ on peut poser $\vec{n} = \vec{u}$ et on retrouve le « cas pur » traité précédemment. L'opérateur $\hat{\rho}$ est alors le projecteur sur l'état $|+\vec{u}\rangle$, et on a $\langle \vec{\sigma} \rangle = \vec{u}$.
- si $|\vec{n}| < 1$ alors \vec{n} est « dans » la boule de Bloch, et on a toujours $\langle \vec{\sigma} \rangle = \vec{n}$.
- si $|\vec{n}| = 0$ alors le spin est dépolarisé : valeur moyenne nulle.

2.0.8 Sous-systèmes et intrication

Description d'un sous-système

Dans cette partie considérons un système \mathcal{S} formé de deux sous-systèmes \mathcal{S}_A et \mathcal{S}_B (un tel système serait un atome dans un champ magnétique ou deux particules de spin 1/2).

Définition 2.2. $\hat{\rho}$ est l'opérateur densité du système complet. On définit alors les **matrices densité réduites** $\hat{\rho}_A$ et $\hat{\rho}_B$ qui agissent respectivement dans \mathcal{S}_A et \mathcal{S}_B par :

$$\langle \psi_n | \hat{\rho}_A | \psi_{n'} \rangle = \sum_m \langle \psi_n, \phi_m | \hat{\rho} | \psi_{n'}, \phi_m \rangle$$

$$\langle \psi_m | \hat{\rho}_B | \psi_{m'} \rangle = \sum_n \langle \psi_n, \phi_m | \hat{\rho} | \psi_n, \phi_{m'} \rangle$$

Ces opérateurs densité partiels sont aussi appelés traces partielles sur \mathcal{S}_A et \mathcal{S}_B , et notés $\hat{\rho}_A = \text{Tr}_{\mathcal{S}_B}(\hat{\rho})$ et $\hat{\rho}_B = \text{Tr}_{\mathcal{S}_A}(\hat{\rho})$.

$\hat{\rho}_A$ et $\hat{\rho}_B$ sont hermitiens et de trace égale à 1. Ces opérateurs sont utiles lorsqu'on s'intéresse à la mesure d'une grandeur qui n'agit que sur l'un des sous-systèmes. Par exemple, si on considère une grandeur physique A , la probabilité de trouver la valeur propre a_α de \hat{A} est donnée par :

$$\mathcal{P}(a_\alpha) = \text{Tr}((P_\alpha \otimes \hat{I}_{\mathcal{S}_B})\hat{\rho}) = \text{Tr}(P_\alpha \hat{\rho}_A)$$

puis la valeur moyenne par :

$$\langle A \rangle = \text{Tr}(\hat{A} \hat{\rho}_A)$$

On remarque donc que utiliser l'opérateur densité revient à ne considérer pour des mesures qu'un des sous systèmes. Il contient toutes l'information nécessaire aux prédictions des résultats sur le sous-système sur lequel il agit.

Evolution des sous-systèmes

On considère ici deux sous systèmes qui n'interagissent pas entre eux. Le hamiltonien du système total \hat{H} s'écrit alors comme la somme des hamiltoniens de \mathcal{S}_A et \mathcal{S}_B :

$$\hat{H} = \hat{H}_A + \hat{H}_B$$

Puis les équations de Schrödinger (découplées) du système :

$$i\hbar \frac{d\hat{\rho}_A}{dt} = [\hat{H}_A(t), \hat{\rho}_A(t)] \quad i\hbar \frac{d\hat{\rho}_B}{dt} = [\hat{H}_B(t), \hat{\rho}_B(t)]$$

Comme les équations ne sont pas couplées, toute l'information pour calculer les mesures portant sur A est disponible à partir de $\hat{\rho}_A$. La connaissance de l'opérateur densité total ou du vecteur d'état du système global n'est pas nécessaire.

- En général, $\hat{\rho} \neq \hat{\rho}_A \otimes \hat{\rho}_B$, l'opérateur densité du système n'est pas factorisable.
- La différence entre $\hat{\rho}$ et $\hat{\rho}_A \otimes \hat{\rho}_B$ correspond aux corrélations contenues dans $\hat{\rho}$ qui ont été perdues lorsqu'on est passé à $\hat{\rho}_A$ et $\hat{\rho}_B$. Si on veut étudier les corrélations entre les deux sous-systèmes il est nécessaire de connaître la matrice densité globale.

