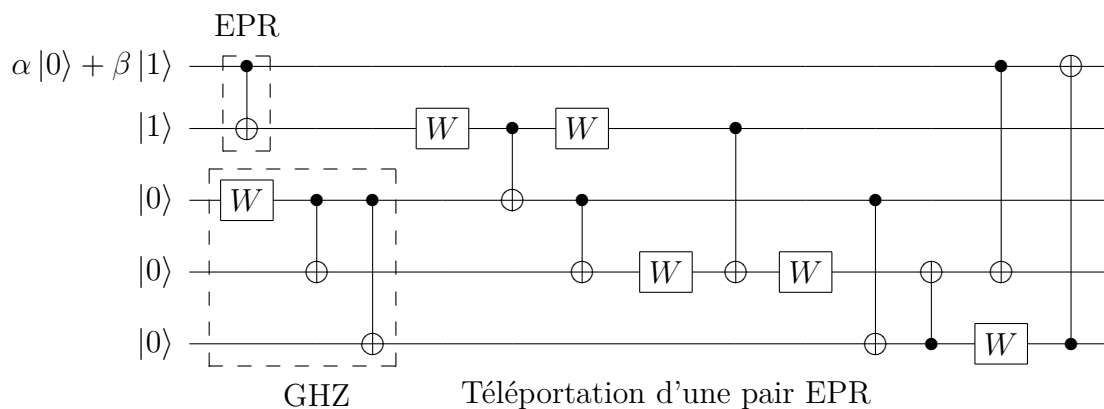




INTRODUCTION A L'INFORMATION QUANTIQUE

MIL4AR08/CS07 - UE Optionnelle
CM : 30h - TD : 20h - Crédits : 5

NANA ENGO



Année académique 2012 – 2013

Copyright © Nana Engo - Sous la licence 3.0

TABLE DES MATIÈRES

Avant-propos	ii
1 Qubits et états quantiques	1
1.1 Qubit ou bit quantique et espace de Hilbert	1
1.1.1 Qubit ou bit quantique	1
1.1.2 Représentation de la sphère de Bloch avec QuTiP	4
1.1.3 Espace de Hilbert	6
1.2 Phénomènes quantiques : Interférence à une particule	10
1.2.1 Fentes d'Young	10
1.2.2 Interférométrie de Mach Zehnder	11
1.2.3 Expérience MZ1	13
1.2.4 Expérience MZ2	13
1.2.5 Expérience MZ3	13
1.2.6 Expérience MZ4	14
1.3 Notion d'amplitude de probabilité	16
1.3.1 Vecteurs d'état et amplitudes de probabilité	16
1.3.2 Règles de calcul des amplitudes de probabilité	19
1.3.3 Chat de Schrödinger	24
1.4 Exercices et problèmes	26
1.4.1 Interféromètre de Mach-Zehnder à deux lames	26
1.4.2 Amplitudes de probabilité de transition	26
1.4.3 Chat de Schrödinger	27
2 Mesure et opérateurs linéaires	28
2.1 Mesure de grandeurs physiques et opérateurs	28
2.1.1 Mesure de grandeurs physiques	29
2.1.2 Autres Expériences	31
2.1.3 Point sur la mesure	32
2.2 Opérateurs linéaires et représentation matricielle	33
2.2.1 Linéarité et représentation matricielle	33
2.2.2 Hermiticité et fonction d'un opérateur	35
2.2.3 Unitarité	38
2.2.4 Projection	39
2.3 Décomposition spectrale des opérateurs hermitiens	40

2.3.1	Diagonalisation d'un opérateur hermitien	40
2.3.2	Ensemble complet d'opérateurs compatibles (ECOC)	45
2.4	Inégalités d'Heisenberg	48
2.5	Exercices et problèmes	50
2.5.1	Représentation matricielle	50
2.5.2	QuTiP - Opérateurs	50
2.5.3	Formule de Baker-Campbell-Hausdorff	51
2.5.4	Opérateur de Hausdorff	51
2.5.5	ECOC	51
2.5.6	QuTiP - ECOC	52
2.5.7	Propriétés des matrices de Pauli	52
2.5.8	Porte logique quantique élémentaire	53
2.5.9	Délocalisation et recombinaison d'un spin $1/2$	54
3	Postulats et évolution temporelle	55
3.1	Postulats de la théorie quantique	55
3.1.1	Postulat 1 : Espace des états	55
3.1.2	Postulat 2 : Amplitudes de probabilité et probabilités	56
3.1.3	Postulat 3 : Grandeurs physiques et opérateurs	56
3.1.4	Postulat 4 : Principe de quantification et de décomposition spectrale	56
3.1.5	Postulat 5 : Principe de réduction du paquet d'onde	57
3.2	Évolution temporelle	59
3.2.1	Postulat 6 : Évolution temporelle du système	59
3.2.2	Opérateur d'évolution et états stationnaires	60
3.2.3	Système à deux états	61
3.3	Manipulations de qubits - Oscillations de Rabi	62
3.3.1	Formalisme classique	62
3.3.2	Formalisme quantique	63
3.4	Exercices et problèmes	67
3.4.1	Moment magnétique du deutéron	67
3.4.2	Précession de Larmor	67
3.4.3	Détection des électrons	68
3.4.4	Réalisation expérimentale d'une porte logique 1-qubit	68
3.4.5	QuTiP - Evolution d'un état de spin $1/2$	70
4	Corrélations quantiques	71
4.1	Produit tensoriel et états intriqués	72
4.1.1	États	72
4.1.2	Opérateurs	73
4.1.3	États corrélés ou intriqués	75
4.2	Théorème de Bell et interférences des états corrélés	77
4.2.1	L'analyse EPR - <i>Dieu ne joue pas au dés</i>	77
4.2.2	Théorème de Bell	78
4.2.3	Interférences à deux quantons	79
4.3	Information quantique	81
4.3.1	Non-clonage quantique	82
4.3.2	Cryptographie quantique	83
4.3.3	Fax quantique ou téléportation quantique	87

