# Traitement quantique de l'information

Notes du cours du Prof. Vincenzo Savona
Institut de théorie des phénomènes physiques (ITP)
Groupe de théorie des nanosystèmes

Gaelle Giesen
23 décembre 2011
version préliminaire

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

# Table des matières

# 1 Introduction

Le traitement quantique de l'information est un nouveau paradigme de représentation et manipulation de l'information, basé sur les lois de la physique quantique. A l'aide de ce nouveau paradigme il est possible d'accomplir certaines tâches qui sont impossibles avec l'informatique classique. Dans ce cours nous allons répondre aux questions suivantes :

i Quel paradigme ? Comment représenter, manipuler et lire l'information quantique ?

ii Quelle utilité ? Dans quels cas le traitement quantique de l'information est-il plus avantageux que l'informatique classique ?

iii Quelle réalisation pratique ? Comment fabriquer des registres de mémoire et effectuer des opérations en pratique ?

iv Comment construire ce paradigme ? Quels sont les détails des algorithmes, des protocoles de communication, des techniques de correction d'erreur, etc ?

La première partie de ce cours abordera principalement les questions (i), (ii), et (iii), tandis que le vaste chapitre de la construction d'algorithmes et de protocoles pour le traitement de l'information quantique sera traité dans le deuxième semestre. Naturellement, il faudra d'abord introduire les principes de la mécanique quantique. Cette introduction sera orientée à l'acquisition des notions nécessaires pour comprendre le traitement quantique de l'information. Beaucoup plus d'importance sera donnée aux éléments formels de la mécanique quantique (par exemple la théorie de la mesure) qu'aux aspects plus physiques (par exemple la mécanique quantique d'une particule soumise à une force). Dans la mesure du possible, nous alternerons aspects physiques du cours et chapitres plus liés à l'information. Par exemple, nous toucherons à la cryptographie quantique, à la téléportation, et à quelques éléments de calcul quantique.

Pour donner une vision d'ensemble du cours, commençons par une introduction, en partie historique, au traitement quantique de l'information, en donnant des réponses sommaires aux quatre questions ci-dessus.

## Le paradigme

L'idée de concevoir un paradigme d'information basé sur la mécanique quantique est presque évidente. Les machines de calcul sont faite de matière et elles fonctionnent sur la base de la conduction de courant dans des semiconducteurs. La plupart des télécommunications modernes se fait par le biais de la propagation de lumière dans des fibres optiques. Quant à elle, la mé-

canique quantique est l'ensemble de lois qui régissent le comportement de la matière et de la lumière, particulièrement à l'échelle microscopique. Il est donc évident qu'un paradigme d'information qui soit réalisable en pratique, doit obéir aux lois de la mécanique quantique.
Nous pourrions objecter que les ordinateurs d'aujourd'hui - et plus en général les technologies pour le traitement de l'information - sont basées sur la micro-électronique à semi-conducteur, dont le fonctionnement est déjà décrit par les lois de la physique quantique. Pourquoi donc il ne sont pas considérés "quantiques". En effet, ces technologies n'utilisent qu'un sous-ensemble des comportements de la matière prévus par la physique quantique. Ce sous-ensemble correspond à des schémas que nous pourrions reproduire avec une technologie classique (pourvu qu'on accepte un ralentissement conséquent de la vitesse de calcul). Par exemple, il serait envisageable de réaliser des registres binaires et leurs connexions avec des élément mécanique, le tout *alimenté* par un moteur ou par une manivelle (c'est d'ailleurs de cette façon que les premières machines de calcul étaient conçues). Tout cela serait très bien décrit par les lois de la mécanique de Newton. Le traitement quantique de l'information, par contre, exploite des comportements de la matière prévus par la physique quantique, mais qui n'ont pas d'analogie dans le monde classique. Ces comportements dans leur ensemble sont connus sous le nom de *corrélations quantiques*. Le fameux paradoxe du chat de Schrödinger et les états *intriqués* de la matière en sont les exemples les plus populaires. Au niveau de la recherche fondamentale, et en se restreignant à un très petit nombre de particules, ces états sont aujourd'hui produit dans des centaines de laboratoires autour du monde. Ils sont également utilisés dans la cryptographie quantique, dont nous parlerons dans la suite.

## L'utilité du paradigme

Il est intéressant de parcourir brièvement l'histoire de l'information quantique. Un soucis des chercheurs dans les années '70 était la *réversibilité* du calcul. Le paradigme actuel - basé sur la représentation numérique de l'information en utilisant le code binaire, et sur les portes logiques élémentaires telles que le $XOR$ - est un paradigme irréversible. Réfléchissez au fonctionnement d'une porte $XOR$. Voici sa table de fonctionnement :

| A | B | C |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

L'opération $XOR$ est clairement irréversible : si on nous donne l'output (0 ou 1), il est impossible de déduire quelles étaient les deux bits en input. L'irréversibilité a une conséquence importante en physique. La thermodynamique nous dit qu'une transformation irréversible d'un système produit une variation de l'entropie de ce système. Á une augmentation d'entropie correspond, selon les principes de la thermodynamique, une dissipation d'énergie. Dans le cas de l'$XOR$, le nombre de combinaisons en entrée est 4 et le nombre de combinaisons en sortie est 2. Á une réduction d'un facteur 2 du nombre de configurations du système correspond une diminution d'entropie de (au minimum) $k_B \ln(2)$ et, selon la thermodynamique, une dissipation d'énergie de (au minimum) $k_B T \ln(2)$ (où $k_B$ est la constante de Boltzmann et $T$ est la température).
Aujourd'hui nous sommes encore lointain de cette limite : les ordinateurs dissipent beaucoup plus d'énergie par opération logique élémentaire. Toutefois, les scientifique se posaient la question de comment réduire cette limite. La réponse est assez immédiate : si on arrive à créer des éléments de calcul réversibles, alors la limite théorique à l'énergie dissipée est arbitrairement petite. Ces portes logiques élémentaires ont été conçues, mais à aujourd'hui elle ne sont pas encore utilisées puisque la limite théorique prévue par la thermodynamique est encore très distante. Le problème de la réversibilité à entraîné la question, s'il est possible physiquement de réaliser des portes logiques réversibles. C'est ici que les physiciens ont joué un rôle essentiel.
Tout d'abord, ils ont observé que les lois de la mécanique quantique impliquent automatiquement la réversibilité, comme nous le verrons dans les prochaines semaines. Il est donc possible de concevoir des dispositifs quantiques qui reproduisent le fonctionnement des portes logiques réversibles élémentaires. C'est à ce point que Richard P. Feynman, Prix Nobel pour la physique en 1965, qui s'intéressait à la physique du traitement de l'information, à fait en 1982 la suggestion donnant naissance à l'information quantique proprement dite. Feynman à observé que la mécanique quantique ouvrait la porte à des opportunités de calcul infiniment plus vastes que la simple réalisation des portes logiques réversibles classiques. Il avait réfléchi de la manière suivante : La simulation - avec un ordinateur classique - du comportement d'un système physique obéissant aux lois de la mécanique quantique, est un

problème de complexité exponentielle (le temps augmente exponentiellement en fonction de la taille du système qu'on souhaite simuler). Par contre, un système obéissant aux lois de la physique classique peut être simulé en un temps polynomial (cf. exercices). Nous pourrions voir cela comme une limitation du calcul classique. Feynman par contre y a vu une opportunité : la nature est capable d'effectuer avec une complexité linéaire (dans le temps) une certaine tâche (l'évolution temporelle d'un système quantique) qu'un ordinateur classique ne peut effectuer qu'avec complexité exponentielle. Donc, si nous arrivions à concevoir une sorte de machine de calcul quantique universelle qui peut traduire une tâche quelconque en la tâche de faire évoluer un système quantique (sans augmentation de complexité), alors nous pourrions utiliser la nature, régie par les lois de la mécanique quantique, comme outil de calcul très efficace.
Une telle machine de calcul universelle (valable pour n'importe quel algorithme) n'existe toujours pas. Par contre nous avons conçu plusieurs algorithmes quantiques capable d'effectuer certaines tâches qui n'étaient pas traitable par les ordinateurs classiques. Le premier algorithme quantique à été pensé par Deutsch en 1985. Il permet de dire si un fonction $f(x)$ d'un registre à un bit $x$ est dégénérée ($f(0) = f(1)$) ou non-dégénérée ($f(0) \neq f(1)$) en une seule opération (avec un ordinateur classique il faut évaluer la fonction deux fois). C'est le premier exemple de *parallélisme quantique*. Plus tard, en 1994, l'algorithme de Shor à été découvert. C'est un algorithme qui permet de trouver un facteur d'un nombre entier avec complexité polynomiale (le problème est notamment NP avec le calcul classique, c-à-d nous savons seulement le résoudre qu'avec complexité exponentielle). L'algorithme de Shor est le moteur de toute la recherche sur le traitement quantique de l'information jusqu'à nos jours, à cause de ses implication pour la transmission sécurisée de données. D'autres algorithmes efficaces ont été trouvés, comme l'algorithme de Grover pour la recherche dans une base de données non structurée, mais l'intérêt fondamental de l'information quantique reste la possibilité de trouver des facteurs premiers de manière efficace.
Pour comprendre cela il faut considérer l'autre innovation introduite par le traitement quantique de l'information : la cryptographie quantique.

## La cryptographie quantique

Commençons pas quelques considérations sur la cryptographie classique. Du point de vue classique, le vrai problème de la cryptographie est le partage de clés. Une fois que A et B partagent la même clé - tout en étant sûrs que personne d'autre a pu y accéder - l'utilisation d'un algorithme de cryptographie standard, du type de l'AES, présente un niveau de sécurité

maximale. Pour partager une clé par contre, A et B doivent utiliser un canal de communication non crypté (autrement le problème se reproduit tout simplement). Ce problème est aujourd'hui résolu grâce aux protocoles dits *à clé publique* ou *à clé asymétrique*. Le principe de fonctionnement du protocole à clé publique - par exemple le RSA - est le suivant. Supposez de connaître une fonction $f(x)$, où $x$ est la clé que nous devons partager, ainsi que sa fonction inverse $f^{-1}(x)$. Supposez également que la tâche de déduire $f^{-1}(x)$ à partir de $f(x)$ soit non traitable par un ordinateur (par exemple, elle est de complexité exponentielle en fonction de la taille de la clé $x$). L'interlocuteur A rend la fonction $f$ publique (par exemple en la publiant sur internet), tout en gardant soigneusement $f^{-1}$ secrète. L'interlocuteur B dispose d'une autre paire de fonctions $g$ et $g^{-1}$ avec les mêmes caractéristiques, et il publie a son tour $g$. Les fonctions $f$ et $g$ sont les clés publiques, tandis que les deux inverses représentent les clés privées. Pour partager une clé $x$ avec B, A télécharge la clé publique de B $g$. Puis il calcule la fonction $y = f^{-1}(g(x))$ et envoie le résultat à B sur un canal non crypté. B télécharge la clé publique $f$ de A, l'applique à $y$ et puis il applique au résultat sa propre clé privée $g^{-1}$. Le résultat est $z = g^{-1}(f(f - 1(g(x)))) = x$. B donc connaît $x$. Pour voler la clé, un espion devrait connaître la fonction $g^{-1}$, mais cela est impossible puisque on ne dispose pas de ressources pour inverser la fonction $g$. La paire de fonctions $f$ et $f^{-1}$ est un exemple de problème que nous ne savons pas inverser. Calculer $f(f^{-1}(x))$ pour vérifier qu'il s'agit de la fonction identique est immédiat. Par contre déduire $f^{-1}$ de $f$ est impossible. Les algorithmes tels que le RSA basent la construction des fonctions $f$ et $f^{-1}$ sur le problème de la factorisation d'un nombre entier $N$ très grand. Trouver les facteurs premiers de $N$ est une tâche pour laquelle nous ne connaissons que des algorithmes ayant complexité exponentielle. Si par contre nous connaissons les facteurs $N_1$ et $N_2$, vérifier que $N_1 * N_2 = N$ est immédiat avec un effort computationnel négligeable.

Vous comprenez maintenant le lien entre la cryptographie et le calcul quantique, en particulier l'algorithme de Shor. Si on disposait d'un ordinateur quantique capable d'exécuter l'algorithme de Shor, on aurait accès à toutes les données échangées par le biais de la cryptographie à clé publique, grâce à la possibilité de déduire l'inverse de la fonction clé publique $f(x)$. Heureusement, la mécanique quantique nous permet de réaliser un nouveau type de protocole de partage de clé, typiquement connu sous le nom de cryptographie quantique. Dans la cryptographie quantique on utilise un seul photon à la fois pour transmettre un bit d'information. La sécurité du protocole se base sur deux principes fondamentaux de la physique quantique : (1) on ne peut pas effectuer un mesure sur un système physique sans en modifier son état ;

(2) on ne peut pas connaître pleinement l'état d'un système avec une mesure. Nous aurons une idée plus précise de cela quand nous discuterons la théorie de la mesure dans le contexte de l'introduction à la mécanique quantique. Si un espion essaie de lire l'information transmise entre A et B, il modifiera l'état des photons utilisés, d'une manière que B peut détecter. Il suffit que B jette les bits qui ont été espionnés, tout en gardant ceux qui sont passés intacts (une clé peut se composer de bits aléatoires). Un signal de communication classique, par contre, est typiquement fait d'un grand nombre de photons, et il devient possible pour l'espion d'effectuer une mesure avec un impact minime - à la limite non détectable - sur le signal.

## Autres technologies

A côté du calcul et de la cryptographie quantique, la mécanique quantique ouvre d'autres possibilités, comme par exemple les expériences de téléportation (à mi chemin entre la téléportation à la "Star Trek" et un processus de télécommunication), ou le *dense coding* permettant de comprimer efficacement l'information. Toutefois, l'immense intérêt de la science moderne et l'énorme quantité de fonds que surtout les USA investissent dans la recherche sur l'information quantique, sont motivés exclusivement par la perspective de l'algorithme de Shor uni à la cryptographie quantique. Il est utile à ce point de préciser que la cryptographie quantique - se basant sur la transmission de photons polarisés - est une technologie déjà accomplie. Quatre entreprises - dont une, Id-Quantique, fondée par Nicolas Gisin et issue de l'université de Genève - fournissent des solutions pour le partage quantique de clé fonctionnant jusqu'à environ 100 Km de distance. Des limites technologiques à la cryptographie quantique existent toujours, mais la route est bien tracée. L'ordinateur quantique, par contre, existe seulement en tant que formalisme. Les efforts considérables dans la recherche ont mené à la démonstration, en laboratoire, de systèmes qui peuvent reproduire le fonctionnement de quelques bits d'information quantique (jusqu'à 7) - et cela en des conditions extrêmes (très baisses températures, ultra-vide, très grandes installations, etc.). La réalisation pratique d'un ordinateur quantique n'est donc pas très proche. A présent, la recherche n'a même pas pu établir quelle type de technologie est la plus appropriée. Ils existent donc cinq types de système physique, complètement différents, sur lesquels les études se concentrent. Nous les illustrerons en détail plus tard durant le semestre.

Toutes les phases du traitement de l'information, telles que stockage, manipulation et lecture, constituent des défis technologiques dans le contexte de l'information quantique, sur lesquels les scientifiques sont penchés depuis

deux décennies. Toutefois, l'ennemie principal du calcul quantique est un processus naturel appelé *décohérence*. Ce phénomène origine de l'interaction du système avec la matière et la lumière environnantes. Il est donc impossible à éviter complètement, dans la mesure où il est impossible d'isoler complètement un système de son environnement. On peut toutefois s'efforcer de le réduire au minimum, ce qui constitue à présent un des objectifs principaux de la recherche en physique de l'information quantique. La décohérence a comme effet celui de faire évoluer très rapidement les états de la matière avec corrélations quantiques - dont nous avons besoin pour le traitement quantique de l'information - vers des états non corrélés, c'est à dire des états de type classique. Ce phénomène est d'autant plus efficace que les système est composé d'un plus grand nombre de particules. En partie, la portée de ce problème a été réduite en montrant qu'un ordinateur quantique peut être composé d'éléments quantiques très petits, qui communiquent entre eux par voie classique. En outre, la recherche est aujourd'hui concentrée sur la réduction de la décohérence, en essayant de comprendre les mécanismes physiques fondamentaux qui en sont à la base. Pour finir, une grande partie de la recherche en informatique quantique vise à développer des méthodes de correction d'erreur quantiques, en analogie avec les techniques correspondantes en informatique classique. Le sujet de la décohérence et les techniques de correction d'erreur seront traités dans le prochain semestre.

Dans le premier semestre de ce cours nous allons présenter une introduction à la mécanique quantique orientée à la compréhension des éléments de calcul quantique. Au cours du semestre nous décrirons des techniques de traitement de l'information telles que la cryptographie quantique et la téléportation. Nous apprendrons aussi les éléments fondamentaux du calcul quantique, en particulier le concept de quantum-bit (ou qu-bit), et de porte logique quantique, et nous verrons les algorithmes élémentaires du calcul quantique, qui seront repris dans le prochain semestre. Un chapitre de ce cours touchera à la description des systèmes physiques qui aujourd'hui sont les candidats les plus prometteurs pour une réalisation pratiques d'un élément fondamental de calcul quantique.

# 2 Rappel d'algèbre linéaire

## 2.1 Espaces Vectoriels

Un espace vectoriel $V$ associé aux nombres réels $\mathbb{R}$ est un ensemble d'éléments $\{\mathbf{u}, \mathbf{v}, \mathbf{w}, \ldots\}$ sur lesquelles on a défini une opération interne de *somme* – $\mathbf{z} = \mathbf{u} + \mathbf{v}$ avec $\mathbf{z} \in V$ – et une opération de produit par un nombre scalaire – $\mathbf{z} = a\mathbf{u}$ avec $a \in \mathbb{R}$ et $\mathbf{z} \in V$. Le produit est distributif par rapport à la somme : $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$.

**Exemple :** Vecteurs dans l'espace cartesien $\mathbb{R}^2$
La somme est définie par la règle du parallélogramme et le produit par un scalaire est donné par le changement de longueur du vecteur.

Un espace vectoriel $V$ associé aux nombres complexes $\mathbb{C}$ est défini de la même manière mais par rapport au corps des nombres complexes.

On défini une *base* d'un espace vectoriel $V$ un ensemble de vecteurs $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N\}$ tel que :

1. pour chaque vecteur $\mathbf{w} \in V$ il est possible d'exprimer ce vecteur comme combinaison linéaire des vecteurs de la base :
   $\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_N\mathbf{v}_N$.
2. il est impossible de trouver un autre ensemble $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_M\}$, avec $M < N$, tel que la propriété 1. est vraie. Donc $N$ est le plus petit nombre de vecteurs nécessaire pour pouvoir exprimer tous les vecteurs de l'espace $V$. On dit que $N$ est la *dimension* de l'espace vectoriel $V$.

Nous n'allons pas démontrer ici qu'il est toujours possible de trouver une base pour un espace vectoriel de dimension finie. Une autre propriété d'une base est que les vecteurs qui la composent sont *linéairement indépendants*. Cela veut dire qu'il est impossible de trouver un ensemble $\{a_1, a_2, \ldots, a_N\}$, pas tous identiquement nuls, tels que $a_1\mathbf{v}_1 + \ldots + a_N\mathbf{v}_N = 0$

**Exemple :**
L'espace cartesien $\mathbb{R}^3$ et les trois vecteurs de longueur unitaire $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$

Pour un espace vectoriel associé à $\mathbb{R}$, nous pouvons définir un *produit scalaire*. Il s'agit d'une opération du type $V \times V \to \mathbb{R}$ avec les propriétés suivantes

1. $(\mathbf{u}, \mathbf{u}) > 0$ si $\mathbf{u} \neq 0$
2. $(\mathbf{u}, \mathbf{v}) = (\mathbf{v}, \mathbf{u})$.
3. $(\mathbf{u}, a\mathbf{v}) = a(\mathbf{u}, \mathbf{v})$, avec $a \in \mathbb{R}$.
4. $(\mathbf{u}, \mathbf{v} + \mathbf{w}) = (\mathbf{u}, \mathbf{v}) + (\mathbf{u}, \mathbf{w})$.

Les propriétés 1-4 impliquent également :

5. $(a\mathbf{u}, \mathbf{v}) = a(\mathbf{u}, \mathbf{v})$, avec $a \in \mathbb{R}$.
6. $(\mathbf{u} + \mathbf{v}, \mathbf{w}) = (\mathbf{u}, \mathbf{w}) + (\mathbf{v}, \mathbf{w})$.

**Exemple :** Produit scalaire de vecteurs en $\mathbb{R}^3$
$(\mathbf{u}, \mathbf{v}) = |\mathbf{u}||\mathbf{v}| \cos(\theta)$, où $|\mathbf{u}|$ est la norme (longueur) du vecteur $\mathbf{u}$ (figure 2.1). Exprimer les deux vecteurs sur la base $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ et utiliser l'orthogonalité pour montrer les propriétés du p.s. Dans cet exemple, $(\mathbf{u}, \mathbf{u}) = |\mathbf{u}|^2$ est la longueur de $\mathbf{u}$ au carré.

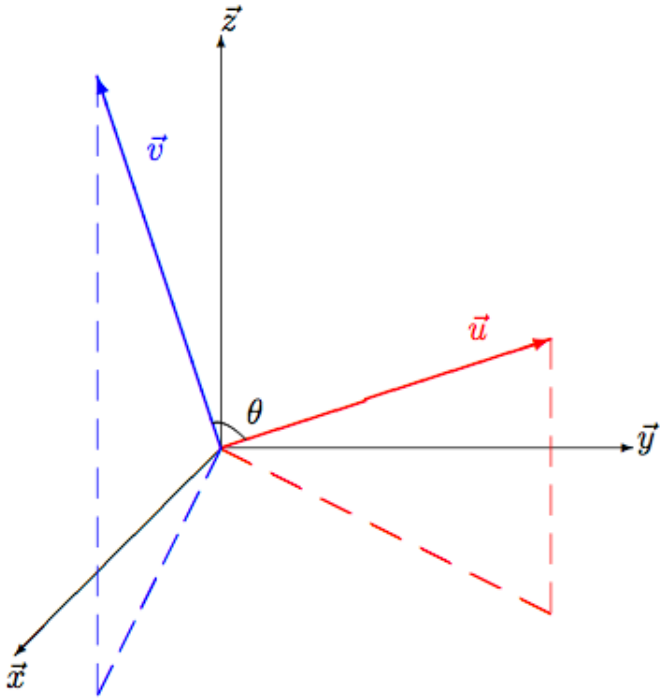



FIGURE 2.1 – Les vecteurs $\mathbf{u}$ et $\mathbf{v}$ dans la base $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$

Nous pouvons aussi définir un produit scalaire pour un espace vectoriel associé à $\mathbb{C}$. Dans ce cas, le produit scalaire est caractérisé par les propriétés suivantes

1. $(\mathbf{u}, \mathbf{u}) > 0$ si $\mathbf{u} \neq 0$
2. $(\mathbf{u}, \mathbf{v}) = (\mathbf{v}, \mathbf{u})^*$.
3. $(\mathbf{u}, a\mathbf{v}) = a(\mathbf{u}, \mathbf{v})$, avec $a \in \mathbb{C}$.
4. $(\mathbf{u}, \mathbf{v} + \mathbf{w}) = (\mathbf{u}, \mathbf{v}) + (\mathbf{u}, \mathbf{w})$.

Les propriétés 1-4 impliquent également

5. $(a\mathbf{u}, \mathbf{v}) = a^*(\mathbf{u}, \mathbf{v})$, avec $a \in \mathbb{C}$.
6. $(\mathbf{u} + \mathbf{v}, \mathbf{w}) = (\mathbf{u}, \mathbf{w}) + (\mathbf{v}, \mathbf{w})$.

Dans ce deuxième cas, on remarque que d'après la propriété 2, le produit scalaire $(\mathbf{u}, \mathbf{u}) \in \mathbb{R}$
Deux vecteurs $\mathbf{u}$ et $\mathbf{v}$ sont orthogonaux si $(\mathbf{u}, \mathbf{v}) = 0$. En effet, pour l'exemple ci-dessus des vecteurs dans l'espace cartesien, cette relation équivaut à l'orthogonalité au sens géométrique.

En présence d'un produit scalaire, nous pouvons construire une base *orthonormée*, c'est à dire une base dont les vecteurs $\mathbf{v}_j$ ont la propriété $(\mathbf{v}_j, \mathbf{v}_k) = \delta_{jk}$, où $\delta_{jk} = 0$ si $j \neq k$ et $\delta_{jk} = 1$ si $j = k$. Pour cela, il faut partir d'une base qualconque $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N\}$. La base orthonormée $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N\}$ est définie ainsi :

$$\begin{aligned}
\mathbf{w}_1 &= \mathbf{v}_1 \\
\mathbf{w}_2 &= \mathbf{v}_2 - \frac{(\mathbf{w}_1, \mathbf{v}_2)}{(\mathbf{w}_1, \mathbf{w}_1)}\mathbf{w}_1 \\
\mathbf{w}_3 &= \mathbf{v}_3 - \frac{(\mathbf{w}_1, \mathbf{v}_3)}{(\mathbf{w}_1, \mathbf{w}_1)}\mathbf{w}_1 - \frac{(\mathbf{w}_2, \mathbf{v}_3)}{(\mathbf{w}_2, \mathbf{w}_2)}\mathbf{w}_2 \\
&\vdots \\
\mathbf{w}_N &= \mathbf{v}_N - \sum_{j=1}^{k-1} \frac{(\mathbf{w}_j, \mathbf{v}_k)}{(\mathbf{w}_j, \mathbf{w}_j)}\mathbf{w}_j
\end{aligned}$$

Nous pouvons facilement vérifier que les vecteurs $\mathbf{w}_j$ sont orthogonaux. Pour obtenir des vecteurs unitaire, il ne reste à définir :

$$\mathbf{u}_j = \frac{\mathbf{w}_j}{\sqrt{(\mathbf{w}_j, \mathbf{w}_j)}}$$

Si un vecteur $\mathbf{v}$ est exprimé par rapport à une base orthonormée, $\mathbf{v} = a_1\mathbf{u}_1 + \ldots + a_N\mathbf{u}_N$, les nombres complexes $a_1, \ldots, a_N$ sont appelé les composantes du vecteur $\mathbf{v}$ dans la base $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N\}$. Le produit scalaire avec un deuxième vecteur $\mathbf{w} = b_1\mathbf{u}_1 + \ldots + b_N\mathbf{u}_N$ s'écrit comme

$$\begin{aligned}
(\mathbf{v}, \mathbf{w}) &= (a_1\mathbf{u}_1 + \ldots + a_N\mathbf{u}_N, b_1\mathbf{u}_1 + \ldots + b_N\mathbf{u}_N) \\
&= a_1^*b_1(\mathbf{v}_1, \mathbf{v}_1) + a_1^*b_2(\mathbf{v}_1, \mathbf{v}_2) + a_2^*b_1(\mathbf{v}_2, \mathbf{v}_1) + a_2^*b_2(\mathbf{v}_2, \mathbf{v}_2) + \ldots \\
&= a_1^*b_1(\mathbf{v}_1, \mathbf{v}_1) + a_2^*b_2(\mathbf{v}_2, \mathbf{v}_2) + \ldots \\
&= a_1^*b_1 + a_2^*b_2 + \ldots + a_N^*b_N
\end{aligned}$$

Donc, le produit scalaire se calcule en faisant le produit composante par composante, et en faisant attention à prendre le complexe conjugué des composantes du vecteur de gauche dans le produit. Ce résultat nous permet d'introduire une notation très utile : Un vecteur $\mathbf{v} = a_1\mathbf{u}_1 + \ldots + a_N\mathbf{u}_N$ peut être représenté par une matrice à $N$ lignes et une colonne :

$$\mathbf{v} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} \tag{2.1}$$

On appelle cela un *vecteur colonne*. Le produit scalaire avec un deuxième vecteur est simplement donné par le produit matriciel avec un *vecteur ligne* :

$$(\mathbf{v}, \mathbf{w}) = (a_1^* \; a_2^* \; \ldots \; a_N^*) \times \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix} \tag{2.2}$$

Pour une base orthonormée, il est aussi très simple de calculer les composantes d'une vecteur $\mathbf{v}$. Nous cherchons les nombres complexes $a_1, \ldots, a_N$ tels que $\mathbf{v} = a_1\mathbf{u}_1 + \ldots + a_N\mathbf{u}_N$. Faisons le produit scalaire de cette expression avec $\mathbf{u}_1$ :

$$\begin{aligned} (\mathbf{u}_1, \mathbf{v}) &= a_1(\mathbf{u}_1, \mathbf{u}_1) + a_2(\mathbf{u}_1, \mathbf{u}_2) + \ldots + a_N(\mathbf{u}_1, \mathbf{u}_N) \\ &= a_1 \end{aligned}$$

où nous avons utilisé la propriété de la base orthonormée. De même, $a_j = (\mathbf{u}_j, \mathbf{v})$ avec $j = 1, \ldots, N$. Etant donné un vecteur quelconque $\mathbf{v}$, nous pouvons donc calculer ses composantes dans une base orthonormée, simplement en faisant le produit scalaire avec les vecteurs de la base.

## 2.2 Opérateurs linéaires

Un opérateur linéaire $A : V \to V$ est un opérateur qui transforme les vecteurs de l'espace $V$ avec la propriété suivante

$$A(a\mathbf{v} + b\mathbf{w}) = a(A\mathbf{v}) + b(A\mathbf{w}) \tag{2.3}$$

avec $a, b \in \mathbb{C}$. Considérons une base orthonormée $\{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$. Si $\mathbf{v} = a_1\mathbf{u}_1 + \cdots + a_N\mathbf{u}_N$, alors le vecteur $\mathbf{w} = A\mathbf{v}$ est de la forme

$$\begin{aligned} \mathbf{w} &= A\mathbf{v} \\ &= a_1 A\mathbf{u}_1 + \cdots + a_N A\mathbf{u}_N \end{aligned}$$

Nous pouvons exprimer $\mathbf{w}$ sur la base : $\mathbf{w} = b_1\mathbf{u}_1 + \cdots + b_N\mathbf{u}_N$. Calculons les coefficients $b_j$ :

$$\begin{aligned} b_j &= (\mathbf{u}_j, \mathbf{w}) \\ &= (\mathbf{u}_j, A\mathbf{v}) \\ &= (\mathbf{u}_j, a_1 A\mathbf{u}_1 + \cdots + a_N A\mathbf{u}_N) \\ &= a_1(\mathbf{u}_j, A\mathbf{u}_1) + \cdots + a_N(\mathbf{u}_j, A\mathbf{u}_N) \end{aligned}$$

Nous pouvons ainsi définir :

$$A_{jk} = (\mathbf{u}_j, A\mathbf{u}_k)$$

$A_{jk}$ est une matrice $N \times N$ avec $A_{jk} \in \mathbb{C}\ \forall j, k$. L'opérateur $A$, exprimé sur la base $\{\mathbf{u}_j\}$, s'écrit donc sous forme de matrice. Si $\mathbf{w} = A\mathbf{v}$, alors les composants de $\mathbf{w}$ s'écrivent comme

$$b_j = \sum_k A_{jk} a_k$$

où $a_k$ sont les composantes de $\mathbf{v}$. En utilisant la représentation en vecteur colonne, nous avons

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1N} \\ A_{21} & A_{22} & \cdots & A_{2N} \\ \vdots & & \ddots & \vdots \\ A_{N1} & A_{N2} & \cdots & A_{NN} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} \tag{2.4}$$

Donc l'application d'un opérateur linéaire équivaut au produit d'une matrice avec un vecteur colonne. Pour les opérateurs linéaires, nous avons les propriétés suivantes :

$$\begin{aligned} (A + B)\mathbf{v} &= A\mathbf{v} + B\mathbf{v} \\ A(c\mathbf{v}) &= c(A\mathbf{v}) \text{ avec } c \in \mathbb{C} \end{aligned}$$

De plus, pour la représentation d'opérateurs linéaires sous forme de matrices, nous avons les relations suivantes :

$$\begin{aligned} C = A + B &\rightarrow C_{jk} = A_{jk} + B_{jk} \\ C = aA &\rightarrow C_{jk} = aA_{jk} \text{ avec } a \in \mathbb{C} \end{aligned}$$

et pour l'application successive de deux opérateurs $A$ et $B$

$$C\mathbf{v} = B(A\mathbf{v}) \rightarrow C_{jk} = \sum_n B_{jn} A_{nk}$$

donc $C = B \times A$ est la multiplication des matrices $A$ et $B$.

Si $A$ est un opérateur linéaire bijectif, c'est à dire $A\mathbf{v} = A\mathbf{w}$ si et seulement si $\mathbf{v} = \mathbf{w}$, alors $A$ est inversible et il est possible de définir l'opérateur inverse $A^{-1}$ tel que, si $\mathbf{w} = A\mathbf{v}$ alors $\mathbf{v} = A^{-1}\mathbf{w}$. Dans ce cas on a $AA^{-1} = A^{-1}A = I$, où $I$ est l'opérateur identité. Il est clair qu'il existe des opérateurs linéaires non-inversibles.

Il est également possible d'effectuer d'autres opérations avec les opérateurs. Un exemple qui nous intéresse particulièrement est l'exponentiel d'un opérateur $A$, qui se fait à l'aide de l'expansion de Taylor de la fonction exponentielle :

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots$$

où $I$ est l'opérateur identité et $A^n = A \times A \times \ldots \times A$ $n$ fois. La même expression est valable pour la représentation sous forme de matrice de l'opérateur $A$. Il est clair que l'opérateur $e^A$ est bien défini seulement si la série de Taylor correspondante est convergente.

Pour chaque opérateur linéaire $A$, nous pouvons définir l'opérateur $A^\dagger$, dit *adjoint* ou *conjugué hermitique*, de la manière suivante :

$$(\mathbf{v}, A^\dagger \mathbf{w}) = (A\mathbf{v}, \mathbf{w}) \qquad \forall \mathbf{v}, \mathbf{w}$$

Par la propriété du produit scalaire, nous avons :

$$(A\mathbf{v}, \mathbf{w}) = (\mathbf{v}, A\mathbf{w})^*$$

En particulier, cette relation est valable pour les vecteurs de la base. D'où, nous avons :

$$(\mathbf{u}_j, A^\dagger \mathbf{u}_k) = (\mathbf{u}_j, A\mathbf{u}_k)^*$$

Il s'ensuit que la matrice correspondant à l'opérateur $A^\dagger$ est donnée par la matrice transposée conjuguée de l'opérateur $A$ sur la même base :

$$(A^\dagger)_{jk} = (A_{kj})^*$$

On peut facilement démontrer les propriétés suivantes :

$$\begin{aligned} (A + B)^\dagger) &= A^\dagger + B^\dagger \\ (cA)^\dagger &= c^* A^\dagger \\ (AB)^\dagger &= B^\dagger A^\dagger \\ (A^\dagger)^\dagger &= A \end{aligned}$$

On définit un opérateur *hermitique* ou *auto-adjoint*, un opérateur $A$ tel que $A^\dagger = A$. Cela implique :

$$\begin{aligned} A_{jk} &= (A_{kj})^* \text{ et en particulier} \\ A_{jj} &\in \mathbb{R}, \quad j = 1, \ldots, N \end{aligned}$$

Pour un opérateur hermitique, nous avons :

$$(\mathbf{v}, A\mathbf{w}) = (A\mathbf{v}, \mathbf{w})$$

Cette propriété est très importante en mécanique quantique. Elle est également à la base de la notation de Dirac, qui est utilisée universellement pour indiquer les états, les opérateurs et les produits scalaires en mécanique quantique. Un conséquence de la propriété ci-dessus est :

$$(\mathbf{v}, A\mathbf{v}) \in \mathbb{R}$$

En mécanique quantique, deux types d'opérateurs linéaires sont très importants. Premièrement les opérateurs hermitiques que nous venons de définir. Le deuxième type est représenté par les opérateurs unitaires. Un opérateur unitaire $U$ est caractérisé par la propriété :

$$U^\dagger U = UU^\dagger = I$$

De cette propriété suit directement que l'opérateur $U$ est inversible et que $U^{-1} = U^\dagger$. A l'aide de la définition d'opérateur adjoint, nous pouvons démontrer qu'un opérateur unitaire conserve les produits scalaires entre vecteurs :

$$(U\mathbf{v}, U\mathbf{w}) = (\mathbf{v}, \mathbf{w}) \quad \forall \mathbf{v}, \mathbf{w} \in V$$

En particulier, puisque la norme carrée d'un vecteur est donnée par $|\mathbf{v}|^2 = (\mathbf{v}, \mathbf{v})$, un opérateur unitaire préserve la norme des vecteurs :

$$|U\mathbf{v}| = |\mathbf{v}| \quad \forall \mathbf{v} \in V$$

Une dernière remarque importante pour la mécanique quantique est la suivante : Soit $A$ un opérateur hermitique, alors $U = e^{iA}$ est un opérateur unitaire. Pour le prouver, nous allons montrer que $UU^\dagger = I$ (de la même manière, nous montrons que $U^\dagger U = I$) :

$$\begin{aligned} UU^\dagger &= e^{iA}\left(e^{iA}\right)^\dagger \\ &= \left(I + iA - \frac{A^2}{2} - i\frac{A^3}{6} + \ldots\right)\left(I - iA - \frac{A^2}{2} + i\frac{A^3}{6} + \ldots\right) \\ &= I - iA + iA + A^2 - \frac{A^2}{2} - \frac{A^2}{2} + i\frac{A^3}{2} - i\frac{A^3}{2} + \ldots \\ &= I \end{aligned}$$

## 2.3 Changement de base

Nous peuvons exprimer un vecteur $\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_N\mathbf{v}_n$ dans une nouvelle base $\{\mathbf{w}_1, \ldots, \mathbf{w}_N\}$. En général, la nouvelle expression de $\mathbf{v}$ s'écrit en termes de nouvelles composantes :

$$\mathbf{v} = a'_1\mathbf{w}_1 + \cdots + a'_N\mathbf{w}_n$$

Exprimons les vecteurs de la nouvelle base en fonction des vecteurs de l'ancienne

$$\mathbf{v}_j = O_{j1}\mathbf{w}_1 + \cdots + O_{jN}\mathbf{w}_N$$

Utilisons cette définition dans l'expression de $\mathbf{v}$

$$\begin{aligned}
\mathbf{v} &= a_1\mathbf{v}_1 + \cdots + a_N\mathbf{v}_n \\
&= a_1(O_{11}\mathbf{w}_1 + \cdots + O_{1N}\mathbf{w}_N) \\
&+ a_2(O_{21}\mathbf{w}_1 + \cdots + O_{2N}\mathbf{w}_N) \\
&\vdots \\
&+ a_N(O_{N1}\mathbf{w}_1 + \cdots + O_{NN}\mathbf{w}_N)
\end{aligned}$$

d'où

$$a'_j = \sum_{k=1}^{N} O_{jk}a_k$$

La matrice $O$ formée des éléments $O_{jk}$ est par définition unitaire. En effet, elle correspond à un opérateur linéaire qui transforme un vecteur avec des composantes $(a_1, \ldots, a_N)$ en un vecteur avec des composantes $(a'_1, \ldots, a'_N)$ et, par définition, $||\mathbf{v}|| = \sqrt{|a_1|^2 + \cdots + |a_N|^2} = \sqrt{|a'_1|^2 + \cdots + |a'_N|^2}$. Donc $O$ conserve la norme des vecteurs.