Systèmes intriqués

Pour illustrer le fait que d'ordre général l'opérateur densité n'est pas factorisable, prenons l'exemple de « l'état singulet » pour 2 spins 1/2. Le vecteur d'état est alors :

$$|\psi_{\text{sing}}\rangle = \frac{1}{2}(|+, -\rangle - |-, +\rangle)$$

dans la base $\{|+, +\rangle, |+, -\rangle, |-, +\rangle, |-, -\rangle\}$ sa matrice densité est alors donnée par :

$$\hat{\rho}_{\text{sing}} = |\psi_{\text{sing}}\rangle\langle\psi_{\text{sing}}| = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \\ 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Nous allons maintenant calculer les opérateurs densités réduits.

Les matrices densités réduites sont des matrices 2×2 . On applique la définition de la matrice densité réduite pour les 4 coefficients :

Pour le sous-système A :

$$\langle + | \hat{\rho}_A | + \rangle = \sum_m \langle +, \phi_m | \hat{\rho} | +, \phi_m \rangle = \langle +, + | \hat{\rho} | +, + \rangle + \langle +, - | \hat{\rho} | +, - \rangle = \frac{1}{2}$$

$$\langle + | \hat{\rho}_A | - \rangle = \sum_m \langle +, \phi_m | \hat{\rho} | -, \phi_m \rangle = \langle +, + | \hat{\rho} | -, + \rangle + \langle +, - | \hat{\rho} | -, - \rangle = 0$$

$$\langle - | \hat{\rho}_A | + \rangle = \sum_m \langle -, \phi_m | \hat{\rho} | +, \phi_m \rangle = \langle -, + | \hat{\rho} | +, + \rangle + \langle -, - | \hat{\rho} | +, - \rangle = 0$$

$$\langle - | \hat{\rho}_A | - \rangle = \sum_m \langle -, \phi_m | \hat{\rho} | -, \phi_m \rangle = \langle -, + | \hat{\rho} | -, + \rangle + \langle -, - | \hat{\rho} | -, - \rangle = \frac{1}{2}$$

On obtient donc une matrice :

$$\hat{\rho}_A = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \hat{I}$$

de même :

$$\hat{\rho}_B = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \hat{I}$$

Il vient alors que :

$$\hat{\rho}_A \otimes \hat{\rho}_B = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{4} \hat{I}_4$$

On retrouve l'identité pour les matrices densités des sous-ensembles, c'est donc que les sous-ensembles sont totalement dépolarisés. On remarque aussi que le produit $\hat{\rho}_A \otimes \hat{\rho}_B \neq \hat{\rho}_{\text{sing}}$, $\hat{\rho}_A \otimes \hat{\rho}_B$ correspond à un système de dimension 2×2 totalement dépolarisé, il y a donc une perte des propriétés d'intrication par passage aux opérateurs densités réduits.

Les matrices densités partielles ne dépendent pas l'une de l'autre, la réduction du paquet d'onde ne permet donc pas de transfert d'information d'un sous-système à l'autre. Dans une expérience du type EPR, on ne peut donc pas transférer de l'information entre les deux particules distantes.

Chapitre 3

Exercices

3.0.9 Exercice 1 : Le paradoxe EPR (Einstein-Podolsky-Rosen) et les inégalités de Bell

Enoncé

On considère deux particules de spin 1/2 dans l'état singulet :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+_z, -_z\rangle - |-_z, +_z\rangle)$$

Les opérateurs spins des deux particules sont notés $\vec{\sigma}_1 = \vec{S}_1/(\hbar/2)$ et $\vec{\sigma}_2 = \vec{S}_2/(\hbar/2)$. Les kets $|\epsilon_{1z}, \epsilon_{2z}\rangle$ désignent les états propres communs à σ_{1z}, σ_{2z} , avec les valeurs propres $\epsilon_{1z} = \pm 1$ et $\epsilon_{2z} = \pm 1$. On suppose que les deux particules sont séparées spatialement, et qu'il sera donc possible de mesurer indépendamment une composante arbitraire de chacun des deux spins.