4.4	Exercices	90
4.4.1	Inégalités de Bell avec des photons	90
4.4.2	Distribution quantique des clefs 1	91
4.4.3	Distribution quantique des clefs 1	92
5	Calculs quantiques	96
5.1	Notion de calculateur	96
5.2	Circuits quantiques	98
5.2.1	Énergie - information - réversibilité	98
5.2.2	Parallélisme quantique	99
5.2.3	Portes single-qubit	100
5.2.4	Portes de contrôle et génération de l'intrication	103
5.3	Portes quantiques universelles	107
5.3.1	Porte CV	108
5.3.2	Porte de TOFFOLI	108
5.3.3	Resumé	110
5.3.4	Évaluation quantique d'une fonction	110
5.4	Algorithme de Deutsch-Jozsa	111
5.4.1	Problème et solution classique	111
5.4.2	Algorithme quantique de Deutsch-Jozsa	111
5.5	Transformation de Fourier quantique	113
5.6	Réalisations physiques	116
5.7	Conclusion	118
5.8	Exercices	119
5.8.1	Effets des erreurs d'amplitude et de phase	119
5.8.2	Opérateur racine carrée NOT	119
5.8.3	Algorithme quantique	120
5.8.4	Circuit intraportation	120
5.8.5	Circuit intraportation avec QuTiP	122
5.8.6	Téléportation d'une paire EPR	122
5.8.7	Transformée de Fourier Quantique	123
A	Installation de QuTiP et commandes usuelles	124
A.1	Installation de QuTiP pour Ubuntu 12.04 et plus récente	124
A.2	Vérification de l'installation	125
A.3	Commandes usuelles	125
A.3.1	Quantum object class	125
A.3.2	États et opérateurs	125
A.3.3	Les attribues d'une classe Qobj	125
A.3.4	Qobj Math	125
A.3.5	Fonction opérant sur une classe Qobj	126
A.4	Manipuler les états et opérateurs	126
A.4.1	États ket et bra	126
A.4.2	Qubit	126
A.4.3	Valeurs moyennes	126
A.5	Produit tensoriel et trace partielle	126
A.5.1	Produit tensoriel	126
A.5.2	Trace partielle	126

A.6	Sphère de Bloch	126
A.6.1	Bloch class	126
A.6.2	Bloch3d class	126
A.6.3	Différences entre Bloch and Bloch3d	126
A.7	Évolution temporelle unitaire	126
B	Théorie de l'information classique	127
B.1	Entropie de Shannon	127
B.2	Information conditionnelle	130
B.3	Information mutuelle	130
B.4	Probabilité conjointe	130
C	Éléments Cryptologie	133
C.1	Fonctionnalités de la cryptographie	133
C.2	Principe du chiffrement symétrique	134
C.3	Problématique de l'authentification	134
C.4	Principe du chiffrement asymétrique	134
D	Code RSA	136
E	Correction des exercices	138
E.1	Qubits et états quantiques	138
E.1.1	Chat de Shrödinger	138
E.2	Mesure et opérateurs linéaires	139
E.2.1	Représentation matricielle	139
E.2.2	ECOC avec QuTiP	141
E.2.3	ECOC Avec QuTiP	141
E.3	Postulats et évolution	142
E.3.1	Évolution d'un état de spin 1/2	142
E.4	Calculs quantiques	142
E.4.1	Circuit intraportation avec QuTiP	142
E.4.2	Téléportation d'une paire EPR	143

Cette unité d'enseignement (UE) a pour objectif d'exposer aux étudiants du cycle Licence des Mentions Mathématique et Informatique, les notions de bases de la théorie quantique nécessaires à la compréhension de l'information quantique. Laquelle permet de traiter et transmettre l'information en s'appuyant sur les spécificités de la théorie quantique.

Les progrès des techniques et de la connaissance permettent aujourd'hui d'agencer de façon contrôlée un petit nombre d'atomes pour fabriquer des objets de taille nanométrique¹ qui présentent des propriétés extraordinaires, d'origine quantique, qui sont exploitées dans la quasi-totalité des domaines industriels.

En effet, le monde de l'information dans lequel nous vivons aujourd'hui résulte de la synergie entre l'informatique et la théorie quantique à travers l'invention du transistor. Cependant, l'ultra-miniaturisation croissante des composants électronique, suit deux lois émise en 1965 par Gordon Moore, co-fondateur de la société INTEL :

- **1ère loi de Moore** : *tous les dix-huit mois, la complexité et les performances (rendement technologique) des circuits seront multipliées par deux ;*
- **2ème loi de Moore** : *à chaque génération le coût des équipements de fabrication sera multiplié par deux.*

En vertu de la 1ère loi,

- L'augmentation du nombre de connexions limite les possibilités d'intégration sur une puce ;
- La réduction du temps de calcul est limitée par les délais de commutations entre transistors ;
- Le nombre important de composants sur une même puce entraîne *ipso facto* une augmentation de la consommation électrique, et par voie de conséquent, à travers la loi de Ohm, celle de la quantité de chaleur dissipée dans la puce.

Ainsi comme on peut le voir sur la figure 0.0.1, par rapport aux nombre de connexions, d'ici 2020 le bit d'information sera stocké sur une puce de dimension atomique. Et alors, les effets quantiques commenceront à être prédominants. Les électrons jusque là bien ordonnés révéleront leur nature quantique, qui est, entre autres, probabiliste. Les transistors pourraient ainsi, ne plus être de manière déterministe dans l'état ON ou OFF, mais se retrouver dans une superposition des deux, avec une certaine probabilité d'être dans l'état ON ou dans l'état OFF. Un tel comportement n'appelle aucune alternative : il faudra soit adapter l'architecture

¹Le millionième de millimètre !

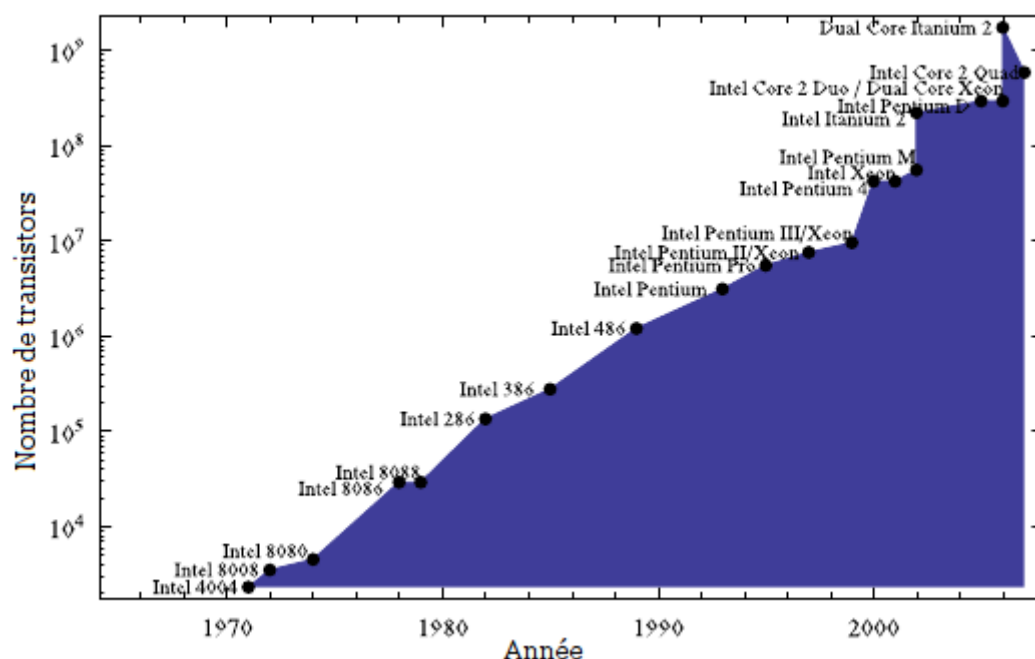


Figure 0.0.1 – Depuis quatre décennies, la densité des transistors réalisés sur une même puce double tous les dix-huit mois.

des ordinateurs pour minimiser les nuisances occasionnées par les effets quantiques, ou alors changer radicalement d'architecture en ouvrant les bras à ces effets quantiques. L'information quantique suit cette deuxième approche.