**Exemple** : Espace cartesien $\mathbb{R}^2$ avec base $\{\mathbf{x}, \mathbf{y}\}$ orthogonale.
Considérons une nouvelle base $\{\mathbf{x}, \mathbf{y}\}$ obtenue par une rotation d'un angle $\theta$ en sens antihoraire. Par des simple considérations de trigonométrie, nous avons $\mathbf{x}' = \mathbf{x}\cos\theta + \mathbf{y}\sin\theta$ et $\mathbf{y}' = -\mathbf{x}\sin\theta + \mathbf{y}\cos\theta$. Donc un vecteur $\mathbf{v} = a_x\mathbf{x} + a_y\mathbf{y}$ dans la nouvelle base est donné par $\mathbf{v} = a'_x\mathbf{x}' + a'_y\mathbf{y}'$ avec :

$$\begin{pmatrix} a'_x \\ a'_y \end{pmatrix} = O \begin{pmatrix} a_x \\ a_y \end{pmatrix}$$

avec

$$O = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Remarquez que, si $O$ est la matrice de changement de base pour les composants, alors les nouveaux vecteurs de base s'expriment en fonction des anciens à l'aide de $O^{-1}$ :

$$\begin{pmatrix} \mathbf{x}' \\ \mathbf{y}' \end{pmatrix} = O^{-1} \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$$

Un opérateur linéaire $A$ est exprimé dans la base $\{\mathbf{v}_1, \ldots, \mathbf{v}_N\}$ par une matrice $A = \{A_{ij}\}$. Nous pouvons exprimer $A$ dans la nouvelle base $\{\mathbf{w}_1, \ldots, \mathbf{w}_N\}$ par une nouvelle matrice. Pour trouver la forme de cette matrice, considérons l'action de $A$ sur un vecteur $\mathbf{v}$ quelconque : $\mathbf{w} = A\mathbf{v}$. En termes de composants cette relation s'écrit

$$b_j = \sum_{k=1}^{N} A_{jk} a_k$$

Ecrivons les expressions des anciennes composantes en fonction des nouvelles :

$$a_k = \sum_l O^{-1}_{kl} a'_l$$

$$b_j = \sum_l O^{-1}_{jm} b'_m$$

remplaçons dans l'expression précédente :

$$\sum_l O^{-1}_{jm} b'_m = \sum_k A_{jk} \sum_l O^{-1}_{kl} a'_l$$

que nous pouvons écrire sous forme compacte :

$$O^{-1} \begin{pmatrix} b'_1 \\ \vdots \\ b'_N \end{pmatrix} = AO^{-1} \begin{pmatrix} a'_1 \\ \vdots \\ a'_N \end{pmatrix}$$

Multiplions par $O$ à gauche et nous obtenons :

$$\begin{pmatrix} b'_1 \\ \vdots \\ b'_N \end{pmatrix} = OAO^{-1} \begin{pmatrix} a'_1 \\ \vdots \\ a'_N \end{pmatrix} = A' \begin{pmatrix} a'_1 \\ \vdots \\ a'_N \end{pmatrix}$$

Et nous avons trouvé l'expression de la nouvelle matrice $A'$ qui décrit l'opérateur dans la nouvelle base : $A' = OAO^{-1}$, ou en termes des composantse $A'_{ij} = \sum_{k,l} O_{ik} A_{kl} (O^{-1})_{lj}$.

## 2.4 Notation de Dirac

Dirac a introduit une notation pour exprimer les opérations d'algèbre linéaire en mécanique quantique. Cette notation s'appuie sur le fait que nous calculons toujours des éléments de matrice d'opérateurs auto-adjoints.

Un vecteur $\mathbf{v}$ appartenant à un espace de Hilbert $V$ est indiqué par un "ket" :

$$|v\rangle$$

Le produit scalaire entre deux vecteurs $\mathbf{v}$ et $\mathbf{w}$ est indiqué par :

$$\langle u|v\rangle$$

Il est clair donc que, si $|v\rangle$ indique un vecteur colonne, le symbole $\langle v|$ indique le vecteur ligne correspondant. Ce symbole s'appelle un "bra", de manière à que le produit scalaire soit un "bra" + "ket" = "braket".

Un élément de matrice d'un opérateur hermitique ou auto-adjoint s'indique avec :

$$(\mathbf{v}, A\mathbf{w}) = (A\mathbf{v}, \mathbf{w}) = \langle v|A|w\rangle$$

L'idée de base de cette notation est qu'on peut placer l'opérateur au milieu de l'expression, puisque il est auto-adjoint et donc il peut agir indifféremment sur le terme de gauche ou sur celui de droite.

Avec cette notation, nous pouvons facilement introduire une nouvelle "opération". Construisons l'objet :

$$A = |v\rangle \langle w|$$

Cet objet est un opérateur linéaire. Au sens des vecteurs ligne et colonne, il correspond à :

$$\begin{aligned} A &= \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} \times (w_1, \ldots, w_N) \\ &= \begin{pmatrix} v_1 w_1 & \cdots & v_1 w_N \\ \vdots & \ddots & \vdots \\ v_N w_1 & \cdots & v_N w_N \end{pmatrix} \end{aligned} \tag{2.5}$$

Dans le cas particulier où $\mathbf{v} = \mathbf{w}$, et $\langle v|v\rangle = 1$, on a :

$$A_v = |v\rangle \langle v|$$

qui est un "projecteur" sur le sous-espace généré par le vecteur $|v\rangle$. En général, un projecteur est un opérateur linéaire $P$ tel que $P^2 = P$. la notation de Dirac nous permet de vérifier facilement cette propriété

$$A_v^2 = |v\rangle \langle v|v\rangle \langle v| = |v\rangle \langle v| = A_v$$

Si nous appliquons $A_v$ à un vecteur $|w\rangle$, nous obtenons le composant de $|w\rangle$ le long de $|v\rangle$ :

$$A_v |w\rangle = |v\rangle \langle v|w\rangle$$

c'est-à-dire la projection de $|w\rangle$ sur $|v\rangle$. Si par exemple $\{|v_i\rangle\}$ est une base orthonormée, nous avons vu que les composantes de $|w\rangle$ se calculent selon :

$$|w\rangle = w_1 |v_1\rangle + \cdots + w_N |v_N\rangle$$

avec

$$w_j = \langle v_j\rangle w$$

Donc le vecteur qui correspond à la projection de $|w\rangle$ sur $|v_j\rangle$ est :

$$w_j |v_j\rangle = |v_j\rangle \langle v_j\rangle w = A_{v_j} |w\rangle$$

Plus en général, un ensemble de vecteurs orthonormés $\{|v_j\rangle, j = 1, \ldots, m\}$ permet de définir un projecteur :

$$P = \sum_{j=1}^{m} |v_j\rangle \langle v_j|$$

Si $\{|v_j\rangle, j = 1, \ldots, N\}$ est une base de $V$, alors :

$$\sum_{j=1}^{N} |v_j\rangle \langle v_j| = I$$

où $I$ est l'opérateur identité. On appelle cette relation la "relation de complétude". On la vérifie facilement en faisant agir l'opérateur sur un vecteur quelconque exprimé sur la base $\{|v_j\rangle\}$.

# 3 Formulation mathématique du quantum bit

## 3.1 Un quantum bit

Avant d'aborder les bases de la mécanique quantique, nous allons étudier la formulation mathématique du quantum bit.

Considérons un registre à un bit d'information classique, qui peut prendre les valeurs 0 ou 1. Dans la formulation classique, ces deux états sont représentés simplement par des nombres entiers. Dans la formulation quantique, nous pouvons représenter ces deux états par deux vecteurs orthogonaux dans un espace de Hilbert $V$ de dimension 2. En utilisant la notation de Dirac, les deux vecteurs sont indiqués par $|0\rangle$ et $|1\rangle$, avec $\langle 0|1\rangle = 0$ et $\langle 1|1\rangle = \langle 0|0\rangle = 1$. Nous avons choisi ces vecteurs ayant une norme unitaire. Nous verrons, dans le contexte de la mécanique quantique, que c'est un choix naturel, puisque chaque état physique est représenté par un vecteur de norme unitaire dans un espace de Hilbert. L'état d'un *quantum bit* ou *qu-bit* est donné par un vecteur quelconque, de norme 1, dans cet espace de Hilbert $V$. En particulier, un état du qu-bit est défini à moins d'une phase complexe : l'état $e^{i\alpha}|1\rangle$, avec $\alpha \in \mathbb{R}$, est équivalent à l'état $|1\rangle$. Autre que $|0\rangle$ et $|1\rangle$, aussi un état $|\psi\rangle = a|0\rangle + b|1\rangle$ (avec $a, b \in \mathbb{C}$ et $|a|^2 + |b|^2 = 1$) est un état possible de ce registre quantique.

Cette formulation nous vient directement d'un principe fondamental de la mécanique quantique : le principe de superposition. Ce principe affirme que, si deux états $|\psi\rangle$ et $|\phi\rangle$ sont de états possibles d'un système physique, alors chaque combinaison linéaire $|\chi\rangle = a|\psi\rangle + b|\phi\rangle$, telle que $\langle\chi|\chi\rangle = 1$, est encore un état possible du système.

Nous avons ici un premier aperçu d'un aspect très important de l'information quantique : le *parallélisme quantique*. Le registre dans l'état $|\psi\rangle = a|0\rangle + b|1\rangle$ prend *en même temps* les valeurs 0 et 1. Hélas, l'expression "en même temps" ici ne veut rien dire. Nous n'avons pas assez de connaissances en mécanique quantique pour comprendre comment réaliser un tel registre en pratique, comment le mettre dans un tel état, et comment lire cette information. Pour cela, il est impératif de comprendre les bases de la mécanique quantique, en particulier la théorie de la mesure. Pour l'instant, nous devons considérer cela comme une formulation abstraite.

Dans notre formulation mathématique, une opération sur un qu-bit est représentée par un opérateur unitaire $U$ agissant dans l'espace de Hilbert $V$ du registre. Cela aussi nous vient directement de la mécanique quantique, où l'évolution temporelle d'un système est donnée par un opérateur unitaire agissant sur l'état du système. L'unitarité est nécessaire pour préserver la

norme du vecteur. A titre d'exemple, nous allons introduire l'opérateur qui correspond à l'opération $NOT$ sur un qu-bit. Dans la base $\{|0\rangle, |1\rangle\}$, la matrice correspondante à cet opérateur s'écrit :

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Il est simple de vérifier que, appliqué sur les deux vecteurs de base, cet opérateur se comporte comme le NOT classique :

$$\begin{aligned} U_{NOT}|0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ U_{NOT}|1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

La linéarité implique que l'opérateur $U_{NOT}$, appliqué sur l'état $|\psi\rangle = a|0\rangle + b|1\rangle$, donne :

$$\begin{aligned} U_{NOT}|\psi\rangle &= U_{NOT}(a|0\rangle) + U_{NOT}(b|1\rangle) \\ &= aU_{NOT}|0\rangle + bU_{NOT}|1\rangle \\ &= a|1\rangle + b|0\rangle \end{aligned}$$

L'opération $NOT$ a été effectuée "en même temps" sur les deux valeurs qui étaient stockés "en même temps" dans le registre. Dans cette phrase, le deuxième "en même temps" n'a toujours pas de signification, comme nous l'avons expliqué avant. Le premier "en même temps" par contre a déjà une signification claire : pour effectuer l'inversion des deux valeurs stockés dans le registre, l'opérateur emploie le même temps qu'il lui faut pour en effectuer une seule. C'est encore un petit avant-goût du parallélisme quantique que nous verrons prochainement.

## 3.2 Plusieurs qu-bits

Comment généraliser cette formulation au cas d'un registre à plusieurs qu-bits ? Considérons deux bits classiques. Les états possibles sont 00, 01, 10 et 11. Par analogie avec le cas précédant, nous pouvons définir un espace de Hilbert de dimension 4, avec une base orthonormée donnée par les quatre vecteurs $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$. Comme pour le cas d'un qu-bit, ce registre peut se trouver dans un état qui est une combinaison linéaire arbitraire :

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

avec $a, b, c, d \in \mathbb{C}$ et $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

On remarque tout de suite que cette définition correspond au produit tensoriel de deux espaces de Hilbert $V_1$ et $V_2$, de dimension 2, correspondant aux deux qu-bits séparés. En effet, nous pouvons interpréter le vecteur $|00\rangle$ comme le produit tensoriel $|0\rangle_1 \otimes |0\rangle_2$, où $|0\rangle_1$ et $|0\rangle_2$ appartiennent aux espaces $V_1$ et $V_2$ respectivement. De même pour les trois autres vecteurs de base. Nous pouvons donc généraliser cette définition de la manière suivante : Les états d'un registre à $N$ qu-bits sont représentés par les vecteurs d'un espace $V = V_1 \otimes V_2 \otimes \cdots \otimes V_N$, produit scalaire des espaces de Hilbert qui représentent les $N$ qu-bits. Nous indiquerons les vecteurs de la base d'un tel espace vectoriel par $|x_1 x_2 \cdots x_N\rangle$, où $x_j$ peuvent prendre les valeurs 0 ou 1.

Une remarque très importante s'impose à ce point. Considérons par exemple l'espace $V = V_1 \otimes V_2$ d'un registre à deux qu-bits. Cet espace contient tous les produits tensoriels possibles de vecteurs des espaces $V_1$ et $V_2$. Par exemple, si $|\psi\rangle = a\,|0\rangle_1 + b\,|1\rangle_1$ et $|\phi\rangle = c\,|0\rangle_2 + d\,|1\rangle_2$, alors l'état :

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= (a\,|0\rangle_1 + b\,|1\rangle_1) \otimes (c\,|0\rangle_2 + d\,|1\rangle_2) \\ &= ac\,|0\rangle_1 \otimes |0\rangle_2 + ad\,|0\rangle_1 \otimes |1\rangle_2 + bc\,|1\rangle_1 \otimes |0\rangle_2 + bd\,|1\rangle_1 \otimes |1\rangle_2 \\ &= ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \end{aligned}$$

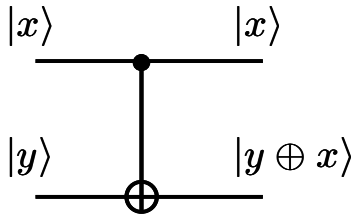
est un état de l'espace $V = V_1 \otimes V_2$. L'espace $V$ toutefois contient une infinité d'autres vecteurs qui ne sont pas simplement des produits tensoriels de vecteurs de $V_1$ et $V_2$. Considérons par exemple le vecteur

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

Il est évident que ce vecteur ne peut pas être exprimé comme produit tensoriel. Pourtant, le principe de superposition en mécanique quantique impose que cet état soit aussi un état possible du système de deux qu-bits. Ce genre d'états *non séparables* sont appelés en mécanique quantique des *états avec corrélation quantique* ou – avec un terminologie très populaire – *états intriqués*. L'existence de tels états constitue la vraie singularité de la mécanique quantique, puisque ils n'ont aucune analogie avec des états classiques de la matière. Nous verrons cela plus en détail quant nous aborderons le sujet de l'inégalité de Bell et du paradoxe EPR. Il n'est donc pas surprenant, que c'est la possibilité de réaliser de tels états qui produit les avantages du traitement quantique de l'information par rapport au paradigme classique.

Essayons de mieux comprendre le potentiel impliqué par ce formalisme et par l'existence des états intriqués. Nous allons décrire la première opération à 2 qu-bits : le *Controlled-NOT*. Il s'agit d'une opération sur un registre à deux

qu-bits (dans l'input et dans l'output, puisque les opérateurs quantiques sont réversibles)




Ici l'opération $\oplus$ indique la somme de bits classiques modulo 2, qui correspond au $NOT$. Le $CNOT$ se comporte de la manière suivante. Le premier bit de output simplement reproduit l'input. Le deuxième bit de output contient la valeur en input sommée modulo 2 à l'autre bit. Cela équivaut à inverser le deuxième bit seulement si le premier bit vaut 1, d'où le nom Controlled-NOT. Grâce au principe de superposition, l'opérateur $U_{CNOT}$ peut agir sur une combinaison linéaire d'états à deux qu-bits. En général :

$$U_{CNOT}(a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle) = a\,|00\rangle + b\,|01\rangle + c\,|11\rangle + d\,|10\rangle$$

La matrice correspondant à cet opérateur, dans la base $\{|00\rangle\,,\ |01\rangle\,,\ |10\rangle\,,\ |11\rangle\}$, est donc donnée par

$$U_{CNOT} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Si nous considérons l'inversion comme une opération de somme modulo 2, alors on peut réécrire l'opérateur $U_{CNOT}$ de la manière suivante :

$$U_{CNOT} \sum_{x,y} a_{xy}\,|x, y\rangle = \sum_{x,y} a_{xy}\,|x, (x \oplus y)\rangle$$

où $x = 0, 1$, $y = 0, 1$ et la somme est sur toutes les valeurs possibles de $x$ et $y$. Cette écriture est très suggestive. Elle nous dit que l'opérateur $U_{CNOT}$ effectue les quatre sommes modulo 2 $x \oplus y$, pour les quatre valeurs possibles de $x, y$, en même temps, et donc un facteur 4 plus vite qu'un ordinateur classique !

Nous pouvons généraliser cet exemple à un registre $|x\rangle = |x_1 \cdots x_N\rangle$ à $N$ qu-bits, et à une opération $y = f(x)$ quelconque, qui pour chaque nombre à $N$ bits $x$ donne un nombre à $N$ bits $y = f(x)$. Considérons l'espace de Hilbert

de dimension $2N$ obtenu par le produit tensoriel des espaces correspondants aux registres $x$ et $y$. Un vecteur $|x, y\rangle = |x\rangle \otimes |y\rangle$ est un élément de cet espace. Supposons de pouvoir construire un opérateur unitaire $U_f$ tel que

$$U_f |x, y\rangle \quad = \quad |x, y \oplus f(x)\rangle$$

où maintenant l'opération $\oplus$ est la somme modulo $2^N$. On remarque en passant, qu'une telle structure de l'opérateur est nécessaire, puisque tous les opérateurs d'évolution en mécanique quantique sont réversibles. Considérons maintenant l'état $|\psi\rangle = \sum_{x=0}^{2^N-1} a_x |x, y\rangle$ pour une valeur de $y$ donnée. L'action de $U_f$ sur cet état donne :

$$U_f |\psi\rangle \quad = \quad \sum_{x=0}^{2^N-1} a_x |x, y \oplus f(x)\rangle$$

En particulier, pour $y = 0$

$$U_f |\psi\rangle \quad = \quad \sum_{x=0}^{2^N-1} a_x |x, f(x)\rangle$$

Ce résultat est remarquable. Nous avons appliqué l'opérateur $U_f$ une seule fois et nous avons un état final où on a calculé toutes les $2^N$ valeurs $f(0)$, $f(1), \ldots, f(2^N - 1)$. En plus l'état contient chaque valeur $f(x)$ associée à la valeur de l'input $x$ correspondant (il s'agit en effet d'un état intriqué). L'accélération par rapport à un procédé classique est d'un facteur $2^N$, donc exponentielle en fonction de la taille du problème.

Malheureusement, nous verrons que la mécanique quantique rend impossible d'extraire cette information dans sa totalité. En d'autres mots, quoique l'état final *contienne* les $2^N$ valeurs de $f(x)$, le processus de mesure permet au maximum d'en connaître un seul, comme nous le verrons. En l'absence de cette limitation, le traitement quantique de l'information aurait rendu infiniment plus rapides **toutes** les tâches de calcul ! En revanche, le processus de mesure quantique rend possible certains types de mesure qui ne visent pas à connaître une valeur spécifique de $f(x)$, mais plutôt une caractéristique collective des $2^N$ valeurs de $f(x)$, comme par exemple leur périodicité. C'est exactement ce type de mesure qui rend le traitement quantique de l'information avantageux par rapport au paradigme classique. L'algorithme quantique le plus important – l'algorithme de Shor pour la factorisation de nombres entiers – se base sur cette possibilité. Pour comprendre cette idée de fonctionnement des algorithmes quantiques, il nous faut d'abord comprendre les bases de la mécanique quantique et en particulier le processus de mesure.

## 3.3 Exemple de qu-bit : La lumière polarisée

Une onde plane électromagnétique est caractérisée par un champ électrique :

$$\vec{E} = \vec{E}_0 \cos(\omega t - \vec{k} \cdot \vec{r})$$

Ici $\vec{k} = (k_1, k_2, k_3)$ est le vecteur d'onde qui indique la direction de propagation de l'onde la et $\omega = c|\vec{k}|$ la fréquence. Nous pouvons aussi définir la longueur d'onde $\lambda = \frac{2\pi}{|\vec{k}|}$. Le champ $\vec{E}$ est un vecteur *trnasverse*. Cela veut dire que : $\vec{k} \cdot \vec{E}_0 = 0$. $\vec{E}_0$ est toujours orthogonale à la direction de propagation de l'onde, définie par $\vec{k}$. Donc, pour un $\vec{k}$ fixé, $\vec{E}_0$ est un vecteur dans un espace à deux dimensions. (De plus, le champs magnétique $\vec{B}$ est aussi champs transverse, il est perpendiculaire à $\vec{k}$, mais aussi à $\vec{E}$). Nous pouvons faire l'analogie avec une corde.

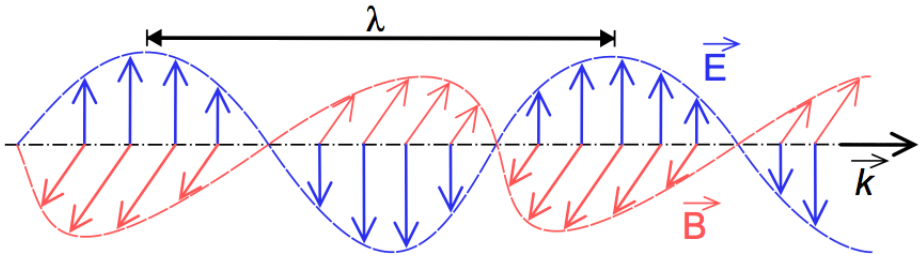



FIGURE 3.1 – Le champs électro-magnétique de la lumière

Admettons que l'onde se propage dans la direction $\hat{z}$ : $\vec{k} = k\hat{z}$ et définissons le vecteur polarisation par $\hat{\epsilon} = \frac{\vec{E}_0}{E_0}$, ainsi :

$$\vec{E}(\vec{r}, t) = \hat{\epsilon} E_0 \cos(\omega t - kz) \quad \text{avec} \quad \hat{\epsilon} = (\cos\theta, \sin\theta)$$

Il existe toutefois une définition plus générale de la polarisation. Supposons que l'oscillation de $E_x(t)$ soit hors phase par rapport à celle de $E_y(t)$. En définissant les déphasages $\delta_x$ et $\delta_y$, les composantes du champs électrique en $z = 0$ sont :

$$E_x = E_0 \cos\theta \cos(\omega t - \delta_x)$$
$$E_y = E_0 \sin\theta \cos(\omega t - \delta_y)$$

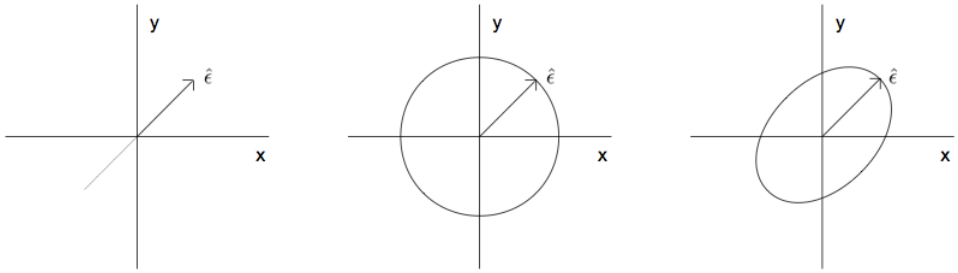



FIGURE 3.2 – Les polaristaions linéaire, circulaire et elliptique

Si par exemple $\delta_x = 0$ et $\delta_y = \frac{\pi}{2}$, alors le vecteur polarisation parcourt un cercle. Plus en général, $\vec{E}(t)$, d'où le nom de polarisation elliptique. Il existe naturellement aussi la polarisation linéaire définie par $\delta_x = \delta_y$, comme représenté sur la figure ci-dessous.
Nous pouvons écrire les composantes du champs électrique en utilisation la notation complexe :

$$E_x = E_0 Re(\cos\theta e^{-i(\omega t+\delta_x)}) = E_0 Re(\lambda e^{-i\omega t}) \quad \text{avec} \quad \lambda = \cos\theta e^{i\delta_x}$$
$$E_y = E_0 Re(\sin\theta e^{-i(\omega t+\delta_y)}) = E_0 Re(\mu e^{-i\omega t}) \quad \text{avec} \quad \mu = \sin\theta e^{i\delta_y}$$

Nous avons naturellement : $|\mu|^2 + |\lambda|^2 = 1$. Puisque l'état physique est défini à moins d'une phase globale (un shift du temps), nous pouvons remplacer $\lambda$, $\mu$ par $\lambda' = \lambda e^{i\phi}$ et $\mu' = \mu e^{i\phi}$. Si nous acceptons le fait de devoir prendre toujours la partie réelle pour avoir le champs physique, alors de champs électromagnétique d'une onde plane est décrit par un vecteur :

$$\hat{\epsilon} = (\lambda, \mu) \quad \text{avec} \quad \lambda, \mu \in \mathbb{C} \quad \text{et} \quad |\hat{\vec{\epsilon}}| = 1$$

De plus, le principe de superposition est valable, puisque le champ résultant de deux cahmps $\vec{E_1}$ et $\vec{E_2}$ est la somme des vecteurs : $\vec{E} = \vec{E_1} + \vec{E_2}$. C'est exactement le modèle mathématique de qu-bit que nous avons décrit.
Mais le champs électromagnétique n'a rien de quantique ! Il est décrit par les équations de Maxwell qui datent de 180 ans ! Peut-on vraiment utiliser des ondes électromagnétiques classiques comme qu-bits ? La réponse est évidemment non. Le système classique ne peut pas reproduire la caractéristique essentielle de la mécanique quantique : les corrélations quantiques. En d'autres mots, avec un champ classique, il n'y a pas de moyen de représenter l'état intriqué de deux qu-bits :

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|11\rangle$$

Si nous cherchons a représenter 2 qu-bits par deux ondes électromagnétiques, le champ résultant est la somme des deux champs, pas un objet défini dans un espace vectoriel de dimension 4.
Nous verrons par la suite que le modèle du qu-bit s'applique à la lumière seulement si nous considérons l'état d'un seul photon. Mais tout d'abord, nous allons discuter l'effet d'un filtre polariseur sur un champs électromagnétique.

Un filtre polariseur est un objet qui laisse passer seulement la lumière polarisée dans une direction donnée $\hat{n}$. Si nous reprenons notre analogie avec la corde, il faut s'imaginer une grille orientée selon $\hat{n}$.

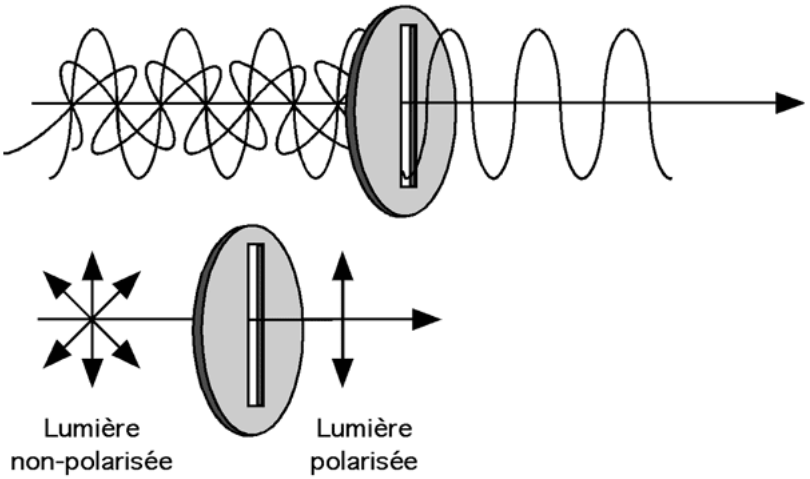



FIGURE 3.3 – Schéma d'un filtre polariseur

A la sortie du filtre, le champ électromagnétique est donnée par :

$$\begin{aligned}\vec{E'} = (\vec{E}\cdot\hat{n})\hat{n} &= E_0\cos\omega t(\hat{\epsilon}\cdot\hat{n})\hat{n} \\ &= E_0\cos\omega t(\cos\theta\cos\alpha+\sin\theta\sin\alpha)\hat{n} \\ &= E_0\cos\omega t\cos(\theta-\alpha)\hat{n}\end{aligned}$$

où nous considérons de la lumière avec une polarisation linéaire $\hat{\epsilon}$ et $\hat{n} = (\cos\alpha, \sin\alpha)$ est le vecteur unitaire qui définit l'orientation de la grille. L'intensité sortante sera :

$$I' = |\vec{E'}|^2 = I\cos^2(\theta-\alpha)$$

C'est la *loi de Malus*. Nous en avons besoin pour comprendre le processus de mesure dans le cas à un seul photon (qui est un qu-bit).

Un autre outil important est la *lame biréfringente*. Il s'agit d'une lame qui a deux index de réfraction différent pour les polarisations selon $\hat{x}$ et $\hat{y}$.

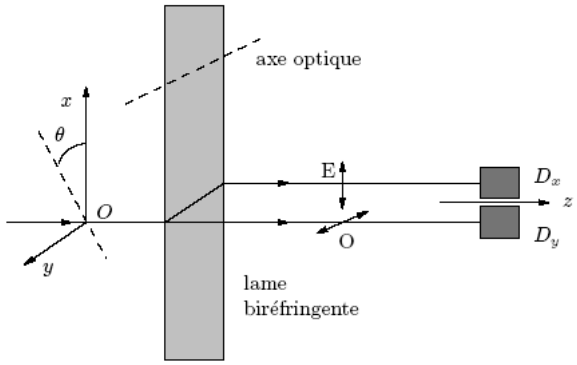



FIGURE 3.4 – Schéma d'une lame biréfringente

Les deux rayons seront polarisés selon $\hat{x}$ et $\hat{y}$. Selon la loi de Malus, les intensités mesurées par les deux détecteurs $D_x$ et $D_y$ seront :

$$I_x = I\cos^2\theta$$
$$I_y = I\sin^2\theta$$

### Le photon

Nous savons (depuis 1908 grâce aux travaux d'Einstein) que la lumière est composée d'unités élémentaires discrètes appelées photons. Aujourd'hui, des centaines de laboratoires effectuent des expériences où l'on produit et manipule des photons individuels. C'est une tâche standard. Mais comment décrire la polarisation dans le cas d'un seul photon ?
Supposons de répéter l'expérience avec la lame biréfringente, mais cette fois avec une source qui produit un photon à la fois. Les détecteurs $D_x$ et $D_y$ sont des compteurs de photons, capables de détecter l'arrivée d'un seul photon (avec un signal sur un ordinateur). Ce que nous observons est que des fois c'est $D_x$ qui de déclenche et des fois $D_y$. Le nombre de fois $N_x$ que $D_x$ de détecte un photon pour un nombre total $N$ de photons envoyés ($N$ doit être assez grand, c'est-à-dire que nous attendons assez longtemps), est :

$$N_x \approx N\cos^2\theta$$

De même : $N_y \approx N\sin^2\theta$. Nous retrouvons la loi de Malus. Mais pour chaque photon un seul détecteur se déclenche. Nous aurions envie de dire que la lame

envoie certains photons vers $x$ et certains vers $y$. Nous verrons que cette façon de penser est fausse. Ce qui arrive réellement et l'interprétation de ce phénomène sont à la base des lois de la mécanique quantique. Il est prématuré d'essayer de comprendre, sans avoir vu les principes de la mécanique quantique et de mesure.
Nous allons juste remarquer qu'un photon semblerait avoir deux états de polarisation que nous appellerons $|x\rangle$ et $|y\rangle$. Tous les états de polarisation vus pour un champ classique, sont possibles pour le photon également :

$$|\psi\rangle = \lambda\,|x\rangle + \mu\,|y\rangle$$

avec $\lambda = \cos\theta e^{i\phi}$ et $\mu = \sin\theta$.

Pour $\phi = 0$, nous avons la polarisation linéaire

Pour $\phi = \frac{\pi}{2}$, nous avons une polarisation circulaire

Pour $\phi$ différent, nous avons une polarisation elliptique

La différence par rapport au cas classique est que maintenant nous parlons d'*état* d'un photon, pas simplement de polarisation. Nous ne l'avons pas dit, mais cet état est représenté par un vecteur dans un espace de Hilbert de dimension 2 avec la base $\mathcal{H} = \{|x\rangle \text{ et } |y\rangle\}$. Il nous manque toujours de savoir comment un tel système évolue dans le temps et comment nous mesurons ses propriétés.
Toutefois, la différence fondamentale par rapport au cas classique est que les états de deux photons seront donnés par les vecteur dans l'espace produit tensoriel $\mathcal{H} \otimes \mathcal{H}$. Donc nous pouvons avoir :

$$|\psi\rangle = \alpha\,|xx\rangle + \beta\,|yy\rangle$$

alors que pour deux champs classiques, nous aurions juste les deux vecteurs de polarisation sommés. C'est un état de *corrélation quantique ou intriqué*, et nous avons vu que c'est grâce à ces états que nous pouvons réaliser le paradigme de l'information quantique.

### Spin d'une particule

Les particules élémentaires ont un moment magnétique $\vec{\mu}$. Elles se comportent donc comme une aiguille d'une boussole en présence d'un champ magnétique $\vec{B}$ Leur énergie est $E = -\vec{\mu} \cdot \vec{B}$. Donc pour minimiser l'énergie, elles vont toujours tendre à aligner $\vec{\mu}$ parallèle à $\vec{B}$.Si de plus $\vec{B}$ varie dans l'espace, la particule va subir une force qui tend à déplacer vers région de grand $\vec{B}$ avec la même orientation que $\vec{\mu}$.
Si toutefois, nous effectuons une expérience (semblable à la lame biréfringente

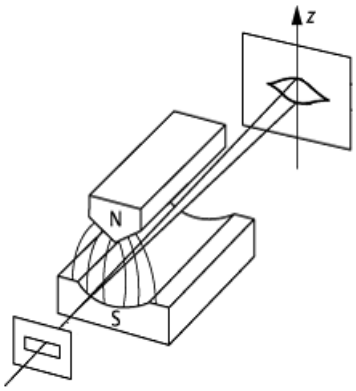



FIGURE 3.5 – Expérience de Stern et Gerlach

pour les photons) où nous faisons passer des protons à travers un champ magnétique variable, les protons sont partagés en deux chemins. Cette expérience a été réalisée par Stern et Gerlach et montre que deux seuls valeurs du moment magnétique sont détectés. Cette expérience a permis de découvrir que les particules élémentaire tel que les électrons ou les protons ont un *spin*, qui le long d'une direction $\hat{n}$, ne peut valoir que $\pm\frac{1}{2}$ (fois une valeur élémentaire $\mu_B = \frac{eh}{2m_e c}$ le magnéton de Bohr). Sans aller dans les détails de la mécanique quantique (que nous comprendrons par la suite), nous pouvons encore une fois décrire l'état s'un électron ou proton par un vecteur dans la base : $\{|+\rangle = |+\frac{1}{2}\rangle, |-\rangle = |-\frac{1}{2}\rangle\}$ :

$$|\psi\rangle = e^{-i\frac{\phi}{2}} \cos\frac{\theta}{2} |+\rangle + e^{i\frac{\phi}{2}} \sin\frac{\theta}{2} |-\rangle$$

Nous pouvons montrer que cet état correspond à un moment magnétique $\vec{\mu}$ orienté vers $\hat{n}$ où :

$$\hat{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

C'est un vecteur sur une sphère 3D de rayon $R = 1$ qu'on appelle sphère de Bloch. Nous pouvons faire les mêmes considérations pour deux particules que pour les photons. Toutefois la paramétrisation est différente : Pour les photon, nous avons $\theta = 0, \frac{\pi}{2}$ et pour les particules (électrons et protons) $\theta = 0, \pi$.

Les particules que nous avons considérées, les photons et les électrons (ou protons), sont à la base de toutes les technologies candidates à l'information quantique.

# 4 Formulation générale de la mécanique quantique

Le progrès qui a eu lieu entre 1900 et 1926 dans la compréhension des phénomènes quantiques, notamment avec les théories de Schrödinger et de Heisenberg, a conduit à une formulation générale de la mécanique quantique. Pour bien comprendre l'information quantique il n'est pas indispensable de reparcourir les étapes historiques de ce développement. Il est suffisant d'introduire la mécanique quantique dans sa formulation générale. Cette formulation réunit, dans une structure conceptuellement cohérente, une méthode mathématique et une interprétation physique complète. Pour cela, la théorie repose sur un certain nombre de postulats. Ainsi, certains aspects très importants – premièrement la théorie de la mesure – n'auront pas une justification précise. Cependant, les conséquences de ces postulats ont été vérifiées dans des milliers de laboratoires durant presque un siècle, faisant de la mécanique quantique la théorie la plus vérifiée de l'histoire de la science.