On rappelle que si on effectue une mesure le long du vecteur unitaire \vec{u} quelconque, repéré par ses angles polaires θ et ϕ (coordonnées sphérique), les états propres $|\pm_{\vec{u}}\rangle$ sont donnés par :

$$|+_{\vec{u}}\rangle = \cos\theta/2e^{-i\phi/2}|+_z\rangle + \sin\theta/2e^{i\phi/2}|-_z\rangle$$

$$|-_{\vec{u}}\rangle = -\sin\theta/2e^{-i\phi/2}|+_z\rangle + \cos\theta/2e^{i\phi/2}|-_z\rangle$$

1. On suppose que les deux particules s'éloignent dans les directions opposées le long de O_y . Donner l'expression de $|\psi\rangle$ dans une base $|\epsilon_{\vec{a}}, \epsilon_{\vec{b}}\rangle$ d'états propres $|\pm_{\vec{a}}\rangle$ pour la particule a et $|\pm_{\vec{b}}\rangle$ pour la particule b, où \vec{a} et \vec{b} sont deux vecteurs unitaires dans le plan xOz ($\phi_1 = \phi_2 = 0$) repérés par les angles θ_1 et θ_2 .
2. On fait une mesure instantanée des composantes $\sigma_{1a} = \vec{\sigma}_1 \cdot \vec{a}$ et $\sigma_{2b} = \vec{\sigma}_2 \cdot \vec{b}$ le long des directions définies par les vecteurs unitaires \vec{a} et \vec{b} .
 - (a) Quels sont les 4 résultats possibles ? Quelles sont les probabilités de ces résultats ?
 - (b) Quels sont les résultats possibles si l'on s'intéresse à une seule particule ? Quelles sont les probabilités de ces résultats ?

- (c) Quelle est la probabilité conditionnelle pour que la mesure effectuée sur la particule 2 donne le résultat $+1$, sachant que la mesure effectuée sur la particule 1 a donné le résultat -1 ?
- (d) On suppose que $\vec{a} = \vec{b}$. Montrer que le résultat de la mesure d'un des spins est parfaitement déterminé par le résultat de la mesure sur l'autre spin. Retrouver ce résultat par application du « principe de réduction du paquet d'onde ». Que peut on dire de la corrélation entre les résultats de ces mesures ?
- (e) Montrer que la valeur moyenne du produit des résultats $E_Q(\vec{a}, \vec{b}) = -\vec{a} \cdot \vec{b}$. Que signifie physiquement la valeur $|E_Q(\vec{a}, \vec{b})| = 1$?
3. Inégalité de Bell (1964) : l'argument avancé par Einstein, Podolsky et Rosen en 1935 est que lorsque les deux particules sont suffisamment éloignées, la valeur du spin de chaque particule doit avoir une valeur déterminée, indépendante de toute mesure effectuée sur l'autre particule. Suivant cette idée, John Bell a cherché à modéliser toutes les théories dans lesquelles il existerait une « variable cachée » λ qui prédéterminerait le résultat ± 1 des mesures de σ_{1_a} et σ_{1_b} par l'intermédiaire de deux fonctions « signe » :

$$A(\lambda, \vec{a}) = \pm 1, B(\lambda, \vec{b}) = \pm 1$$

Ce modèle est « local », car $A(\lambda, \vec{a})$ ne dépend pas de \vec{b} , ni $B(\lambda, \vec{b})$ de \vec{a} .

En notant $P(\lambda)$ la distribution de probabilité des variables λ , qui vérifient $\int d\lambda P(\lambda) = 1$, on a alors

$$E_C(\vec{a}, \vec{b}) = \int d\lambda P(\lambda) A(\lambda, \vec{a}) B(\lambda, \vec{b})$$

- (a) On considère 4 vecteurs $\vec{a}, \vec{a}', \vec{b}, \vec{b}'$, et on forme :

$$s(\lambda) = A(\lambda, \vec{a})B(\lambda, \vec{b}) + A(\lambda, \vec{a}')B(\lambda, \vec{b}) + A(\lambda, \vec{a}')B(\lambda, \vec{b}') - A(\lambda, \vec{a})B(\lambda, \vec{b}')$$

Montrer que $s(\lambda) = \pm 2$. On pourra mettre $s(\lambda)$ sous la forme :