Mais hormis ces effets quantiques, les considérations économiques, que met en évidence la 2ème loi de Moore, vont aussi rendre inopérants la 1ère loi de Moore. En effet, pour réduire les coûts de fabrication, on pense de plus en plus à l'**auto-assemblage** des composants. Celui-ci est possible depuis le début des années 1980 par la *capacité des physiciens à manipuler et observer des objets quantiques élémentaires individuels* : atomes, photons, électrons, etc. Il est à noter que c'est l'auto-assemblage que suit la vie en pratiquant l'assemblage des molécules pour créer les protéines, enchaînement d'acides aminés, que de super-molécules, les acides nucléiques (ARN, ADN), savent faire produire au sein de cellules pour former des organismes, les faire fonctionner et se reproduire tout en se complexifiant. Cette voie, dite **bottom-up**, vise à organiser la matière à partir des *briques de base*, dont les atomes eux-mêmes sont les plus petits constituants, à l'instar du monde vivant. La nanoélectronique du futur cherche à emprunter cette voie d'assemblage pour aboutir à moindre coût à la fabrication d'éléments fonctionnels, puisque **la technologie ne progresse qu'en devenant moins chère !**

Grâce à l'information quantique, on peut par exemple concevoir de nouvelles méthodes de cryptographie dont la sécurité s'appuie sur les bases du formalisme quantique, ou de nouvelles méthodes de calculs qui peuvent être exponentiellement plus efficaces que les méthodes classiques. L'information quantique ne concerne donc pas seulement les physiciens, mais aussi les théoriciens de l'information, les algorithmiciens, et les mathématiciens travaillant sur la théorie de la complexité.

Ces notes de cours sont volontairement très détaillées et enrichies de nombreux exemples afin de palier à la carence d'ouvrages appropriés dans l'environnement actuel de l'étudiant de la Faculté des Sciences de l'Université de Ngaoundéré.

Le contenu du cours est le suivant :

- **Chapitre I : Qubits et états quantiques**

Qubit ou bit quantique et espace de Hilbert. Phénomènes quantiques (Interférence à une particule). Vecteurs d'état et amplitudes de probabilité. Règles de calcul des amplitudes de probabilité.

- **Chapitre II : Mesure et opérateurs linéaires**

Mesure de grandeurs physiques et opérateurs. Opérateurs linéaires et représentation matricielle. Diagonalisation d'un opérateur hermitien. Ensemble complet d'opérateurs qui commutent (ECOC).

- **Chapitre III : Postulats et évolution temporelle**

Postulats de la théorie quantique. Évolution temporelle. Inégalités d'Heisenberg. Manipulations des qubits : oscillations de Rabi.

- **Chapitre IV : Corrélations quantiques**

Produit tensoriel. Interférences des états corrélés. Analyse EPR et inégalités de Bell. Non-clonage quantique. Cryptographie quantique. Téléportation quantique.

- **Chapitre V : Calculs quantiques**

Calculs réversibles. Portes logiques et circuits quantiques. Bases de Bell. Algorithme de Deutsch-Jozsa. Transformation de Fourier quantique.

CHAPITRE 1

QUBITS ET ÉTATS QUANTIQUES

Sommaire

- 1.1 Qubit ou bit quantique et espace de Hilbert
- 1.2 Phénomènes quantiques : Interférence à une particule
- 1.3 Notion d'amplitude de probabilité
- 1.4 Exercices et problèmes

Dans ce chapitre nous présentons le cadre général de la théorie quantique en utilisant la puissante et élégante algèbre de Dirac. La **section 1.2** est consacrée à la découverte de l'étrange monde quantique à travers quelques expériences d'interférences à une particule. Ces expériences montrent que l'intuition et le *bon sens* hérités de la physique classique sont inadaptés dans le monde quantique du fait de la nature fondamentalement **probabiliste** ou **indéterministe** des phénomènes quantiques. Cette nature impose l'introduction, à la **section 1.3**, des concepts nouveaux et essentiels d'état quantique, d'amplitude de probabilité ou amplitude de transition, de superposition d'état ou **qubit** et de l'espace de Hilbert. Ces concepts ont été auparavant présenté de façon *mathématique* à la **section 1.1**.

1.1 Qubit ou bit quantique et espace de Hilbert

1.1.1 Qubit ou bit quantique

L'unité fondamentale de l'informatique classique est le bit (de l'anglais *binary digit*). Un bit peut prendre deux valeurs que l'on note habituellement 0 et 1. Évidemment, ce choix de notation, complètement arbitraire, n'est que la représentation symbolique du stockage du bit dans un système à deux états. En effet, la valeur 0 d'un bit peut être représentée physiquement dans un ordinateur par un condensateur non chargé et la valeur 1, représentée par le même condensateur chargé (voir la figure 1.1.1). La différence entre les deux états (chargé

et non chargé) se traduit par le déplacement de plusieurs millions d'électrons. Ainsi, un bit d'information classique implique environ 10^9 électrons dans la mémoire vive d'un ordinateur. Il s'agit donc d'un comportement *collectif*.

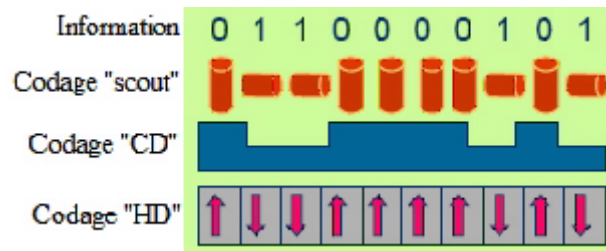


Figure 1.1.1 – Codage classique. L'information, que l'on représente par les **bits** 0 et 1, est toujours codée dans des systèmes physiques bistables.

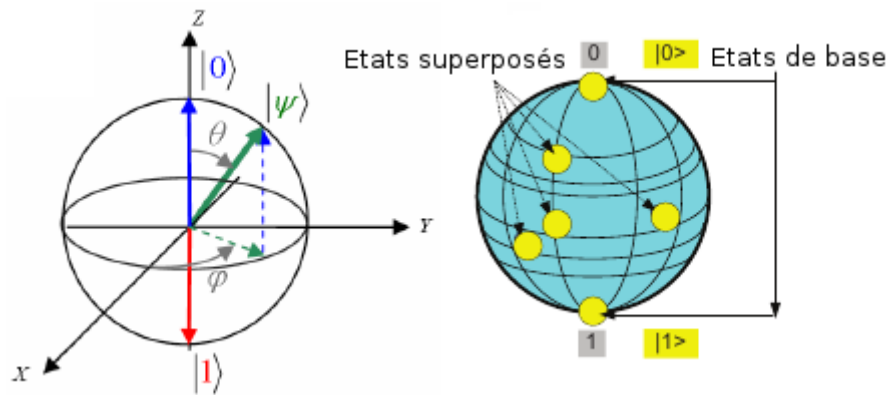


Figure 1.1.2 – Codage quantique. Le qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (avec $\alpha = \cos \frac{\theta}{2}$, $\beta = e^{i\varphi} \sin \frac{\theta}{2}$ et $|\alpha|^2 + |\beta|^2 = 1$), offre une description différente des systèmes physiques. Les états binaires classiques sont aux pôles de la sphère. Il opère dans un univers multidimensionnel, ces états propres correspondant à la surface de la sphère, alors que les états logiques classiques correspondent aux pôles de cette sphère.