## 4.1 Etats et principe de superposition

Avant de passer à l'exposition de ces postulats, nous allons brièvement discuter le lien conceptuel entre le formalisme de la mécanique quantique et certains faits physiques importants. Loin de vouloir démontrer les principes de la mécanique quantique, cette discussion est censée donner des éléments de plausibilité du formalisme qui suivra. L'aspect formel nouveau sur lequel se tient toute la théorie formelle, est le *principe de superposition*. Le principe de superposition dit que, si un système admet deux états possibles, alors toutes les *superpositions linéaires* de ces deux états seront encore des états possibles pour le système. Ce concept est en même temps très nouveau pour la mécanique des particules, et très évident pour la physique des phénomènes ondulatoires. Si nous tirons une balle de fusil dans une direction donnée, la mécanique classique nous permet de bien décrire sa trajectoire. De la même façon pour une balle de fusil tirée dans une autre direction. Toutefois, l'idée qu'une superposition linéaire des deux trajectoires soit encore une trajectoire possible pour la balle, est totalement étrangère à notre intuition et aux lois de la mécanique classique. Si par contre, nous considérons un champ électromagnétique, régi par les équations de Maxwell. Le fait que ces équations soient linéaires a une conséquence très simple :
Si $\mathbf{E}_1 = e^{i\mathbf{k}_1\cdot\mathbf{r}}$ est une solution des équations de Maxwell et si $\mathbf{E}_2 = e^{i\mathbf{k}_2\cdot\mathbf{r}}$ est une deuxième solution possible, alors $\mathbf{E} = \mathbf{E}_1 + \mathbf{E}_2 = e^{i\mathbf{k}_1\cdot\mathbf{r}} + e^{i\mathbf{k}_2\cdot\mathbf{r}}$ est aussi

une solution des équations. L'intensité du champs sera dans ce cas :

$$|\mathbf{E}|^2 = |\mathbf{E}_1 + \mathbf{E}_2|^2 = 2(1 + \cos(\mathbf{k}_1 - \mathbf{k}_2) \cdot \mathbf{r})$$

Nous voyons que le deuxième terme entre parenthèses produit une oscillation de l'intensité dans l'espace : c'est le phénomène de l'interférence qui est une conséquence directe d'un phénomène ondulatoire et du principe de superposition.
Un grand développement qui a eu lieu entre 1900 et 1926 a été la compréhension que la matière peut manifester un comportement ondulatoire. A ce propos, l'expérience de Young est une très bonne illustration.

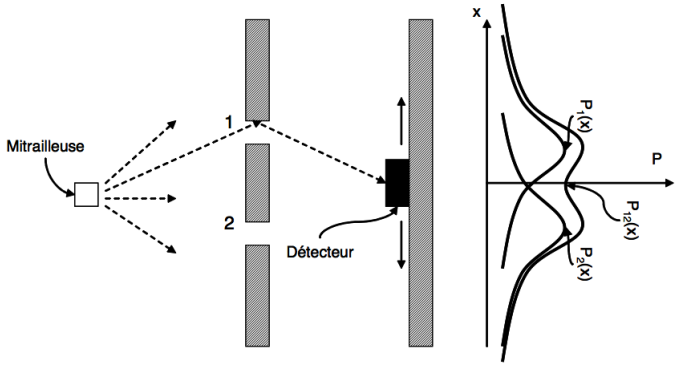



FIGURE 4.1 – Expérience des fentes de Young

Supposons qu'une source de particules (par exemple électrons) soit posée devant un écran avec deux fentes. Les électrons qui passent à travers les fentes sont récoltés sur un deuxième écran (cela pourrait être une plaque photographique, capable de montrer une marque à l'endroit où une particule arrive). Si les particules étaient des vraies objets classiques – par exemple des balles de fusil – on observerait la chose suivante : Si on couvre la fente 1, les balles passées par la fente 2 formerait une figure sur l'écran. Vice-versa, si la fente 2 est couverte, les balles passées par 1 formeraient une autre figure. Avec les deux fentes ouvertes en même temps, la figure serait simplement la somme des deux.
Par contre, pour des électrons, le résultat est très inattendu. L'effet de laisser les deux fentes ouvertes produit une figure d'interférence, avec des oscillations d'intensité qui ne correspondent pas simplement à la somme des deux figures obtenues avec une seule fente ouverte. Les électrons se comportent donc comme des ondes diffractées par les fentes. En plus, si on baisse l'intensité de la source jusqu'à avoir un seul électron à la fois et si on attend

suffisamment longtemps pour donner le temps à la figure sur la plaque de devenir assez marquée, le résultat sera la même.
Comment peut-on expliquer cela si on garde l'idée qu'un électron est une particule qui peut passer soit par un fente soit par l'autre ? Il est impossible ! Si c'était possible, alors par définition le résultat des deux fentes ouvertes ne pourrait qu'être la somme des deux cas avec une seule fente ouverte. Si par contre on imagine associer à un électron un champ ondulatoire $\varphi(\mathbf{r})$, et si on suppose que la figure finale sur la plaque va être proportionnelle à $|\varphi(\mathbf{r})|^2$, alors on a une explication très naturelle. Les deux cas de figure (fente 1 ou 2 ouverte) produisent un "champ" $\varphi_1(\mathbf{r})$ et $\varphi_2(\mathbf{r})$ respectivement. L'effet total est $\varphi(\mathbf{r}) = \varphi_1(\mathbf{r}) + \varphi_2(\mathbf{r})$, et la figure sur la plaque est donnée par

$$|\varphi(\mathbf{r})|^2 = |\varphi_1(\mathbf{r}) + \varphi_2(\mathbf{r})|^2 = |\varphi_1(\mathbf{r})|^2 + |\varphi_2(\mathbf{r})|^2 + 2\mathrm{Re}(\varphi^*(\mathbf{r}\varphi_2(\mathbf{r}))$$

qui contient un terme d'interférence. Cet interférence pour des électrons a été mesurée en 1927. Cette image d'un électron est décrit par une onde reste très arbitraire et sans justification. C'est l'ensemble des observations et des études entre 1900 et 1926 qui permettent d'encadrer cette description dans un contexte plus rigoureux. Elle continue par contre un cadre très naturel pour expliquer le principe de superposition.

## 4.2 Les postulats de la mécanique quantique

Les postulats qui suivent sont appropriés pour la description d'un système isolé, pour lequel il n'y a pas un *environnement* avec qui le système peut interagir. Cette remarque est très importante en liaison avec le processus de mesure. Sous cette hypothèse, nous pouvons en effet décrire le processus de mesure comme un processus *projectif* (dont la définition est donnée ci-dessous). Tout le formalisme de la mécanique quantique est à modifier si nous considérons le problème de la description d'un système en interaction avec un milieu environnant. Dans ce cas, il faut introduire le formalisme de l'*opérateur densité* et un concept généralisé des mesures qu'on appelle en anglais *Positive Operator-Valued Measure* (POVM). Cette généralisation deviendra importante pour décrire en détail le processus de décohérence qui détruit l'information quantique. Il sera principalement sujet du deuxième semestre et donc ne sera introduit plus tard.

### Postulat I : état d'un système

**L'état** d'un système physique est représenté par un vecteur dans un espace vectoriel (sur $\mathbb{C}$) de dimension infinie, muni d'un produit scalaire (espace de Hilbert).

**Commentaires**

1. Remarquez l'immense différence entre cette représentation mathématique et celle d'un système en physique classique, dont l'état est représenté par sa trajectoire dans l'espace des phases (en spécifiant donc les coordonnées et les impulsions à chaque instant du temps).
2. Puisque l'espace des états est un espace vectoriel, nous pouvons faire un pas conceptuel vers l'avant et postuler que *chaque* vecteur dans cet espace vectoriel représente un état possible du système. Cette extension du postulat implique donc très naturellement le principe de superposition : *une combinaison linéaire de deux états possibles du système est aussi un état possible du système*. Comme nous l'avons vu, le principe de superposition est très bien compris pour d'autres phénomènes ondulatoires, comme par exemple le champ électromagnétique. La mécanique quantique est régie par le même principe puisqu'à sa base il y a un phénomène qu'on peut considérer ondulatoire : la fonction d'onde régie par l'équation de Schrödinger. Nous n'allons pas traiter le lien entre la formulation en termes de fonction d'onde et celle et termes de vecteurs dans un espace de Hilbert, mais nous pouvons montrer qu'elles sont équivalentes. La nature ondulatoire de la matière peut donc être considérée comme une justification du principe de superposition.
3. Par hypothèse, seulement la "direction" du vecteur est importante pour la définition de l'état physique. Si nous multiplions un vecteur par un nombre complexe arbitraire non nul, cela ne nous conduit pas à un état physique différent. Pour simplifier la définition des probabilités d'une mesure (voir postulat sur la mesure ci-dessous), nous allons toujours supposer que les états sont normés à 1 : $\langle\psi\rangle\,\psi = 1$. Le vecteur d'état est ainsi défini à moins d'un facteur complexe de module unitaire, de type $e^{i\phi}$.
4. L'espace de Hilbert des états est un espace "abstrait". Il ne représente pas l'espace des phases d'une ou de toutes les particules d'un système.
5. Un changement d'état physique d'un système correspond à un changement du vecteur d'état dans l'espace de Hilbert. Il s'ensuit que l'évolution temporelle d'un système est régie par des équations du mouvement qui décrivent le changement dans le temps du vecteur d'état.

**Postulat II : quantités observables, probabilité et processus de mesure**

Chaque quantité physique "observable" (qui peut être obtenue comme résultat d'un processus de mesure), est représentée par un opérateur linéaire hermitique (c.-à.-d. auto-adjoint), agissant dans l'espace de Hilbert des états. Lorsqu'on effectue une mesure d'une quantité physique représentée par un opérateur hermitique $\hat{A}$, sur un système physique représenté par un vecteur $|\psi\rangle$, les seules valeurs possibles fournies par la mesure sont les valeurs propres de $\hat{A}$. La théorie ne permet pas, en général, de prévoir avec certitude la valeur qui sera fournie par la mesure. Elle établit seulement l'espérance (valeur moyenne, ou "expectation value" en anglais) du résultat de la mesure. Cette espérance est donnée par :

$$\langle A \rangle = \langle \psi | \hat{A} | \psi \rangle \,. \tag{4.1}$$

Si $|\psi\rangle$ est un vecteur propre de $\hat{A}$, par exemple $|\psi\rangle = |a_n\rangle$ avec valeur propre $a_n$ de $\hat{A}$, alors la mesure de l'observable $|A\rangle$ donnera **avec certitude** la valeur $a_n$. Ceci est consistent avec l'espérance définie par l'équation (4.1) : $\langle A \rangle = \langle a_n | \hat{A} | a_n \rangle = a_n \langle a_n \rangle a_n = a_n$.
Si par contre $|\psi\rangle$ n'est pas état propre de $A$, alors la mesure peut donner des résultats différents, choisis parmi les valeurs propres de $\hat{A}$. La moyenne du résultat de la mesure (au sens statistique : imaginons qu'elle soit répétée plusieurs fois sur des répliques identiques du système), appelée "espérance" de $\hat{A}$, et est donnée par :

$$\begin{aligned} \langle \hat{A} \rangle &= \langle \psi | \hat{A} \psi \rangle \\ &\equiv \langle \psi | \hat{A} | \psi \rangle \qquad \text{(notation)} \end{aligned}$$

L'opération de mesure perturbe le système. Supposons que la mesure de l'observable $A$ donne comme résultat une valeur propre $a_n$ non dégénérée (c'est-à-dire qu'il y a un seul vecteur propre $|a_n\rangle$ correspondant à cette valeur propre). Le postulat dans ce cas dit que le nouvel état du système est $|a_n\rangle$. Si par contre la valeur propre $a_n$ qu'on mesure est dégénérée, alors le postulat dit que l'état du système après la mesure sera une combinaison linéaire $|\psi\rangle = \sum_n \alpha_n |a_n\rangle$, où la somme est faite sur tous les vecteurs propres $|a_n\rangle$ qui correspondent à la valeur propre $a_n$. En d'autre mots, l'état après la mesure est un vecteur dans le sous-espace généré par les vecteurs propres correspondant à la valeur propre qu'on a mesurée.

**Commentaires**

1. La linéarité des opérateurs observables est nécessaire pour assurer le principe de superposition.
2. Les opérateurs observables doivent être hermitiques pour avoir des valeurs propres réelles. Ceci sert à assurer que le résultat d'une observation physique (la mesure d'une quantité) soit toujours un nombre réel. Pour mieux comprendre ce commentaire il faut introduire le troisième postulat qui définit le processus de mesure.
3. Ce postulat établit le contenu physique principal de la théorie, puisque il relie le formalisme mathématique aux résultats du processus de mesure.
4. Ce postulat est le plus problématique d'un point de vue conceptuel, puisque il remet apparemment en question l'idée du déterminisme, c'est-à-dire la possibilité de prévoir le comportement d'un système. Plusieurs physiciens, parmi lesquels Einstein ("Gott würfelt nicht") ont eu des difficultés à l'accepter.
5. Si $|\psi\rangle$ est un état arbitraire du système, nous pouvons l'écrire sous forme d'une expansion sur la base complète des vecteurs propres de $\hat{A}$, $\{|a_n\rangle\}$

$$|\psi\rangle = \sum_n |a_n\rangle \langle a_n\rangle \psi \,.$$

Dans ce cas général, l'espérance de la mesure de $\hat{A}$ est donnée (en appliquant les règles du produit scalaire) par :

$$\begin{aligned}
\langle\psi|\hat{A}|\psi\rangle &= \sum_n \sum_m (\langle\psi\rangle a_n)^* \langle a_n|\hat{A}|a_m\rangle \langle a_m\rangle \psi \\
&= \sum_n \sum_m (\langle\psi\rangle a_n)^* a_m \langle a_n\rangle a_m \langle a_m\rangle \psi \\
&= \sum_n \sum_m (\langle\psi\rangle a_n)^* a_m \langle a_m\rangle \psi \delta_{nm} \\
\langle\psi|\hat{A}|\psi\rangle &= \sum_m a_m |\langle a_m\rangle \psi|^2 \qquad (4.2)
\end{aligned}$$

Ce résultat doit être interprété comme une valeur moyenne au sens statistique. Le résultat de la mesure est l'une des valeurs propres $a_m$, avec probabilité $|\langle a_m\rangle \psi|^2$. En d'autres termes, admettons que nous ayons $N$ répliques identiques d'un système dans un état $|\psi\rangle$ et que nous effectuons la même mesure de $\hat{A}$ sur chacun des ces systèmes. L'interprétation correcte du concept de probabilité est que chaque mesure donnera une parmi les valeurs propres $a_n$. Pour $N$ suffisamment grand, nous pourrions en principe calculer la distribution statistique

des résultats des $N$ mesures. Cette distribution serait exactement donnée par $|\langle a_m \rangle \psi|^2$.
Dans ce sens, la théorie de la mécanique quantique est parfaitement déterministe, puisque elle définit tous les résultats possibles d'une mesure et en donne avec précision les différentes probabilités.

6. Il est très important de remarquer que la nature de cette distribution de probabilité définie par les $|\langle a_m \rangle \psi|^2$ est fondamentalement différente de la notion de probabilité en physique statistique classique. En physique statistique, la notion de probabilité est introduite pour pouvoir décrire un système composé d'un très grand nombre de particules. Elle constitue une simplification par rapport à la connaissance exacte des trajectoire dans l'espace des phases de toutes les particules, qui reste en principe possible. En mécanique quantique, même pour une seule particule, la connaissance précise de toutes les quantités physiques est impossible, et le concept de probabilité est une *caractéristique intrinsèque de la nature*. C'est ici que nous retrouvons la différence profonde entre la physique classique et la physique quantique.

7. Nous pourrions nous poser la question, si le concept de probabilité est vraiment nécessaire. Une question beaucoup plus profonde est celle concernant les *variables cachées* : le fait que la même mesure, effectuée sur des répliques identiques d'un système dans un état $|\psi\rangle$, donne des résultats différents, pourrait-il découler d'une caractéristique intrinsèque de la nature ? Ou exprime-t-il seulement une limitation du processus de mesure ? Dans cette deuxième hypothèse, l'incertitude du résultat serait due à certaines variables physiques dont nous ne connaissons pas l'existence (variables cachées). Ces variables pourraient avoir des valeurs différentes pour les différentes répliques du système, ce qui entraînerait les différents résultats des mesures. La probabilité ne serait donc pas une propriété intrinsèque du système, mais plutôt une conséquence de la connaissance incomplète que nous avons du système.
Par analogie, nous pouvons penser à la théorie statistique classique d'un gaz composé d'un grand nombre de molécules. Dans ce cas, les variables cachées seraient les trajectoires dans l'espace des phases de chaque molécule. Leur connaissance serait en principe possible, et les équations du mouvement de toutes les molécules (avec leurs interactions mutuelles) constitueraient une description totalement déterministe. Toutefois, étant donné la complexité d'un tel ensemble d'équations, nous acceptons plutôt une description statistique du système, qui est beaucoup plus simplifiée et nous donne accès à des valeurs moyennes des quantités physiques d'intérêt.

Le problème des variables cachées a été étudié par plusieurs scientifiques. Cette question était cependant considérée comme une question purement philosophique, jusqu'en 1964. En cette année, John S. Bell a démontré son fameux théorème. Le théorème affirme qu' "Il est impossible de concevoir une théorie faisant intervenir des variables cachées, qui reproduise de manière complète le prévisions de la mécanique quantique". Ensemble avec son théorème, Bell donne une méthode opérationnelle – basée sur une inégalité entre certains résultats de la mesure – pour établir si un système physique peut être décrit par une théorie faisant intervenir des variables cachées. A présent, cette méthode a été appliquée à des centaines d'expériences physiques, et a toujours confirmé la validité de la mécanique quantique. Nous pouvons donc affirmer que le théorème de Bell a été, après le principe de complémentarité de Bohr, la deuxième petite révolution conceptuelle apportée par la mécanique quantique.

Prenons un exemple de processus de mesure. Considérons le système d'un photon avec deux possibles états de polarisation. Nous pouvons imaginer un instrument qui mesure la polarisation selon les axes $|x\rangle$ et $|y\rangle$, donnant la valeur 1 pour la polarisation $|x\rangle$ et $-1$ pour la polarisation $|y\rangle$. L'opérateur hermitique qui correspond à cet observable est construit à partir de sa représentation spectrale : $P_{xy} = 1 \times |x\rangle \langle x| - 1 \times |y\rangle \langle y|$, ce qui correspond, dans la base $\{|x\rangle, |y\rangle\}$, à la matrice :

$$P_{xy} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Nous pouvons maintenant imaginer un autre instrument capable de mesurer le degré de polarisation circulaire. Cet instrument donne avec certitude la valeur 1 si l'état est $|+\rangle = 2^{-1/2}(|x\rangle + i\,|y\rangle)$ et -1 si l'état est $|-\rangle = 2^{-1/2}(|x\rangle - i\,|y\rangle)$. Si on reste dans la base $\{|x\rangle, |y\rangle\}$, la représentation spectrale de cet opérateur est $P_{+-} = 1 \times \frac{1}{2}(|x\rangle + i\,|y\rangle)(\langle x| - i\,\langle y|) - 1 \times \frac{1}{2}(|x\rangle - i\,|y\rangle)(\langle x| + i\,\langle y|)$. Sous forme de matrice :

$$P_{+-} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Un troisième instrument donne +1 et -1 respectivement pour les deux états de polarisation linéaire à $45^\circ |\frac{\pi}{4}\rangle$ et $|\frac{3\pi}{4}\rangle$. Le même raisonnement nous conduit à l'expression :

$$P_{\frac{\pi}{4}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ces trois matrices sont connues en mécanique quantique comme les matrices de Pauli (elles sont toujours indiquées par $\sigma_z$, $\sigma_y$ et $\sigma_x$, dans l'ordre de notre exposition). Elles jouent un rôle très important dans la physique du spin d'une particule.
Considérons maintenant un photon dans l'état $|x\rangle$. Faisons une mesure de $P_{\frac{\pi}{4}}$. Nous avons 50% de probabilité d'obtenir +1 et 50% de probabilité d'obtenir -1. Nous pouvons facilement vérifier cela en calculant, par exemple, $p(+1) = |\langle\frac{\pi}{4}|x\rangle|^2 = 1/2$ (à vérifier). Si on obtient +1, le nouvel état après la mesure est $|\frac{\pi}{4}\rangle$ et, si on obtient -1 le nouvel état après la mesure est $|\frac{3\pi}{4}\rangle$. Supposons avoir obtenu +1. Maintenant, si nous effectuons une nouvelle mesure de $P_{\frac{\pi}{4}}$, on obtient +1 avec 100% de probabilité et l'état reste le même qu'avant la mesure. Supposons par contre mesurer $P_{xy}$. L'état avant la mesure est $|\frac{\pi}{4}\rangle$. Maintenant nous aurons +1 avec une probabilité de 50% et -1 avec une probabilité de 50%. L'état final sera $|x\rangle$ dans le premier cas et $|y\rangle$ dans le deuxième. Et ainsi de suite.

Cet exemple est utile pour comprendre un fait très important en physique quantique : Il y a des paires d'observables *non compatibles*. Cela veut dire qu'il est impossible d'avoir en même temps la certitude sur la mesure de $P_{xy}$ et de $P_{\pi/4}$. Si l'état est $|x\rangle$ par exemple, la mesure de $P_{xy}$ donne +1 avec certitude. Par contre la mesure de $P_{\pi/4}$ peut donner deux valeurs avec la même probabilité (donc le résultat de la mesure est indéterminé). Si l'état est $|\pi/4\rangle$, alors c'est $P_{\pi/4}$ qui donnera +1 avec certitude, alors que la mesure de $P_{xy}$ peut donner les deux valeurs avec même probabilité. Existe-t-il un état pour lequel les deux mesures donnent un résultat sûr à 100% ?
La réponse est non. Pour que cela soit possible, il faudrait que cet état soit un vecteur propre de $P_{xy}$ et de $P_{\pi/4}$ en même temps. Cela est impossible puisque $P_{xy}$ et $P_{\pi/4}$ n'ont pas de vecteurs propres en commun. En effet, si $|\alpha\rangle$ était vecteur propre des deux opérateurs, alors le vecteur orthogonal $|\alpha_\perp\rangle$ serait aussi vecteur propre des deux opérateurs (puisque nous sommes en 2 dimensions). Or cela est impossible puisque nous vérifions que $[P_{xy}, P_{\pi/4}] \neq 0$ ($[A, B] = AB - BA$ est le *commutateur* de A et B). Si $|\alpha\rangle$ et $|\alpha_\perp\rangle$ sont vecteurs propres des deux, nous pourrions écrire les deux opérateurs en représentation spectrale comme :

$$P_{xy} = a_{xy} |\alpha\rangle \langle\alpha| + b_{xy} |\alpha_\perp\rangle \langle\alpha_\perp|$$

$$P_{\frac{\pi}{4}} = a_{\frac{\pi}{4}} |\alpha\rangle \langle\alpha| + b_{\frac{\pi}{4}} |\alpha_\perp\rangle \langle\alpha_\perp|$$

où $a_{xy}$ et $b_{xy}$ sont les valeurs propres pour $P_{xy}$ et $a_{\frac{\pi}{4}}$ et $b_{\frac{\pi}{4}}$ sont les valeurs propres pour $P_{\frac{\pi}{4}}$. Avec cette représentation spectrale, les deux matrices seraient diagonales dans la même base et nous aurions forcement $[P_{xy}, P_{\frac{\pi}{4}}] = 0$,

un résultat incorrecte.
En général deux observables qui ne commutent pas, c'est-à-dire dont leur commutateur est non-nul, sont appelés observables non compatibles. Cela implique qu'il est impossible, pour un système dans un état quelconque, de mesurer la valeur d'une première observable et la valeur d'une deuxième observable avec certitude. C'est à partir de cette propriété que découle le principe d'incertitude de Heisenberg, comme nous le verrons par la suite.

**Postulat III : équation de Schrödinger**

L'évolution d'un système physique décrit par un état $|\varphi(t)\rangle$, au cours du temps $t$, est régie par l'équation de Schrödinger dépendante du temps :

$$i\hbar\frac{\partial}{\partial t}|\varphi(t)\rangle = \hat{H}(\hat{x},\hat{p},t)\,|\varphi(t)\rangle\ , \tag{4.3}$$

**Commentaires**

1. L'équation de Schrödinger détermine l'état $|\varphi(t)\rangle$ – et donc la distribution de probabilité de la mesure de toutes observables – de manière complète au cours du temps, une fois une condition initiale donnée. Dans ce sens, la mécanique quantique est une théorie complètement déterministe. C'est seulement la nature qui ne permet pas de connaître le résultat d'une mesure avec certitude.
2. Considérons un système dont l'Hamiltonien $\hat{H}$ ne dépend pas explicitement du temps. Si nous faisons l'hypothèse qu'un état soit caractérisé par une évolution de type stationnaire au cours du temps :

$$\varphi(x,t) = \varphi_n(x)\exp\left(-\frac{iE_nt}{\hbar}\right)\ , \tag{4.4}$$

alors l'équation de Schrödinger dépendante du temps implique l'équation de Schrödinger aux valeurs propres

$$H\left(x,-i\hbar\frac{\partial}{\partial x}\right)\varphi_n(x) = E_n\varphi_n(x)\,. \tag{4.5}$$

**Postulat IV : systèmes composés**

L'état d'un système composés de deux sous-systèmes, dont les états sont décrits par des vecteurs dans les espaces de Hilbert $V_1$ et $V_2$, est décrit par les vecteurs dans l'espace produit tensoriel $V = V_1 \otimes V_2$.

## 4.3 Le processus de mesure

Le Postulat II relie la structure mathématique de la mécanique quantique au processus de mesure. Il dit que, pour un système dans un état $|\psi\rangle$, la probabilité de mesurer la valeur propre $a_n$ de l'opérateur $\hat{A}$, représentant une quantité observable, est :

$$|< a_n|\psi >|^2 \tag{4.6}$$

et que la valeur moyenne de ce processus de mesure, au sens statistique, est :

$$< \psi|\hat{A}|\psi > . \tag{4.7}$$

Il est très important de souligner l'interprétation statistique de ce postulat. Pour bien comprendre les deux résultats (4.6) et (4.7), nous devons imaginer avoir préparé un ensemble statistique composé d'un grand nombre de répliques identiques du système dans l'état $|\psi\rangle$, et d'effectuer la mesure une fois sur chacun de ces systèmes. Le Postulat II affirme que l'analyse statistique des différents résultats obtenus, donnera une distribution de probabilité (4.6) et une valeur moyenne (4.7).
Une question est toutefois légitime : Qu'arrive-t-il si on effectue une mesure de $\hat{A}$ plusieurs fois à la suite sur le même système ? La réponse que nous allons donner à cette question doit être considérée comme une extension du Postulat II. En particuliers, elle est en accord avec l'immense nombre de vérifications expérimentales de la mécanique quantique. Supposons que nous effectuons la mesure une première fois et que nous obtenons le résultat $a_n$. Le processus de mesure va induire un changement d'état du système. Le nouvel état, après la mesure, est l'état propre $|a_n\rangle$ correspondant à la valeur propre $a_n$ de $\hat{A}$. Si la valeur propre $a_n$ est dégénérée et si nous notons $|a_n^{(1)}\rangle, \ldots, |a_n^{(r)}\rangle$ les vecteurs propres associés, la probabilité de trouver $a_n$ est donnée par :

$$P_{a_n} = \sum_{i=1}^{r} \left| \langle a_n^{(i)} \rangle \, \psi \right|^2 \tag{4.8}$$

et juste après la mesure, le système est dans l'état $\frac{1}{N} \sum_{i=1}^{r} < a_n^{(i)}|\psi > |a_n^{(i)}\rangle$ avec $N = \left( \sum_{i=1}^{r} \left| \langle a_n^{(i)} \rangle \, \psi \right|^2 \right)^{\frac{1}{2}}$, assurant la normalisation de l'état. Une deuxième mesure de $\hat{A}$ sur le nouvel état du *même* système nous donnera donc de nouveau la même valeur $a_n$.
Il faut donc accepter le fait qu'un processus de mesure en mécanique quantique modifie l'état du système sur lequel la mesure est effectuée. Cela est une conséquence naturelle du fait que l'outil de mesure (par exemple les photons

utilisés pour détecter le passage des électrons dans l'expérience de pensée de Young) est aussi un système régi par le lois de la mécanique quantique et qu'il interagit avec le système qui est mesuré. Cela n'est pas en contradiction avec la version généralisée du principe de complémentarité quantique dont nous avons discuté dans le premier chapitre. Dans le cas de l'expérience de Young avec des dédoubleurs, par exemple, nous avons vu que le principe est vérifié indépendamment du fait d'effectuer la mesure. La complémentarité quantique ne doit donc pas être attribuée à l'action de la mesure sur le système. Toutefois, il faut accepter que, si une mesure est effectuée, alors l'état du système sera modifié par conséquent.

Il est intéressant d'élargir cette discussion au cas où nous mesurons deux quantités observables distinctes, représentées par les opérateurs $\hat{A}$ et $\hat{B}$. Deux cas sont possibles :

1. Premièrement, le cas où les deux observables commutent : $[\hat{A}, \hat{B}] = 0$. Dans ce cas, d'après l'algèbre linéaire il est possible de trouver une base orthonormée $\{|a_n, b_m\rangle\}$ de l'espace de Hilbert, qui soit simultanément base de vecteurs propres de $\hat{A}$ et de $\hat{B}$, avec valeurs propres $a_n$ et $b_m$ respectivement. Imaginons effectuer une mesure de $\hat{A}$ sur un état $|\psi\rangle$, et obtenir la valeur $a_n$. Maintenant le nouvel état du système est l'état propre de $\hat{A}$ donné par [1]

$$|\psi'\rangle = \sum_{m,n=1}^{\infty} < a_n, b_m|\psi > |a_n, b_m\rangle \ . \tag{4.9}$$

   Effectuons maintenant une mesure de $\hat{B}$ et supposons obtenir la valeur $b_m$. Maintenant le nouvel état du système est aussi un état propre de $\hat{B}$. Si $b_m$ est aussi non dégénérée, le nouvel état sera $|a_n, b_m\rangle$. Il est clair que maintenant une nouvelle mesure de $\hat{A}$ sur le même système dans son nouvel état, nous donnera toujours la valeur $a_n$. De même, des nouvelles mesures de $\hat{B}$ nous donnerons toujours la valeur $b_m$.
2. Le deuxième cas est représenté par deux observables $\hat{A}$ et $\hat{B}$ dont le commutateur n'est pas zéro, comme par exemple la coordonné spatiale $\hat{x}$ et la quantité de mouvement $\hat{p}_x$. D'après l'algèbre linéaire, nous savons qu'il n'est maintenant plus possible de trouver une base d'états propres simultanément de $\hat{A}$ et $\hat{B}$. Supposons que la mesure de $\hat{A}$ sur un état initial $|\psi\rangle$ donne la valeur propre $a_n$ de $\hat{A}$. Le nouvel état du système sera maintenant $|a_n\rangle$. Si nous effectuons maintenant une mesure de $\hat{B}$, avec le résultat $b_m$, l'état du système après la mesure sera

1. Pour simplifier, nous allons supposer que la valeur propre $a_n$ est non dégénérée. La généralisation au cas dégénéré est immédiate.

un état propre de $\hat{B}$, $|b_m\rangle$. Cet état n'est en général pas un état propre de $\hat{A}$. Il s'ensuit qu'une nouvelle mesure de $\hat{A}$ peut de nouveau donner une valeur quelconque parmi les valeurs propres $a_j$ de $\hat{A}$, pas nécessairement la valeur $a_n$ mesurée auparavant. La mesure de $\hat{B}$ a donc annulé l'effet de la précédente mesure de $\hat{A}$, qui était d'avoir mis le système dans un état propre de $\hat{A}$. La deuxième mesure de $\hat{A}$ va donc conduire le système dans un autre état propre $|a_j\rangle$. Une mesure successive de $\hat{B}$ donnera en général une valeur propre $b_j$ différente du précèdent résultat, et le nouvel état sera $|b_j\rangle$, et ainsi de suite. La non-commutativité des opérateurs $\hat{A}$ et $\hat{B}$ est à l'origine de ce résultat singulier du processus de mesure, qui est la manifestation directe du *principe d'incertitude de Heisenberg* : Nous ne pouvons pas connaître simultanément avec certitude la valeur des deux observables $\hat{A}$ et $\hat{B}$ et, en effet, si nous essayons d'effectuer les deux mesures plusieurs fois sur le même système, nous obtenons des résultats variables, dont la distribution de probabilité est donnée par la loi établie par le Postulat II.

Cette impossibilité de mesurer les deux quantités simultanément avec précision arbitraire se traduit par la *relation d'incertitude généralisée* :

$$\Delta\hat{A}_{|\psi\rangle}\Delta\hat{B}_{|\psi\rangle} \geq \frac{1}{2}\left|\langle\psi|\left[\hat{A},\hat{B}\right]|\psi\rangle\right|, \tag{4.10}$$

où nous avons utilisé la notation $\Delta\hat{O}_{|\psi\rangle}$ pour indiquer l'écart type de l'observable $\hat{O}$ calculé sur l'état $|\psi\rangle$. Nous rappelons que cet écart type est défini comme :

$$\Delta\hat{O}_{|\psi\rangle} = \sqrt{\langle\psi|\hat{O}^2|\psi\rangle - \langle\psi|\hat{O}|\psi\rangle^2} \tag{4.11}$$

Démonstration : Nous remarquons d'abord que, pour chaque paire d'opérateurs $\hat{A},\hat{B}$ hermitiques, $\langle\psi|\left[\hat{A},\hat{B}\right]|\psi\rangle$ est imaginaire pur. En effet,

$$\begin{aligned}&\left[\hat{A},\hat{B}\right]^\dagger = \left(\hat{A}\hat{B}-\hat{B}\hat{A}\right)^\dagger = \hat{B}^\dagger\hat{A}^\dagger - \hat{A}^\dagger\hat{B}^\dagger = \hat{B}\hat{A}-\hat{A}\hat{B} = -\left[\hat{A},\hat{B}\right]\\ &\Rightarrow \quad \langle\psi|\left[\hat{A},\hat{B}\right]^\dagger|\psi\rangle = \langle\psi|\left[\hat{A},\hat{B}\right]|\psi\rangle^* = -\langle\psi|\left[\hat{A},\hat{B}\right]|\psi\rangle\end{aligned} \tag{4.12}$$

Nous définissons les opérateurs hermitiques :

$$\begin{aligned}\hat{A}_0 &= \hat{A} - \langle\psi|\hat{A}|\psi\rangle\hat{I}\\ \hat{B}_0 &= \hat{B} - \langle\psi|\hat{B}|\psi\rangle\hat{I}\end{aligned} \tag{4.13}$$

qui satisfont les propriétés :

1. $\langle\psi|\hat{A}_0^2|\psi\rangle = \langle\psi|\hat{A}^2|\psi\rangle - 2\langle\psi|\hat{A}|\psi\rangle\langle\psi|\hat{A}|\psi\rangle + \langle\psi|\hat{A}|\psi\rangle^2 = \Delta\hat{A}^2_{|\psi\rangle}$

2. $\left[\hat{A}_0, \hat{B}_0\right] = \left[\hat{A}, \hat{B}\right]$
3. $\hat{A}_0^\dagger = \hat{A}_0$

et nous considérons

$$\begin{aligned} & f(\lambda) = \left\| \left(\hat{A}_0 - i\lambda \hat{B}_0\right) |\varphi\rangle \right\|^2 \geq 0 \quad (\forall \lambda) \\ \text{Mais} \quad & f(\lambda) = \langle\psi| \left(\hat{A}_0 + i\lambda \hat{B}_0\right) \left(\hat{A}_0 - i\lambda \hat{B}_0\right) |\psi\rangle \\ \text{soit} \quad & f(\lambda) = \langle\psi|\hat{A}_0^2|\psi\rangle + \lambda^2 \langle\psi|\hat{B}_0^2|\psi\rangle - i\lambda\langle\psi|\hat{A}_0\hat{B}_0|\psi\rangle + i\lambda\langle\psi|\hat{B}_0\hat{A}_0|\psi\rangle \\ & \quad = \langle\psi|\hat{A}_0^2|\psi\rangle + \lambda^2 \langle\psi|\hat{B}_0^2|\psi\rangle + \lambda \underbrace{\left(-i\langle\psi| \left[\hat{A}_0, \hat{B}_0\right] |\psi\rangle\right)}_{\in \mathbb{R}} \end{aligned} \tag{4.14}$$

Pour que ce polynôme du second degré soit positif $\forall\lambda$, il faut qu'il n'ait pas de racine réelle (parabole au-dessus de l'axe $\lambda$), donc que son discriminant soit négatif :

$$\begin{aligned} & \Delta = \left(-i\langle\psi| \left[\hat{A}_0, \hat{B}_0\right] |\psi\rangle\right)^2 - 4\langle\psi|\hat{A}_0^2|\psi\rangle\langle\psi|\hat{B}_0^2|\psi\rangle \leq 0 \\ \Rightarrow \quad & \left(\langle\psi|\hat{A}^2|\psi\rangle - \langle\psi|\hat{A}|\psi\rangle^2\right) \left(\langle\psi|\hat{B}^2|\psi\rangle - \langle\psi|\hat{B}|\psi\rangle^2\right) \geq \frac{1}{4} \left|\langle\psi| \left[\hat{A}, \hat{B}\right] |\psi\rangle\right|^2 \\ \Rightarrow \quad & \Delta\hat{A}_{|\psi\rangle} \Delta\hat{B}_{|\psi\rangle} \geq \frac{1}{2} \left|\langle\psi| \left[\hat{A}, \hat{B}\right] |\psi\rangle\right| \end{aligned} \tag{4.15}$$

Il est donc impossible de mesurer simultanément et avec une précision arbitraire deux observables qui ne commutent pas. En particulier, pour $\hat{A} = \hat{x}$ et $\hat{B} = \hat{p}_x$, ce résultat coïncide avec le principe d'incertitude de Heisenberg pour la position et la quantité de mouvement.