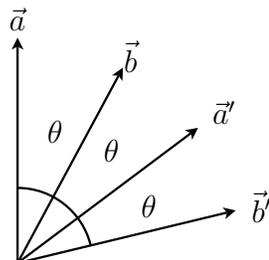
$$(A(\lambda, \vec{a}) + A(\lambda, \vec{a}'))B(\lambda, \vec{b}) + (A(\lambda, \vec{a}') - A(\lambda, \vec{a}))B(\lambda, \vec{b}')$$

et examiner les différentes valeurs possibles de $A(\lambda, \vec{a}) \pm A(\lambda, \vec{a}')$.

- (b) En déduire l'inégalité de Bell : $|S_C| \leq 2$ avec :

$$S_C = E_C(\vec{a}, \vec{b}) + E_C(\vec{a}', \vec{b}) + E_C(\vec{a}', \vec{b}') - E_C(\vec{a}, \vec{b}')$$

4. Le conflit Mécanique Quantique - Théorie à variables cachées. On considère la situation suivante :



(a) Montrer que la quantité :

$$S_Q = E_Q(\vec{a}, \vec{b}) + E_Q(\vec{a}', \vec{b}) + E_Q(\vec{a}', \vec{b}') - E_Q(\vec{a}, \vec{b}')$$

peut s'écrire : $S_Q = \cos(3\theta) - 3\cos(\theta)$.

(b) Montrer qu'il y a conflit entre les prédictions de S_Q et de S_C pour certaines valeurs de θ . Conclusion ?

Réponses

1. En inversant les relations de l'énoncé pour $\phi = 0$ on obtient :

$$|+_z\rangle = \cos(\theta/2)|+_u\rangle - \sin(\theta/2)|-_u\rangle$$

$$|-_z\rangle = \sin(\theta/2)|+_u\rangle + \cos(\theta/2)|-_u\rangle$$

d'où en omettant les vecteurs :

$$|+_z, -_z\rangle = \cos(\theta_1/2)\sin(\theta_2/2)|+_a, +_b\rangle + \cos(\theta_1/2)\cos(\theta_2/2)|+_a, -_b\rangle$$

$$- \sin(\theta_1/2)\sin(\theta_2/2)|-_a, +_b\rangle - \sin(\theta_1/2)\cos(\theta_2/2)|-_a, -_b\rangle$$

$$|-_z, +_z\rangle = \sin(\theta_1/2)\cos(\theta_2/2)|+_a, +_b\rangle - \sin(\theta_1/2)\sin(\theta_2/2)|+_a, -_b\rangle$$

$$+ \cos(\theta_1/2)\cos(\theta_2/2)|-_a, +_b\rangle - \cos(\theta_1/2)\sin(\theta_2/2)|-_a, -_b\rangle$$

et donc :

$$|\psi\rangle = (\sin((\theta_2 - \theta_1)/2)|+_a, +_b\rangle + \cos((\theta_2 - \theta_1)/2)|+_a, -_b\rangle - \cos((\theta_2 - \theta_1)/2)|-_a, +_b\rangle + \sin((\theta_2 - \theta_1)/2)|-_a, -_b\rangle)/\sqrt{2}$$

2. (a) Chaque mesure est normalisée pour donner un résultat ± 1 , donc on obtient les 4 possibilités $(+_a, +_b)$, $(+_a, -_b)$, $(-_a, +_b)$ et $(-_a, -_b)$ avec les probabilités :

$$P_{++} = P_{--} = \frac{1}{2}\sin^2\left(\frac{\theta_2 - \theta_1}{2}\right), P_{+-} = P_{-+} = \frac{1}{2}\cos^2\left(\frac{\theta_2 - \theta_1}{2}\right)$$

(b) Pour une particule on somme sur les résultats possibles pour l'autre, d'où :

$$P_+ = P_{++} + P_{+-} = 1/2 \text{ et } P_- = P_{--} + P_{-+} = 1/2$$

(c) $P_{\text{cond}} = PP_{+-}/P_- = \cos^2((\theta_2 - \theta_1)/2)$

(d) Si $\theta_2 = \theta_1$ alors $P_{\text{cond}} = 1$: corrélation totale entre les mesures.