L'unité fondamentale de l'information quantique est le bit quantique ou, plus simplement, **qubit** (de l'anglais *quantum bit*). Il est superficiellement similaire au bit classique, mais comme nous le ferons, il est fondamentalement différent et cette différence fondamentale permet le traitement de l'information de façons nouvelles et très prometteuses.

Comme le bit, le qubit peut-être dans un des états 0 ou 1. Pour une raison qu'on expliquera ci-dessous, on notera ces états $|0\rangle$ et $|1\rangle$ et on lira **ket de 0** et **ket de 1**. Cette notation est appelée **notation de Dirac** et représente un *vecteur d'état* ou un *état* tout simplement.

A la différence du bit classique, le qubit peut-être **à la fois** dans l'état $|0\rangle$ et $|1\rangle$. On dit alors qu'il est dans **état superposé** que l'on note

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1.1.1)$$

où α et β sont des nombres complexes qui vérifient

$$|\alpha|^2 + |\beta|^2 = 1, \quad (1.1.2)$$

appelée **relation de complétude** ou **condition de normalisation** du qubit. La figure 1.1.2 donne une représentation du qubit sur une sphère de Bloch.

Tant qu'on effectue aucune mesure ou alors tant que le qubit est isolé du monde extérieur, il reste dans cet état superposé. Dès qu'une mesure est effectuée ou dès que le qubit est en contact avec son environnement, il adopte un comportement classique en prenant **soit** l'état $|0\rangle$, **soit** l'état $|1\rangle$. Et les lois de la théorie quantique nous disent que

- on trouve le qubit $|\psi\rangle$ dans l'état $|0\rangle$ avec la **probabilité** $|\alpha|^2$;
- on trouve le qubit $|\psi\rangle$ dans l'état $|1\rangle$ avec la **probabilité** $|\beta|^2$.

D'une manière générale, si un qubit est une superposition de N états¹ $|i\rangle$,

$$|\psi\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle, \quad (1.1.3a)$$

on a

$$\sum_{i=0}^{N-1} |\alpha_i|^2 = |\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{N-1}|^2 = 1. \quad (1.1.3b)$$

Les coefficients α_i sont appelés **amplitudes de probabilité**. Puisque ce sont des nombres complexes en général, on calcule les probabilités $|\alpha_i|^2$ de la façon suivante,

$$|\alpha_i|^2 = \alpha_i^* \alpha_i, \quad (1.1.4)$$

où α_i^* est le complexe conjugué de α_i .

La dichotomie qu'il y a entre le comportement du qubit quand il n'est pas observé (ou lorsqu'il est isolé) et lorsqu'il est observé (ou en contact avec l'environnement), est au cœur même de la théorie quantique.

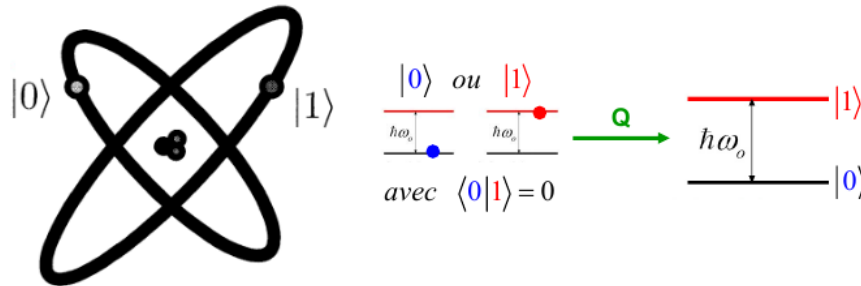


Figure 1.1.3 – Qubit représenté par deux états électroniques d'un atome [Après Nielsen et Chuang[MNIC2000]]

Malgré son comportement étrange, le qubit existe réellement. En effet, nombre de systèmes physiques peuvent être utilisés pour réaliser un qubit. C'est le cas par exemple des deux états d'un électron orbitant autour du noyau d'un atome qu'illustre la figure 1.1.3. Dans le modèle de l'atome, un électron est soit dans un état fondamental soit dans un état excité, que l'on peut représenter respectivement par $|0\rangle$ ou $|1\rangle$. Lorsqu'on envoie un rayonnement électromagnétique avec une énergie appropriée, il est possible de déplacer l'électron de l'état $|0\rangle$ vers $|1\rangle$ et vice-versa. Mais il est encore plus intéressant d'éclairer l'atome avec un rayonnement ayant une

¹Lorsqu'on a un état quantique de dimension $d \geq 3$ on parle de **qudit**. Par exemple, pour $d = 3$, on a un **qutrit** et pour $d = 4$ on a un **ququart**.

énergie telle que, l'électron initialement dans l'état $|0\rangle$ se trouve à mi-chemin entre $|0\rangle$ et $|1\rangle$, dans l'état

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (1.1.5)$$

On retient que

*La différence entre le bit classique et le bit quantique ou qubit se situe au niveau de la description d'un système physique (ses propriétés), étant entendu que l'état d'un système est l'ensemble des propriétés que le système possède. Si on pose par exemple la question **est-il possible de trouver la propriété P du système lors d'une mesure ?** La théorie classique répond **NON** alors que la théorie quantique répond **OUI mais avec une probabilité** $|\alpha|^2$ par exemple.*

1.1.2 Représentation de la sphère de Bloch avec QuTiP

En utilisant le logiciel QuTiP², on peut représenter sur la sphère de Bloch un qubit.

Les commandes suivantes représentent respectivement les états $|0\rangle$, $|1\rangle$ et $(|0\rangle + |1\rangle)/\sqrt{2}$. Le symbole `#` introduit un commentaire.

```
from qutip import *
B=Bloch() # crée une sphère de Bloch vide
ket0 = basis(2,0) # définit le  $|0\rangle$ 
ket1 = basis(2,1) # définit le  $|1\rangle$ 
B.add_states(ket0) # représente le  $|0\rangle$  sur B
B.add_states(ket1) # représente le  $|1\rangle$  sur B
B.add_states((ket0+ket1)/sqrt(2)) # représente l'état  $(|0\rangle + |1\rangle)/\sqrt{2}$  sur B
B.show() # permet de visualiser la sphère B avec les trois états ajoutés. L'image obtenue peut être sauvegardé pour utilisation ultérieur.
```

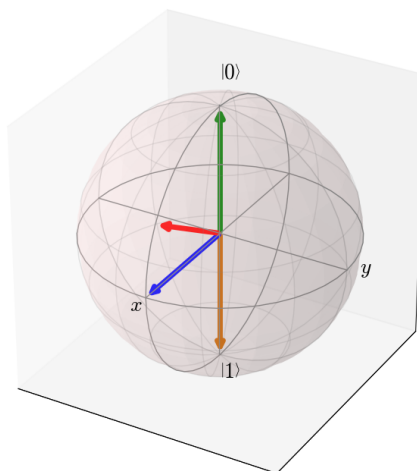


Figure 1.1.4 – Représentation avec QuTiP de la sphère de Bloch avec les états $|0\rangle$, $|1\rangle$ et $(|0\rangle + |1\rangle)/\sqrt{2}$.