## 4.4 Cryptographie quantique

### Rappel : Détection d'un photon après un filtre polariseur

Supposons que nous ayons un photon polarisé selon $\hat{x}$. Sur la base $\{|x\rangle, |y\rangle\}$, son état est $|x\rangle$. Un filtre polariseur orienté selon $\hat{x}$ est représenté par un opérateur hermitique :

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

C'est un projecteur dur l'état $|x\rangle$. Le résultat du passage du photon est :

Photon dans l'état $|x\rangle$

- Le photon est transmis avec 100 % de probabilité

- Le photon est dans l'état $|x\rangle$ après le filtre

Photon dans l'état $|y\rangle$

- Le photon n'est pas transmis

Plus en générale, pour un état : $|\psi\rangle = \lambda |x\rangle + \mu |y\rangle$, nous avons :

- Le photon est transmis avec $|\lambda|^2$ de probabilité
- Le photon est dans l'état $|x\rangle$ après le filtre

Le même discours est valable pour un polariseur orienté selon un axe arbitraire. Par exemple, pour un polariseur orienté selon $\hat{n} = (\cos\theta, \sin\theta)$, avec $\theta = \frac{\pi}{4}$, nous avons :

$$P_{\frac{\pi}{4}} = |\frac{\pi}{4}\rangle \langle\frac{\pi}{4}| = \frac{1}{2}(|x\rangle + |y\rangle)(\langle x| + \langle y|) = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Un photon dans l'état $|\frac{\pi}{4}\rangle$ est :

- est transmis 100 % des fois
- est dans l'état $|\frac{\pi}{4}\rangle$ après le filtre

Un photon dans l'état $|x\rangle$ est :

- est transmis avec une probabilité $|\langle x|\, \frac{\pi}{4}\rangle|^2 = \frac{1}{2}$
- est dans l'état $|\frac{\pi}{4}\rangle$ après le filtre

Si donc nous savons selon quelle base un photon a été polarisé ($X = \{|x\rangle, |y\rangle\}$ ou $Z = \{|\frac{\pi}{4}\rangle, |\frac{3\pi}{4}\rangle\}$), nous pouvons en déduire avec certitude (à moins des erreurs statistiques du canal de communication) dans quel état était le photon avant le filtre.

Par exemple, si le photon est produit dans l'état $|x\rangle$ ou dans l'état $|y\rangle$, nous utilisons un polariseur $P_x$, orienté selon $\hat{x}$ ($P_y$ serait également efficace). Si le photon est transmis, son état initial était $|x\rangle$. S'il n'est pas passé, alors son état initial était $|y\rangle$.

### Quantum Key Distribution (QKD)

La cryptographie quantique, ou plus correctement *distribution quantique de clé*, est un protocole qu'on peut prouver sûr, pour transmettre de manière secrète une séquence aléatoire de bits d'information. Cette clé pourra être utilisée ensuite pour un algorithme de cryptographie conventionnel, comme par exemple le AES.

La QKQ est sûre grâce aux principes de la mécanique quantique. En particulier, la sécurité vient de l'impossibilité de cloner un état quantique arbitraire $|\psi\rangle$, ou d'extraire de l'information de cet état sans le perturber.

Le premier protocole de QKD est appelé BB84, d'après Bennett et Brassard et l'année de sa découverte 1984. Alice génère deux séquences de bits aléatoires :

$$a = \{0, 1, 1, 0, 1, 1, 0, 0, 0, ..\}$$
$$b = \{1, 0, 0, 1, 0, 1, 0, 0, ...\}$$

La première séquence contient les bits qu'elle essaie de transmettre à Bob. Et la deuxième indique à chaque fois quelle base Alice choisit pour coder le bit correspondant de $a$. Elle va utiliser la base :

$$\{|x\rangle, |y\rangle\} \quad \text{si} \quad b_j = 0$$
$$\{|\frac{\pi}{4}\rangle, |-\frac{\pi}{4}\rangle\} \quad \text{si} \quad b_j = 1$$

Alice commence par envoyer des photons un à la fois, dans les états :

$$|\psi_{a_i b_j}\rangle = \begin{cases} |x\rangle & \text{si } a_i = 1 \text{ et } b_j = 0 \\ |y\rangle & \text{si } a_i = 0 \text{ et } b_j = 0 \\ |\frac{\pi}{4}\rangle & \text{si } a_i = 1 \text{ et } b_j = 1 \\ |-\frac{\pi}{4}\rangle & \text{si } a_i = 0 \text{ et } b_j = 1. \end{cases}$$

*Remarque :* Nous pouvons naturellement décomposer les vecteur de la base $\{|\frac{\pi}{4}\rangle, |-\frac{\pi}{4}\rangle\}$ en fonction des vecteurs de l'autre base (et inversement) :

$$\begin{aligned} |\frac{\pi}{4}\rangle &= \cos\frac{\pi}{4}|x\rangle + \sin\frac{\pi}{4}|y\rangle \\ &= \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle) \\ |-\frac{\pi}{4}\rangle &= \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle) \end{aligned}$$

Bob de son coté génère une séquence aléatoire de bits : $b' = \{1, 0, 1, 0, 0, 0, ...\}$ Le nombre de bits dans a,b et b' est $4n + \delta$, avec $n$ assez grand et $\delta$ que nous expliquerons plus tard. La séquence $b'$ indique la base que Bob choisit pour détecter le photon.
Si Bob choisit $\{|x\rangle, |y\rangle\}$, il oriente son polariseur selon $|x\rangle$. S'il voit passer le photon, il enregistre 1, autrement il enregistre 0. De même, s'il choisit $\{|\frac{\pi}{4}\rangle, |-\frac{\pi}{4}\rangle\}$, il oriente son polariseur selon $\frac{\pi}{4}$ et enregistre 1 si le photon passe et 0 sinon. De cette manière il construit une autre séquence de $(4n+\delta)$ bits $a'$. Résumons tous les cas de figures possibles :

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Alice** | $b$ | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| | $a$ | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| | $\|\psi\rangle$ | $\|y\rangle$ | $\|x\rangle$ | $\|\frac{\pi}{4}\rangle$ | $\|y\rangle$ | $\|\frac{\pi}{4}\rangle$ | $\|\frac{\pi}{4}\rangle$ | $\|-\frac{\pi}{4}\rangle$ | $\|y\rangle$ | $\|-\frac{\pi}{4}\rangle$ |
| **Bob** | $b'$ | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| | Polariseur | $x$ | $\frac{\pi}{4}$ | $x$ | $x$ | $\frac{\pi}{4}$ | $\frac{\pi}{4}$ | $x$ | $x$ | $\frac{\pi}{4}$ |
| | $a'$ | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| **Bits** | **retenus** | 0 | - | - | 0 | 1 | 1 | - | 0 | 0 |

Il est claire que Bob est certain de mesurer le même bit que Alice avait l'intention de lui transmettre seulement s'ils utilisent la même base, donc si $b'_j = b_j$. En effet, $'_{-j} \neq b_j$, Bob a 50 % de chance de mesurer 0 ou 1 indépendamment du bit que Alice voulait envoyer.
Le protocole continue donc de la manière suivante : Après que les $4n + \delta$ à bits aient été transmis, Alice et Bob rendent leurs choix de base $b$ et $b'$ publics et ils les comparent. Ils retiennent seulement les cas où ils ont choisis la même base, donc $b'_j = b_j$. Dans ces cas, ils sont surs que $a'_j = a_j$ à moins d'un espionnage de la part de Eve qui aurait pu modifier l'état du photon, ou d'erreurs dans le cana de communication.
En moyenne $b'_j = b_j$, une fois sur deux. Nous pouvons donc retenir une séquence de $2n$ bits pour lesquels $b'_j = b_j$. Le nombre $\delta$ est choisis de manière que la probabilité qu'il y ait moins que $2n$ bits $b'_j = b_j$ soit expérimentalement petite. En l'absence d'espionnage, les $2n$ bits en $a = a'$ peuvent être utilisés comme clé. Mais nous ne savons pas comment découvrir si la transmission a été espionnée.

L'efficacité de ce protocole est dans le fait que, avant la fin de la transmission, $b$ et $b'$ ne sont pas publics. Eve va aussi utiliser un filtre polariseur pour espionner. Puisqu'elle ne connaît pas $b$, elle va deviner l'orientation 50% des fois. Sans perte de généralité donc, elle va orienter son polariseur toujours selon $\hat{x}$ (on peut montrer que de différent choix mènent pas à une meilleure stratégie). Si $b_j = 0$, alors Eve fait le "bon" choix. Elle va pouvoir mesurer avec certitude $a_j$. Si elle mesure 1, alors elle laisse simplement passer le photon. Si elle mesure 0, le photon ne passe pas. Elle va alors produire un autre photon polarisé selon $|y\rangle$ et l'envoyer à Bob, pour essayer de cacher son acte. si $b_j = 1$, alors Eve fait le "mauvais" choix. Son polariseur va changer l'état du photon. Elle aura toujours 50% de probabilité de mesurer $|x\rangle$ ou $|y\rangle$ :

| | | | | |
|---|---|---|---|---|
| Alice | $\|\frac{\pi}{4}\rangle$ | $\|-\frac{\pi}{4}\rangle$ | $\|\frac{\pi}{4}\rangle$ | $\|-\frac{\pi}{4}\rangle$ |
| Eve mesure | $\|x\rangle$ | $\|x\rangle$ | $\|y\rangle$ | $\|y\rangle$ |

Eve renvoie un photon dans l'état qui correspond à sa mesure $|x\rangle$ ou $|y\rangle$. Si $b'_j = b_j$ (seuls cas intéressants), Bob aura 50 % de probabilité de mesurer 0 ou 1 indépendamment du bit initial $a_j$ transmis par Alice. Dans ce cas, une fois sur 2 $a_j \neq a'_j$ même si $b'_j = b_j$. C'est les fois où Bon et Alice peuvent détecter que Ave a espionné le photon. Combien de fois cela arrive ? Nous avons vu que si $b'_j = b_j = 0$, la stratégie de Eve est optimale. Si par contre $b'_j = b_j = 1$, alors Eve sera découverte ($a_j \neq a'_j$) une fois sur deux. Le total est donc de 25 % : Parmi les $2n$ bits pour lesquels $b'_j = b_j$, on s'attend à avoir $a_j \neq a'_j$ une fois sur quatre. Rappelons que $a$ et $a'$ sont secrètes. La manière pour comprendre si un espionnage a eu lieu est la suivante : Alice et Bob choisissent $n$ bits parmi les $2n$ de $a$ et $a'$ (les mêmes) et ils les rendent publics et les comparent.
Dans le cas idéal (pas d'erreurs dans le canal de communication), si Eve a espionné, ils s'attendent à trouver 25 % de fautes. Si c'est le cas, ils annulent tout et recommencent. Sinon, ils gardent les autres $n$ bits qui n'ont pas été rendus publics comme clé. Si $n$ est suffisamment grand, la probabilité que les $n$ bits publics soient par hasard tel que $a_j = a'_j$ toujours, est extrêmement petite.

C'était la version idéale du protocole. Questions ouvertes : Comment traiter les erreurs de communication dans le canal ? Supposons que le contrôle donne un taux de fautes de 5%. Ce n'est probablement pas de l'espionnage, mais nous avons une clé avec 5% de fautes. Eve peut aussi étudier des stratégies plus complexes. Elle peut faire des mesures collectives. Les $4n + \delta$ photons, même si espacés de 1 s chacun, forment un seul état quantique :

$$\otimes_{i,j=1}^{4n+\delta} |\psi_{a_i,b_j}\rangle$$

Eve pourrait mesurer des observables dans le grand espace des $4n + \delta$ photons d'une manière à perturber chaque photon de façon minimale. Tout cela a donné lieu à de nombreux travaux d'amélioration des protocoles et des stratégies pour Eve.
En particulier, nous pouvons montrer que le BB84 est efficace si le taux de fausse transmission du photon est <11%. Cela pose une limite sur la distance de transmission.

## 4.5 Le spin et la manipulation de qu-bits

Le spin d0une particule est un excellent exemple de comment manipuler l'état d'un qu-bit. Autour de 1925, les physiciens ont découvert que les particules élémentaires ont un moment cinétique intrinsèque. C'est comme si chacune de ces particules élémentaires était une petite sphère tournant autour

d'un axe. Pour les particules chargées, cela comporte aussi une aimantation, que nous appelons le moment magnétique. L'expérience de Stern-Gerlach a montré que le spin ne peut prendre que des valeurs discrètes.
Si nous indiquons avec $\vec{\mu}$ le vecteur aimantation d'un électron en présence d'un champs magnétique $\vec{B}$. L'énergie de la particule est :

$$E = -\vec{\mu} \cdot \vec{B}$$

L'électron a "envie" d'aller vers les endroits qui minimisent cette énergie. Si $\vec{B}$ varie dans l'espace, il y aura une force qui agit sur l'électron. L'expérience de Stern-Gerlach montre qu'un faisceau d'électrons passant par un gradient de $\vec{B}$ se divisent en deux faisceaux.
Le moment cinétique $\vec{S}$ de l'électron est un vecteur dont la direction implique l'axe de rotation. Chaque composante est une quantité observable qui peut prendre deux valeurs. Toutefois, ces trois composantes ne sont pas des observables indépendantes. En effet, l'état du spin de l'électron est décrit dans un espace de Hilbert de dimension 2 (Donc un qu-bit). Quels son les opérateurs qui correspondent aux composantes de $\vec{S}$ ? Ce sont les matrices de Pauli.

$$\vec{S} = \frac{\hbar}{2}\vec{\sigma} \quad \text{avec} \quad \vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$$

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

**Propriétés**

- Ce sont des matrices hermitiques
- $\sigma_j^2 = I$
- Chaque matrice hermitique peut s'exprimer en fonction de ces matrices et de l'identité :

$$M = \lambda_0 I + \sum_{j=x}^{z} \lambda_j \sigma_j$$

- Nous avons les relations de commutation : $[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$

Cette dernière propriété est très importante. Elle nous dit qu'auparavant par connaître en même temps les trois composantes pour une particule. La matrice $\sigma_z$ est diagonale dans la base choisie Donc c'est la base des états propres de $\sigma_z$ avec $\langle \sigma_z \rangle = \pm 1$.
Considérons maintenant l'état :

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

$$\text{avec :} \quad \alpha = e^{-i\frac{\varphi}{2}} \cos\frac{\theta}{2}$$

$$\beta = e^{i\frac{\varphi}{2}} \sin\frac{\theta}{2}$$

Nous pouvons montrer que cet état est un état propre de $\vec{\sigma} \cdot \hat{n} = \sigma_x n_x + \sigma_y n_y + \sigma_z n_z$ avec

$$\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

et avec valeur propre $+1$ :

$$\vec{\sigma} \cdot \hat{n} \, |\psi\rangle = +1 \, |\psi\rangle$$

Donc l'état $|\psi\rangle$ a un spin orienté dans la direction $\hat{n}$. La sphère définie par $\hat{n}$ est la sphère de Bloch

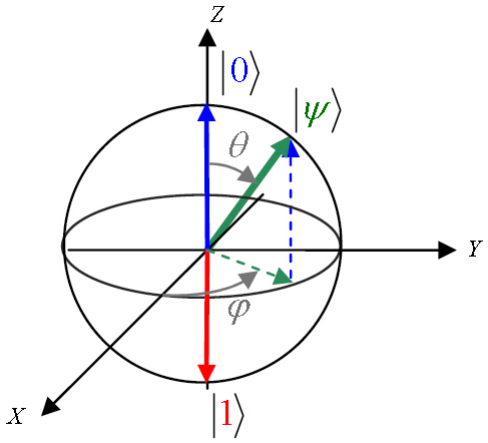



FIGURE 4.2 – Schéma de la sphère de Bloch

**Exemples**

- $\theta = \frac{\pi}{2}$ et $\varphi = 0 \rightarrow \hat{n} = (1, 0, 0)$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \rightarrow \quad \sigma_x \, |\psi\rangle = + \, |\psi\rangle$$

  $|\psi\rangle$ est donc l'état avec un spin $+\frac{\hbar}{2}$ selon $\hat{x}$.
- $\theta = -\frac{\pi}{2}$ et $\varphi = 0 \rightarrow \hat{n} = (-1, 0, 0)$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad \rightarrow \quad \sigma_x \, |\psi\rangle = - \, |\psi\rangle$$

  $|\psi\rangle$ est donc l'état avec un spin $-\frac{\hbar}{2}$ selon $\hat{x}$.

- $\theta = \frac{\pi}{2}$ et $\varphi = \frac{\pi}{2} \rightarrow \hat{n} = (0, 1, 0)$

$$|\psi\rangle = \frac{e^{-i\frac{\pi}{4}}}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \;\; \rightarrow \;\; \sigma_y\,|\psi\rangle = +\,|\psi\rangle$$

  $|\psi\rangle$ est donc l'état avec un spin $+\frac{\hbar}{2}$ selon $\hat{y}$.
- $\theta = \frac{\pi}{2}$ et $\varphi = -\frac{\pi}{2} \rightarrow \hat{n} = (0, -1, 0)$

$$|\psi\rangle = \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}}(|0\rangle - i\,|1\rangle) \;\; \rightarrow \;\; \sigma_y\,|\psi\rangle = +\,|\psi\rangle$$

  $|\psi\rangle$ est donc l'état avec un spin $+\frac{\hbar}{2}$ selon $\hat{y}$.

### Manipulation du qu-bit de spin

Nous avons vu que le moment magnétique d'une particule est proportionnel à son spin. La constante de proportionnalité est dite constante $g$.

$$\vec{\mu} = g\mu_B\vec{S} \;\; \text{où} \;\; \mu_B = \frac{\hbar e}{2mc} \;\; \text{est le magnéton de Bohr}$$

Pour un électron : $g = 2.002...$ et $m = m_e$
Pour un proton : $g = 5.59...$ et $m = m_p$
La constante $\gamma = g\mu_B$ est dite *constante gyromagnétique*. Donc l'observable $\vec{\mu} = (\mu_x, \mu_y, \mu_z)$ est définie à l'aide des matrices de Pauli :

$$\vec{\mu} = \frac{1}{2}\gamma\vec{\sigma}$$

Nous avons vu que l'énergie d'un objet avec un moment magnétique $\vec{\mu}$ en présence d'un champ magnétique $\vec{B}$ est donné par :

$$E = -\vec{\mu} \cdot \vec{B}$$

Nous sommes intéressés à déduire l'Hamiltonien du système, puisque c'est cet opérateur qui détermine l'évolution temporelle. Puisque $\hat{H}$ est l'opérateur d'énergie, il est naturel d'écrire :

$$\hat{H} = -\vec{\mu} \cdot \vec{B}$$

où nous définissons l'observable moment magnétique :

$$\vec{\mu} = \frac{1}{2}\gamma\vec{\sigma}$$

D'où :

$$\hat{H} = -\frac{1}{2}\gamma_p \vec{\sigma} \cdot \vec{B}$$

L'idée est d'utiliser un champs magnétique externe pour manipuler le spin grâce à son évolution temporelle.

Commençons par le cas d'un champ magnétique $\vec{B} = B_0\hat{z}$ constant et dirigé selon $z$. L'Hamiltonien est alors :

$$\hat{H} = -\frac{\gamma_p}{2} B_0 \sigma_z = -\frac{\gamma_p B_0}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Nous définissons $\hbar\omega_0 = \gamma_p B_0$. Nous pouvons vérifier que $\gamma_p B_0$ a les dimensions d'une énergie. Donc :

$$\hat{H} = \frac{1}{2} \begin{pmatrix} \hbar\omega_0 & 0 \\ 0 & -\hbar\omega_0 \end{pmatrix}$$

$\omega_0$ est dite *fréquence de Lamor*. L'Hamiltonien $\hat{H}$ est indépendant du temps, l'opérateur d'évolution temporelle $U$ est donc donné par :

$$U(t, t_0) = \exp\left[-i\hat{H}\frac{(t - t_0)}{\hbar}\right]$$

$\hat{H}$ est aussi diagonal. L'exponentielle d'un opérateur diagonal est immédiat :

$$U(t, t_0) = \begin{pmatrix} e^{i\frac{\omega_0}{2}(t-t_0)} & 0 \\ 0 & e^{-i\frac{\omega_0}{2}(t-t_0)} \end{pmatrix}$$

Posons $t_0 = 0$ pour simplifier la notation. Si à l'instant $t = 0$ le spin est dans l'état

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

alors à l'instant $t$, nous avons :

$$\begin{aligned} |\psi(t)\rangle &= U(t, 0)\,|\psi(0)\rangle \\ &= \begin{pmatrix} e^{i\frac{\omega_0}{2}t} & 0 \\ 0 & e^{-i\frac{\omega_0}{2}t} \end{pmatrix} \begin{pmatrix} \alpha(0) \\ \beta(0) \end{pmatrix} \\ &= e^{i\frac{\omega_0}{2}t}\alpha(0)\,|0\rangle + e^{-i\frac{\omega_0}{2}t}\beta(0)\,|1\rangle \end{aligned}$$

Nous pouvons réexprimer l'état comme :

$$\begin{aligned} |\psi(t)\rangle &= \alpha(t)\,|0\rangle + \beta(t)\,|1\rangle \\ \alpha(t) &= e^{i\frac{\omega_0}{2}t}\alpha(0) \\ \beta(t) &= e^{-i\frac{\omega_0}{2}t}\beta(0) \end{aligned}$$

En général, l'état du système change au cours du temps. Faisons quelques exemples :

- Si $|\psi(0)\rangle = |0\rangle$ alors $|\psi(t)\rangle = e^{i\frac{\omega_0}{2}t}|0\rangle$ qui correspond au même état qu'au début. De même pour $|1\rangle$. C'était évident puisque $|0\rangle$ et $|1\rangle$ sont des états propres de $\hat{H} = -\frac{\hbar\omega_0}{2}\sigma_z$ et sont donc des états stationnaires.
- Considérons maintenant un état initial $|\psi(0)\rangle$ qui correspond à un état propre du spin orienté selon $\hat{n}$ avec $\theta \neq 0$ et $\varphi = 0$ sur la sphère de Bloch.
$$|\psi(0)\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$$
A l'instant $t$ nous avons
$$\alpha(t) = e^{i\frac{\omega_0}{2}t}\cos\frac{\theta}{2}$$
$$\beta(t) = e^{-i\frac{\omega_0}{2}t}\sin\frac{\theta}{2}$$
Nous rappelons que l'état le plus général sur la sphère de Bloch est défini par :
$$|\psi\rangle = e^{-i\frac{\varphi}{2}}\cos\frac{\theta}{2}|0\rangle + e^{i\frac{\varphi}{2}}\sin\frac{\theta}{2}|1\rangle$$
Nous reconnaissons dans $|\psi(t)\rangle$ un état de la même forme que précédemment avec $\varphi = -\omega_0 t$. Nous obtenons donc qui se déplace sur un cercle sur la sphère de Bloch avec $\theta$ fixé et $\varphi$ qui varie selon $\varphi = -\omega_0 t$. Le point parcourt un cercle en un temps $T = \frac{2\pi}{\omega_0}$ avec $\omega_0$ la fréquence de Larmor. Ce mouvement est appelé *précession*. Il est typique d'un objet avec un moment cinétique placé dans un champs de force.
L'analogie classique est une toupie qui tourne soumise à la force de gravité. SI la toupie est parfaitement verticale $\theta = 0$ et elle y reste. Si $\theta \neq 0$, la toupie va tourner autour de son axe, cette rotation est connue sous le nom de précession.

Idéalement, nous pouvons utiliser cet effet pour manipuler le qu-bit. Par exemple nous pouvons appliquer $B_0$ (ou imaginer de pouvoir allumer et éteindre la source de champs magnétique) pendant un temps déterminé $\tau$. Par exemple si $\tau = \frac{\pi}{2\omega_0}$, le vecteur sur la sphère de Bloch fera un quart de tour à $\theta = cst$.
Nous remarquons que ce n'est pas encore suffisant pour produire un manipulation arbitraire. Par exemple, nous ne pouvons pas varier $\theta$. Si $\theta = 0$, nous sommes en $|0\rangle$ et nous ne pouvons pas faire l'opération élémentaire pour passer à l'état $|1\rangle$.Nous allons voir par la suite qu'il est possible de produire un changement arbitraire en utilisant un champ magnétique oscillant. Il faut toutefois remarquer que nous faisons ici une approximation. Nous avons imaginé un champs constant $B_0\hat{z}$ pour trouver l'évolution temporelle, mais ensuite nous avons imaginé d'allumer et éteindre le champ. Pour cela,

il aurait fallu utiliser la théorie avec $\hat{H}$ dépendant du temps, et le résultat aurait été différent. Il faudrait refaire les calculs pour comprendre comment réaliser par exemple. la rotation de $\varphi = \frac{\pi}{2}$. Nous allons faire cela directement avec un champ $\vec{B}$ oscillant.

Nous allons rajouter au champ magnétique $B_0\hat{z}$ constant une autre composante qui varie dans le temps.

$$\vec{B} = B_0 + B_1(\hat{x}\cos\omega t - \hat{y}\sin\omega t)$$

Maintenant la flèche du champs magnétique décrit un cercle autour de l'axe $\hat{z}$ avec zne période $T = \frac{2\pi}{\omega}$. L'hamiltonien est alors :

$$\begin{aligned}\hat{H} &= -\vec{\mu}\cdot\vec{B} = -\frac{1}{2}\gamma\vec{B}\vec{\sigma} \\ &= -\frac{1}{2}\gamma B_0\sigma_z - \frac{1}{2}\gamma B_1(\sigma_x\cos\omega t - \sigma_y\sin\omega t) \\ &= -\frac{\hbar}{2}\omega_0\sigma_z - \frac{\hbar}{2}\omega_1(\sigma_x\cos\omega t - \sigma_y\sin\omega t)\end{aligned}$$

Ici $\omega_0$ est la fréquence de Larmor que nous avons déjà défini. $\omega_1$ est dite *fréquence de Rabi* et est définie par : $\hbar\omega_1 = \gamma B_1$. Si nous explicitons sous la form des matrices de Pauli nous obtenons (à vérifier) :

$$\hat{H}(t) = -\frac{\hbar}{2}\begin{pmatrix}\omega_0 & \omega_1 e^{i\omega t} \\ \omega_1 e^{i\omega t} & -\omega_0\end{pmatrix}$$

Nous allons maintenant calculer comment un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ évolue au cours du temps dans ce champs magnétique. Ici $\hat{H} = \hat{H}(t)$ dépend du temps explicitement. Nous n'avons pas d'expression explicite pour $U(t, t_0)$ et nous devons résoudre l'équation de Schrödinger :

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

En remplaçons la forme générale de $|\psi(t)\rangle = \alpha(t)|0\rangle + \beta(t)|1\rangle$ dans l'équation de Schrödinger :

$$\begin{aligned}i\hbar\left(\frac{\partial\alpha(t)}{\partial t}|0\rangle + \frac{\partial\beta(t)}{\partial t}|1\rangle\right) = &-\frac{\hbar}{2}\left(\omega_0\alpha(t) + \omega_1 e^{i\omega t}\beta(t)\right)|0\rangle \\ &-\frac{\hbar}{2}\left(-\omega_0\beta(t) + \omega_1 e^{-i\omega t}\alpha(t)\right)|1\rangle\end{aligned}$$

L'équation obtenue peut être séparée en deux composantes (c'est-à-dire, pour que l'équation soit satisfaite pour chaque $t$, il faut que les termes proportionnel à $|0\rangle$ et à $|1\rangle$ soient satisfait séparément).

$$\begin{cases} i\frac{\partial}{\partial t}\alpha(t) = -\frac{\omega_0}{2}\alpha(t) - \frac{\omega_1}{2}e^{i\omega t}\beta(t) \\ i\frac{\partial}{\partial t}\beta(t) = -\frac{\omega_1}{2}e^{-i\omega t}\alpha(t) + \frac{\omega_0}{2}\beta(t) \end{cases}.$$

qui est un système de deux équations différentielles linéaires du 1er ordre couplées pour $\alpha(t)$ et $\beta(t)$. Redéfinissons $\alpha(t)$ et $\beta(t)$, comme suit :

$$\alpha(t) = \tilde{\alpha}(t)e^{i\frac{\omega_0}{2}t}$$
$$\beta(t) = \tilde{\beta}(t)e^{i\frac{\omega_0}{2}t}$$

L'idée de cette définition est de faire tomber un terme dans chacune des deux équations. En effet, en remplaçant dans les équations différentielles, nous obtenons pour les quantités $\tilde{\alpha}(t)$ et $\tilde{\beta}(t)$.

$$i\left(\frac{\partial}{\partial t}\tilde{\alpha}(t)\right)e^{i\frac{\omega_0 t}{2}} - \tilde{\alpha}(t)\frac{\omega_0}{2}e^{i\frac{\omega_0 t}{2}} = -\frac{\omega_0}{2}\tilde{\alpha}(t)e^{i\frac{\omega_0 t}{2}} - \frac{\omega_1}{2}e^{i\omega t}e^{-i\frac{\omega_0 t}{2}}\tilde{\beta}(t)$$
$$i\frac{\partial}{\partial t}\tilde{\alpha}(t) = -\frac{\omega_1}{2}e^{i\omega t}e^{-i\omega_0 t}\tilde{\beta}(t),$$

Nous multiplions par $e^{-i\frac{\omega_0}{2}t}$ et nous obtenons :

$$i\frac{\partial}{\partial t}\tilde{\alpha}(t) = -\frac{\omega_1}{2}e^{i(\omega-\omega_0)t}\tilde{\beta}(t)$$

Le terme en $\frac{\omega_0}{2}\alpha$ est tombé comme prévu. Si nous faisons les même opérations pour la deuxième équations, nous avons :

$$i\frac{\partial}{\partial t}\tilde{\beta}(t) = -\frac{\omega_1}{2}e^{-i(\omega-\omega_0)t}\tilde{\alpha}(t)$$

C'est un nouveau système pour $\tilde{\alpha}$ et $\tilde{\beta}$. Nous pouvons éliminer $\tilde{\beta}$, par exemple en prenant la dérivée de la 1ère équation. Nous allons considérer le cas spécial $\omega = \omega_0$. Ce cas est dis *résonnant*. En effet, nous avons choisis $\omega$ (une vraie fréquence d'oscillation du champ B) égale à la fréquence de Larmor qui est un paramètre de notre système. Alors :

$$i\frac{\partial\tilde{\alpha}}{\partial t} = -\frac{\omega_1}{2}\tilde{\beta}$$
$$i\frac{\partial\tilde{\beta}}{\partial t} = -\frac{\omega_1}{2}\tilde{\alpha}$$

Prenons la dérivée de la 1ère équation :

$$i\frac{\partial^2\tilde{\alpha}}{\partial t^2} = -\frac{\omega_1}{2}\frac{\partial\tilde{\beta}}{\partial t}$$

et remplaçons $\frac{\partial\tilde{\beta}}{\partial t}$ par la deuxième équation. Nous obtenons :

$$\frac{\partial^2\tilde{\alpha}(t)}{\partial t^2} = -\frac{\omega_1^2}{4}\tilde{\alpha}(t)$$

la solution de cette équation est :

$$\tilde{\alpha}(t) = a\cos\frac{\omega_1 t}{2} + b\sin\frac{\omega_1 t}{2}$$

et pour la première équation :

$$\tilde{\beta}(t) = ia\sin\frac{\omega_1 t}{2} - ib\cos\frac{\omega_1 t}{2}$$

Ici les constantes $a$ et $b$ sont déterminées par les conditions initiales pour $|\psi(0)\rangle$. Les définitions précédente nous donneront alors directement les expressions pour $\alpha(t)$ et $\beta(t)$.
Supposons par exemple que l'état initial soit $|0\rangle$ : $|\psi(0)\rangle = |0\rangle$ et donc $\alpha(0) = 1$ et $\beta(0) = 0$. Donc nous avons : $a = 1$ et $b = 0$. Dans ce cas :

$$\alpha(t) = \cos\frac{\omega_1 t}{2}e^{i\frac{\omega_0}{2}t}$$
$$\beta(t) = i\sin\frac{\omega_1 t}{2}e^{-i\frac{\omega_0}{2}t}$$

Si nous choisissons $B_1$ ou $t$ t.q. $\frac{\omega_1 t}{2} = \frac{\pi}{2}$, nous disons que nous avons choisis une impulsion $\pi$ ($\pi$-pulse en anglais). $\alpha(t) = 0$ et $\beta(t) = ie^{-i\frac{\omega_0}{2}t}$. L'état final est donc $|\psi(t)\rangle = |1\rangle$. Nous avons réussi à produire l'opération $|0\rangle \to |1\rangle$. Plus en général, l'état avec $a = 1$ et $b = 0$ au cours du temps est :

$$|\psi(t)\rangle = \cos\frac{\omega_1 t}{2}e^{i\frac{\omega_0}{2}t}|0\rangle + i\sin\frac{\omega_1 t}{2}e^{-i\frac{\omega_0}{2}t}|1\rangle$$

A un instant $t$ quelconque, la probabilité de l'état de donner comme mesure la valeur 0 (spin $-\frac{\hbar}{2}$ selon $\hat{z}$) est :

$$P_0(t) = |\alpha(t)|^2 = \cos^2\frac{\omega_1 t}{2}$$

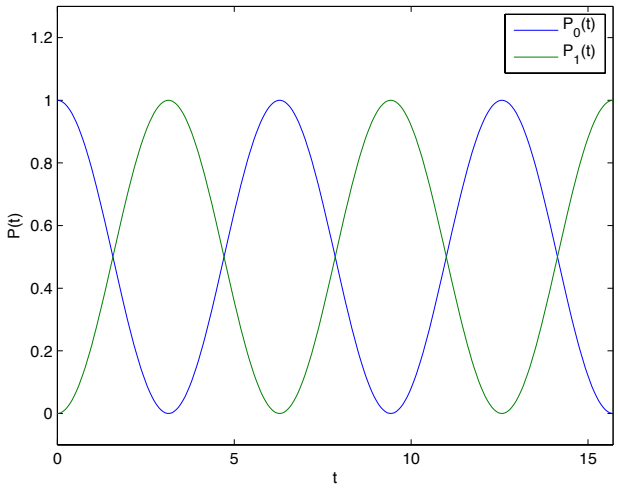



FIGURE 4.3 – Oscillations de Rabi : Les probabilités $P_0(t)$ et $P_1(t)$ en fonction du temps

et la probabilité de mesurer 1 :

$$P_1(t) = |\beta(t)|^2 = \sin^2 \frac{\omega_1 t}{2}$$

Avec un abus de langage, nous pouvons dire que le qu-bit oscille entre 0 et 1 (mais nous savons que cela n'a de sens seulement dans le contexte de la mesure en mécanique quantique). Sur la sphère de Bloch, le chemin est de la forme
puisque le point tourne en même temps selon $\theta$ avec fréquence $\omega_1$ et selon $\varphi$ avec une fréquence $\omega_0$. Quels sont les états intermédiaires ? Pour une impulsion $\frac{\pi}{2}$ ($\frac{\omega_1 t}{2} = \frac{\pi}{4}$), on a :

$$\begin{aligned} |\psi(t)\rangle &= \frac{1}{\sqrt{2}} \left( e^{i\frac{\omega_0}{2}t} |0\rangle + ie^{-i\frac{\omega_0}{2}t} |1\rangle \right) \\ &= \frac{e^{i\omega_0 t}}{\sqrt{2}} \left( |0\rangle + ie^{-i\omega_0 t} |1\rangle \right) \end{aligned}$$

Nous avons la probabilité d'être en $|0\rangle$ et $|1\rangle$. Nous pourrions imaginer choisir $B_0$ tel que $e^{i\omega_0 t} = -i$ pour $t = \frac{\pi}{2\omega_1}$. Dans ce cas :

$$|\psi(t)\rangle = \frac{i}{\sqrt{2}}(|0\rangle + |1\rangle)$$

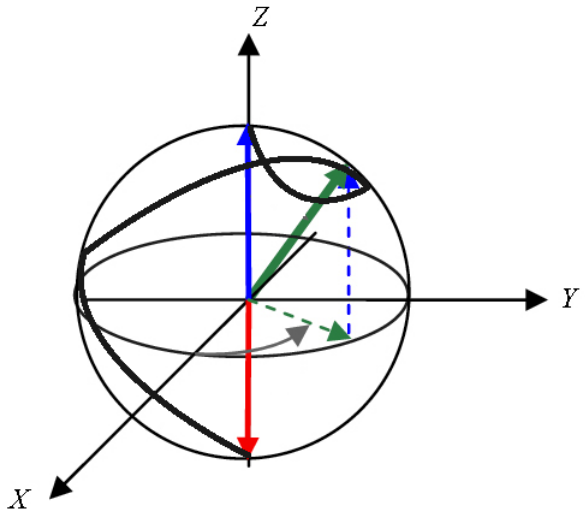



FIGURE 4.4 – Chemin parcouru par le vecteur du qu-bit sur la sphère de Bloch

Les mêmes considérations montrent que si à $t = 0$, nous avons $|\psi(0)\rangle = |1\rangle$, alors en $t = \frac{\pi}{2\omega_1}$, nous aurions :

$$|\psi(t)\rangle = \frac{i}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Nous pouvons oublier le $i$ puisqu'il ne s'agit que d'une phase globale. Nous avons donc réalisé un mécanisme qui transforme :

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

Mais c'est pas exactement la porte logique de Hadamard ! Il est donc possible de réaliser les portes logiques que nous avons illustrés de manière formelle jusqu'à aujourd'hui. Ce système du spin dans un champ magnétique à 3 paramètre libres : $B_0$, $B_1$ et $\omega$ ainsi que le temps $t$ pendant lequel nous laissons les champs allumés. En choisissant ces paramètres, il est possible de se déplacer d'un point à un autre de façon arbitraire.
La réalité est un peu plus complexe puisque les interactions avec l'environnement influencent l'évolution du spin. Il faut tenir compte du déphasage (décohérence) dans les équations. Nous verrons cela par la suite, après avoir introduit l'opérateur densité.