(e) $E_Q = P_{++} - P_{+-} - P_{-+} + P_{--}$: fonction de corrélation.

$$E_Q = -\cos^2((\theta_2 - \theta_1)/2) + \sin^2((\theta_2 - \theta_1)/2) = -\cos(\theta_2 - \theta_1) = -\vec{a} \cdot \vec{b}$$

Si $|E_Q| = 1$ corrélation (ou anti-corrélation) totale entre les mesures.

3. $A(\lambda, \vec{a})$ et $A(\lambda, \vec{a}')$ sont soit égaux soit opposés.

- si égaux $A(\lambda, \vec{a}) + A(\lambda, \vec{a}') = \pm 2$ et $A(\lambda, \vec{a}) - A(\lambda, \vec{a}') = 0$ donc $s(\lambda) = \pm 2$

- si opposés $A(\lambda, \vec{a}) + A(\lambda, \vec{a}') = 0$ et $A(\lambda, \vec{a}) - A(\lambda, \vec{a}') = \pm 2$ donc $s(\lambda) = \pm 2$ cqfd. De plus, la moyenne sur une distribution de probabilité (positive normalisée) d'une quantité égale à ± 2 est comprise entre $+2$ et -2 , cqfd.

4. Pour les angles indiqués on a :

$$S_Q = -3 \cos(\theta) + \cos(3\theta)$$

Donc $dS_Q/d\theta = 3(\sin(\theta) - \sin(3\theta))$.

La dérivée s'annule pour $3\theta = \theta + 2n\pi$, ie $\theta = n\pi$ (minimum), ou $3\theta = \pi - \theta + 2n\pi$, ie $\theta = \pi/4 + n\pi/2$ (maximum).

On a donc $\theta = \pi/4$ ou $3\pi/4$, e

$$S_Q = -3 \cos(\pi/4) + \cos(9\pi/4) = -4 \cos(\pi/4) = -2\sqrt{2}$$

Finalement on a donc $|S_{Q,\max}| = 2\sqrt{2} > 2$: conflit !

3.0.10 Exercice 2 : Décomposition de Schmidt et « mise en gage de bit quantique »

Enoncé

On considère deux particules décrites dans des espaces d'états respectifs \mathcal{E}_A et \mathcal{E}_B . L'état quantique le plus général de la paire de particules s'écrit :

$$|\psi_{AB}\rangle = \sum_{i,j} c_{i,j} |u_i\rangle_A |v_j\rangle_B$$

où $\{|u_i\rangle_A\}$ et $\{|v_j\rangle_B\}$ sont des bases orthonormées de espaces \mathcal{E}_A et \mathcal{E}_B .

1. Montrer que l'on peut écrire : $|\psi_{AB}\rangle = \sum_i |u_i\rangle_A |w_i\rangle_B$ et donner l'expression de $|w_i\rangle_B$.
2. On considère maintenant l'opérateur densité $\hat{\rho} = |\psi_{AB}\rangle\langle\psi_{AB}|$ des deux particules, et on définit les opérateurs densité réduits : $\hat{\rho}_A = \text{Tr}_B(\hat{\rho})$, et $\hat{\rho}_B = \text{Tr}_A(\hat{\rho})$. Donner l'expression de $\hat{\rho}_A$ en fonction des produits scalaires $\langle w_i | w_j \rangle$.
3. On suppose que $\hat{\rho}_A$ est diagonal dans la base $\{|u_i\rangle_A\}$, c'est-à-dire que :

$$\hat{\rho}_A = \sum_i p_i (|u_i\rangle\langle u_i|)_A.$$

En déduire que les vecteurs $\{|w_j\rangle_B\}$ sont orthogonaux. Quelle est la valeur de la norme de $|w_j\rangle_B$?

4. En déduire que l'on peut écrire :

$$|\psi_{AB}\rangle = \sum_{i,j} \sqrt{p_i} |u_i\rangle_A |\tilde{w}_i\rangle_B$$

où $\{|\tilde{w}_i\rangle_B\}$ est une base orthonormée que l'on précisera.