²Voir l'Annexe A pour l'installation de QuTiP.

Exercice 1.1.1 For each of the following qubits, if a measurement is made, what is the probability that we find the qubit in the state $|0\rangle$? What is the probability that we find the qubit in the state $|1\rangle$?

$$1. |\psi\rangle = \frac{1}{\sqrt{3}} |0\rangle + \sqrt{\frac{2}{3}} |1\rangle.$$

$$2. |\psi\rangle = \frac{i}{2} |0\rangle + \frac{\sqrt{3}}{2} |1\rangle.$$

$$3. |\psi\rangle = \frac{1+i}{\sqrt{3}} |0\rangle - \frac{i}{\sqrt{3}} |1\rangle.$$

Compute with QuTiP the probabilities of finding the state $|\psi\rangle$ in $|0\rangle$ or in $|1\rangle$. Plot on the Bloch sphere the state $|0\rangle$, $|1\rangle$ and $|\psi\rangle$.

Solution 1.1.1 To find the probability that each qubit is found in the state $|0\rangle$ or the state $|1\rangle$, we compute the modulus squared of the appropriate coefficient.

1. The probability of finding $|\psi\rangle$ in the state $|0\rangle$ is

$$\left| \frac{1}{\sqrt{3}} \right|^2 = \frac{1}{3}, \quad (1.1.6a)$$

whereas probability of finding $|\psi\rangle$ in the state $|1\rangle$ is

$$\left| \sqrt{\frac{2}{3}} \right|^2 = \frac{2}{3}. \quad (1.1.6b)$$

These probabilities verified

$$\sum_{i=0}^1 |\alpha_i|^2 = \frac{1}{3} + \frac{2}{3} = 1. \quad (1.1.6c)$$

2. The next state has coefficients that are complex numbers. So that the probability of finding $|\psi\rangle$ in the state $|0\rangle$ is

$$\left| \frac{i}{2} \right|^2 = \left(\frac{i}{2} \right)^* \left(\frac{i}{2} \right) = \left(-\frac{i}{2} \right) \left(\frac{i}{2} \right) = \frac{1}{4}, \quad (1.1.7a)$$

whereas probability of finding $|\psi\rangle$ in the state $|1\rangle$ is

$$\left| \frac{\sqrt{3}}{2} \right|^2 = \frac{3}{4}. \quad (1.1.7b)$$

Again, we check that the probabilities sum to 1 :

$$\sum_{i=0}^1 |\alpha_i|^2 = \frac{1}{4} + \frac{3}{4} = 1. \quad (1.1.7c)$$

3. Finally, for the last state, the probability of finding $|\psi\rangle$ in the state $|0\rangle$ is

$$\left| \frac{1+i}{\sqrt{3}} \right|^2 = \left(\frac{1+i}{\sqrt{3}} \right)^* \left(\frac{1+i}{\sqrt{3}} \right) = \left(\frac{1-i}{\sqrt{3}} \right) \left(\frac{1+i}{\sqrt{3}} \right) = \frac{1-i+i+1}{3} = \frac{2}{3}, \quad (1.1.8a)$$

whereas probability of finding $|\psi\rangle$ in the state $|1\rangle$ is

$$\left| \frac{-i}{\sqrt{3}} \right|^2 = \left(\frac{-i}{\sqrt{3}} \right)^* \left(\frac{-i}{\sqrt{3}} \right) = \left(\frac{i}{\sqrt{3}} \right) \left(\frac{-i}{\sqrt{3}} \right) = \frac{1}{3}. \quad (1.1.8b)$$

Again, these probabilities sum to 1 :

$$\sum_{i=0}^1 |\alpha_i|^2 = \frac{2}{3} + \frac{1}{3} = 1. \quad (1.1.8c)$$

As the probability of finding the state $|\psi\rangle$ in $|i\rangle$ is given by $p_i = |\langle i|\psi\rangle|^2 = \langle i|\psi\rangle \langle i|\psi\rangle^*$, $i = 0, 1$, the QuTiP script should be

```
from qutip import *
ket0 = basis(2,0)
bra0 = ket0.dag()
ket1 = basis(2,1)
bra1 = ket1.dag()
psi = (ket0+sqrt(2)*ket1)/sqrt(3)
p0 = (bra0*psi)*(bra0*psi).dag()
p1 = (bra1*psi)*(bra1*psi).dag() Do the same for the other cases.
```

Pas du tout compliqué n'est-ce pas ?

1.1.3 Espace de Hilbert

L'espace mathématique où ont lieu les calculs quantiques est l'**espace de Hilbert** \mathcal{H} , qui est un espace Euclidien complexe, muni d'un produit scalaire. C'est un espace de dimension infinie, mais nous nous limiterons dans cette section au cas de la dimension finie.

1. Le **ket** $|i\rangle$ est un vecteur de l'espace des états ou **espace de Hilbert** \mathcal{H} ;
2. Le **bra** $\langle f|$ est un vecteur de l'espace dual \mathcal{H}^* , autrement, c'est le **conjugué hermitien** du $|f\rangle$,

$$(|f\rangle)^\dagger = \langle f|. \quad (1.1.9)$$

Il existe une correspondance biunivoque entre les vecteurs de ces deux espaces. On utilise le même symbole pour représenter un vecteur de l'un de ces espaces et celui qui lui correspond dans l'autre espace. Ainsi, le vecteur de l'espace des états correspondant au bra $\langle f|$ est le ket $|f\rangle$.

Base hilbertienne

Définition 1.1.1 L'ensemble $\mathcal{B} = \{|i\rangle\}$ est **une base hilbertienne**, si

$$\langle i|j\rangle = \delta_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{sinon,} \end{cases} \quad (1.1.10)$$

et

$$\sum_{i \in \mathcal{B}} |i\rangle \langle i| = \mathbf{1}. \quad (1.1.11)$$

La **relation de fermeture** (1.1.11) permet la projection d'un vecteur d'état dans la base \mathcal{B} .

Ainsi, le ket $|y\rangle$ se développe dans la base hilbertienne \mathcal{B} , compte tenu de la relation de fermeture (1.1.11), sous la forme

$$|y\rangle = \sum_{i \in \mathcal{B}} |i\rangle \langle i|y\rangle = \alpha_i |i\rangle, \quad (1.1.12a)$$

avec

$$\alpha_i = \langle i|y\rangle, \quad (1.1.12b)$$

considérée ici comme la **coordonnée** ou la **projection** ou plus précisément **l'amplitude de probabilité de projection** de $|y\rangle$ suivant $|i\rangle$.