Ce que nous avons illustré est le principe de base de la Résonance Magnétique Nucléaire (RMN) et ce n'est pas par hasard que les spins des noyaux atomiques et le RMN aient été pensé comme la première réalisation possible du qu-bits. Plus tard, nous allons revenir sur cette technologie et parler du problème de la décohérence ainsi que des avantages et inconvénients de cette réalisation.

# 5 Etats à plusieurs qu-bits et intrication

Nous avons déjà vu comment construire l'état d'un système composé de plusieurs sous-systèmes, à l'aide du produit tensoriel. Si $H_a$ est l'état de Hilbert du sous-système $A$ et $H_b$ celui du sous-système $B$, alors l'espace vectoriel des états du système total est donné par $H = H_A \otimes H_B$. L'aspect le plus important de cette règle est que l'espace $H$ ne contient pas que les états produits tensoriels des états des deux sous-systèmes.
Considérons directement le cas de deux qu-bits. Ici, les espaces $H_A$ et $H_B$ sont de dimension 2, avec bases $\{|0_A\rangle, |1_A\rangle\}$ et $\{|0_B\rangle, |1_B\rangle\}$. Pour l'instant nous allons distinguer les deux qu-bits dans la notation, avec les indexes $A$ et $B$. Une base pour l'espace $H$ est $\{|0_A\rangle\otimes|0_B\rangle, |1_A\rangle\otimes|0_B\rangle, |0_A\rangle\otimes|1_B\rangle, |1_A\rangle\otimes|1_B\rangle\}$ ou, dans la notation simplifiée, $\{|0_A0_B\rangle, |1_A0_B\rangle\, |0_A1_B\rangle, |1_A1_B\rangle\}$. Cet espace contient tous les produits tensoriels entre un vecteur $|\phi_A\rangle$ de $H_A$ et $|\phi_B\rangle$ de $H_B$. En effet, en exprimant les états sur les bases respectives :

$$|\phi_A\rangle = \lambda_A |0_A\rangle + \mu_A |1_A\rangle$$

$$|\phi_B\rangle = \lambda_B |0_B\rangle + \mu_B |1_B\rangle$$

Ainsi l'état :

$$|\phi_A\rangle \otimes |\phi_B\rangle = \lambda_A\lambda_B |0_A0_B\rangle + \lambda_A\mu_B |0_A1_B\rangle + \mu_A\lambda_B |1_A0_B\rangle + \mu_A\mu_B |1_A1_B\rangle$$

est évidemment un état de $H$. De plus, si les deux vecteurs de départ sont normés, nous pouvons facilement montrer que l'état produit tensoriel est aussi normé. Pour l'état obtenu, nous remarquons que les quatre coefficients ne sont pas totalement arbitraires. L'état le plus arbitraire de $H$ est :

$$|\psi\rangle = \alpha_{00} |0_A0_B\rangle + \alpha_{01} |0_A1_B\rangle + \alpha_{10} |1_A0_B\rangle + \alpha_{11} |1_A1_B\rangle$$

avec $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$.
Nous remarquons tout de suite que, pour que cet état corresponde à $|\phi_A\rangle \otimes |\phi_B\rangle$, il faudrait que $\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$, ce qui n'est pas vrai a-priori. De plus, le fait de ne pas pouvoir exprimer un état comme un seul produit tensoriel, est indépendant de la base choisie pour les deux sous-systèmes. Considérons par exemple l'état :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$$

Nous avons vu dans un exercice que la forme de cet état est indépendante de la base choisie. Si

$$\begin{aligned}
|a_1\rangle &= \cos\theta\,|0_A\rangle + \sin\theta\,|1_A\rangle \\
|a_2\rangle &= -\sin\theta\,|0_A\rangle + \cos\theta\,|1_A\rangle \\
|b_1\rangle &= \cos\theta\,|0_B\rangle + \sin\theta\,|1_B\rangle \\
|b_2\rangle &= -\sin\theta\,|0_B\rangle + \cos\theta\,|1_B\rangle
\end{aligned}$$

alors $|\psi\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) = \frac{1}{\sqrt{2}}(|a_1 b_1\rangle + |a_2 b_2\rangle)$. Nous voyons que pour cet état, par rapport aux coefficients de l'état le plus général de $H$,

$$\begin{aligned}
\alpha_{00} = \alpha_{11} &= \frac{1}{\sqrt{2}} \\
\text{et} \quad \alpha_{01} = \alpha_{10} &= 0
\end{aligned}$$

Les états qui ne peuvent pas être exprimés simplement comme un seul produit tensoriel, s'appellent *états avec corrélation quantique*, ou *états intriqués*. Leur nature très spéciale deviendra claire par la suite.

Pour un système composé, nous avons aussi défini la manière de combiner les opérateurs. Si $M_A$ est un opérateur qui agit sur $H_A$ et $M_B$ un opérateur qui agit sur $H_B$, alors l'opérateur correspondant qui agit sur $H$ est $M = M_A \otimes M_B$. Si dans les bases computationnelles :

$$M_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad M_B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

Alors dans la base introduite ci-dessus, l'opérateur $M = M_A \otimes M_B$ s'écrit sous la forme :

$$M_A \otimes M_B = \begin{pmatrix} aM_B & bM_B \\ cM_B & dM_B \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix}.$$

Quelle est la caractéristique physique fondamentale d'un état intriqué ? La réponse est la suivante : Dans un état intriqué de deux qu-bits, l'état du qu-bit $A$ et celui du qu-bit $B$ ne sont jamais définis avec certitude.
Pour mieux comprendre, considérons d'abord le système d'un qu-bit. Supposons que les états $|0\rangle$ et $|1\rangle$ soient les états propres de la composante **z** du spin d'une particule. Pour un état quelconque $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, si nous effectuons une mesure du spin, nous avons probabilité $|\alpha|^2$ d'obtenir $+\frac{\hbar}{2}$ et probabilité $|\beta|^2$ d'obtenir $-\frac{\hbar}{2}$. Pour cet état, la mesure du spin

dans la direction **z** donne un résultat incertain, avec une valeur moyenne $\langle S_z\rangle = |\alpha|^2\langle 0|S_z|0\rangle + |\beta|^2\langle 1|S_z|1\rangle$. Pourtant, nous pouvons mesurer le spin dans la direction $\mathbf{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, avec $\alpha = e^{-i\phi/2}\cos(\theta/2)$ et $\beta = e^{i\phi/2}\sin(\theta/2)$. Nous avons vu que l'état $|\phi\rangle$ est un état propre du spin dans cette direction spécifique. Nous allons donc obtenir $\frac{\hbar}{2}$ avec certitude. Au contraire, pour chaque observable de spin $S_{\mathbf{n}}$, nous savons construire un état $\phi_{\mathbf{n}}$ qui soit état propre de $S_{\mathbf{n}}$, pour lequel la mesure de $S_{\mathbf{n}}$ donne $+\frac{\hbar}{2}$ avec certitude.
Considérons maintenant l'état à deux qu-bits

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_B\rangle)$$

Supposons de mesurer le spin $S_z$ sur le sous-système $A$. La probabilité d'obtenir $+\hbar/2$ est donnée par

$$p(+) = |\langle 0_A 0_B\rangle\,\psi|^2 + |\langle 0_A 1_B\rangle\,\psi|^2 = \frac{1}{2}$$

De manière plus générale, considérons un observable $M$ sur le qu-bit $A$. La moyenne de la mesure de $M$ est donnée par l'élément de matrice sur $|\psi\rangle$ de l'opérateur $M \otimes I_B$. Nous obtenons :

$$\begin{aligned}\langle\psi|M\otimes I_B|\psi\rangle &= \frac{1}{2}[\langle 0_A 1_B| + \langle 1_A 0_B|]M\otimes I_B[|0_A 1_B\rangle + |1_A 0_B\rangle] \\ &= \frac{1}{2}(\langle 0_A|M|0_A\rangle + \langle 1_A|M|1_A\rangle)\end{aligned}$$

A première vue, ce résultat parait normal, mais en réalité il est très spécial. Tout d'abord nous remarquons qu'il est vrai pour n'importe quel opérateur hermitique $M$ sur $H_A$. Il nous dit donc que la valeur moyenne d'une observable quelconque $M$ est la moyenne des valeurs moyennes qu'aurait la même observable sur les états $|0_A\rangle$ et $|1_A\rangle$. Ce résultat suggère donc que l'état $|\psi\rangle$ se comporte comme un mélange statistique des deux états $|0_A\rangle$ et $|0_B\rangle$. Nous nous posons donc la question : est-il possible de trouver un état du système $A$, $|\phi_A\rangle = \lambda\,|0_A\rangle + mu\,|1_A\rangle$, tel que pour chaque observable $M$ de $A$ on a

$$\langle\psi|M\otimes I_B|\psi\rangle = \langle\phi_A|M|\phi_A\rangle \ ?$$

Calculons la moyenne $\langle\phi_A|M|\phi_A\rangle$ :

$$\langle\phi_A|M|\phi_A\rangle = |\lambda|^2\langle 0_A|M|0_A\rangle + \lambda^*\mu\langle 0_A|M|1_A\rangle + \lambda\mu^*\langle 1_A|M|0_A\rangle + |\mu|^2\langle 1_A|M|1_A\rangle$$

Pour reproduire le résultat précédant, il faut que $|\lambda|^2 = 1/2$, $|\mu|^2 = 1/2$, et que $\lambda^*\mu = 0$, pour un $M$ quelconque. Ces trois conditions sont impossibles à

réaliser, comme nous pouvons facilement démontrer.
La conclusion est qu'un état intriqué décrit un mélange statistique des états de chacun de ses sous-systèmes – une situation qui ne peut pas être décrite par aucun état pur du sous-système en question. Ce fait est très important, par exemple, dans la description des systèmes ouverts. Un système est toujours en interaction avec son environnement. Si on considère système et environnement comme deux sous-systèmes du système total (l'univers), alors on doit admettre qu'en général ce système peut se trouver dans un état intriqué pour les deux sous-systèmes. Dans ce cas, le système que nous sommes en train de considérer n'est pas dans un état bien défini (on parle d'*état pur*) mais plutût dans un *mélange statistique* d'états, à cause de l'intrication avec l'environnement. Nous allons reprendre cet argument par la suite, dans le contexte de l'opérateur statistique.
Une autre propriété remarquable des états intriqués est la corrélation quantique. Nous avons déjà vu dans un exercice que si Alice et Bob ont chacun un qu-bit de la paire intriquée, alors leurs mesures donneront des résultats totalement corrélés. Ce mécanisme, connu sous le nom de *paradoxe de Einstein-Podolsky-Rosen* (ou EPR), est à la base de plusieurs applications de l'information quantique, comme par exemple la téléportation quantique ou le superdense coding que nous allons illustrer ici.

Si nous utilisons deux qu-bits dans des états intriqués, il est utile d'introduire une base de l'espace de Hilbert, dont les états sont caractérisés par l'intrication maximale. Ce sont les états de Bell

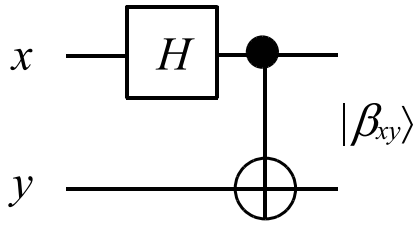
$$\begin{aligned} |\beta_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ |\beta_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ |\beta_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |\beta_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned}$$

La notation est choisie selon la règle qui suit

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \bar{y}\rangle}{\sqrt{2}}$$

où $\bar{y}$ indique la négation du bit $y$. Nous vérifions facilement que ces quatre états sont normés et réciproquement orthogonaux, donc ils forment une base. Nous pouvons même concevoir un circuit quantique pour les produire à partir

d'états de la base computationnelle $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ (figure ci-dessous). Nous vérifions facilement que, si nous applique l'état $|xy\rangle$ en entrée, nous obtienons l'état $|\beta_{xy}\rangle$ à la sortie.




Ce circuit suggère qu'il est possible de produire des états intriqués dans la pratique. En effet, nous avons déjà vu comment appliquer l'opérateur de Hadamard à l'aide des oscillations de Bloch pour un qu-bit représenté par l'état di spin d'une particule. Nous verrons qu'il est possible également de réaliser sur le même système une opération de type $CNOT$.

## Exemple : Superdense Coding

Comme premier exemple des possibilités offertes par les corrélations quantiques, nous allons illustrer une application appelée *superdense coding*. Il s'agit d'une méthode pour transmettre de l'information classique sur un canal de communication quantique. Grâce aux corrélations quantiques, cette méthode est plus efficace que les méthodes classiques, puisqu'elle permet de transmettre deux bits d'information classique en envoyant un seul qu-bit.
Supposons qu'Alice doit transmettre deux bits d'information classique à Bob. Un canal de communication est établi en générant deux qu-bits dans un état intriqué

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Alice est en possession d'un des deux qu-bits et Bob de l'autre (les deux qu-bits dans ce cas pourraient être les états de polarisation de deux photons qui sont envoyés vers Alice et Bob respectivement). Ce partage de qu-bits est fait préalablement par une troisième partie. Alice est censée effectuer une opération sur le qu-bit en sa possession et l'envoyer après à Bob. Voici le protocole :
Si les bits classiques à transmettre sont indiqués par $i$ et $j$ (prenant les valeurs 0 ou 1), alors Alice applique à son qu-bit l'opérateur :

$$A = \sigma_x^i \sigma_z^j$$

où $\sigma_x$ et $\sigma_z$ sont les matrices de Pauli. Examinons les quatre résultats :

$$i = 0,\ j = 0 : |\psi\rangle \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$i = 0,\ j = 1 : |\psi\rangle \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$i = 1,\ j = 0 : |\psi\rangle \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$i = 1,\ j = 1 : |\psi\rangle \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Ce sont exactement les quatre états de Bell. Ces états forment une base orthonormée. Ils peuvent donc être distingués par la mesure d'une observable appropriée. Il suffit que Bob ait à disposition une observable qui a comme états propres les quatre états de Bell, avec quatre valeurs propres différentes. Il lui suffira d'effectuer la mesure pour comprendre quel est l'état de la paire de qu-bits et donc quelle était la paire de bits classiques qu'Alice a envoyée. Même si deux qu-bits sont impliqués dans le protocole, Alice ne doit jamais effectuer des opérations sur le deuxième et doit envoyer seulement son qu-bit vers Bob. Un canal d'information classique n'aurait jamais permis ce résultat. Comme la plupart des réalisations simples de l'information quantique, le superdense coding a été réalisé en laboratoire. En plus, il pourrait jouer un rôle essentiel comme protocole de communication entre éléments de calcul quantique séparés. En résumant, le superdense coding est un exemple des possibilités incroyables offertes par la mécanique quantique.

## 5.1 Indiscernabilité d'états quantiques

Un aspect très important de la mécanique quantique est l'impossibilité de connaître de manière exacte l'état quantique d'un système. Ce fait singulier est à la base de plusieurs applications telles que la cryptographie quantique et la téléportation quantique. Il joue aussi un rôle très important dans la manière dont les algorithmes quantiques sont construits. Dans ce paragraphe et le suivant, nous allons formaliser cette propriété en démontrant deux faits : l'impossibilité de discerner entre deux états quantiques et l'impossibilité de cloner un état quantique. Il est clair que ces deux propriétés sont liées : s'il était possible de connaître l'état quantique d'un système, alors on pourrait préparer un deuxième système dans le même état. Au contraire, s'il était possible de cloner un système quantique N fois, on pourrait le faire et puis effectuer plusieurs mesures – une sur chaque clone – jusqu'à avoir la certitude de l'état quantique du système sous examen.

Nous allons commencer par la preuve qu'on ne peut pas distinguer entre deux états quantiques. Supposons que $|\psi_1\rangle$ et $|\psi_2\rangle$ soient les états quantiques en question. Tout d'abord nous allons montrer que, si les états sont orthogonaux, alors il est possible de les distinguer. Supposons que les états soient orthogonaux : $\langle\psi_1|\psi_2\rangle = 0$. Nous pouvons construire une base orthonormée qui contient les deux états $|\psi_1\rangle$ et $|\psi_2\rangle$. Ensuite nous pouvons construire un opérateur hermitique $A$ diagonal dans cette base, avec les valeurs propres $a_1$ et $a_2$ ($a_1 \neq a_2$), correspondant à $|\psi_1\rangle$ et $|\psi_2\rangle$. A l'aide de la mesure de l'observable $A$ il est donc possible de discerner les états : si le résultat de la mesure est $a_1$ alors l'état est $|\psi_1\rangle$ ; si le résultat de la mesure est $a_2$ alors l'état est $|\psi_2\rangle$. Si par contre le résultat est différent de $a_1$ et $a_2$, alors l'état n'est ni $|\psi_1\rangle$ ni $|\psi_2\rangle$.

Cette preuve est exclusivement valable pour des états orthogonaux. Supposons maintenant que $|\psi_1\rangle$ et $|\psi_2\rangle$ soient non-orthogonaux. L'idée est toujours la même : construire un opérateur hermitique $A$ avec valeurs propres $\{a_1, \ldots, a_N\}$ et vecteurs propres $\{|a_1\rangle, \ldots, |a_N\rangle\}$, tel que la mesure de l'observable correspondant donne comme résultat un certain sous-ensemble des valeurs propres $\{a_1, \ldots, a_m\}$ si l'état est $|\psi_1\rangle$, et le sous-ensemble complémentaire $\{a_{m+1}, \ldots, a_N\}$ si l'état est $|\psi_2\rangle$. Cela implique que :

$$\sum_{j=1}^{m} |\langle a_j\rangle \psi_1|^2 = 1$$

Puisque la probabilité totale de mesurer un des $\{a_1, \ldots, a_m\}$ sur $|\psi_1\rangle$ est 1 :

$$\langle a_j|\psi_1\rangle = 0, \qquad j = m+1, \ldots, N$$

De même :

$$\sum_{j=m+1}^{N} |\langle a_j\rangle \psi_2|^2 = 1 \qquad \text{et}$$

$$\langle a_j|\psi_2\rangle = 0, \qquad j = 1, \ldots, m$$

Or, par l'hypothèse de non-orthogonalité, nous pouvons écrire $|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\phi\rangle$, avec $|\alpha|^2 + |\beta|^2 = 1$, $\alpha, \beta \neq 0$, et $\langle\phi|\psi_1\rangle = 0$. Cela nous permet de réécrire la relation précédente :

$$\sum_{j=m+1}^{N} |\langle a_j\rangle \psi_2|^2 = |\beta|^2 \sum_{j=m+1}^{N} |\langle a_j\rangle \phi|^2 \leq |\beta|^2 < 1$$

étant donné que $|\phi\rangle$ est un vecteur normé et la somme dans le deuxième terme indique aussi une probabilité de mesure, qui doit être plus petite que 1. Nous avons atteint une contradiction, ce qui implique la preuve de notre proposition.

## 5.2 Impossibilité de cloner un état quantique

Supposons que nous ayons un système quantique dans un état arbitraire $|\psi_1\rangle$ et que nous voudrions le cloner. Cela veut dire que nous souhaitons prendre un deuxième système identique au premier, et le mettre dans le même état que le premier. Donc, si l'état du deuxième système avant l'opération de clonage est $|\phi\rangle$, alors l'état total des deux systèmes est $|\psi_1\rangle \otimes |\phi\rangle$. Nous cherchons à transformer cet état en l'état $|\psi_1\rangle \otimes |\psi_1\rangle$, où les deux sous-systèmes sont dans le même état. Il faut supposer que l'opération de clonage est représentée par un opérateur unitaire agissant sur l'espace de Hilbert des deux systèmes :

$$U(|\psi_1\rangle \otimes |\phi\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle \ .$$

Cette opération doit fonctionner pour n'importe quel état de départ. En d'autre mot, l'opérateur $U$ est le même pour cloner n'importe quel état (autrement il faudrait choisir l'opérateur selon l'état, ce qui est impossible puisque nous ne pouvons connaître l'état d'un système de manière précise). Donc cloner un deuxième état $|\psi_2\rangle$ implique :

$$U(|\psi_2\rangle \otimes |\phi\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle \ .$$

Calculons maintenant le produit scalaire :

$$(\langle\psi_1| \otimes \langle\phi|)U^\dagger U(|\psi_2\rangle \otimes |\phi\rangle)$$

Cet objet n'est rien d'autre que la norme au carré du vecteur $U(|\psi_2\rangle \otimes |\phi\rangle)$. Puisque $U$ est unitaire, $U^\dagger U = I$ c'est l'identité, et le produit scalaire est égal à :

$$(\langle\psi_1| \otimes \langle\phi|)(|\psi_2\rangle \otimes |\phi\rangle) = \langle\psi_1|\psi_2\rangle\langle\phi|\phi\rangle = \langle\psi_1|\psi_2\rangle \, .$$

Si par contre nous utilisons le résultat après le clonage de l'état, alors le même produit scalaire devient :

$$(\langle\psi_1| \otimes \langle\psi_1|)(|\psi_2\rangle \otimes |\psi_2\rangle) = (\langle\psi_1|\psi_2\rangle)^2 \, .$$

Pour que l'opérateur $U$ soit bien défini, il faut donc avoir :

$$(\langle\psi_1|\psi_2\rangle)^2 = \langle\psi_1|\psi_2\rangle \, .$$

Pour satisfaire cette équation, il n'y a que deux possibilités :

- $|\psi_1\rangle = |\psi_2\rangle$ ou
- $\langle\psi_1|\psi_2\rangle = 0$.

Nous voyons donc qu'il serait possible de cloner un ensemble d'états qui sont mutuellement orthogonaux, mais pas un ensemble d'états arbitraire. C'est pourquoi pour le protocole BB84 de cryptographie quantique nous avons introduit deux bases de polarisations qui ne sont pas réciproquement orthogonales. Si nous nous étions limités à la base $\{|x\rangle, |y\rangle\}$, alors Eve aurait pu cloner l'état de chaque photon plusieurs fois et puis, en faisant plusieurs mesures, déduire l'état de polarisation du photon.

## 5.3 Téléportation quantique

L'idée générale à la base des applications que nous avons vues jusqu'à maintenant, est que la mécanique quantique permet d'exploiter au mieux les ressources que la nature nous met à disposition, pour le traitement de l'information. Par exemple, nous avons vu comment un canal quantique de communication (deux qu-bits dans un état intriqué) nous permettent d'optimiser la transmission d'information classique avec le superdense coding. Un autre exemple très important de cette idée est la téléportation quantique. Avec ce protocole, il est possible pour Alice de transmettre à Bob un qu-bit dans un état arbitraire. Pensez au fait que cette opération est à priori difficile étant donnés la non discernabilité des états et le no-cloning theorem : nous ne pouvons pas connaitre l'état du qu-bit pour le transmettre à Bob sur un canal classique, et nous ne pouvons pas non plus cloner l'état pour l'envoyer à Bob.
Comme la plupart de ces application, la téléportation quantique se base sur l'existence d'un canal quantique entre Alice et Bob, constitué par une paire de qu-bits dans un état intriqué (une paire EPR). Supposons donc que deux qu-bits (deux photons par exemple) soient préparés dans l'état :

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

et que le premier des deux qu-bits soit envoyé à Alice, et le deuxième à Bob. Alice en plus est en possession d'un qu-bit dans un état arbitraire (qu'elle ne connaît pas en principe) :

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

avec $|\alpha|^2 + |\beta|^2 = 1$. Donc l'état total du qu-bit à transmettre et des deux qu-bits du canal quantique est :

$$|\psi_0\rangle = |\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle \otimes (|00\rangle + |11\rangle) + \beta\,|1\rangle \otimes (|00\rangle + |11\rangle)\right]$$

Ici, les deux qu-bits plus à gauche sont ceux de Alice et le qu-bit plus à droite est celui de Bob. Maintenant Alice applique à ses deux qu-bits une opération CNOT- Le résultat est :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle \otimes (|00\rangle + |11\rangle) + \beta\,|1\rangle \otimes (|10\rangle + |01\rangle)\right]$$

Ensuite, Alice applique à son premier qu-bit une opération de Hadamard. Maintenant, l'état est :

$$\begin{aligned}|\psi_2\rangle =& \frac{1}{2}[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) \\ &+ |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)]\end{aligned}$$

Nous voyons que les quatre termes de cette expression ont une interprétation très simple. Dans le premier terme, les deux qu-bits de Alice sont dans l'état $|00\rangle$ et le qu-bit de Bob est dans l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Donc si Alice fait une mesure de l'état de ses deux qu-bits (nous pouvons imaginer une observable capable de distinguer parmi les quatre états de la base computationnelle, puisque ils sont orthogonaux) et obtient que le système est projeté sur l'état $|00\rangle$. Dans ce cas, elle aura atteind son but puisque Bob aura son qu-bit dans l'état $|\psi\rangle$, le qu-bit qu'il fallait transmettre. En général, selon les résultats de la mesure d'Alice, voici les quatre états que prendra le qu-bit de Bob :

$$\begin{aligned}00 &\rightarrow \alpha\,|0\rangle + \beta\,|1\rangle \\ 01 &\rightarrow \alpha\,|1\rangle + \beta\,|0\rangle \\ 10 &\rightarrow \alpha\,|0\rangle - \beta\,|1\rangle \\ 11 &\rightarrow \alpha\,|1\rangle - \beta\,|0\rangle\end{aligned}$$

Le point clé du protocole est que Alice doit maintenant communiquer à Bob, sur un canal de communication classique, quel est le résultat de sa mesure. Une fois appris le résultat de la mesure d'Alice, Bob peut modifier son propre qu-bit de manière à obtenir toujours l'état $|\psi\rangle$ à la fin. Si la mesure de Alice a donné le résultat 01, alors Bob peut appliquer sur son qu-bit l'opérateur $\sigma_x$. Si le résultat est 10, Bob va appliquer $\sigma_z$. Si le résultat est 11, Bob applique avant $\sigma_x$ et après $\sigma_z$. En général, Bob doit appliquer à son qu-bit l'opérateur $\sigma_z^y \sigma_x^x$, où $xy$ est le résultat de la mesure d'Alice. De cette manière il obtiendra avec probabilité 1 le qu-bit $|\psi\rangle$ à la fin de l'opération.

Nous pouvons faire plusieurs remarques :

1. Tout d'abord, il est impossible par ce protocole de transmettre de l'information plus vite que la lumière. Nous avons vu que le protocole est

basé sur la transmission du résultat d'Alice vers Bob. Cette transmission se fait sur un canal classique et donc à une vitesse maximale plus petite que la vitesse de la lumière. Sans transmettre le résultat d'Alice, nous pouvons montrer qu'il est impossible pour Alice d'utiliser cette méthode pour transmettre de l'information à Bob. Donc ce résultat ne contredit pas le principe de la relativité restreinte qui dit que nul ne voyage plus vite que la lumière.

2. La deuxième remarque concerne la clonation d'état. Nous voyons que ce protocole n'effectue pas de clonage de l'état $|\psi\rangle$. L'état est simplement transféré au qu-bit de Bob. Le qu-bit initiallement dans l'état $|\psi\rangle$ se trouve après la téléportation dans l'état $|0\rangle$ ou $|1\rangle$ selon le résultat de la mesure d'Alice. Ce résultat ne donne aucune information sur quel était l'état (les valeurs de $\alpha$ et $\beta$) et donc il serait impossible pour Alice de le préparer à nouveau.

La téléportation quantique a été réalisée dans plusieurs laboratoires, principalement avec des photons. Son utilité n'est certainement pas celle de réaliser une téléportation de matière à la Star Trek. Ici, aucune matière n'est transférée : qui serait prêt à accepter de faire transférer l'état quantique de chacun de ses atomes vers un tas de matière non spécifiée (par exemple de l'eau) disposée préalablement à l'endroit de destination ? Par contre le protocole de la téléportation est très utile pour agir contre la décohérence et pour concevoir des méthodes efficaces de correction d'erreurs quantique.

## 5.4 Inégalité de Bell

Nous allons continuer notre discussion sur la nature non classique des états intriqués. Notre intuition des propriétés de la nature nous suggère que les résultats des mesures nous donnent simplement connaissance des propriétés d'un système. Par exemple, la position d'un objet est une propriété de l'objet, et la mesure de la position sert tout simplement à nous informer de cette propriété. Cette remarque apparemment simple, prend une importance fondamentale en information quantique, où nous utilisons les propriétés des systèmes physiques pour représenter l'information. La présence ou absence d'un électron dans un élément électronique d'un circuit, indique qu'un bit de mémoire est dans l'état zéro ou un.
La mécanique quantique telle que nous l'avons vue jusqu'à maintenant, nous dit quelques choses de différent. Elle nous dit qu'un système n'est pas caractérisé de propriétés qui existent indépendamment du processus de mesure. Au contraire, ces propriétés sont déterminées en quelques sortes par le processus même de la mesure. Par exemple, la direction d'un spin n'a pas une

composante déterminée le long de l'axe **x** ET une composante déterminée le long de l'axe **z**, de manière à que les deux quantités puissent être mesurées indépendamment. Selon la mécanique quantique, tout ce que nous pouvons établir sont des probabilités pour les résultats des différentes mesures.

Au début de l'ère quantique, beaucoup de chercheurs n'étaient pas convaincu par ce point de vue. L'idée était que dans le contexte de la *réalité*, les propriétés physiques doivent appartenir aux systèmes indépendamment de l'acte de la mesure. Une théorie comme la mécanique quantique, qui ne permet pas de prévoir ces *éléments de réalité*, devait nécessairement être une théorie incomplète. Parmi les plus illustres supporteurs de ce point de vue étaient Albert Einstein, Boris Podolsky et Nathan Rosen, qui ont discuté le problème dans un célèbre article. Ils ont pris comme exemple un état quantique qu'on aurait appelé 50 ans après un état de Bell (en réalité ils ont proposé une expérience de pensée avec utilisant particules, qui peut être reconduite à cet état quantique) :

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Les deux particules décrites par cet état sont données à Alice et Bob respectivement. Alice et Bob se trouvent à grande distance l'un de l'autre. Nous savons maintenant que pour Alice les probabilités de mesurer 0 ou 1 sont données par 1/2, et de même pour Bob. Toutefois, la mécanique quantique prévoit une corrélation parfaite entre les résultats des mesurer d'Alice et de Bob. Imaginons de répéter l'expérience avec plusieurs paires de particules préparées dans le même état : si Alice mesure la séquence $\{1, 0, 0, 1, 1, 0, 0, 0\}$, alors elle est sure que Bob mesurera la séquence $\{0, 1, 1, 0, 0, 1, 1, 1\}$. En plus, nous avons vu que si nous effectuons un changement de base (par exemple nous décidons de mesurer la polarisation du photon selon une système d'axes différent), la forme de l'état ne change pas et nous aurons encore une corrélation totale entre les mesures d'Alice et de Bob. La critique de EPR (Einstein-Podolsky-Rosen) est la suivante : Si Alice est parfaitement capable de prévoir le résultat de la mesure de Bob (après avoir effectué sa propre mesure), cela veut dire que le résultat de la mesure de Bob est un élément de réalité – une propriété intrinsèque au système que Bob détecte par l'acte de sa mesure. Donc la théorie devrait être en mesure de prévoir avec certitude cette caractéristique. Par contre, la mécanique quantique ne peut pas prévoir ce résultat mais seulement établir des probabilités.

Est-il possible de reproduire le comportement d'un état de Bell avec des concepts de physique classique (donc en faisant intervenir des éléments de

réalité) ? La réponse est apparemment oui. Considérons par exemple deux billes, une noire et une blanche. Nous attribuons à la mesure de la couleur des billes les valeurs $-1$ pour la bille noire et $+1$ pour la bille blanche. Nous prenons les deux billes aux hasard et nous les envoyons la première à Alice et la deuxième à Bob, les deux enfermées dans des boîtes. Alice effectue sa mesure en ouvrant la boîte. Elle trouve une bille blanche, donc elle mesure $+1$. Elle est donc certaine (par la manière dont l'expérience a été conçue) du résultat de la mesure de Bob, qui trouvera la bille noire. Il semblerait donc que nous arrivons à reproduire le scénario du paradoxe EPR avec un système classique – et donc caractérisé par des éléments de réalité.
En réalité, l'état de Bell nous donne le même comportement, même si Alice et Bob devait choisir de changer de base et de mesurer les deux états du qu-bit dans la nouvelle base. Nous pouvons généraliser notre expérience classique de manière à reproduire cette situation. Supposons que nous ayons deux au lieu des deux billes. Sur chaque bâtonnet, nous pouvons tracer des bandes de couleurs différents. Nous associons les couleurs en paires, correspondants aux valeurs $+1$ et $-1$. Par exemple, blanc $= +1$ et noir $= -1$, vert $= +1$ et bleu $= -1$. Admettons que le premier bâtonnet ait une bande blanche en première position et une bleue en deuxième position. Le deuxième bâtonnet a une bande noire en première position et une bande verte en deuxième position. Comme avant, nous choisissons les deux bâtonnets au hasard pour les envoyer à Alice et Bob. Supposons d'abord qu'Alice et Bob décident les deux de mesurer la première bande. Alors Alice effectue sa mesure (elle observe la couleur de la première Bande de son bâtonnet) et trouve $+1$ (blanc). Elle est à ce moment sure que Bob mesurera $-1$ (noir). Supposons que Alice et Bob se mettent par contre d'accord pour mesurer la deuxième bande. Dans ce cas aussi, les résultats des mesures d'Alice et Bob seront totalement corrélés. Si par contre Alice et Bob ne se mettent pas d'accord sur quelle bande mesurer, alors leurs mesures seront en principe décorrélées. Si par exemple Alice décide de mesurer la première bande (et donc de ne pas regarder la couleur de l'autre) et Bob la deuxième, alors Alice n'est pas à mesure de connaître le résultat de la mesure de Bob.
Nous comprenons mieux la décorrélation entre les deux résultats si nous imaginons de répéter l'expérience plusieurs fois avec à chaque fois deux bâtonnets coloriés de manière différente (mais en suivant la même règle). Chaque bâtonnet sera donc caractérisé par deux bits $\{x, y\}$ (les deux bandes) qui peuvent prendre les valeurs $\pm 1$. La règle est qu'à chaque répétition de l'expérience, une troisième personne (Charlie) prépare les deux bâtonnets en choisissant les couleurs des deux bandes de manière aléatoire mais totalement corrélée. Si par exemple un bâtonnet est noir et bleu, le deuxième sera blanc et vert. Si à chaque répétition de l'expérience Alice et Bob décident de mesurer la

même bande, alors leur résultats seront totalement corrélés. Si par contre ils décident de mesurer deux bandes différentes, alors les deux séquences de valeurs seront totalement indépendantes. Remarquons que Alice et Bob peuvent se trouver à des années lumière de distance l'un de l'autre. Il n'y a donc aucune manière que la mesure d'Alice puisse influencer le résultat de Bob.

Il est surprenant à quel point cette situation ressemble à celle des protocoles de cryptographie quantique ! Et pourtant il est clair qu'Eve pourrait intercepter l'un des bâtonnets, prendre note des couleurs et le renvoyer, en réussissant ainsi à espionner la communication sans être aperçue. Mais ce n'est pas cette remarque qui nous aide à comprendre quelle est la vraie différence profonde entre un phénomène classique et un phénomène avec corrélations quantique. C'est pourquoi la discussion de ce problème a intéressé la communauté scientifique pendant plusieurs décennies. La question fondamentale est la suivante : La théorie de la mesure, que nous connaissons en mécanique quantique, est-elle une simple conséquence de la mauvaise connaissance du comportement de la nature ? Il se pourrait que la mécanique quantique soit une théorie incomplète. En d'autres mots, l'aspect probabiliste du processus de mesure pourrait être dû à un manque de connaissance de la part de l'expérimentateur. Il pourrait y avoir des *variables cachées*, que la théorie de prend pas en compte et qui sont difficilement accessibles pour les expérimentateurs. La connaissance de ces variables nous permettrait de retrouver un comportement *réaliste* de la Nature, selon lequel les valeurs qui résultent des mesures sont des propriétés intrinsèques du système, indépendamment du processus de mesure.