5. Cette expression s'appelle la décomposition de Schmidt de l'état ψ_{AB} . En utilisant cette décomposition donner une expression simple de $\hat{\rho}_B$, et montrer que $\hat{\rho}_A$ et $\hat{\rho}_B$ ont les mêmes valeurs propres non nulles. Le nombre de telles valeurs propres est appelé *nombre de Schmidt*.
6. On dit que l'état ψ_{AB} est *séparable* si et seulement si il peut s'écrire sous une forme factorisée $\psi_{AB} = |\phi_A\rangle |\chi_B\rangle$. Un état non séparable appelé aussi *intriqué*. Montrer qu'un tel état est séparable si et seulement si le nombre de Schmidt est égal à 1.
7. Mise en gage de bit quantique (« Quantum Bit Commitment »)

La mise en gage de bit est une « primitive » cryptographique, qui est très utile pour construire des protocoles plus complexes, en particulier dans les d'enchères ou de paris. Le protocole se déroule en deux étapes :

1. mise en gage : Alice confie à Bob un bit qu'il ne peut pas lire, mais qu'Alice ne peut plus changer. Par exemple, Bob reçoit un coffre-fort contenant le bit, mais Alice conserve la clé.
2. révélation : Alice permet à Bob de lire le bit. Dans l'exemple ci-dessus, elle donne la clé du coffre à Bob.

Existe-t-il une version quantique de ce protocole, c'est-à-dire une *mise en gage de bit quantique (quantum bit commitment)*?

Imaginons par exemple le protocole suivant :

1. Alice prépare deux états intriqués **orthogonaux** $|\psi_{AB}^{(0)}\rangle$ et $|\psi_{AB}^{(1)}\rangle$. Si elle veut gager le bit 0 (resp. le bit 1) elle donne à Bob la partie B de $|\psi_{AB}^{(0)}\rangle$ (resp. de $|\psi_{AB}^{(1)}\rangle$), et conserve la partie A. Quelle est la condition pour que Bob soit incapable de distinguer entre les deux choix d'Alice?

Pouvez-vous donner un exemple simple de deux états vérifiant ces conditions ?

2. Lors de la révélation, Alice donne la partie A à Bob, qui peut alors faire une mesure distinguant les deux états (puisque'ils sont orthogonaux) et en déduire le choix d'Alice. Ce protocole est-il satisfaisant (penser aux décompositions de Schmidt...)?

Réponses

1. On a $|\psi_{AB}\rangle = \sum_{i,j} c_{ij} |u_i\rangle |v_j\rangle$, en sommant d'abord sur j puis sur i, on obtient :

$$|\psi_{AB}\rangle = \sum_{i,j} c_{ij} |u_i\rangle_A |v_j\rangle_B = \sum_i |u_i\rangle_A \left(\sum_j c_{ij} |v_j\rangle_B \right) = \sum_i |u_i\rangle_A |w_i\rangle_B$$

en identifiant $\sum_j c_{ij} |v_j\rangle_B = |w_i\rangle_B$

2. En utilisant l'expression de $|\psi_{AB}\rangle$ précédente, on a :

$$\rho = |\psi_{AB}\rangle \langle \psi_{AB}| = \sum_{i,j} (|u_i\rangle \langle u_j|)_A (|w_i\rangle \langle w_j|)_B$$

Il vient pour ρ_A que :

$$\begin{aligned} \langle u_n | \rho_A | u_{n'} \rangle &= \sum_k \langle u_n, v_k | \rho | u_{n'}, v_k \rangle = \langle u_n |_A (\sum_k \langle v_k | \rho | v_k \rangle) | u_{n'} \rangle_A \\ \rho_A &= \sum_k \langle v_k | \rho | v_k \rangle \\ &= \sum_{i,j,k} (| u_i \rangle \langle u_j |)_A \langle v_k | w_i \rangle \langle w_j | v_k \rangle \\ &= \sum_{i,j,k} (| u_i \rangle \langle u_j |)_A \langle w_j | v_k \rangle \langle v_k | w_i \rangle \\ &= \sum_{i,j} (| u_i \rangle \langle u_j |)_A \langle w_j | \sum_k (| v_k \rangle \langle v_k |) ket w_i \\ &= \sum_{i,j} (| u_i \rangle \langle u_j |)_A \langle w_j | w_i \rangle \end{aligned}$$

en utilisant le fait que $\sum_k (| v_k \rangle \langle v_k |) = I$.