Puisque le bra $\langle x|$ appartient à l'espace dual \mathcal{H}^* , on a la correspondance antilinéaire **ket** \rightarrow **bra** :

$$\lambda |\psi\rangle \longrightarrow \lambda^* \langle\psi|, \quad (1.1.13a)$$

$$\lambda_1 |\psi_1\rangle + \lambda_2 |\psi_2\rangle \longrightarrow \lambda_1^* \langle\psi|_1 + \lambda_2^* \langle\psi|_2. \quad (1.1.13b)$$

Par suite,

$$\langle x| = \sum_{i \in B} \langle x|i\rangle \langle i| = \sum_{i \in B} \langle i|x\rangle^* \langle i| = \alpha_i^* \langle i|. \quad (1.1.14)$$

C'est ainsi que, dans base $\{|i\rangle\}$, les vecteurs d'états sont représentés dans \mathcal{H} par des nombres, valeurs des composantes ou amplitudes de transition ou de projection :

$$|\psi\rangle = \sum_i |i\rangle \langle i|\psi\rangle = \sum_i \alpha_i |i\rangle \text{ avec } \langle i|\psi\rangle = \alpha_i \Rightarrow |\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_i \\ \vdots \end{pmatrix}, \quad (1.1.15a)$$

$$\langle\psi| = \sum_i \langle\psi|i\rangle \langle i| = \sum_i \langle i|\alpha_i^* \text{ avec } \langle\psi|i\rangle = \alpha_i^* \Rightarrow \langle\psi| = (\alpha_1^*, \alpha_2^*, \dots, \alpha_i^*, \dots). \quad (1.1.15b)$$

Si un vecteur $|\varphi\rangle$ se décompose sur la base $\{|i\rangle\}$ suivant

$$|\varphi\rangle = \sum_i \beta_i |i\rangle, \quad (1.1.16)$$

alors, en utilisant (1.1.10)

$$\langle\psi|\varphi\rangle = \sum_{i,j=1} \langle\psi|i\rangle \langle i|j\rangle \langle j|\varphi\rangle = \sum_i \alpha_i^* \beta_i. \quad (1.1.17)$$

La notion d'état de la base hilbertienne peut être très bien comprise à travers l'analogie avec l'espace \mathcal{V} des vecteurs réels tridimensionnels.

Considérons les vecteurs de base de \mathcal{V}

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad (1.1.18)$$

et deux vecteurs de \mathcal{V}

$$\mathbf{A} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}. \quad (1.1.19)$$

Le vecteur

$$\mathbf{B} = \sum_{i=1}^3 \mathbf{e}_i (\mathbf{e}_i \cdot \mathbf{B}) = \sum_{i=1}^3 \mathbf{e}_i b_i = b_1 \mathbf{e}_1 + b_2 \mathbf{e}_2 + b_3 \mathbf{e}_3. \quad (1.1.20)$$

qui apparaît comme la somme de ces composantes ou projections sur les vecteurs de base, est l'analogue de la relation (1.1.12).

L'analogie de la relation (1.1.17) est

$$\begin{aligned}\mathbf{A} \cdot \mathbf{B} &= \sum_{i=1}^3 (\mathbf{A} \cdot \mathbf{e}_i)(\mathbf{e}_i \cdot \mathbf{B}) \\ &= (\mathbf{A} \cdot \mathbf{e}_1)(\mathbf{e}_1 \cdot \mathbf{B}) + (\mathbf{A} \cdot \mathbf{e}_2)(\mathbf{e}_2 \cdot \mathbf{B}) + (\mathbf{A} \cdot \mathbf{e}_3)(\mathbf{e}_3 \cdot \mathbf{B}) \\ &= a_1 b_1 + a_2 b_2 + a_3 b_3.\end{aligned}\tag{1.1.21}$$

On note que les vecteurs \mathbf{A} et \mathbf{B} correspondent aux deux vecteurs états $|\psi\rangle$ et $|\varphi\rangle$ et l'ensemble des vecteurs de base correspondent à l'ensemble des vecteurs d'états de la base hilbertienne.

Exemple 1.1.1 Dans la base $\{|+\rangle, |-\rangle\}$, l'état superposé $|\psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ a pour composantes

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.\tag{1.1.22}$$

Exemple 1.1.2 Soit un système quantique décrit dans la base d'états $\{|a\rangle, |b\rangle, |c\rangle\}$. Dans cette représentation, les états $|\psi\rangle$ et $|\varphi\rangle$ ont les amplitudes

$$\langle a|\psi\rangle = \frac{1}{\sqrt{3}}, \quad \langle b|\psi\rangle = 0, \quad \langle c|\psi\rangle = i\sqrt{\frac{2}{3}},\tag{1.1.23a}$$

$$\langle a|\varphi\rangle = \frac{1+i}{\sqrt{3}}, \quad \langle b|\varphi\rangle = \frac{1}{\sqrt{6}}, \quad \langle c|\varphi\rangle = \frac{1}{\sqrt{6}}.\tag{1.1.23b}$$

La probabilité de trouver le système dans l'état $|\varphi\rangle$ alors qu'il se trouvait initialement dans l'état $|\psi\rangle$ est

$$\mathcal{P}_{\varphi\psi} = |\langle\varphi|\psi\rangle|^2 = \left| \sum_i \langle\varphi|i\rangle \langle i|\psi\rangle \right|^2 = \left| \frac{1 \times (1-i)}{3} + 0 + i\sqrt{\frac{2}{3 \times 6}} \right|^2 = \left| \frac{1}{3} \right|^2 = \frac{1}{9}.\tag{1.1.24}$$

Il est facile de vérifier que $\mathcal{P}_{\psi\varphi} = \left| \frac{1}{3} \right|^2 = \frac{1}{9}$.

Exercice 1.1.2 Two vectors in \mathbb{C}^3 are given by $|a\rangle = \begin{pmatrix} -2 \\ 4i \\ 1 \end{pmatrix}$ and $|b\rangle = \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix}$.

Find

1. $\langle a|$, $\langle b|$.
2. $\langle a|b\rangle$, $\langle b|a\rangle$.
3. $|c\rangle = |a\rangle + 2|b\rangle$, $\langle c|a\rangle$.