Ce genre de considérations se sont poursuivies jusqu'en 1965, quand John Bell a suggéré une méthode rigoureuse pour tester le caractère complet de la mécanique quantique. Voici un résumé simple des résultats de Bell : Reprenons notre expérience avec les bâtonnets. Alice peut choisir de mesurer une parmi deux quantités (la première bande de couleur ou la deuxième). Appelons les deux quantités $A_1$ et $A_2$. Chacune de ces résultats peut prendre les valeurs $\pm 1$. En même temps, Bob peut choisir si mesurer une parmi les quantités $B_1$ et $B_2$, qui peuvent aussi prendre les valeurs $\pm 1$. Nous soulignons ici encore une fois que Alice et Bob effectuent leur mesures de façon indépendante, sans qu'il soit possible pour la mesure d'Alice d'influencer physiquement la mesure de Bob. Considérons la quantité :

$$A_1 B_1 + A_2 B_1 + A_2 B_2 - A_1 B_2$$

Remarquons d'abord que cette quantité peut être écrite comme :

$$(A_1 + A_2)B_1 + (A_2 - A_1)B_2$$

Puisque $A_1 = \pm 1$ et $A_2 = \pm 1$, il s'ensuit que :
soit $(A_1 + A_2)B_1 = 0$,
soit $(A_2 - A_1)B_2 = 0$.
Dans le premier cas nous avons $A_1 = -A_2$, donc $A_2 - A_1 = \pm 2$ et aussi $(A_2 - A_1)B_2 = \pm 2$. Dans le deuxième cas, $A_1 = A_2$ et donc $(A_1 + A_2)B_1 = \pm 2$. Nous venons de montrer que :

$$A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2 = \pm 2$$

Si nous supposons que la Nature est caractérisée par des éléments de réalité, alors il faut imaginer qu'à chaque réalisation de l'expérience, les valeurs de $A_1$, $A_2$, $B_1$ et $B_2$ sont toutes déterminées, et cela à priori du processus de mesure. Elles caractérisent l'état du système sur lequel les mesures sont effectuées (les deux bâtonnets dans l'exemple précédant). Dans ce cas, nous pouvons définir une distribution de probabilité $p(A_1, A_2, B_1, B_2)$ que chaque combinaison possible de quatre valeurs se réalise. Cette distribution de probabilité est essentiellement déterminée par Charlie qui prépare chaque instance de l'expérience. Utilisons cette distribution de probabilité pour calculer des valeurs moyennes au sens statistique. Indiquons avec $E(X)$ la moyenne de la quantité $X$. Nous pouvons calculer la moyenne de la quantité considérée précédemment :

$$\begin{aligned}
&E(A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2) \\
&\quad = \sum_{A_1,A_2,B_1,B_2} p(A_1, A_2, B_1, B_2)(A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2) \\
&\quad \leq \sum_{A_1,A_2,B_1,B_2} p(A_1, A_2, B_1, B_2) \times 2 \\
&\quad = 2
\end{aligned}$$

Ici nous avons utilisé le fait que la quantité $A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2$ est égale à $\pm 2$ et donc est toujours plus petite que 2. Il est également clair que la moyenne est une fonction linéaire de son argument. Donc :

$$\begin{aligned}
&E(A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2) \\
&\quad = \sum_{A_1,A_2,B_1,B_2} p(A_1, A_2, B_1, B_2)A_1B_1 + \sum_{A_1,A_2,B_1,B_2} p(A_1, A_2, B_1, B_2)A_2B_1 \\
&\quad + \sum_{A_1,A_2,B_1,B_2} p(A_1, A_2, B_1, B_2)A_2B_2 - \sum_{A_1,A_2,B_1,B_2} p(A_1, A_2, B_1, B_2)A_1B_2 \\
&\quad = E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2)
\end{aligned}$$

La comparaison des deux expressions précédentes nous permet de conclure :

$$E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2) \leq 2$$

Ce résultat est un exemple d'inégalité de Bell (elle est appelée spécifiquement inégalité CHSH). Nous avons obtenu cette inégalité en faisant deux hypothèses. La première est que les résultats possibles de toutes le mesures sont des éléments de réalisme, donc caractérisent l'état du système indépendamment de la mesure. La deuxième est l'hypothèse de localité : la mesure effectuée par Alice ne peut en aucune manière influencer le résultat que Bob va obtenir de sa mesure. Ces deux hypothèse ensemble constituent ce que le physiciens appellent l'hypothèse de *réalisme local*. Alice et Bob peuvent vérifier l'inégalité de Bell en faisant l'expérience. Ils répètent plusieurs fois l'expérience (Charlie envoie à chaque fois deux bâtonnets choisis au hasard selon la règle $p(A_1, A_2, B_1, B_2)$). D'abord, Alice et Bob décident de mesurer $A_1$ et $B_1$ pendant $N$ fois successives. De cette manière, ils calculent $E(A_1B_1)$ avec précision arbitraire (il suffit de choisir $N$ très grand). Après ils mesurent $A_1$ et $B_2$ pendant $N$ fois et calculent ainsi $E(A_1B_2)$, et ainsi de suite. A la fin, ils peuvent vérifier l'inégalité de Bell.

Revenons maintenant à la mécanique quantique. Choisissons comme avant l'état EPR :

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Comme d'habitude, le premier qu-bit est envoyé à Alice et le deuxième à Bob. Alice et Bob peuvent décider d'utiliser pour leurs mesures des filtres polariseurs orientés à un angle $\theta$ par rapport à l'axe $\mathbf{x}$. Si le photon passe à travers le filtre, il sera projeté sur l'état $|\theta\rangle$. Au cas contraire, il sera projeté sur l'état $|\theta_\perp\rangle = |\theta + \pi/2\rangle$. Dans le premier cas, nous attribuons à la mesure la valeur $-1$, dans le deuxième $+1$. Les états $|\theta\rangle$ et $|\theta_\perp\rangle$ s'écrivent comme :

$$|\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$

$$|\theta_\perp\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$$

Il est clair que si Alice et Bob décident de mesurer avec leurs filtres orientés selon le même angle $\theta$, leurs mesures vont être totalement anti-corrélées. Cela puisque l'état $|\psi\rangle$, exprimé dans la base des états $|\theta\rangle$ et $|\theta_\perp\rangle$, prend exactement la même forme qu'avant :

$$|\psi\rangle = \frac{|\theta, \theta_\perp\rangle - |\theta_\perp, \theta\rangle}{\sqrt{2}}$$

Si donc $A$ et $B$ correspondent aux filtres orientés selon $\theta = 0$, nous aurons $E(AB) = -1$. Le calcul est simple. La probabilité que la mesure donne $(1,-1)$ est $p(1,-1) = |\langle 10|\psi\rangle|^2 = 1/2$. De même, la probabilité de mesurer $(-1,1)$ est $p(-1,1) = |\langle 01|\psi\rangle|^2 = 1/2$. Les probabilités de mesurer $(1,1)$ et $(-1,-1)$ sont zéro. Donc la moyenne est donnée par

$$E(AB) = \frac{1}{2}(+1)\times(-1) + \frac{1}{2}(-1)\times(+1) = -1$$

Supposons par contre que Alice reste dans la base computationnelle, alors que Bob mesure avec son filtre orienté selon $\theta$. Dans ce cas, il est mieux d'écrire l'état en fonction de la base computationnelle pour le qu-bit d'Alice et de la nouvelle base pour Bob :

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|0\rangle \otimes (\sin\theta\,|\theta\rangle + \cos\theta\,|\theta_\perp\rangle) - |1\rangle \otimes (\cos\theta\,|\theta\rangle - \sin\theta\,|\theta_\perp\rangle)$$

Dans ce cas nous avons :

$$\begin{aligned}
p(-1,-1) &= |\langle 0,\theta|\psi\rangle|^2 = \frac{1}{2}\sin^2\theta \\
p(1,1) &= |\langle 1,\theta_\perp|\psi\rangle|^2 = \frac{1}{2}\sin^2\theta \\
p(-1,1) &= |\langle 0,\theta_\perp|\psi\rangle|^2 = \frac{1}{2}\cos^2\theta \\
p(1,-1) &= |\langle 1,\theta|\psi\rangle|^2 = \frac{1}{2}\cos^2\theta
\end{aligned}$$

La moyenne est donnée par :

$$\begin{aligned}
E(AB) &= \frac{1}{2}[\sin^2\theta(+1)\times(+1) + \sin^2\theta(-1)\times(-1) \\
&+ \cos^2\theta(-1)\times(+1) + \cos^2\theta(+1)\times(-1)] \\
&= \frac{1}{2}[2\sin^2\theta - 2\cos^2\theta] \\
&= -\cos(2\theta)
\end{aligned}$$

Nous remarquons maintenant que ce résultat ne dépend que de l'angle entre le filtre de Bob et celui d'Alice. En effet, l'état prend la même forme si les deux filtres sont orientés selon $\theta$. Il s'ensuit que, si Alice oriente son filtre selon $\theta$ et Bob selon $\theta+\phi$, alors nous pouvons considérer $\theta$ comme le nouveau zéro pour la mesure de l'angle et la situation est totalement équivalente à celle où Alice oriente son filtre selon $\theta = 0$ et Bob selon $\phi$. Nous pouvons conclure que la moyenne entre la mesure d'Alice $A$ et celle de Bob $B$ est simplement donnée par :

$$E(AB) = -\cos[2(\theta_B - \theta_A)]$$

Supposons maintenant qu'Alice choisisse pour ses deux possibles mesures les angles $\theta_{A_1} = 0$ et $\theta_{A_2} = 3\pi/4$, et que Bob choisisse $\theta_{B_1} = 3\pi/8$ et $\theta_{B_2} = \pi + \pi/8$. Nous pouvons maintenant construire la quantité nécessaire pour vérifier l'inégalité de Bell :

$$\begin{aligned}
&E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2) \\
&= -\cos[2(\theta_{B_1} - \theta_{A_1})] - \cos[2(\theta_{B_1} - \theta_{A_2})] - \cos[2(\theta_{B_2} - \theta_{A_2})] + \cos[2(\theta_{B_2} - \theta_{A_1})] \\
&= -\cos(3\pi/4) - \cos(-3\pi/4) - \cos(3\pi/4) + \cos(2\pi + \pi/4) \\
&= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \\
&= 2\sqrt{2} \simeq 2.82 \text{ !!!}
\end{aligned}$$

Le résultat prévu par la mécanique quantique viole l'inégalité de Bell ! Donc, la théorie de la mécanique quantique ne remplit pas l'hypothèse de réalisme local. La chose formidable est que grâce à l'inégalité de Bell nous avons une méthode opérationnelle de déterminer si la Nature se comporte comme prévu par la mécanique quantique ou si la Nature obéit au réalisme local et la mécanique quantique est une théorie incomplète.
Des centaines d'expériences ont été réalisées depuis les années '70 pour vérifier l'inégalité de Bell. Le résultat est que l'inégalité de Bell est toujours violée, et la valeur mesurée est toujours celle prévue par la mécanique quantique. Ce résultat constitue une vraie révolution conceptuelle. Il nous dit que la Nature n'obéit pas à l'hypothèse du réalisme local et que les corrélations quantiques sont une propriété intrinsèque d'un système physique. Cette conclusion est très importante pour l'information quantique. Nous avons vu que l'intrication est à la base de presque toutes les applications de l'information quantique qui produisent un vrai avantage par rapport au traitement classique de l'information. En particulier, le parallélisme quantique, le superdense coding, la téléportation quantique et d'autres applications que nous n'avons pas encore traitées. Le résultat de Bell nous dit essentiellement que cet avantage est vrai et non pas juste une conséquence des limites du processus de mesure (limites qui pourraient être repoussées dans un futur prochain). D'une certaine manière, il s'agit d'une validation importante de l'idée de base que la mécanique quantique constitue une ressource précieuse pour le traitement de l'information.

# 6 Matrice densité

## 6.1 Propriétés de la matrice densité

Nous allons maintenant introduire un formalisme pour décrire un système formé de deux (ou plusieurs) sous-systèmes. Nous aimerions prendre le point de vue d'un observateur qui n'a accès qu'un seul sous-système. C'est par exemple le cas des systèmes ouverts, ou le sous-système qui nous intéressé est couplé à l'environnement.
Considérons deux sous-systèmes A et B décrit respectivement par les bases orthonormées $\{|i\rangle\}$ et $\{|\mu\rangle\}$. L'état le plus général du système total est :

$$|\psi\rangle = \sum_{i,\mu} \alpha_{i\mu} |i\rangle \otimes |\mu\rangle$$

Supposons que nous voulons étudier une propriété du sous-système A, comme par exemple une observable M. Pour le système total, cet observable est représentée par l'opérateur $M \otimes I_B$, où $I_B$ est l'identité sur B. Donc l'action de M sur $|\psi\rangle$ est :

$$(M \otimes I_B) |\psi\rangle = \sum_{i,\mu} \alpha_{i\mu} (M |i\rangle) \otimes |\mu\rangle$$

La valeur moyenne de M sur $|\psi\rangle$ est donnée par :

$$\begin{aligned}
\langle M \rangle &= \langle\psi| (M \otimes I_B) |\psi\rangle \\
&= \sum_{j,\nu} \sum_{i,\mu} \alpha^*_{j\nu} \alpha_{i\mu} (\langle j| \otimes \langle\nu|)(M |i\rangle) \otimes |\mu\rangle \\
&= \sum_{i,j} \sum_{\mu} \alpha^*_{j\mu} \alpha_{i\mu} \langle j| M |i\rangle \\
&= \sum_{i,j} \rho_{ij} \langle j| M |i\rangle \\
&= \sum_{i,j} \rho_{ij} M_{ji} \\
\langle M \rangle &= Tr(\rho M)
\end{aligned}$$

où nous avons introduit la "trace" d'une matrice A : $Tr(A) = \sum_i A_{ii}$, la somme de ces éléments diagonaux. Ici, nous avons utilisé le fait que les bases sont orthonormées et que donc $\langle\mu|\,\nu\rangle = \delta_{\mu\nu}$.
Dans cette dérivation, nous avons défini l'opérateur densité du sous-système A, décrit par la matrice :

$$\rho_{ij} = \sum_{\mu} \alpha_{i\mu} \alpha^*_{j\mu} = \sum_{\mu} \langle i\mu|\,\psi\rangle \langle\psi|\, j\mu\rangle$$

L'opérateur correspondant, agissant sur le sous-système A, est :

$$\rho_A = \sum_{i.j} \sum_{\mu} |i\rangle \langle i\mu| \psi\rangle \langle \psi| j\mu\rangle \langle j|$$

Cet opérateur est appelé opérateur (ou matrice) densité réduit au sous-système A.
Nous avons déjà vu que pour un état connu $|\psi\rangle$ à, le sous-système A ne peut pas être décrit par un état "pur" du type $\varphi \in \mathcal{H}_A$. Ce formalisme sert donc à décrire l'état physique de A par le biais d'un opérateur densité $\rho_A$ qui nous permet de calculer les moyennes, en utilisant la trace :

$$\langle M\rangle = Tr(\rho_A M)$$

Nous remarquons que cette expression est indépendante de la base choisie, puisque la trace d'une matrice est change pas selon la base. Les propriétés de cette matrice sont :

- Elle est hermitique :
$$\rho_A^\dagger = \rho_A$$
- Sa trace est égale 1 :
$$Tr(\rho_A) = \sum_i \rho_{A,ii} = \sum_{i,\mu} |\alpha_{i\mu}|^2 = ||\psi||^2 = 1$$
- Elle est défini positive : $\forall |\varphi\rangle$, on a $\langle\varphi| \rho_A |\varphi\rangle > 0$. En effet :
$$\begin{aligned}\langle\varphi| \rho_A |\varphi\rangle &= \sum_{i,j} \sum_{\mu} \langle\varphi| i\rangle \langle j| \varphi\rangle \langle i\mu| \psi\rangle \langle \psi| j\mu\rangle \\ &= \sum_{\mu} \beta_\mu \beta_\mu^* = ||\beta||^2 > 0 \\ \text{avec } \beta_\mu &= \sum_i \langle\varphi| i\rangle \langle i\mu| \psi\rangle\end{aligned}$$
- Ces valeurs propres sont toutes positives. C'est le cas de tous les opérateurs définis positifs. Nous pouvons donc diagonaliser $\rho_A$ qui, dans la base de vecteurs propres, s'écrit :
$$\rho_A = \sum_k p_k |k\rangle \langle k| \quad \text{avec } p_k > 0$$
De plus, la condition $Tr(\rho_A) = 1$ implique :
$$\sum_k p_k = 1$$

et la moyenne de M devient :

$$\langle M\rangle = Tr(\rho_A M) = \sum_k p_k \langle k| M |k\rangle = \sum_k p_k \langle M\rangle_k$$

Cette expression est très importante. Elle souligne un phénomène déjà rencontré dans un cas particulier : Un système intriqué à un autre système se comporte, vis-à-vis de la mesure d'une observable M quelconque, comme un mélange statistique de plusieurs états $|k\rangle$, chacun avec une probabilité $p_k$. La situation est équivalente à un grand nombre de systèmes et que chaque état $|k\rangle$ intervient avec une probabilité $p_k$.

Naturellement, la question suivant se pose : Quelle est la matrice densité correspondant à un état "pur" $\psi$ ? supposons vouloir calculer la moyenne de l'observable $M = 0$ :

$$\langle M\rangle = \langle\psi| 0 |\psi\rangle$$

Si nous définissons :

$$\rho = |\psi\rangle \langle\psi|$$

Alors la moyenne de 0 devient :

$$\langle 0\rangle = Tr(\rho 0) = Tr(|\psi\rangle \langle\psi| 0)$$

Calculons cette trace sur une base $\{|j\nu\rangle\}$ :

$$\begin{aligned} Tr(|\psi\rangle \langle\psi| 0) &= \sum_{j\nu} \langle j\nu| \psi\rangle \langle\psi| 0 |j\nu\rangle \\ &= \langle\psi| 0 \left( \sum_{j\nu} \langle j\nu| \psi\rangle |j\nu\rangle \right) \\ Tr(|\psi\rangle \langle\psi| 0) &= \langle\psi| 0 |\psi\rangle = \langle 0\rangle \end{aligned}$$

Donc l'opérateur densité d'un état dit "pur" (c'est-à-dire un état qui n'est pas un mélange statistique, mais décrit par un seul vecteur) est le projecteur sur l'état. Donc, pour un état pur :

$$\rho^2 = \rho$$

Nous pouvons interpréter cela comme si l'état pur est mélange statistique de $|k = 1\rangle = |\psi\rangle$ et $|k\rangle$ pour $k = 2, 3, ...$ avec $p_1 = 1$ et $p_k = 0$ pour $k > 1$.
Nous comprenons donc que $\rho^2 = \rho$ est une condition nécessaire et suffisante pour que l'état décrit par un opérateur densité $\rho$ à soit un état pur.
Considérons à nouveau l'état intriqué :

$$|\psi\rangle = \sum_{i,\mu} \alpha_{i\mu} |i\mu\rangle$$

Une autre question se pose : Comment pouvons-nous relier $\rho_A$ à $\rho$ ?

$$\rho = |\psi\rangle\langle\psi| = \sum_{i,\mu;j,\nu} \alpha_{i\mu}\alpha^*_{j\nu} |i\mu\rangle\langle j\nu|$$

La matrice correspondante est : $\rho_{i\mu,j\nu} = \alpha_{i\mu}\alpha^*_{j\nu}$. Mais, par définition :

$$\rho_A = \sum_{\mu} \alpha_{i\mu}\alpha^*_{j\nu}$$

Donc :

$$\rho_A = Tr_B(\rho)$$

où nous indiquons par $Tr_B$ la trace relativement à la base du sous-système B : Si $\{|\mu\rangle\}$ est la base de $\mathcal{H}_B$, alors :

$$\begin{aligned}
\rho_A = Tr_B(\rho) &= \sum_{\mu'} \langle\mu'| \rho |\mu'\rangle \\
&= \sum_{\mu'} \sum_{i,\mu;j,\nu} \alpha_{i\mu}\alpha^*_{j\nu} \langle\mu'| (|i\rangle \otimes |\mu\rangle) (\langle j| \otimes \langle\nu|) |\mu'\rangle \\
&= \sum_{\mu'} \sum_{i,\mu;j,\nu} \alpha_{i\mu}\alpha^*_{j\nu}\delta_{\mu\mu'}\delta_{\nu\mu'} |i\rangle\langle j| \\
\rho_A &= \sum_{ij} \sum_{\mu} \alpha_{i\mu}\alpha^*_{j\mu} |i\rangle\langle j|
\end{aligned}$$

Ce qui correspond en effet à l'expression trouvée précédemment. L'opérateur $Tr_B(\rho)$ s'appelle "trace partielle".

L'opérateur densité est un outil fondamental en physique quantique : il permet de décrire un système dont nous connaissons qu'une partie. Dans notre cas, nous n'avons pas acces à l'état $|\psi\rangle$ (en effet nous ne sommes pas à mesure de caractériser le sous-système B). Mais nous pouvons tout savoir sur le système A grâce à $\rho_A$. En particulier, si nous mesurons l'observable M sur A, nous pouvons en décrire la valeur moyenne $\langle M\rangle = Tr(\rho_A M)$ et, comme nous le verrons plus tard, les probabilités de résultats de la mesure, l'évolution temporelle du système, etc...
Ce formalisme est indispensable pour la description de systèmes ouverts, où B représente l'univers, que nous ne pas décrire. L'idée est donc de connaître le comportement de $\rho_A$ à en introduisant des modèles s'interaction avec B qui ont plus ou moins approximés. Nous verrons cela avec un modèle pour la décohérence.

## 6.2 Matrice densité d'états mixtes

En général les systèmes étudiés ici sont dans des états mixtes, puisque l'univers est un état pur :

$$|\psi\rangle = \sum_{i\mu} \alpha_{i\mu} |i\rangle \otimes |\mu\rangle$$

et cet état pur est un état intriqué entre le système sous examen et le reste de l'univers. Mais quelques remarques s'imposent :

1. L'écriture de $\rho_A$ sous la forme diagonale $\rho_A = \sum_k p_k |k\rangle \langle k|$ n'indique pas que les états $\{|k\rangle\}$ ont une signification spéciale. En effet, nous disons que le système est dans un mélange statistique des états $|k\rangle$ avec probabilité $p_k$. Toutefois, par rapport aux états possibles (purs) pour A, ce n'est pas la seule manière d'écrire $\rho_A$ comme un mélange statistique.
   supposons par exemple que nous avons, pour un qu-bit :

   $$\rho = \frac{3}{4} |0\rangle \langle 0| + \frac{1}{4} |1\rangle \langle 1|$$

   Définissons :

   $$|a\rangle = \sqrt{\frac{3}{4}} |0\rangle + \sqrt{\frac{1}{4}} |1\rangle$$
   $$|b\rangle = \sqrt{\frac{3}{4}} |0\rangle - \sqrt{\frac{1}{4}} |1\rangle$$

   Ces deux états ne sont visiblement pas orthogonaux. Construisons maintenant un mélange statistique, avec probabilité 1/2 pour les états $|a\rangle$ et $|b\rangle$ :

   $$\begin{aligned} \rho' &= \frac{1}{2} |a\rangle \langle a| + \frac{1}{2} |b\rangle \langle b| \\ &= ... = \frac{3}{4} |0\rangle \langle 0| + \frac{1}{4} |1\rangle \langle 1| = \rho !!! \end{aligned}$$

   Le nouveau mélange statistique correspond au précédent. Ceci est possible car la diagonalisation de la matrice densité est totalement indépendante du changement de base dans l'espace de Hilbert : la transformation unitaire qui diagonalise $\rho_A$ ne correspond donc pas au choix d'une base dans $\mathcal{H}_A$. Physiquement, cela veut dire qu'il n'existe pas de manière unique de décrire un système comme mélange statistique d'états. Toutefois, les propriétés physiques, telle que la valeur moyenne $\langle M \rangle$ d'une observable, ne dépendent pas de cette description. Ceci rend le formalisme physiquement intéressant et utile.

2. Si le sous-système $A$ est dans un état pur $|\phi_A\rangle$ et le sous-système $B$ dans un état pur $|\phi_B\rangle$, alors les matrices densité $A$ sont $\rho_A = |\phi_A\rangle \langle\phi_A|$ et $\rho_B = |\phi_B\rangle \langle\phi_B|$. Et la matrice densité totale est :

$$\rho = (|\phi_A\rangle \langle\phi_A|)(|\phi_B\rangle \langle\phi_B|) = \rho_A \otimes \rho_B$$

Plus en général, si $\rho_A$ est une matrice densité pour $A$ (même dans un état mixte) et $\rho_B$ celle pour $B$, alors nous pouvons construire :

$$\rho = \rho_A \otimes \rho_B$$

Cette définition d'une matrice densité pour le système total est compatible avec ce que nous avons vu. En particulier :

$$\rho_A = Tr_B(\rho) = Tr_B(\rho_A \otimes \rho_B) = \rho_A Tr(\rho_B) = \rho_A$$

Et de même pour $\rho_B$. Toutefois, ce n'es pas toujours vrai que $\rho = \rho_A \otimes \rho_B$. Considérons par exemple $|\psi\rangle$ comme état pur :

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Il est alors possible de calculer :

$$\begin{aligned}
\rho = |\psi\rangle \langle\psi| &= \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) \\
&= \frac{1}{2}(|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|) \\
\rho &= \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \\
\rho_A = Tr(\rho_B) = ... &= \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{1}{2}I \\
\rho_B = Tr(\rho_A) = ... &= \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|) = \frac{1}{2}I
\end{aligned}$$

Nous pouvons maintenant calculer le produit tensoriel des deux matrices $\rho_A$ et $\rho_B$ :

$$\rho_A \otimes \rho_B = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \neq \rho$$

Après avoir instaurer le formalisme de la matrice densité, nous pouvons parcourir les postulats de la mécanique quantique dans ce contexte.

1. L'état d'un système est décrit par l'opérateur densité $\rho$ qui agit sur l'espace des états $\mathcal{H}$. Les propriétés de $\rho$ sont celles que nous avons vues auparavant : $Tr(\rho) = 1$ et $\rho > 0$.
2. L'évolution temporelle est décrite par un opérateur unitaire $U(t_1, t_2)$. Si $\rho = \sum_i \rho_i |\psi_i\rangle \langle\psi_i|$ au temps $t = t_1$, alors au temps $t = t_2$ $|\psi_i\rangle \to U |\psi_i\rangle$ et :
$$\rho \to \sum_i \rho_i U |\psi_i\rangle \langle\psi_i| U^\dagger = U\rho U^\dagger$$
ce qui définit comment la matrice densité évolue au cours du temps.
3. Une observable est décrite par un opérateur auto-adjoint $M$. Les résultats d'une mesure sont les valeurs propres de $M$. La valeur moyenne des résultats possibles est donnée par :
$$\langle M \rangle = Tr(\rho M)$$
La probabilité de mesurer $m$ est donné par : $p(m) = \langle m| \rho |m\rangle$. En effet, pour chaque état $|\psi_i\rangle$, nous avons : $p_i(m) = |\langle m|\psi_i\rangle|^2$. La probabilité totale est, par définition :
$$\begin{aligned} p(m) &= \sum_i \rho_i p_i(m) \\ &= \sum_i \rho_i |\langle m|\psi_i\rangle|^2 \\ &= \sum_i \rho_i \langle m|\psi_i\rangle \langle m|\psi_i\rangle \\ &= \langle m| \left( \sum_i \rho_i |\psi_i\rangle \langle\psi_i| \right) |m\rangle \\ &= \langle m| \rho |m\rangle \end{aligned}$$
Après la mesure, le système est dans l'état décrit par l'état pur $|m\rangle$ donc $\rho \to |m\rangle \langle m|$.
4. Si deux systèmes sont décrits pas $\rho_A$ et $\rho_B$, alors l'état du système total est $\rho = \rho_A \otimes \rho_B$. Par contre, la réciproque n'est vraie : le système total n'est pas nécessairement décrit par un état produit tensoriel, comme nous l'avons vu.

Considérons maintenant un qu-bit dans l'état

$$|\varphi\rangle = \lambda\,|0_a\rangle + \mu\,|1_A\rangle$$

Si ce qu-bit représente un système isolé, alors sa matrice densité est :

$$\begin{aligned}\rho_A = |\varphi\rangle\langle\varphi| &= |\lambda|^2\,|0_A\rangle\langle 0_A| + \lambda\mu^*\,|0_A\rangle\langle 1_A| + \lambda^*\mu\,|1_A\rangle\langle 0_A|\,|\mu|^2\,|1_A\rangle\langle 1_A| \\ &= \begin{pmatrix} |\lambda|^2 & \lambda\mu^* \\ \lambda^*\mu & |\mu|^2 \end{pmatrix}\end{aligned}$$

Nous remarquons que les élément de la matrice contiennent toutes les informations nécessaires pour déduire $\lambda$ et $\mu \in \mathcal{C}$. Ceci n'est pas étonnant, puisque pour un état pur la représentation en matrice densité doit coïncider avec celle du vecteur.

## 6.3 La décohérence

Supposons maintenant que deux qu-bits soient dans un état produit :

$$\begin{aligned}|\varphi_A\rangle &= \lambda\,|0_A\rangle + \mu\,|1_A\rangle \\ |\varphi_B\rangle &= \alpha\,|0_B\rangle + \beta\,|1_B\rangle\end{aligned}$$

La matrice densité totale est comme d'habitude :

$$\begin{aligned}|\psi\rangle &= |\varphi_A\rangle \otimes |\varphi_B\rangle \\ \rho = |\psi\rangle\langle\psi| &= (|\varphi_A\rangle \otimes |\varphi_B\rangle)(\langle\varphi_A| \otimes \langle\varphi_B|)\end{aligned}$$

La matrice densité contient 4x4=16 termes que nous savons calculer, puisque pour un état produit $\rho = \rho_A \otimes \rho_B$ :

$$\rho = \begin{pmatrix} |\lambda|^2\rho_B & \lambda\mu^*\rho_B \\ \lambda^*\mu\rho_B & |\mu|^2\rho_B \end{pmatrix}$$

Nous pouvons calculer $\rho_A$ :

$$\begin{aligned}\rho_A &= Tr_B(\rho) \\ &= \begin{pmatrix} |\lambda|^2 Tr(\rho_B) & \lambda\mu^* Tr(\rho_B) \\ \lambda^*\mu Tr(\rho_B) & |\mu|^2 Tr(\rho_B) \end{pmatrix} \\ &= \begin{pmatrix} |\lambda|^2 & \lambda\mu^* \\ \lambda^*\mu & |\mu|^2 \end{pmatrix}\end{aligned}$$

Cette matrice coïncide avec celle pour un qu-bit isolé dans l'état $|\varphi_A\rangle$.

Cet exemple nous montre que les états qui formé d'un produit tensoriel entre deux états des sous-systèmes A et B sont des états spéciaux. Chaque sous-système a les mêmes propriétés qu'il était isolé, donc indépendant de l'état $|\varphi_B\rangle$ de l'autre sous-système.

Calculons maintenant la matrice densité d'un état intriqué des deux sous-systèmes :

$$|\psi\rangle = \lambda\,|0_A 0_B\rangle + \mu\,|1_A 1_B\rangle$$

$$\begin{aligned}
\rho &= |\psi\rangle\langle\psi| \\
&= |\lambda|^2\,|0_A 0_B\rangle\langle 0_A 0_B| + \lambda\mu^*\,|0_A 0_B\rangle\langle 1_A 1_B| \\
&+ \lambda^*\mu\,|1_A 1_B\rangle\langle 0_A 0_B| + |\mu|^2\,|1_A 1_B\rangle\langle 1_A 1_B| \\
\rho &= \begin{pmatrix} |\lambda|^2 & 0 & 0 & \lambda\mu^* \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \lambda^*\mu & 0 & 0 & |\mu|^2 \end{pmatrix}
\end{aligned}$$

La matrice densité réduite de $A$ est donc :

$$\begin{aligned}
\rho_A &= Tr_B(\rho) = \langle 0_B|\,\rho\,|0_B\rangle + \langle 1_B|\,\rho\,|1_B\rangle \\
&= |\lambda|^2\,|0_A\rangle\langle 0_A| + |\mu|^2\,|1_A\rangle\langle 1_A| \\
\rho_A &= \begin{pmatrix} |\lambda|^2 & 0 \\ 0 & |\mu|^2 \end{pmatrix}
\end{aligned}$$

La différence entre ce résultat et celui obtenu dans l'exemple précédent est que dans ce cas, si nous effectuons des mesures sur le système $A$, nous ne pouvons obtenir que des informations sur $|\lambda|^2$ et $|\mu|^2$. Nous n'avons pas accès aux phases complexes de $\lambda$ et $\mu$ si nous mesurons les propriétés du système total. Ici, une mesure sur $N$ répliques de $|\psi\rangle$ donne une statistique des résultats qui peut s'interpréter simplement comme si $A$ était un mélange statistique de systèmes dans les états $|0_A\rangle$ et $|0_B\rangle$. Donc c'est comme si une fraction $|\lambda|^2$ des $N$ états correspondent à $A$ dans l'état $|0_A\rangle$ et une fraction $|\mu|^2$ à $A$ dans $|1_A\rangle$. Toute observable $M$ sur $A$ aura somme valeur moyenne :

$$\langle M\rangle = |\lambda|^2\,\langle 0_A|\,M\,|0_A\rangle + |\mu|^2\,\langle 1_A|\,M\,|1_A\rangle$$

et les probabilités de mesurer $0_A$ ou $1_A$ sont données par $|\lambda|^2$ et $|\mu|^2$ respectivement.
C'est un scénario classique, un comportement qui pourrait être reproduit par une expérience de billes de couleur différentes tirées au sort dans un sac. Et

nous avons appris que l'information quantique n'est possible que par un nouveau paradigme de représentation d'un qu-bit, qui fait intervenir les phases complexes et les états de superposition linéaire. K'état de $A$ décrit par :

$$\rho_A = \begin{pmatrix} |\lambda|^2 & 0 \\ 0 & |\mu|^2 \end{pmatrix}$$

est la pire des choses qui puisse nous arriver pour un qu-bit, puisqu'il le ramène à une représentation classique de l'information.
L'ensemble des processus physique qui permettent le système d'évoluer vers un tel état est appelé *décohérence*. Ce nom peut se comprendre en considérant les matrices densités de l'état $|\varphi\rangle$ et du mélange :

$$\rho_A = \begin{pmatrix} |\lambda|^2 & \lambda\mu^* \\ \lambda^*\mu & |\mu|^2 \end{pmatrix} \quad \rho_A = \begin{pmatrix} |\lambda|^2 & 0 \\ 0 & |\mu|^2 \end{pmatrix}$$

La décohérence correspond à la perte d'information sur les phases complexes qui interviennent dans la matrice densité (et qui sont seulement dans les éléments hors diagonaux, puisque les éléments diagonaux doivent être réels). Ces phases sont physiquement à l'origine de tous les phénomènes d'interférence quantiques, donc des effets cohérents. On appelle aussi "cohérence" les éléments hors-diagonaux de $\rho$. Il faut toutefois faire attention : la décohérence n'est pas toujours équivalente à une matrice densité diagonale. Si par exemple, nous réexprimons $\rho_A$ dans la base :

$$|\pm_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle \pm |1_A\rangle)$$

nous obtenons :

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & |\lambda|^2 = |\mu|^2 \\ |\lambda|^2 = |\mu|^2 & 1 \end{pmatrix}$$

Cette matrice n'est pas diagonale, même su elle ne nous permet pas de connaître les phases de $\lambda$ et $\mu$.

L'idée générale est que les deux sous-systèmes décrivent le système sous examen (par exemple une porte logique quantique) et l'environnement. L'environnement à tendance à faire évoluer le sous-système vers un état intriqué avec les degré de liberté de l'environnement. ceci a pour effet de perdre toute l'information sur la phase du système pour un observateur que ne mesure que le sous-système et pas l'environnement (C'est toujours le cas, tout simplement parce que l'environnement est très difficile à mesurer).
La décohérence est un processus dynamique induit par des interactions. Si nous préparons le sous-système dans l'état initial $|\varphi_A\rangle$, cela veut dire que nous

l'état initial du système total (sous-système+environnement) est $|\varphi_A\rangle \otimes |\psi_E\rangle$, où $|\psi_E\rangle$ est l'état dans lequel se trouve l'environnement (nous supposons un état pur $|\psi_E\rangle$ puisque nous imaginons l'environnement comme étant le reste de l'univers). C'est au cours du temps que le tout va évoluer vers un état intriqué. Cette évolution est donnée par un opérateur unitaire qui agit sur le système total (sous-système+environnement). Toutefois, l'action de cet opérateur sur l'espace $\mathcal{H}_A$ du système n'est pas un processus unitaire.
De plus la décohérence a besoin d'interaction entre le sous-système et l'environnement. En effet, si nous supposons que l'environnement et le sous-système n'interagissent pas, nous pouvons caractérisé le système total par un Hamiltonien $H$ :

$$H = H_A + H_E$$

où $H_A$ est l'Hamiltonien du sous-système $A$ et $H_E$ celui de l'environnement. Ici nous n'avons pas de troisième terme $H_I$ qui contiendrais à la fois les degrés de liberté du sous-système et de l'environnement et qui décrirait leur interaction. Par conséquent les Hamiltoniens $H'_A$ et $H'_E$, correspondant $H_A$ et $H_E$ dans l'espace de Hilbert du système total, commutent :

$$H_A \to H_A \otimes I_E = H'_A$$
$$H_E \to H_E \otimes I_E = H'_E$$

$$[H'_A, H'_E, =] \, 0$$

Dans ce cas, l'opérateur d'évolution temporelle s'écrit comme :

$$\begin{aligned} U(t_1, t_2) &= e^{-i\frac{H'_A + H'_E}{\hbar}(t_2 - t_1)} \\ &= e^{-i\frac{H'_A}{\hbar}(t_2 - t_1)} e^{-i\frac{H'_E}{\hbar}(t_2 - t_1)} \end{aligned}$$

Si nous appliquons cet opérateur à l'état $|\varphi_A\rangle \otimes |\psi_E\rangle$, nous obtenons un état produit tensoriel. :

$$\begin{aligned} U(t_1, t_2) \, |\varphi_A\rangle \otimes |\psi_E\rangle &= \left[ e^{-i\frac{H'_A}{\hbar}(t_2 - t_1)} \, |\varphi_A\rangle \right] \left[ e^{-i\frac{H'_E}{\hbar}(t_2 - t_1)} \, |\psi_E\rangle \right] \\ &= |\varphi_A(t_2)\rangle \otimes |\psi_E(t_2)\rangle \end{aligned}$$

Dans la nature, les interactions sont toujours présentes et il est pratiquement impossible de s'en débarrasser. C'est pourquoi nous ne pouvons pas éviter la décohérence.