3. Pour montrer que les $\{w_i\}$ sont orthogonaux ont identifie les deux expression de ρ_A :

$$\sum_{i,j} (| u_i \rangle \langle u_j |)_A \langle w_j | w_i \rangle = \sum_i p_i (| u_i \rangle \langle u_i |)_A$$

On remarque que :

$\langle w_j | w_i \rangle = 0$ si $i \neq j$, donc les $\{w_i\}$ sont orthogonaux.

$\langle w_i | w_i \rangle = p_i$ donc la norme de $| w_i \rangle$ est égale à $\sqrt{p_i}$.

4. On pose $| \tilde{w}_i \rangle = \frac{| w_i \rangle}{\sqrt{p_i}}$, alors par la question précédente, la base $\{\tilde{w}_i\}$ est orthonormée et on a la relation :

$$| \psi_{AB} \rangle = \sum_{i,j} \sqrt{p_i} | u_i \rangle_A | \tilde{w}_i \rangle_B$$

5. En utilisant la décomposition de Schmidt de l'état $| \psi_{AB} \rangle$:

$$\begin{aligned} \rho_A &= \sum_k \langle u_k | \rho | u_k \rangle \\ &= \sum_{i,j,k} \sqrt{p_i} \sqrt{p_j} \langle u_k | u_i \rangle \langle u_j | u_k \rangle | \tilde{w}_i \rangle \langle \tilde{w}_j | \\ &= \sum_{i,k} p_i \langle u_k | u_i \rangle \langle u_i | u_k \rangle | \tilde{w}_i \rangle \langle \tilde{w}_i | \\ &= \sum_{i,k} p_i \langle u_i | u_k \rangle \langle u_k | u_i \rangle | \tilde{w}_i \rangle \langle \tilde{w}_i | \\ &= \sum_i p_i \langle u_i | (\sum_k | u_k \rangle \langle u_k |) | u_i \rangle | \tilde{w}_i \rangle \langle \tilde{w}_i | \\ &= \sum_i p_i \langle u_i | u_i \rangle | \tilde{w}_i \rangle \langle \tilde{w}_i | \\ &= \sum_i p_i | \tilde{w}_i \rangle \langle \tilde{w}_i | \end{aligned}$$

car $\langle u_i | u_i \rangle = 1$ ($\{u_i\}$ est orthonormée).

Les matrices densités partielles ρ_A et ρ_B ont donc bien les mêmes valeurs propres non nulles, qui valent p_i .

6. Par les question précédentes, le nombre de Schmidt est le égal à 1 si et seulement si il n'y a qu'un seul p_i donc $\psi_{AB} = | \phi_A \rangle | \chi_B \rangle$, ce qui est équivalent à dire que ψ_{AB} est séparable.
7. Bob sera incapable de distinguer entre les deux choix d'Alice si les matrices densités « tracées » (ie les composantes de la diagonale de ρ_B sont identiques) :

$$\rho_B^{(0)} = Tr_A(| \psi_{AB}^{(0)} \rangle \langle \psi_{AB}^{(0)} |) = \rho_B^{(1)} = Tr_A(| \psi_{AB}^{(1)} \rangle \langle \psi_{AB}^{(1)} |)$$

Un exemple simple d'états vérifiant ces conditions pour 2 spins 1/2 est :

Mais ce protocole n'est pas satisfaisant car Alice peut tricher. Pour le voir écrivons les décompositions de Schmidt :

Mais les matrices densité du côté de Bob doivent être identiques, donc on a :

Pour tricher, c'est-à-dire pour passer de $|\psi_{AB}^{(0)}\rangle$ à $|\psi_{AB}^{(1)}\rangle$ sans que Bob s'en aperçoive, il suffit qu'Alice transforme ses états $\{|\phi_A\rangle\}$ en états $\{|\psi_A\rangle\}$.

Il faut donc qu'elle fasse sur la partie qu'elle a conservée un changement de base (entre deux bases orthogonales), c'est-à-dire une transformation unitaire. C'est précisément ce que peut faire un ordinateur quantique.

De façon générale, il a été démontré que le « quantum bit commitment » ne peut pas être sûr face à un ordinateur quantique de puissance illimitée (théorèmes de Mayers, Lo et Chau).