Solution 1.1.2 1. The Hermitian conjugate is the complex conjugate of the transpose. Then,

$$\langle a| = (|a\rangle)^\dagger = (|a\rangle^t)^* = (-2 \quad -4i \quad 1),\tag{1.1.25a}$$

$$\langle b| = (|b\rangle)^\dagger = (|b\rangle^t)^* = (1 \quad 0 \quad -i).\tag{1.1.25b}$$

2. From (1.1.17), the probability amplitude

$$\langle a|b\rangle = \begin{pmatrix} -2 & -4i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix} = -2 + 0 + i = -2 + i. \quad (1.1.26a)$$

As $\langle a|b\rangle = \langle b|a\rangle^*$, we should find $\langle b|a\rangle = -2 - i$. We verify this with an explicit calculation

$$\langle b|a\rangle = \begin{pmatrix} 1 & 0 & -i \end{pmatrix} \begin{pmatrix} -2 \\ 4i \\ 1 \end{pmatrix} = -2 + 0 - i = -2 - i. \quad (1.1.26b)$$

3. We apply the rules of vector addition and scalar multiplication to obtain

$$|c\rangle = |a\rangle + 2|b\rangle = \begin{pmatrix} -2 \\ 4i \\ 1 \end{pmatrix} + 2 \begin{pmatrix} 1 \\ 0 \\ i \end{pmatrix} = \begin{pmatrix} -2 + 2 \\ 4i + 0 \\ 1 + 2i \end{pmatrix} = \begin{pmatrix} 0 \\ 4i \\ 1 + 2i \end{pmatrix} \quad (1.1.27a)$$

Therefore

$$\begin{pmatrix} 0 & -4i & 1 - 2i \end{pmatrix} \begin{pmatrix} -2 \\ 4i \\ 1 \end{pmatrix} = 0 + 16 + 1 - 2i = 17 - 2i. \quad (1.1.27b)$$

Aussi simple que ce qu'on apprend au Secondaire n'est-ce pas ?

Produit scalaire

Si on a

$$\langle x|y\rangle = 0, \quad (1.1.28)$$

alors $|x\rangle$ et $|y\rangle$ sont **orthogonaux**. La symétrie hermitienne du produit scalaire

$$\langle x|y\rangle^* = \langle y|x\rangle, \quad (1.1.29)$$

implique que $\langle y|y\rangle$ est un nombre réel défini positif

$$\langle y|y\rangle \leq 0, \quad (1.1.30a)$$

et

$$\langle y|y\rangle = 0 \Rightarrow |y\rangle = 0. \quad (1.1.30b)$$

La **norme** d'un vecteur d'état $|y\rangle$ est définie par

$$\| |y\rangle \| = \sqrt{\langle y|y\rangle}. \quad (1.1.31)$$

Lorsque

$$\langle x|x\rangle = 1, \quad (1.1.32)$$

on dit que le vecteur d'état $|x\rangle$ est **normalisé**.

Si chaque élément d'une base est normalisé et que les éléments de la base sont orthogonaux les uns par rapport aux autres, on dit que la base est **orthonormée**. C'est par exemple le cas de la base $\{|+\rangle, |-\rangle\}$ avec

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \quad (1.1.33)$$

' Une des propriétés importantes du produit scalaire est l'*inégalité de Cauchy-Schwarz*

$$|\langle x|y\rangle|^2 \leq \langle x|x\rangle \langle y|y\rangle = \| |x\rangle \|^2 \| |y\rangle \|^2. \quad (1.1.34)$$

Maintenant que nous sommes un tout peu outillé en manipulations mathématiques du qubit, des amplitudes de probabilités, des probabilités, essayons de mieux les comprendre physiquement.

1.2 Phénomènes quantiques : Interférence à une particule

Afin de mettre en évidence l'étrange comportement des qubits, quelques expériences ont été réalisées avec des objets quantiques (photons, électrons, neutrons, atomes, molécules) isolées, ce qui écarte l'hypothèse des effets collectifs³.

Rendons-nous donc au laboratoire !!

1.2.1 Fentes d'Young

Commençons par le dispositif des fentes d'Young de la figure 1.2.1 qui nous est très familier. La source S émet un faisceau lumineux et le détecteur mesure l'intensité lumineuse pour différentes positions de x . Si une seule fente est ouverte, l'intensité est maximale à la position x alignée horizontalement sur la fente F_1 . Lorsqu'on éloigne le détecteur de cette position x , l'intensité diminue progressivement et devient nulle. Cependant, lorsque les deux fentes sont ouvertes, la figure des intensités n'est pas la somme des deux figures d'intensité des fentes individuelles ouvertes, mais plutôt une figure d'interférence : on observe au détecteur une alternance de franges brillantes et de franges sombres (voir la figure 1.2.2). Il y a donc interférence entre les faisceaux lumineux provenant des deux fentes.

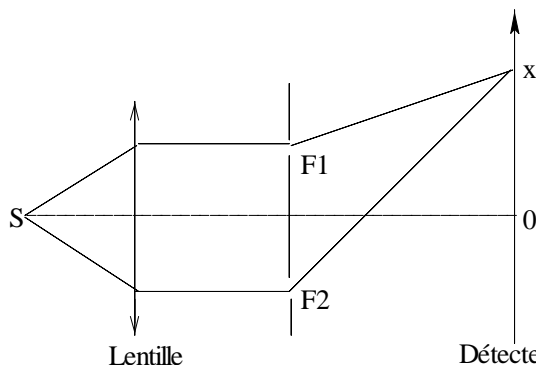


Figure 1.2.1 – Dispositif des fentes de Young

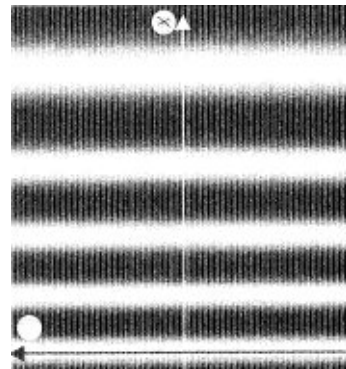


Figure 1.2.2 – Interférence lumineuse lorsque les deux fentes sont ouvertes. On a une alternance de franges brillantes et de franges sombres.

Utilisons maintenant un dispositif spécial dont la source S ne produit que des électrons uniques qui sont dirigés vers les fentes F_1 et F_2 . L'électron a une charge bien déterminée et la proposition *un seul électron est bien passé soit par F_1 , soit par F_2* est bien décidable (deux chemins possibles). Chaque électron est capté en un point bien précis du détecteur comme on peut le voir sur la figure 1.2.3 (a). Ces points d'impact sont cependant **aléatoires** : les différents électrons indépendants préparés dans les *mêmes* conditions ont des impacts *différents*. Ce qui est en contradiction avec le **déterminisme** classique qui veut à des *conditions initiales identiques*, correspondent des *conditions finales identiques*.

Au bout d'un temps suffisamment long, on observe avec surprise que les impacts des électrons forment une figure d'interférence comme illustrée par la figure 1.2.3 (d). Ce résultat est surprenant en ce sens que l'électron est un **corpuscule**. Or nous savons qu'une onde emplit tout

³Mécanisme au terme duquel le sort d'un objet quantique conditionnerait celui du suivant.