Pour comprendre pourquoi la décohérence fait évoluer le système vers des états intriqués, prenons un exemple pratique :

Supposons que nous avons un objet (une grosse molécule par exemple) que nous avons préparer dans un état superposition linéaire de deux états correspondant à deux position $r_1$ et $r_2$ différents. C'est un état non-classique puisque des objets de grandes taille ont toujours une tendance à être localisés. L'état initial de la molécule est :

$$|\varphi_A\rangle = \lambda\,|\varphi_{r_1}\rangle + \mu\,|\varphi_{r_2}\rangle$$

Et l'état initial du système total est $|\varphi_A\rangle \otimes |\psi_E\rangle$. Supposons que l'environnement est constitué d'un gaz d'atomes. Nous ne connaissons pas son état, mais nous pensons qu'un gaz a une température fixe et est caractérisé par un comportement classique, où chaque molécule est bien localisée dans l'espace. Il est donc probable que, par l'interaction de Coulomb entre les constituants dans des molécules, la molécule dans l'état $|\varphi_{r_1}\rangle$ interagisse avec un atome du gaz très proche de $r_1$. Après la collision, le système a effectué une mesure sur l'environnement et l'état $|\psi_E\rangle$ est projeté sur un état qu'on appelle $|r_1, \psi'_E\rangle$ qui représente un atome du gaz en position $r_1$ et le reste su gaz en $\psi'_E$. De même l'état $|\varphi_{r_2}\rangle$ de la molécule induit une collision avec un atome près de $r_2$ et projète l'état de l'environnement sur $|r_2, \psi''_E\rangle$-. Mais si à $|\varphi_{r_1}\rangle$ et $|\varphi_{r_2}\rangle$ correspondent ces deux évolutions, alors à $|\varphi_A\rangle = \lambda\,|\varphi_{r_1}\rangle + \mu\,|\varphi_{r_2}\rangle$ correspond l'évolution :

$$|\varphi_A\rangle \otimes |\psi_E\rangle \to \lambda\,|\varphi_{r_1}\rangle \otimes |r_1, \psi'_E\rangle + \mu\,|\varphi_{r_2}\rangle \otimes |r_2, \psi''_E\rangle$$

ce qui est un état intriqué. L'intrication a lieu puisque les interactions ont un caractère local (un atome interagit avec la molécule seulement s'il est assez proche d'elle). Si nous partons d'un état délocalisé, la tendance est donc à intriquer chaque composant localisé du système avec un état également localisé de l'environnement. Il semblerait donc que parmi tous les états possibles, les états localisés aient un rôle spécial. Dans la théorique de la décohérence c'est un exemple de "états pointeurs".
La réalité est beaucoup plus complexe que cette simple description. En particulier, la mécanique quantique ne peut guère expliquer pourquoi l'interaction évolue entre système et environnement exactement de cette manière, ni pourquoi un certain type 'état serait privilégié par rapport é d'autres. Ces problèmes sont à la base de la recherche sur la décohérence, sur le passage de la réalité microscopique (peu de particules) au monde macroscopique ($\approx 10^{24}$ particules) et plus en général sur une éventuelle formulation nouvelle de la mécanique quantique (qui n'a pas encore été atteinte).

Revenons sur l'idée que la décohérence est un processus dynamique. L'évolution d'un état pur vers un mélange statistique se produit dynamiquement. La durée de ce processus est dite *temps de décohérence*, et est caractéristique de chaque système spécifique. Dans la réalisation physique d'une porte logique quantique, il faut donc veiller à ce que l'opération dure beaucoup mois longtemps que le temps de décohérence. Si c'est le cas, alors la matrice densité de l'état final $\rho_A$ sera très peu différente de $\rho_A^{(0)}$ qui représente l'état pur prévu par le fonctionnement idéal de la porte logique. Des techniques de correction d'erreur quantique, dont nous parlerons dans la suite de ce cours, permettent de remonter à $\rho_A^{(0)}$ avec une probabilité que nous pouvons rendre arbitrairement proche de 1. Si par contre le temps de décohérence est court par rapport au temps de l'opération, alors $\rho_A$ sera un mélange statistique total et l'information sur les phases, nécessaire pour le paradigme quantique, sera perdue à jamais.
La mesure de la différence entre $\rho_A$ et $\rho_A^{(0)}$ pour un dispositif est dite *fidélité*. Pour le caractériser, il faut construire des modèles de décohérence. Ces modèles sont nécessairement approximés, puisqu'il est presque impossible de décrire le comportement détaillé de l'environnement qui est typiquement un système extrêmement grand et complexe. Certains modèles peuvent s'attaquer à une description approximée de l'environnement. Toutefois, les modèles les plus utilisés en information quantique se limitent à décrire l'effet de l'environnement sur le système sous forme d'une probabilité pour le système +l'environnement de changer son état total. Un tel changement peut être vu comme la conséquence d'un processus d'interaction (par ex. collision avec un atome).

Prenons d'abord un exemple élémentaire. Supposons que l'environnement produit l'effet suivant sur le qu-bit :

$$|0\rangle \to |0\rangle$$
$$|1\rangle \to -|1\rangle$$

L'état $|0\rangle$ reste le même tandis que l'état $|1\rangle$ reste aussi le même, mais la phase prend une phase -1. Cette phase a un effet physique important si le qu-bit est dans l'état $\alpha|0\rangle + \beta|1\rangle$. Ce changement se produit de manière aléatoire et a une probabilité par unité de temps $\Gamma$ de se produire. $\Gamma$ est le *taux de décohérence*. Si nous attendons un temps $\Delta t$, le changement se produit avec une probabilité $p = \Gamma\Delta t$. Donc le temps de décohérence est $\tau_\Delta = \frac{1}{\Gamma}$. Ce modèle est trop simple, puisqu'il n'introduit qu'un changent du qu-bit. Aucune intrication avec l'environnement se produit.
Cet exemple nous sert toutefois à comprendre le rôle de la taille du système.

SI le qu-bit est dans l'état :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Après le processus de décohérence, il devient :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

qui est un état différent et ne montre aucune mémoire de quel était l'état initial, avec ses phases. Nous avons vu que ce changement se produit en un temps $\tau_\Delta = \frac{1}{\Gamma}$. Supposons maintenant qu'un système de $N$ qu-bits soit soumis au même environnement. Chaque qu-bit interagit avec l'environnement indépendamment des autres. Si l'état initial est.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00..0\rangle + |11..1\rangle)$$

alors la probabilité de passer à un état

$$|\psi^*\rangle = \frac{1}{\sqrt{2}}(|00..0\rangle - |11...1\rangle)$$

avec perte de la mémoire de la phase, est $p = N\Gamma\Delta t$, puisque c'est la somme des probabilité de $N$ processus indépendants. Pour ce système le temps de décohérence est :

$$\tau_\Delta(N) = \frac{\tau_\Delta}{N}$$

donc $N$-fois plus court qu'un processus à un qu-bit. En règle générale donc, plus un système est grand, plus court est $\tau_\Delta(N)$.

Finalement, nous allons introduire un modèle de décohérence très utilisé. Il est appelé *phase damping channel*. Il est important de souligner qu'il ne s'agit pas du seul mécanisme possible. Comme nous avons déjà vu, seul une description microscopique de l'environnement permettrait de modéliser correctement la décohérence. Toutefois, un tel modèle est très difficile à réaliser et nous nous limiterons à des modèles phénoménologiques comme le suivant : Dans ce modèle, nous supposons que si le qu-bit se trouve dans l'état $|0\rangle$ ou $|1\rangle$, alors l'état ne change pas comme conséquence de l'interaction avec l'environnement. Ces états seraient des états *pointeurs*, qui se comportent de manière spéciale par rapport à la décohérence. L'environnement par contre change son état. Nus admettons qu'au début, il se trouve dans l'état $|0_E\rangle$. Si le qu-bt est dans l'état $|0\rangle$, l'environnement a une probabilité $p$ (durant un temps $\Delta t$) de passer de $|0_E\rangle$ à $|1_E\rangle$. De même, si le qu-bit est dans $|1\rangle$, nous

avons une probabilité $p$ de passer de à $|0_E\rangle$ à $|2_E\rangle$. Nous pouvons représenter cette situation par les états suivants (avant et après l'interaction) :

$$\begin{aligned}|00_E\rangle \rightarrow & \sqrt{1-p}\,|00_E\rangle + \sqrt{p}\,|01_E\rangle \\ & = |0\rangle \otimes (\sqrt{1-p}\,|0_E\rangle + \sqrt{p}\,|1_E\rangle) \\ |10_E\rangle \rightarrow & \sqrt{1-p}\,|10_E\rangle + \sqrt{p}\,|12_E\rangle \\ & = |1\rangle \otimes (\sqrt{1-p}\,|0_E\rangle + \sqrt{p}\,|2_E\rangle)\end{aligned}$$

Ces deux états ne sont pas intriqués. Toutefois, si le qu-bit initial est dans :

$$|\varphi\rangle = \lambda\,|0\rangle + \mu\,|1\rangle$$

L'état initial du système : qu-bit +environnement est :

$$|\psi\rangle = (\lambda\,|0\rangle + \mu\,|1\rangle) \otimes |0_E\rangle$$

avec une matrice densité initiale :

$$\rho_A = Tr_{\text{env}}(\rho) = \begin{pmatrix} |\lambda|^2 & \lambda\mu^* \\ \lambda^*\mu & |\mu|^2 \end{pmatrix}$$

Après interaction, l'état est :

$$|\psi'\rangle = \lambda\sqrt{1-p}\,|00_E\rangle + \lambda\sqrt{p}\,|01_E\rangle + \mu\sqrt{1-p}\,|10_E\rangle + \mu\sqrt{p}\,|12_E\rangle$$

et la matrice densité devient :

$$\begin{aligned}\rho'_A = Tr_{\text{env}}(\rho') &= |\lambda|^2\,|0\rangle\langle 0| + |\mu|^2\,|1\rangle\langle 1| + \lambda\mu^*(1-p)\,|0\rangle\langle 1| + \lambda^*\mu(1-p)\,|1\rangle\langle 0| \\ &= \begin{pmatrix} |\lambda|^2 & \lambda\mu^*(1-p) \\ \lambda^*\mu(1-p) & |\mu|^2 \end{pmatrix}\end{aligned}$$

Si nous laissons passer $n$-fois $\Delta t$, en itérant le processus, nous avons :

$$\rho_A^{\prime(n)} = \begin{pmatrix} |\lambda|^2 & \lambda\mu^*(1-p)^n \\ \lambda^*\mu(1-p)^n & |\mu|^2 \end{pmatrix}$$

Pour $n \rightarrow \infty$, si nous supposons que $p = \Gamma\Delta t$ et que nous posons $t = n\Delta t$, $\Delta t \rightarrow 0$ :

$$\rho'_A(t) \xrightarrow{t\rightarrow\infty} \begin{pmatrix} |\lambda|^2 & \lambda\mu^* e^{-\Gamma t} \\ \lambda^*\mu e^{-\Gamma t} & |\mu|^2 \end{pmatrix}$$

en effet

$$(1-\Gamma\Delta t)^{\frac{t}{\Delta t}} \xrightarrow{\Delta t\rightarrow 0} e^{-\Gamma t}$$

Comme attendu, le résultat est que les éléments hors-diagonaux de $\rho_A$ tendent vers zéro avec un temps caractéristique $\tau_\Delta = \frac{1}{\Gamma}$. La matrice $\rho_A(t)$ tend vers un mélange statistique, sonc un état purement classique.
Nous remarquons qu'aucune transformation unitaire peut causer cette évolution, en posant :

$$\rho_A(t) = U\rho_A(0)U^\dagger$$

En effet, une transformation unitaire transforme un état pur en un autre état pur.

# 7 Circuits quantiques

Pour construire des algorithmes quantiques, il faut développer un formalisme de circuits quantiques analogue à celui des circuits numériques en électronique classique. Ce formalisme permet aussi de :

- trouver un standard : des portes logiques universelles
- fixer les défis technologiques : quelles portes logiques ? Comment contraster la décohérence ?

Nous allons :

- Etudier les portes logiques à 1 et 2 qu-bits
- Etablir des portes logiques universelles
- Etudier le processus de mesure (lecture des outputs)

## 7.1 Portes à 1 et 2 qu-bits

Rappelons que le qu-bit est toujours représenté par :

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \quad \text{avec} \quad |a|^2 + |b|^2 = 1$$

Les portes logiques sont des opérateurs unitaires 2×2. Voici quelques exemples :

- Les Matrices de Pauli

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

  En information quantique, elles s'écrivent simplement $X$, $Y$ et $Z$.
- Le Hadamard gate

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

  et donc : $H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Le Phase Gate

  $$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \text{alors :} \quad S\,|0\rangle = |0\rangle \quad S\,|1\rangle = i\,|1\rangle$$

- Le $\frac{\pi}{8}$-gate

  $$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}$$

Nous pouvons vérifions que :

$$H = \frac{X + Z}{\sqrt{2}} \qquad S = T^2$$

Donc ces portes ne sont pas toutes indépendantes.
Nous allons maintenant introduire la représentation d'un qu-bit sur la sphère de Bloch. Nous définissons deux nouveaux paramètres pour décrire ce qu-bit : $\varphi$ et $\theta$, de la façon suivante

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \text{avec} \quad \alpha = \cos\frac{\theta}{2}e^{-i\frac{\varphi}{2}} \;\text{ et }\; \beta = \sin\frac{\theta}{2}e^{i\frac{\varphi}{2}}$$

Nous considérons le vecteur unitaire ($|\hat{n}| = 1$) :

$$\hat{n} = (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$$

Nous pouvons voir que $|\psi\rangle$ est une vecteur propre de $\hat{n}\cdot\vec{\sigma}$ (Ce vecteur est défini par $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, les matrices de Pauli) avec une valeur propre $+1$. Nous définissons les opérateurs de rotation d'angle $\theta$ autour de l'axe $\hat{n}$ sur la sphère de Bloch :

$$R_{\hat{n}}(\theta) = e^{-i\frac{\hat{n}\cdot\sigma}{2}\theta}$$

Nous pouvons monter que si $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ est un vecteur propre de $\hat{n}_1\cdot\vec{\sigma}$, alors $R_{\hat{n}}(\theta)\,|\psi\rangle$ est un vecteur propre de $\hat{n}_2\cdot\vec{\sigma}$, où $\hat{n}_2$ est obtenu par $\hat{n}_2 = R_{\hat{n}}(\theta)\hat{n}_1$. En particulier, nous pouvons considérer la rotation autour des axes $x$, $y$ et $z$ :

$$\begin{aligned}
R_x(\theta) &= e^{-i\frac{X}{2}\theta} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{pmatrix}\\
R_y(\theta) &= e^{-i\frac{Y}{2}\theta} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y\\
R_z(\theta) &= e^{-i\frac{Z}{2}\theta} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z
\end{aligned}$$

où nous avons exploité $X^2 = Y^2 = Z^2 = I$ et $X^3 = X$, $Y^3 = Y$ et $Z^3 = Z$. De plus, les autres portes logiques peuvent être exprimées en fonction de $R_{\hat{n}}(\theta)$, par exemple :

$$T = e^{i\frac{\pi}{8}}\begin{pmatrix}e^{-i\frac{\pi}{8}} & 0\\ 0 & e^{i\frac{\pi}{8}}\end{pmatrix} = e^{i\frac{\pi}{8}}R_z\left(\frac{\pi}{4}\right)$$

De manière générale, une opération unitaire arbitraire peut toujours être écrite comme

$$U = e^{i\alpha}R_{\hat{n}}(\theta)$$

avec $\alpha$, $\hat{n}$ et $\theta$ choisis.

**Exemple** Hadamard Gate
Nous pouvons décomposer la matrice de la porte de Hadamard pour faire apparaître les rotations autours des axes $x$, $y$, et $z$ grâce les matrices de Pauli et en introduisant des coefficients $n_x$, $n_y$ et $n_z$ :

$$\begin{aligned} H &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= e^{i\alpha}\begin{pmatrix} \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}n_z & -i\sin\frac{\theta}{2}(n_x - in_y) \\ -i\sin\frac{\theta}{2}(n_x + in_y) & \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}n_z \end{pmatrix} \end{aligned}$$

Sur la diagonale, nous voulons avoir +1 et -1 à une phase prêt, il faut donc que $\cos\frac{\theta}{2} = 0$, ce qui implique que $\frac{\theta}{2} = \frac{\pi}{2}$ et donc $\sin\frac{\theta}{2} = 1$. La matrice devient alors :

$$H = e^{i\alpha}\begin{pmatrix} -in_z & -i(n_x - in_y) \\ -i(n_x + in_y) & in_z \end{pmatrix}$$

Pour que $H_{12} = H_{21}$ il faut que $n_y = 0$ et donc $n_z = n_x = \frac{1}{\sqrt{2}}$. Finalement, nous pouvons trouver $\alpha$ :

$$H = \frac{e^{i\alpha}}{\sqrt{2}}\begin{pmatrix} -i & -i \\ -i & i \end{pmatrix} \Rightarrow -ie^{i(\alpha - \frac{\pi}{2})} = 1 \Rightarrow \alpha = \frac{\pi}{2}$$

## Z-X décomposition

**Théorème :** Un opérateur unitaire $U$ sur un qu-bit peut toujours s'écrire comme

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$$

*Preuve*
Les lignes et les colonnes de $U$ sont des vecteurs othornormés, nous pouvons donc les écrire de la façon suivante :

$$U = \begin{pmatrix} e^{i(\alpha - \frac{\beta}{2} - \frac{\delta}{2})}\cos\frac{\gamma}{2} & e^{i(\alpha - \frac{\beta}{2} + \frac{\delta}{2})}\sin\frac{\gamma}{2} \\ e^{i(\alpha + \frac{\beta}{2} - \frac{\delta}{2}}\sin\frac{\gamma}{2} & e^{i(\alpha + \frac{\beta}{2} + \frac{\delta}{2})}\cos\frac{\gamma}{2} \end{pmatrix}$$

pour un choix approprié de $\alpha$, $\beta$, $\gamma$ et $\delta$. Cette expression coïncide avec celle énoncée dans le théorème.

**Corollaire :** Il existent $A$, $B$ et $C$ unitaires avec $ABC = I$ tel que :

$$U = e^{i\alpha}AXBXC$$

*Preuve*
Il suffit de poser :

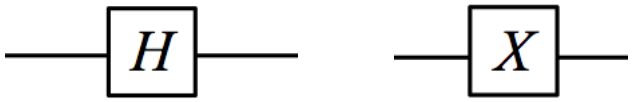
$$A = R_z(\beta)R_y(\frac{\gamma}{2})$$
$$B = R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)$$
$$C = R_z\left(-\frac{\delta-\beta}{2}\right)$$

Et nous avons la preuve directement en utilisant le théorème ci-dessus.

Ce corollaire est très important pour construire des opérations contrôlées à plusieurs qu-bits. Il est aussi utilisé pour introduire des identités entre les portes logiques. L'étudiant intéressé pourra vérifier par exemple :

$$HXH = Z$$
$$HYH = -Y$$
$$HZH = X$$

Les portes logiques sont représentées de la façon suivante :




Dans ces symboles, l'input est à gauche et l'output est à droite.

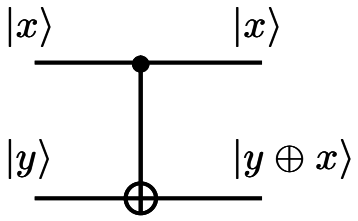
## Opérateurs "controlés

Les opérateurs à deux qu-bits les plus typiques sont les opérateurs contrôlés. Le premier exemple est le $C-NOT$. Ici nous avons un qu-bit de contrôle $|c\rangle$ et un qu-bit $|x\rangle$ sur lequel l'opération se fait :

$$U_{CNOT}\,|c\rangle\,|x\rangle = |c\rangle\,|x \oplus c\rangle$$

L'opérateur sous forme matricielle dans la base computationelle est :

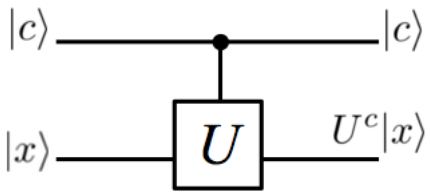
$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$




Et le symbole est : Plus en général, nous pouvons concevoir un opérateur controlled-U, où $U$ est un n'importe quel opérateur à 1 qu-bit. Si $c = 0$, nos pouvons rien faire, mais si $c = 1$ nous appliquons $U$ à $|x\rangle$ :

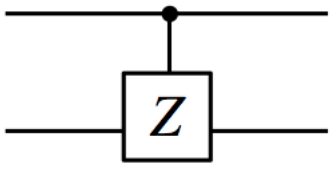
$$|c\rangle\,|x\rangle \rightarrow |c\rangle\,U^c\,|x\rangle$$

Et donc le symbole et l'action sont :

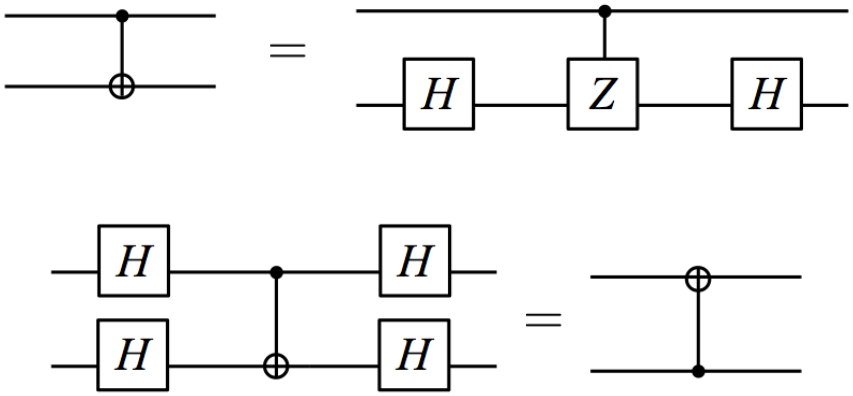



Comme exemple, nous pouvons citer le $C - Z$ gate, dont la matrice et le symbole sont :

$$U_{C-Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$




Il est possible de vérifier les égalités suivantes (en utilisant par exemple la représentation matricielle des opérateurs :

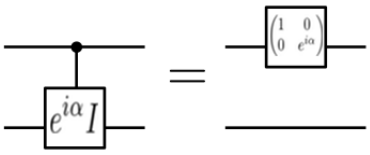



Nous remarquons ici que l'opérateur $C-NOT$ agit comme un inverse si nous utilisons la base $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

Notre but final est de montrer que le $C-NOT$ est une porte universelle qui avec d'autres opérateur à 1 qu-bit permettent de réaliser toutes les opérations possibles. Pour cela, nous allons commencer par montrer qu'une opération $C-U$ peut être composée avec des $C-NOT$ et des opérateurs unitaires à 1 qu-bit. Commençons par le controlled-phase shift, défini par :

Si $|c\rangle = |0\rangle$, rien ne se passe
Si $|c\rangle = |1\rangle$, alors $|x\rangle \to e^{i\alpha}|x\rangle$

Nous allons montrer l'égalité suivante :

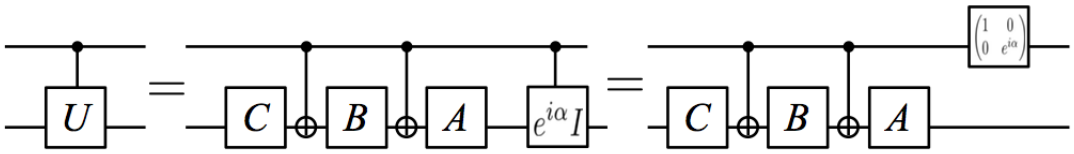



En effet, ce circuit coïncide avec l'application de l'opérateur $U_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ à $|c\rangle$ indépendamment de $|x\rangle$.

$$\begin{aligned} |c\rangle|x\rangle &\to (U_\alpha|c\rangle)|x\rangle \\ &= (U_\alpha \otimes I)(|c\rangle|x\rangle) \end{aligned}$$

$$U_\alpha \otimes I = \begin{pmatrix} U_{\alpha,11}I & U_{\alpha,12}I \\ U_{\alpha,21}I & U_{\alpha,22}I \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}$$

Ce qui correspond exactement au $C-\alpha$. A partir de ce résultat, nous pouvons construire le $C-U$ comme suit : Ce circuit reproduit exactement le résultat




du corollaire précédent, qui dit que :

$$U = e^{i\alpha}AXBXC$$

avec $A$, $B$, $C$ des opérateurs unitaire à 1 qu-bit tels $ABC = I$.Etudions le fonctionnement :

1. $|c\rangle = |1\rangle$
   Alors nous appliquons à $|x\rangle$ dans la suite : $C$, un $NOT$ (qui correspond à $X$),$B$, un autre $X$, $A$ et $e^{i\alpha}$. Le résultat est :

   $$|x\rangle \rightarrow e^{i\alpha}AXBXC\,|x\rangle = U\,|x\rangle$$

2. $|c\rangle = |0\rangle$
   Dans ce cas, on applique $|x\rangle$ dans la suite : $C$, l'identité (un $C-NOT$ sans le bit de contrôle à 1), $B$, l'identité, $A$, l'identité. Le résultat est :

   $$|x\rangle \rightarrow ABC\,|x\rangle = |x\rangle$$

## 7.2 Opérations à plusieurs qu-bits

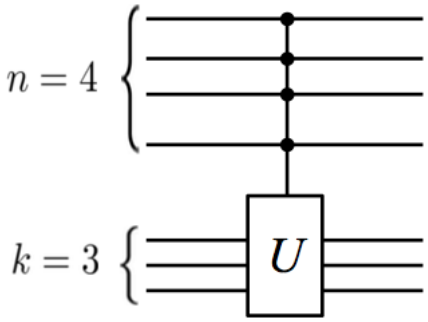
Nous souhaitons aussi faire des opérations contrôlées sur des qu-bits multiples. Supposons d'avoir $n+k$ qu-bits et $U$ est un opérateur qui agit sur $k$ qu-bits. L'opération contrôlée est alors :

$$C^n(U)\,|x_1, x_2, ..., x_n\rangle\,|\psi\rangle = |x_1, x_2, ..., x_n\rangle\,U^{x_1x_2...x_n}\,|\psi\rangle$$

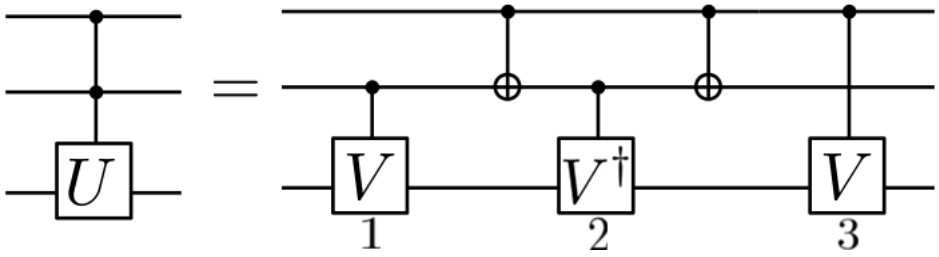
Ici l'état à $n$ qu-bits de contrôle $|x_1, x_2, ..., x_n\rangle$ reste le même, comme pour $C-U$. En plus :

$$|\psi\rangle \to U^{x_1 x_2 ... x_n} |\psi\rangle$$

ici $x_1 x_2 ... x_n$ est le produit algébrique des qu-bits. Il est égal à 1 seulement si $x_1 = x_2 = .. = x_n = 1$, ce qui réalise le contrôle. Le circuit est décrit par le symbole :



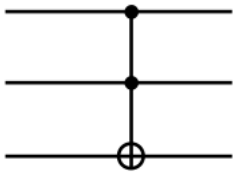

Pour le construire, nous partons du cas avec $k = 1$ (nous pouvons généraliser si nous savons comment réaliser des $U$ à $k > 1$ qu-bits). Définissons l'opérateur $V$ t.q. $V^2 = U$. Dans ce cas, $C^2(u)$ est donné par :



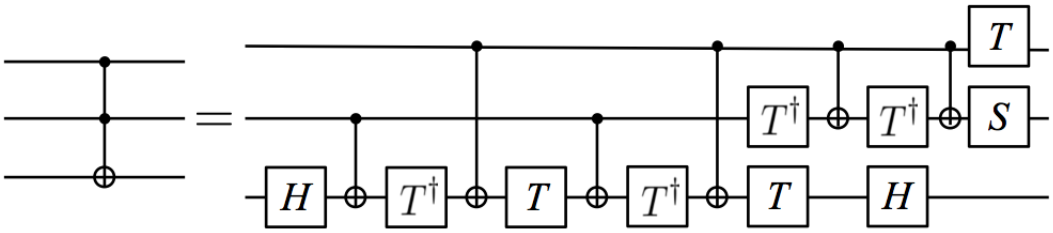

*Preuve*

- $|x_1 x_2\rangle = |00\rangle$
  $|\psi\rangle \underset{1}{\longrightarrow} |\psi\rangle \underset{2}{\longrightarrow} |\psi\rangle \underset{3}{\longrightarrow} |\psi\rangle$
- $|x_1 x_2\rangle = |01\rangle$
  $|\psi\rangle \underset{1}{\longrightarrow} V|\psi\rangle \underset{2}{\longrightarrow} V^\dagger V|\psi\rangle = |\psi\rangle \underset{3}{\longrightarrow} |\psi\rangle$
- $|x_1 x_2\rangle = |10\rangle$
  $|\psi\rangle \underset{1}{\longrightarrow} |\psi\rangle \underset{2}{\longrightarrow} V^\dagger|\psi\rangle \underset{3}{\longrightarrow} VV^\dagger|\psi\rangle = |\psi\rangle$
- $|x_1 x_2\rangle = |11\rangle$
  $|\psi\rangle \underset{1}{\longrightarrow} V|\psi\rangle \underset{2}{\longrightarrow} V|\psi\rangle \underset{3}{\longrightarrow} V^2|\psi\rangle = U|\psi\rangle$

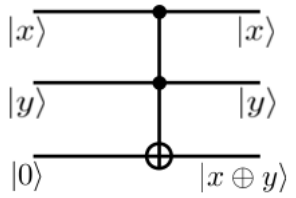
*Cas spécial : $U = X$*
Nous définissons $V = \frac{1-i}{2}(I + iX)$, $V^2 = x$ et nous avons le circuit :



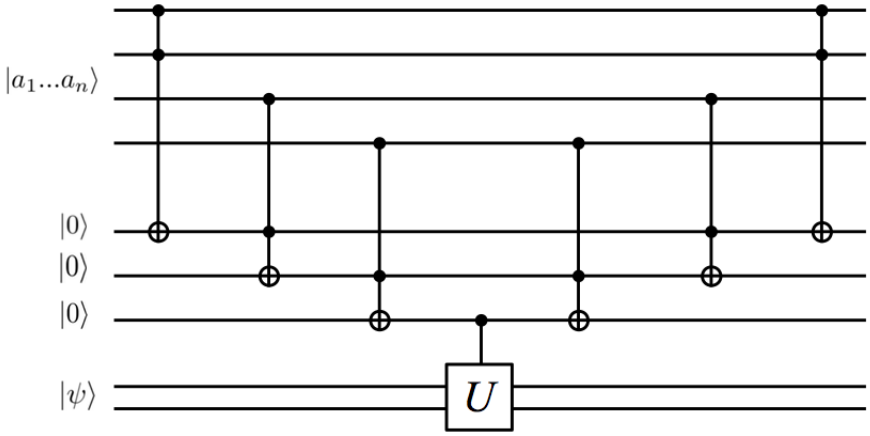
qui est connu comme le Toffoli gate. Il est très important en information classique et est une porte réversible. Nous pouvons montrer qu'il s'agit de la pus petite porte logique nécessaire pour fonctionner comme porte logique universelle pour l'information classique *réversible*.
Nous ne pouvons pas faire de l'information classique réversible en n'utilisant que des portes à 1 et 2 qu-bits. Il est remarquable que par contre en information quantique, la porte de Toffoli puisse se construire à partir d'opération à 1 et 2 qu-bits. C'est un bel exemple de comme l'information quantique mette à disposition des ressources additionnelles.
Nous allons montrer par la suite que tous les circuits quantiques peuvent être construits à partir des opérations $H$, $S$, $C - NOT$ et $T$. Il est intéressant de montrer que c'est le cas pour le Toffoli gate (à vérifier) :



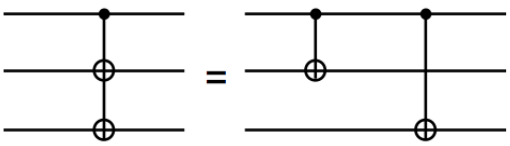

Il est aussi simple de voir que le Toffoli gate permet de réaliser un $AND$ sur la base computationnelle :




Nous l'utilisons aussi pour faire un autre type de $C^n(U)$ qui n'utilise pas de $V$ (donc si nous savons faire $U$, nous pouvons de même faire $C^n(U)$).




Ce circuit utilise $n-1$ qu-bits de travail, qui sont initialisés à $|0\rangle$ en entrée. De cette manière, nous faisons $a_1 AND a_2$, puis $(a_1 AND a_2) AND a_3$, etc. A la fin, nous avons un $C(U)$ en input sur le contrôle $a_1 \oplus a_2 \oplus ... \oplus a_n$. ce qui correspond à $C^n(U)$. Ensuite le circuit applique les AND à l'inverse pour remettre les bits de contrôle et de travail dans l'état initial.
Nous pouvons aussi construire des opérations sur des qu-bits multiples. Exemple : $C-NOT$ à 2 qu-bits :



## 7.3 Processus de mesure dans les circuits quantiques

Chaque circuit utilisé pour du calcul quantique implique un ou plusieurs processus de mesure à la fin ou même au milieu du circuit. Ici, nous allons nous restreindre aux mesures dites *projectives*. Une mesure projective est caractérisée par un opérateur observable qui est un projecteur :

$$P_\psi = |\psi\rangle \langle\psi|$$

Nous pouvons voir ceci comme un élément s'une observable plus complexe qui s'exprime selon sa représentation spectrale comme :

$$A = \sum_j a_j |\psi_j\rangle \langle\psi_j|$$

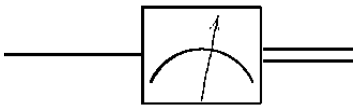
Par exemple, un filtre polariseur qui projette l'état du photon dans la direction $\theta$ peut être vu comme un opérateur (un projecteur) :

$$P_\theta = |\theta\rangle \langle\theta|$$

Nous allons uniquement considérer les mesures sur la base computationnelle,c'est-à-dire les opérateurs :

$$P_0 = |0\rangle \langle 0|$$
$$P_1 = |1\rangle \langle 1|$$

Chaque autre mesure peut s'obtenir par une transformation unitaire et une mesure du type $P_0$ ou $P_1$ ensuite. Nous indiquons la mesure par le symbole :

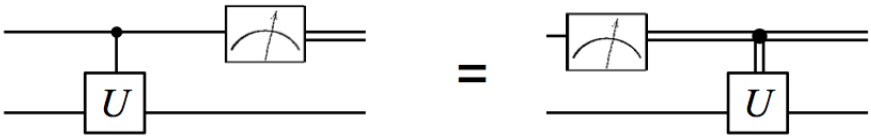


La double ligne indique un circuit classique qui contient le résultat (0 ou 1) de la mesure.

Concernant la mesure dans les circuits quantiques, nous pouvons énoncer deux principe fondamentaux.

1. **Principe de la mesure différée**
   Une mesure peut toujours être différée à la fin du circuit. En particulier, si au milieu d'un circuit, nous devons faire une mesure dont le résultat

est utilisé pour contrôler une partie du circuit, nous pouvons remplacer le contrôle classique par un contrôle quantique et déplacer la mesure à la fin. Pour bien comprendre, prenons l'exemple suivant :




Les deux circuits ci-dessus sont totalement équivalents. Commençons par le prouver pour des états purs. L'entrée la plus générale est :

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

Selon le premier circuit, après le $C(U)$, on a :

$$|\psi'\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|1\rangle \otimes U\,|0\rangle + \delta\,|1\rangle \otimes U\,|1\rangle$$

Si maintenant, nous mesurons le qu-bit 1, nous avons deux possibilités :

$$\begin{aligned} 0_1 \to |\varphi_2\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ 1_1 \to |\varphi_2\rangle &= U(\gamma\,|0\rangle + \delta\,|1\rangle) \end{aligned}$$

(La probabilité des deux résultats est $|\alpha|^2 + |\beta|^2$ et $|\gamma|^2 + |\delta|^2$ respectivement).
Etudions maintenant le deuxième circuit. Ici la mesure est effectuée sur $|\psi\rangle$. Donc, nos avons a nouveau deux possibilités :

$$\begin{aligned} 0_1 \to |\psi\rangle \to |\psi''\rangle &= |0_1\rangle\,(\alpha\,|0_2\rangle + \beta\,|1_2\rangle) \\ 1_1 \to |\psi\rangle \to |\psi''\rangle &= |1_1\rangle\,(\gamma\,|0_2\rangle + \delta\,|1_2\rangle) \end{aligned}$$

Dans le deuxième cas, le contrôle classique sur $U$ est présent et le deuxième bit devient :

$$|\varphi''\rangle = U(\gamma\,|0_2\rangle + \delta\,|1_2\rangle)$$

Dans le premier cas, il n'y a pas de contrôle et

$$|\varphi''\rangle = \alpha\,|0_2\rangle + \beta\,|1_2\rangle$$

Les deux circuits coïncident donc bien.
Il est utile de répéter la preuve pour un input donnée par une matrice densité. Pour cela, il est toutefois plus judicieux d'introduire le deuxième principe.

**2. Principe de la mesure implicite**

Sans perte de généralité, chaque ligne de circuit non terminée à la fin d'un circuit peut-être considérée comme mesurée (mais sans connaître le résultat de la mesure).

Pour bien comprendre ce principe, il faut reprendre la théorie de la matrice densité et étudier comment elle change après une mesure : Nous nous posons le problème de trouver la matrice densité d'un système après que nous ayant effectué une mesure d'une observable $A$. Considérons la représentation spectrale de $A$ :

$$A = \sum_m a_m |m\rangle \langle m| = \sum_m a_m P_m$$

où nous avons indiqué $P_m = |m\rangle \langle m|$, le projecteur sur l'état propre $|m\rangle$ de $A$.

Le système se trouve au début dans un état décrit par la matrice densité $\rho$. Donc les probabilités de mesurer chaque valeur propre $a_m$ sont :

$$p(m) = \langle m| \rho |m\rangle$$

Nous pouvons exprimer $\rho$ comme un mélange d'états $|\psi_i\rangle$ avec probabilité $p(i)$ :

$$\rho = \sum_i p(i) |\psi_i\rangle \langle \psi_i|$$

Sur chaque état pur $|\psi_i\rangle$, le fait de mesurer $a_m$ projette l'état sur $|m\rangle$. Donc si nous avons mesuré $a_m$, nous pouvons définir la matrice densité $\rho_m$ du système après mesure :

$$\rho_m = \sum_i p(i|m) \frac{P_m |\psi_i\rangle \langle \psi_i| P_m}{|\langle m| \psi_i\rangle|^2}$$

Ici, nous avons utilisé l'identité :

$$|m\rangle = \frac{P_m |\psi_i\rangle}{\langle m| \psi_i\rangle} = \frac{|m\rangle \langle m| \psi_i\rangle}{\langle m| \psi_i\rangle}$$

Nous pouvons considérer cette identité valable même dans le cas $\langle m| \psi_i\rangle = 0$ : il suffit de prendre la limite de $|\psi_i'\rangle = |\psi_i\rangle + \epsilon |\varphi_i\rangle$ pour $\epsilon \to 0$ avec $|\varphi_i\rangle$ tel que $\langle m| \varphi_i\rangle \neq 0$.

Nous avons aussi introduit la probabilité conditionnelle $p(i|m)$ : probabilité de se trouver dans l'état $|\psi\rangle$ à condition d'avoir mesuré $a_m$. Les lois élémentaires de la théorie des probabilités nous disent que :

$$p(i|m)p(m) = p(i,m) = p(m,i) = p(m|i)p(i)$$

c'est-à-dire la probabilité totale de mesurer $i$ ET $m$ est donnée par la probabilité de mesurer $i$ à condition d'avoir mesuré $m$, multiplié par la probabilité de mesurer $m$. La deuxième égalité est évidente, et la troisième s'explique par le même argument que ci-dessus (avec les rôle de $m$ et $i$ échangés).
Nous remarquons que $p(i|i)$ est la probabilité de mesurer $m$ à condition que le système soit dans l'état $|\psi_i\rangle$, donc est par :

$$P(m|i) = |\langle m|\psi_i\rangle|^2$$

Pour finir, nous remplaçons l'expression pour $p(i|m)$ dans l'équation pour $\rho_m$ :

$$\begin{aligned}\rho_m &= \sum_i \frac{p(m|i)p(i)}{p(m)} \frac{P_m |\psi_i\rangle \langle\psi_i| P_m}{|\langle m|\psi_i\rangle|^2} \\ &= \sum_i \frac{p(i)}{p(m)} \frac{|\langle m|\psi_i\rangle|^2}{|\langle m|\psi_i\rangle|^2} P_m |\psi_i\rangle \langle\psi_i| P_m \\ &= \frac{P_m \rho P_m}{p(m)} = \frac{P_m \rho P_m}{\langle m|\rho|m\rangle}\end{aligned}$$

Nous remarquons que cette expression a été obtenue avec l'hypothèse que la mesure de $A$ a donné la valeur $a_m$.
Supposons maintenant que nous préparons beaucoup de répliques identiques du système dans le même état $\rho$. Avant de recevoir chaque système, un agent externe effectue une mesure de $A$. Pour chaque réplique, il obtient une valeur $a_m$ avec une probabilité $p(m)$. Donc, nous allons avoir la matrice $\rho_m$ avec une probabilité $p(m)$.
Puisque nous ne connaissons pas le résultat des mesures de l'agent, pour nous, les répliques du système se comporteront comme un ensemble statistique de systèmes dans des états $\rho_m$ avec probabilité $p(m)$. Donc, toutes nos mesures sur les systèmes seront décrites par une matrice densité qui définie par :

$$\begin{aligned}\rho' &= \sum_m p(m)\rho_m = \sum_m p(m) \frac{P_m \rho P_m}{p(m)} \\ &= \sum_m P_m \rho P_m\end{aligned}$$

Ce résultat est très important en information quantique. Il nous dit que, après avoir effectué une mesure sur le système $\rho$, son état est différent pour un observateur qui connaît le résultat de la mesure (dans ce cas $\rho \to \rho_m$) et un autre observateur qui ne connaît pas le résultat (ici, $\rho \to \sum_m P_m \rho P_m$).

Nous appliquerons ce résultat aux circuits quantiques, pour déterminer la matrice densité d'une ligne de circuit, en supposant qu'une mesure a été effectuée sur l'autre ligne mais sans connaître le résultat.
Il est important de souligner que ce résultat s'applique également au de valeurs propres dégénérées. Supposons que $S$ soit un sous-système de deux vecteurs propres $a_{m_1} = a_{m_2}$. Pour un état $|\psi_i\rangle$, nous avons après la mesure :

$$|\psi_i\rangle \to P_S |\psi_i\rangle = \frac{|m_1\rangle \langle m_1|\psi_i\rangle + |m_2\rangle \langle m_2|\psi_i\rangle}{|\langle m_1|\psi_i\rangle|^2 + |\langle m_2|\psi_i\rangle|^2}$$

Nous pouvons réécrire $\rho_m$ avec l'état $P_S |\psi_i\rangle$ comme un des états de la base ou $\rho_m$ est diagonale. La relation $p(i|m)p(m) = p(m|i)p(i)$ reste valable.Ici,

$$p(m) = \langle m_1| \rho |m_1\rangle + \langle m_2| \rho |m_2\rangle$$

et $p(i|m)$ est la probabilité d'être en $|\psi_i\rangle$ à condition d'avoir mesuré $m_1$ ou $m_2$.

$$p(m|i) = |\langle m_1|\psi_i\rangle|^2 + |\langle m_2|\psi_i\rangle|^2$$

Nous retrouvons

$$\rho_A = \frac{P_S \rho P_S}{p(m)}$$

et par conséquent

$$\rho' = \sum_m P_m \rho P_m$$

où la somme est maintenant considérée sur tous les sous-espaces dégénérés.

Considérons maintenant un circuit à 2 qu-bits dont la sortie est décrite par la matrice densité $\rho$. Si nous effectuons une mesure sur le 1er qu-bit, nous pouvons calculer la matrice $\rho'$ après mesure. Nous supposons de ne pas connaître le résultat de la mesure :

$$\rho' = \sum_m P_m \rho P_m$$

Ici $P_m$ est le projecteur dans le sous-espace du système à 2 qu-bits correspondant au premier qu-bit en $|0\rangle$ ou $|1\rangle$ respectivement :

$$P_0 = |0_1\rangle \langle 0_1| \otimes I_2$$
$$P_1 = |1_1\rangle \langle 1_1| \otimes I_2$$

Donc

$$P_0 \rho P_0 = \begin{pmatrix} \rho_{11} & \rho_{12} & 0 & 0 \\ \rho_{21} & \rho_{22} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$P_1 \rho P_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \rho_{33} & \rho_{34} \\ 0 & 0 & \rho_{43} & \rho_{44} \end{pmatrix}$$

Et

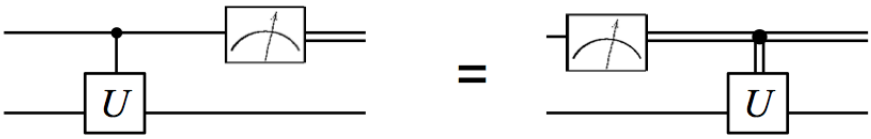
$$\rho' = \begin{pmatrix} \rho_{11} & \rho_{12} & 0 & 0 \\ \rho_{21} & \rho_{22} & 0 & 0 \\ 0 & 0 & \rho_{33} & \rho_{34} \\ 0 & 0 & \rho_{43} & \rho_{44} \end{pmatrix}$$

Nous voulons calculer les matrices $\rho_2 = Tr_1(\rho)$ et $\rho'_2 = Tr_1(\rho')$. Nous avons :

$$\rho_2 = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} + \begin{pmatrix} \rho_{33} & \rho_{34} \\ \rho_{43} & \rho_{44} \end{pmatrix}$$

et nous avons le même résultat pour $\rho'_2$.
$\rho_2 = \rho'_2$ signifie que la mesure effectuée sur le qu-bit 1 ne change pas l'information quantique dans le qu-bit 2. Ceci est une preuve du principe de la mesure implicite.

Revenons à l'exemple de $C(U)$ :




Pour le premier circuit, nous avons :

$$C(U) = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

(Nous utilisons une notation en blocs 2x2 : $\rho = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix}$ avec $\rho_{ij}$ matrice 2x2). Nous avons :

$$\begin{aligned} \rho' &= C(U)\rho C(U)^\dagger \\ &= \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & U^\dagger \end{pmatrix} \\ &= \begin{pmatrix} \rho_{11} & \rho_{12}U^\dagger \\ U\rho_{21} & U\rho_{22}U^\dagger \end{pmatrix} \end{aligned}$$

Pour le 2ème qu-bit la matrice densité réduite est :

$$\rho^{(1)} = Tr_1(\rho') = \rho_{11} + U\rho_{22}U^\dagger$$

Dans le deuxième cas, nous avons $\rho \to \rho'$ à cause de la mesure. Nous venons de voir :

$$\rho' = P_0\rho P_0 + P_1\rho P_1 = \begin{pmatrix} \rho_{11} & 0 \\ 0 & \rho_{22} \end{pmatrix}$$

Maintenant si le 1er qu-bit est mesuré à 0, nous ne faisons rien et $\rho_{11} \to \rho_{11}$. Si le 1er qu-bit est mesuré à 1, nous appliquons $\rho_{22} \to U\rho_2 2U^\dagger$.
Donc après le $C(U)$, nous avons :

$$\rho' \to \rho'' = \begin{pmatrix} \rho_{11} & 0 \\ 0 & U\rho_{22}U^\dagger \end{pmatrix}$$

Et pour le 2ème qu-bit :

$$\rho^{(2)} = Tr_1(\rho'') = \rho_{11} + U\rho_{22}U^\dagger$$

Les deux circuits coïncident donc bien même pour un input donné par une matrice densité. Nous pouvons conclure que, pour une porte logique quantique, nous devons pouvoir effectuer une mesure sur chaque ligne, sur la base computationnelle.

## 7.4 One-way quantum computing

Commençons par illustrer un protocole de téléportation quantique un peu différent de celui traité auparavant. Alice et Bob partagent un intriqué de type :

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle \otimes |0\rangle + |-\rangle \otimes |1\rangle\right)$$

Cet état est intriqué tout comme un état de Bell (nous pourrions renommer $|+\rangle \to |0\rangle$ et $|-\rangle \to |1\rangle$). Remarquons que cet état est aussi égal à :

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |+\rangle + |1\rangle \otimes |-\rangle\right)$$

Nous voulons téléporter l'état $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. L'état initial est donc :

$$|\varphi\rangle \otimes |\psi\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \frac{1}{\sqrt{2}}\left(|+0\rangle + |-1\rangle\right)$$

Alice applique maintenant un C(Z) à ses deux qu-bits. Le résultat est :

$$\frac{1}{\sqrt{2}}\left[\alpha\left(|0+0\rangle + |0-1\rangle\right) + \beta\left(|1+0\rangle + |1-1\rangle\right)\right]$$

(Nous remarquons que $C(Z)$ agit sur la base $\{|+\rangle, |-\rangle\}$ pour le 2ème qu-bit comme un C(NOT) sur la base $\{|0\rangle, |1\rangle\}$). Exprimons le 1er qu-bit dans la base $\{|+\rangle, |-\rangle\}$ :

$$\frac{1}{\sqrt{2}}[\alpha(|++0\rangle + |-+0\rangle + |+-1\rangle + |--1\rangle) + \beta(|+-0\rangle + |--0\rangle + |++1\rangle + |-+1\rangle)]$$

que nous pouvons réexprimer comme :

$$\frac{1}{\sqrt{2}}[|++\rangle(\alpha|0\rangle + \beta|1\rangle + |+-\rangle(|1\rangle + \beta|0\rangle) |-+\rangle(\alpha|0\rangle - \beta|1\rangle) + |--\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

Nous voyons qu'une mesure sur la base $\{|+\rangle, |-\rangle\}$ pour les 2 qu-bits d'Alice permet de réaliser la téléportation avec une probabilité 100 %, pourvu que Bob applique ses opérateurs $\sigma_x$, $\sigma_z$ selon le résultat de la mesure d'Alice. Nous remarquons que dans la première partie, Alice n'a du applique qu'un $C(Z)$, sans aucun Hadamard. Un $C(Z)$ dans la base computationnnelle est donné par :

$$C(Z) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Maintenant, il faut encore savoir comment construire l'état $|\psi\rangle$. Il est intéressant de voir que cet état est issu de l'état $|++\rangle$ après l'application d'un $C(Z)$ :

$$\begin{aligned} C(Z)|++\rangle &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|+0\rangle + |-1\rangle) \end{aligned}$$

Donc le même opérateur qu'Alice utilise pour la téléportation est aussi nécessaire pour préparer l'état intriqué. Supposons maintenant que $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ soit l'état initial d'un qu-bit dans un circuit quantique. Réexprimons-le dans la base $\{|+\rangle, |-\rangle\}$ :

$$\begin{aligned} |\varphi\rangle &= \alpha'|+\rangle + \beta'|-\rangle \\ &= (\alpha' + \beta'\sigma_z)|+\rangle \end{aligned}$$

Pour notre téléportation nous pouvons donc partir de l'état $|+++\rangle$ et appliquer :

$$C(Z)_{12}(\alpha' I + \beta\sigma_{z1})C(Z)_{23}\,|+++\rangle$$

et il manque juste de mesurer les qu-bits 1,2 et d'appliquer les opérateurs $\sigma_x$, $\sigma_z$ correspondant au qu-bit 3. Or, les trois opérateurs ci-dessus commutent comme nous le voyons facilement dans la base computationnelle. Donc le protocole est équivalent à :

$$(\alpha' I + \beta\sigma_{z1})C(Z)_{12}C(Z)_{23}\,|+++\rangle$$

L'état $C(Z)_{12}C(Z)_{23}\,|+++\rangle$ est un *cluster state*. Nous voyons qu'il est une ressource universelle pour la téléportation si nous sommes capable de le créer, après la téléportation consiste simplement en des opérations à 1 qu-bit, mesures 1 à un qu-bit et des communications classiques. Nous pouvons itérer le processus. Par exemple :

$$C(Z)_{12}C(Z)_{23}C(Z)_{34}C(Z)_{45}\,|+++++\rangle$$

permet la téléportation d'un état inscrit sur le 1er qu-bit au 3ème et de là sur le 5ème en itérant la procédure.

Nous venons de créer un protocole de "conducteur" quantique, qui nous permet par des opérations à 1 qu-bit de transporter l'état d'un qu-bit le long d'un "fil" (nous imaginons les $2n+1$ qu-bits alignés sur une chaine), pourvu que nous arrivons é préparer le cluster state initial.
Un cluster state d'un network de qu-bits est défini à partir d'un Hamiltonien :

$$H = g \sum_{\langle a,a'\rangle} \frac{1+\sigma_z^{(a)}}{2} \otimes \frac{1-\sigma_z^{(a)}}{2}$$

où $\langle a, a'\rangle$ compte les paires de premiers voisins (les noeuds connectés par une seule ligne, dans le sens des réseaux). L'opérateur d'évolution temporelle correspondant est :

$$U(t,0) = \exp\left(-ig \sum_{\langle a,a'\rangle} \frac{1+\sigma_z^{(a)}}{2} \otimes \frac{1-\sigma_z^{(a)}}{2}\right) \tag{7.1}$$

Pour $gt = \pi$ en particulier, nous avons $U\,|+++...++\rangle = |\psi_C\rangle$ l'état cluster qui nous intéresse. Remarquons que :

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow \frac{1+\sigma_z}{2} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

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

et que :

$$\frac{1+\sigma_z^{(1)}}{2} \otimes \frac{1-\sigma_z^{(2)}}{2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

et donc :

$$U_{12} = \exp\left(-i\pi \frac{1+\sigma_z^{(1)}}{2} \otimes \frac{1-\sigma_z^{(2)}}{2}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = C(Z)_{12}$$

De plus, nous voyons que les matrices à l'exposant 7.1 pour différentes paires de qu-bits commutent, donc nous pouvons factoriser l'exponentiel en produit d'exponentielles. Pour finir nous avons donc :

$$U = \prod_{\langle a,a' \rangle} C(Z)_{a,a'}$$

Ces états dépendent donc de la topologie du réseau de qu-bits. Ils satisfont à une propriété générale :

$$\sigma_x^{(a)} \otimes_{a'=voisin(a)} \sigma_z^{(a')} \left|\psi_C\right\rangle = \pm \left|\psi_C\right\rangle$$

ou la valeur propre $\pm$ dépend de la topologie du réseau. Cette propriété est essentielle pour la réalisation du protocole. Nous remarquons également que le Hamiltonien :

$$\begin{aligned} H &= g \sum_{\langle a,a' \rangle} \frac{1+\sigma_z^{(1)}}{2} \otimes \frac{1-\sigma_z^{(2)}}{2} \\ &= -\frac{1}{4} g \sum_{\langle a,a' \rangle} \sigma_z^{(a)} \otimes \sigma_z^{(a')} \end{aligned}$$

à moins de l'identité et d'opérations à un seul qu-bit. Donc l'Hamiltonien de préparation d'un cluster state peut être préparé à partir d'une interaction spin-spin typique, si nous pouvons contrôler le temps pendant lequel elle agit. Nous pouvons faire mieux. Une opération arbitraire à 1 q-bit $U_R(\xi, \eta, \zeta) = U_x(\zeta)U_z(\eta)U_x(\xi)$ peut être effectuée par des mesures, pendant la téléportation. Si nous avons un état :

$$\left|\psi_{in}\right\rangle \left|++++\right\rangle = (\alpha I_1 + \beta\sigma_{z1}) \left|+++++\right\rangle$$

Nous appliquons d'abord $U$ :

$$(\alpha I_1 + \beta\sigma_{z1}) U \left|+++++\right\rangle$$

Puis nous effectuons la téléportation en mesurant sur chacun des 4 qu-bits la base :

$$B_j(\alpha_j) = \left\{ \frac{|0\rangle_j + e^{i\alpha_j}|1\rangle_j}{\sqrt{2}}, \frac{|0\rangle_j - e^{i\alpha_j}|1\rangle_j}{\sqrt{2}} \right\}$$

avec $j = 1, 2, 3, 4$. Si nous posons $\alpha_1 = 0$, l'état final sera :

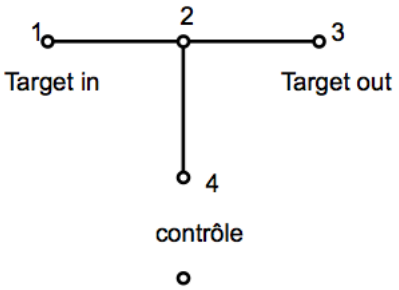
$$|s_1\rangle_{\alpha_1} \otimes |s_2\rangle_{\alpha_2} \otimes |s_3\rangle_{\alpha_3} \otimes |s_4\rangle_{\alpha_4} \otimes |\psi_{out}\rangle$$

Ici pour chaque qu-bit $|s_j\rangle_{\alpha_j} = \{|0_j\rangle_{\alpha_j}, |1\rangle_{\alpha_j}\}$, c'est la base si-dessus. Donc : $s_j = 0, 1$. Nous pouvons donc montrer que :

$$|\psi_{out}\rangle = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}U_R\left((-1)^{s_1+1}\alpha_2, (-1)^{s_2}\alpha_3, (-1)^{s_1+s_3}\alpha_4\right)$$

Il suffit donc de choisir : $(-1)^{s_1+1}\alpha_2 = \xi$ (ici $s_1$ vient de la mesure précédente), $(-1)^{s_2}\alpha_3 = \eta$ ($s_2$ vient de la mesure précédente) et $(-1)^{s_1+s_3}\alpha_4 = \zeta$ ($s_1$ et $s_2$ viennent des mesures précédentes) et d'"annuler" après les $\sigma_x$ et $\sigma_z$.

Comment faire un $C(NOT)$ ? Nous choisissons le réseau de qu-bit suivant :




Ceci correspond à un état de cluster :

$$C(Z)_{24}C(Z)_{23}C(Z)_{12}|++++\rangle$$

Après nous inscrivons le target-in et le contrôle en 1 et le 4 respectivement.

$$(\alpha_1 I_1 + \beta_1\sigma_{z1})(\alpha_4 I_4 + \beta_4\sigma_{z4})C(Z)_{24}C(Z)_{23}C(Z)_{12}|++++\rangle$$

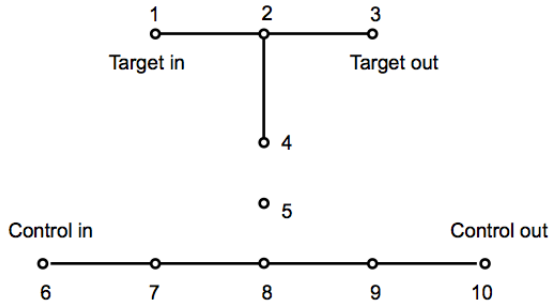
où : $|\psi_1\rangle = \alpha_1|+\rangle + \beta_1|-\rangle$ et $|\psi_4\rangle = \alpha_4|+\rangle + \beta_4|-\rangle$. Puis nous mesurons les qu-bits 1 et 2 sur la base $\{|+\rangle, |-\rangle\}$ et nous obtenons $|s_1 s_2\rangle$. Nous pouvons montrer que l'état final est :

$$|s_1\rangle_1 \otimes |s_2\rangle_2 \otimes U_{34}|i_4\rangle_4 \otimes |i_1 \oplus i_4\rangle_3$$

Si $|\psi_1\rangle = |i_1\rangle$ et $|\psi_4\rangle = |i_4\rangle$ sont choisis dans la base computatinnelle $i_j = 0, 1$. Ici :

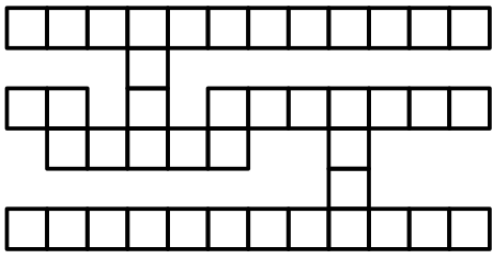
$$U_{34} = \sigma_{z3}^{s_1+1}\sigma_{x3}^{s_2}\sigma_{z4}^{s_1}$$

Il faut donc "annuler" ce dernier opérateur après le circuit pour réaliser le $C(NOT)$. Si de plus, nous pouvons avoir un circuit $C(NOT)$ "traditionnel" avec deux entrée et 2 sortie, nous pouvons montrer que le "circuit" à utiliser est :

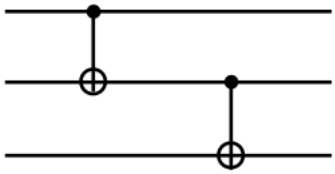



où les mesure dur la base $\{|+\rangle, |-\rangle\}$ sont effectuées sur les qu-bits 1, 2, 4, 5, 6, 7, 8, 9.

Une remarque importante est que dans un circuit quantique, l'output est l'input de l'autre. Puisque nous avons vu que l'opérateur $U$ pour créer le cluster state commute avec la création de l'état initial, il est clair que $U$ peut être effectué tout au début pour tout circuit.
De plus, nous pouvons remplacer la préparation de l'état initial par un bout de circuit qui effectue des rotations appropriés à partir de $|+++++\rangle$ pour chaque qu-bit. Nou voyons donc que le cluster state est une ressource universelle pour le cicuit quantique. Par exemple, le réseau de qu-bits suivant :



peut être utilisé pour effectuer la circuit quantique suivant



Pourvu que nous mesurons les qu-bits justes dans la base $\{|+\rangle, |-\rangle\}$ selon les prescriptions de la téléportation et du $C(NOT)$.

# 8 Réalisations physiques de qu-bits

Nous allons maintenant discuter les différentes tentatives de réaliser pratiquement des systèmes de plusieurs qu-bits. Le progrès dans ce domaine est très rapide. Cependant, nous ne connaissons pas encore la technologie idéale pour une telle réalisation pratique. Il y a à présent cinq classes de systèmes physiques candidats pour cette réalisation, avec des nombreuses sous-variantes. Chaque classe présente des avantages et des inconvénients. Avant de les examiner, il faut bien spécifier quelles sont les caractéristiques que nous demandons d'une réalisation pratique d'une porte logique quantique. Ces conditions ont été caractérisée avec précision par le travail de plusieurs scientifiques dans le domaine de l'information quantique. Ils sont résumés par *les cinq critères de DiVincenzo*, d'après David P. Di Vincenzo, le celèbre scientifique de IBM qui est un des pères de l'information quantique. [2]

1. Le système physique d'un et de plusieurs qu-bits doit être bien caractérisé. Il doit aussi être "scalable".
2. Nous devons pouvoir initialiser l'état des qu-bits à un état de départ bien déterminé, par exemple $|000\ldots\rangle$.
3. Le temps de décohérence doit être beaucoup plus long que le temps que prend une opération effectuée par une porte logique.
4. Le système doit pouvoir reproduire le fonctionnement d'un ensemble universel de portes logiques quantiques (p.e. le $C-NOT$ et certains opérations à un qu-bit).
5. Nous devons pouvoir effectuer des mesures sur chaque qu-bit individuellement.

Nous allons discuter ces critères.

## 8.1 Le système physique d'un et de plusieurs qu-bits doit être bien caractérisé et scalable

Nous avons déjà vu quel est le modèle mathématique d'un qu-bit et discuté certains systèmes physiques qui le reproduisent. Un qu-bit pourrait être un photon avec ses degrés de liberté de polarisation ; le spin d'une particule ; deux états électroniques parmi les plusieurs qui caractérisent un atome ou une molécule ; etc. "Bien caractérisé" veut dire qu'on connaît tous ses paramètres physiques. En particulier, il faut bien connaître l'Hamiltonien du système, la présence et le couplage avec d'autres états du qu-bit (souvent

2. David P. DiVincenzo, *The Physical Implementation of Quantum Computation*, `arXiv:quant-ph/0002077` (2000)

non désirés), l'interaction avec d'autres qu-bits, le couplage avec des champs externes qui pourraient être utilisés pour manipuler le qu-bit. En particulier, si le qu-bit a d'autres états que les deux choisis pour représenter $|0\rangle$ et $|1\rangle$, il faut que la probabilité d'aller dans ces états (par le champ externe ou par l'évolution propre du système) soit petite. Combien petite, dépend des techniques de correction d'erreur quantique qu'on sait mettre en place pour ce système.
Il y a à présent cinq classes de systèmes qui ont été envisagés pour réaliser de qu-bits :

1. Etat de polarisation d'un photon (possiblement couplé à un atome dans une cavité électromagnétique).
2. Le spin d'un noyaux atomique dans une molécule, par la technique de RMN
3. Les niveaux électroniques de ions piégés dans un champ électromagnétique
4. Les degrés de liberté (spin ou orbitaux) des électrons dans des boîtes quantiques à semiconducteur
5. Les états quantisés des courants dans des dispositifs supraconducteurs.

Pour chaque classe il y a un grand nombre de variations, que nous discuterons par la suite.

## 8.2 On doit pouvoir initialiser l'état des qu-bits à un état de départ bien déterminé

Ce critère est évident, puisque pour chaque opération quantique il faut initialiser l'input du système. L'opération d'initialisation demande qu'on connaisse l'état de départ de chaque qu-bit, puisque il faut le faire évoluer dans l'état qui constitue l'input du calcul. Il y a une autre raison. Les techniques de correction d'erreur nécessitent d'un grand nombre de qu-bits préparés dans l'état $|0\rangle$.
Pour initialiser un qu-bit il faut un temps caractéristique, qui dépend de la manière dont cette initialisation a lieu. Il faut que ce temps soit court ou comparable au temps nécessaire pour l'opération quantique. En effet, les opérations quantiques sont produites par une évolution temporelle dictée par un Hamiltonien. On ne peut pas faire un pause dans un calcul quantique. Donc, si pour préparer l'état initial du calcul suivant il faut plus longtemps que pour l'opération précédente, alors il faut penser à préparer à l'avance un grand nombre de qu-bits dans l'état standard et puis les transporter partout dans l'ordinateur quantique.

Il y a deux manières d'initialiser un qu-bit. La première est par le mécanisme de *relaxation*, qui mène naturellement le système dans son état fondamental si la température est suffisamment basse. L'autre méthode est simplement par une opération de mesure, qui permet le projection du système dans un état spécifique. La deuxième approche est à préférer puisque sa durée est la même des opérations quantiques (aussi bien la mesure que la manipulation sont effectuées par l'interaction contrôlée avec un agent externe). La relaxation par contre, a par définition la même durée que la décohérence. Ce type d'initialisation donc n'est possible que si on dispose d'une méthode de correction d'erreur quantique assez efficace. Dans des système comme par exemple le RMN de molécules complexes, l'initialisation s'avère tellement difficile, que pour l'instant on y renonce. On utilise par contre une méthode statistique : on travaille sur un grand nombre de répliques du système ($10^{18}$ au minimum, chaque système étant une molécule), sachant que statistiquement il y aura une fraction de ces répliques qui seront dans l'état initial souhaité. On peut augmenter cette fraction par des techniques complexes, mais on est très loin de réaliser le critère 2. En plus, la lecture du résultat d'un calcul demande aussi des techniques spéciales pour séparer les bons résultats du reste de l'ensemble. Toutes ces techniques ont comme conséquence que le signal mesuré diminue si le nombre de qu-bits qu'on veut réaliser augmente. Tant qu'on n'est pas capables de remplir le critère 2, le RMN ne sera donc pas "scalable". Cela dit, le RMN est une méthode très intéressante puisque c'est la seule qui a permis de réaliser de vrais ordinateurs quantiques à plusieurs qu-bits (jusqu'à 7, ce qui a permis la seule réalisation de l'algorithme de Shor jusqu'à présent).

## 8.3 Temps de decohérence plus long que le temps d'une opération

Nous savons déjà quel est l'effet de la decohérence sur le calcul quantique. Il faut donc que le système soit conçu pour que le temps de décohérence relevant soit très long. Que veut dire *relevant*, et combien c'est très long ?
La question sur le temps relevant est très importante. Un système peut être caractérisé par plusieurs temps de decohérence liés à des différents degrés de liberté. Par exemple, le spin du noyaux d'un atome est caractérisé par un temps de décohérence beaucoup plus long que celui du degré de liberté de position de l'atome. Nous pouvons préparer un atome dans une combinaison linéaire de deux positions différentes et il sera très rapidement localisé dans une des deux positions. Son spin par contre n'aura pas subi de décohérence entre temps. Cette remarque suggère une solution très efficace pour l'infor-

mation quantique : celle du codage des qu-bits. On peut penser de *coder* les états d'un ordinateur quantique avec un sous-ensemble des états physiques d'un système. Ce sous-ensemble sera choisi en choisissant les états qui sont moins soumis à la décohérence. Le codage présente une forte analogie avec les techniques de correction d'erreur en information classique, oï on utilise un sous-ensemble des possibles valeurs d'un array pour coder l'information. En plus de l'avantage de choisir les états les moins soumis à la decohérence, il y a aussi l'avantage de pouvoir mettre en place des techniques de correction d'erreur quantique. Très intuitivement, les états qui ne font pas partie du codage peuvent être utilisés pour détecter si de la decohérence à eu lieu. Ces états doivent être toujours réinitialisés pour permettre la correction d'erreur. Les techniques de correction d'erreur quantique sont très développées du point de vue théorique, et on peut montrer qu'elle sont fault-tolerant : si la decohérence est assez lente, on peut les rendre arbitrairement efficaces. Les études ont indiqué que, grâce à ces techniques, on peut accepter des temps de décohérence $10^4$-$10^5$ fois plus lents de la durée d'une opération. C'est un contrainte très stricte, mais réalisable. Du point de vue pratique, les systèmes ne sont pas assez développés pour pouvoir vérifier l'efficacité de ces techniques.

## 8.4 Un ensemble universel de portes logiques quantiques

A une porte logique quantique correspond un opérateur unitaire. Il est clair que ces opérateurs unitaires sont, dans la pratique, les opérateurs d'évolution temporelle liés à des Hamiltoniens $H_1$ $H_2$, etc. Il suffirait de pouvoir allumer l'Hamiltonien $H_1$ pendant un certain temps, puis l'éteindre et allumer $H_2$ pendant un autre temps, etc. Malheureusement, on ne peut pas en général éteindre et allumer de interactions physiques (ce serait comme si on pouvait éteindre la gravité et commencer à flotter en l'air !). Plusieurs remarques donc s'imposent.
Tout d'abord, nous allons voir qu'on peut se restreindre à des opérations quantiques à 1 et 2 qu-bits pour réaliser toutes autres opérations. En plus, l'opération à 2 qu-bits peut être de plusieurs types différents (donc on pourra les choisir sur la base du système spécifique et de leur réalisabilité). Pour les opérations à 1 qu-bit, nous avons déjà discuté la faisabilité de ces opérations pour la plupart des système envisagés.

Un problème c'est que une opération à 2 qu-bits demande une interaction physique entre les dégrés de liberté des qu-bits. Dans les cas oï une telle interaction est présente (et on doit se contenter de celle que la nature nous

met à disposition !), le problème c'est qu'on ne peut souvent pas la controler. Pour certains systèmes, ce n'est pas grave. Par exemple en RMN l'interaction entre deux spins des noyeaux est associée à une évolution temporelle beaucoup plus lente de celle qui caractérise les opérations à 1 qu-bit, induites par des champs externes. Le controle donc est fait tout simplement en attendant un temps donné, avant d'effecture la prochaine opération à 1 qu-bit. Le fait que pendant l'opération à 2 qu-bit 'les autres contributions à l'Hamiltonien du système sont toujours présentes ne pose pas un problème. Aprês le temps du calcul, l'évolution aura été celle induite par l'interaction plus celle induite par les autre contributions. On peut appliquer un technique dite de "refocusing" pour annuler la deuxième évolution (on ne parlera pas de cet aspect plutït technique).
Dans d'autres cas, l'interaction n'existe pas ou est trop petite. Par exemple, les ions piégés sont si distants qu'aucune interaction existe. Il est toutefois possible d'induire une interaction à l'aide d'un autre système intermédiaire qui est couplé aux deux qu-bits. Par exemple, pour deux photons (qui notamment n'interagissent pas) on peut utiliser un atome qui présente une transition optique à l'énergie des photons. Pour les ions, on couple leurs états électroniques aux degrés de liberté de vibration des ions dans le potentiel piégeant. L'introduction de dégrés de liberté additionnels toutefois n'est jamais sans conséquences. Elle peut en particulier produire de la decohérence qu'il faut garder sous contrôle.
Un autre problème est lié à la durée de l'opération. Un principe physique de base nous dit quê plus la durée est longue, moins on impliquera d'autres états non souhaités du système dans l'évolution temporelle. Ceci pose une autre contrainte puisque la decohérence doit être 10'000 fois plus longue d'un temps qu'il faut faire le plus long possible.
Un autre problème est dans le mécanisme de contrôle externe. On suppose toujours que ce soit un mécanisme classique (par exemple, le champ magnétique que nous avons vu pour la manipulation d'un spin). Ceci pourrait ne pas être le cas : les degrés de liberté quantiques du mécanisme de contrôle pourraient devenir intriqués avec ceux du système, introduisant encore de la decohérence.
Pour finir, une porte logique quantique ne fonctionne jamais de manière idéale. On peut avoir des erreurs, qui sont exprimés par la "fidélité" du système (distance entre le fonctionnement réel et celui idéal). Pour ces erreurs on a des contraintes analogues à celles pour la decohérence : il faut que le taux d'erreur soit d'environ $10^{-4}$. Dans ce cas, on peut appliquer des techniques de correction d'erreur avec succès.

## 8.5 Possibilité de mesures spécifiques sur chaque qu-bit

Cela veut dire que, pour un qu-bit avec matrice densité

$$\rho = \begin{pmatrix} p & \alpha \\ \alpha^* & 1-p \end{pmatrix}$$

on doit pouvoir effectuer une mesure qui nous donne 0 avec probabilité $p$, 1 avec probabilité $1-p$, et ceci indépendamment de $\alpha$ et des états des autres qu-bits qui composent le système. Idéalement, une mesure a 100% d'efficacité. En réalité ceci n'est jamais le cas. La solution à ce problème est la répétition du calcul quantique. Si l'efficacité est 90%, alors en répétant 4 fois le calcul on arrive à 97%. Répéter implique pouvoir "copier" l'input du calcul, ce qui est possible seulement si les états à copier sont choisis dans un ensemble d'états orthogonaux. Ceci est souvent possible, et la technique de la répétition est très efficace. Elle est aussi nécessaire, puisque les algorithmes quantiques donnent un résultat avec une probabilité toujours plus petite que 1. Pour des réalisations spécifiques, comme la RMN, la répétition est extrême ($10^{18}$ molécules !), et la mesure prend une signification physique très différente : elle est réalisée sur l'ensemble et l'état de chaque réplique du système n'est presque pas perturbé.

## 8.6 Condition additionnelles pour la transmission de l'information quantique

Les cinq critères que nous avons vus, sont nécessaires pour une réalisation pratique du calcul quantique. En réalité, le paradigme de l'information quantique implique également que l'information puisse être transmise d'un point à un autre. Cela est nécessaire d'abord pour des applications spécifiques comme la cryptographie quantique. Il est aussi indispensable en vue d'un ordinateur quantique complexe, fait de plusieurs parties qui sont distribuées dans l'espace, comme pour les ordinateurs traditionnels. En plus des cinq critères, on peut donc introduire deux nouveaux critères spécifiques à la transmission de l'information.

1. La capacité de transmettre des "qu-bits volants" de manière efficace.
2. La capacité de convertir un qu-bit statique en un qu-bit volant et vice-versa.

Nous introduisons ici le concept de "qu-bit volant" (flying qu-bit en anglais). C'est un concept très récurrent en information quantique. Il indique une réalisation physique de qu-bit qu'on peut transmettre sur des grandes distances.

Pour l'instant, nous connaissons l'état de polarisation du photon comme exemple de qu-bit volant. Il est aussi possible d'utiliser d'autres degrés de liberté du photon, mais le résultat est le même : les photons sont la meilleure réalisation de qu-bit volant à présent. En effet, la question des qu-bit volants est celle à laquelle on a donné la meilleure réponse dans le cadre de la recherche sur l'information quantique. L'autre problème – celui de convertir un qu-bit stationnaire en un qu-bit volant – est le vrai problème qui reste à résoudre. Il faut tout de même remarquer que pour certaine tâches comme la cryptographie quantique, nous n'avons pas du tout besoin de qu-bits statiques et le problème ne se pose pas. Pour l'instant il existent très peu d'idées sur comment effectuer cette conversion (par exemple d'un spin d'un électron à un photon) de manière efficace.