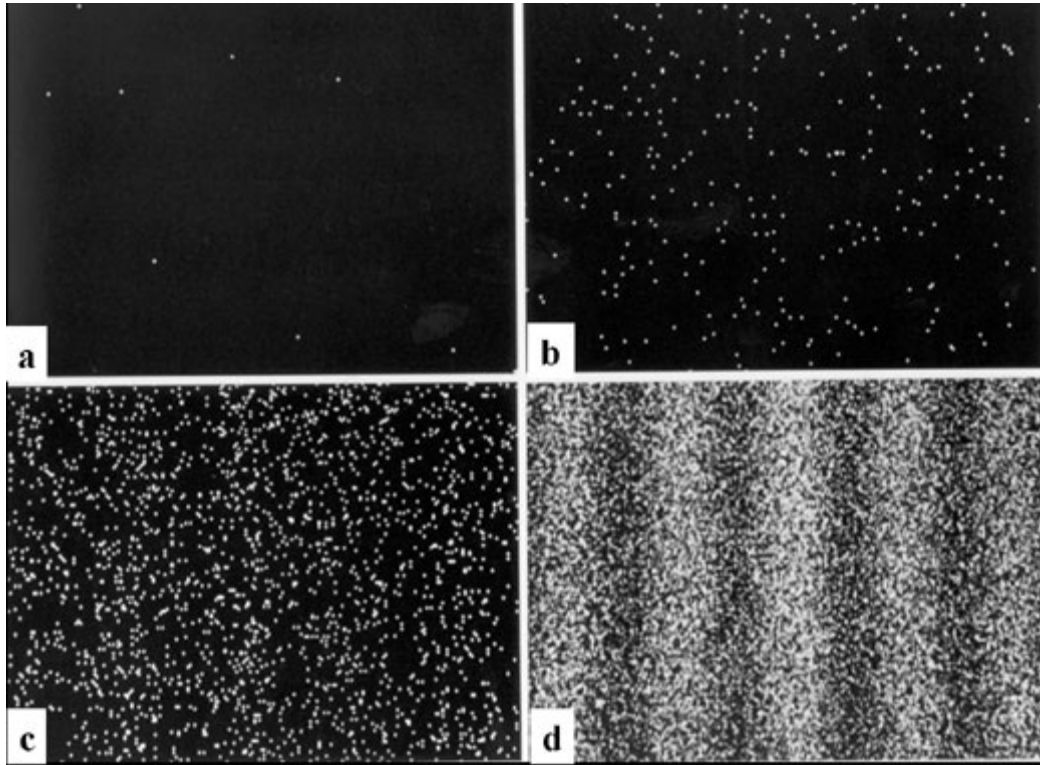


Figure 1.2.3 — Figures d'interférence obtenues avec des électrons uniques. Le nombre d'électrons sur le détecteur augmente au cours du temps. Le temps d'exposition entre la figure (a) et la figure (d) est multiplié par 20. (a) 8 électrons; (b) 270 électrons; (c) 2000 électrons; (d) 6000 électrons. [D'après Hitachi Advanced Research Laboratory, Saitama, Japan].

l'espace ! Les électrons sont uns et **indivisibles**, donc il n'y a pas de fragmentation d'un quantum d'énergie $\hbar\omega$. D'après Paul Dirac, **chaque électron interfère avec lui-même** comme une onde⁴. Il y a donc antinomie : *les concepts classiques d'onde et de corpuscules semblent ne plus être valables pour les objets quantiques*.

Lorsqu'on réalise une autre expérience où le chemin emprunté par l'électron est **discernable**, F_1 ouvert seul ou F_2 ouvert seul, on n'observe pas de figure d'interférence, mais plutôt des impacts distribués autour des sorties F_1 ou F_2 . La somme de ces deux distributions distinctes ne ressemble en rien la figure obtenue quand les deux fentes sont ouvertes. On ne peut donc analyser le phénomène d'interférence des électrons uniques en termes de probabilité classique : ***lorsqu'à la même issue correspondent des processus indépendants différents, la probabilité de cette issue n'est pas la somme des probabilités individuelles***.

1.2.2 Interférométrie de Mach Zehnder

Afin de mieux analyser le comportement des objets quantiques, examinons, après V. Scarani[VSC2004], les expériences qui mènent à l'interférométrie de Mach Zehnder. On a (voir les figures 1.2.4-1.2.7) :

- une *source* qui envoie des objets quantiques isolés, un à un, l'un après l'autre ;
- des *séparateurs* qui sont des miroirs semi-transparentes ;

⁴En fait, avant la mesure, l'électron est dans une **superposition d'états**, et c'est chacun de ces états qui a interféré avec les autres.

- et des *détecteurs*, dispositifs de mesure permettant de compter les objets quantiques.

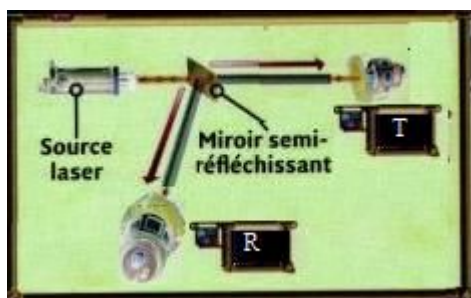


Figure 1.2.4 – Expérience MZ1 : Montage à 2 chemins ou fonctionnement d'un miroir semi-transparent.

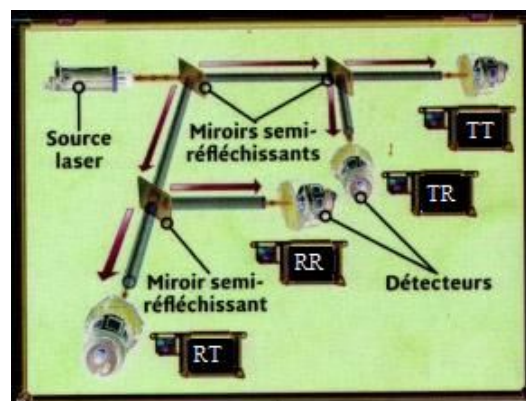


Figure 1.2.5 – Expérience MZ2 : Montage à 4 chemins avec 3 miroir semi-transparentes.

1.2.3 Expérience MZ1

Figure 1.2.4 : Les objets quantiques arrivent individuellement sur le séparateur et on compte combien d'entre eux sont réfléchis (R), et combien sont transmis (T). Après le passage d'un grand nombre d'objets quantiques, on fait les deux observations suivantes :

1. Les deux détecteurs ne s'activent jamais au même instant, donc l'objet est **indivisible**, il est soit réfléchi, soit transmis (deux **chemins** possibles) ;
2. On dénombre la moitié des objets en R et l'autre en T, donc la probabilité pour qu'un objet quantique soit réfléchi est la même qu'il soit transmis et les deux probabilités sont 50%.

1.2.4 Expérience MZ2

Il y a lieu de se poser la question de savoir si en sortant de la source, chaque objet n'a pas une *instruction* lui permettant, chaque fois qu'il rencontre un séparateur, d'être soit seulement réfléchi, soit seulement transmis ?

Afin d'élucider cela, à chaque sortie du premier séparateur, on place un autre séparateur et on obtient *quatre* chemins possibles (figure 1.2.5) : l'objet quantique peut être réfléchi deux fois (RR), réfléchi puis transmis (RT), transmis puis réfléchi (TR) ou transmis deux fois (TT).

Si chaque objet avait une *instruction* lui permettant, chaque fois qu'il rencontre un séparateur, d'être soit seulement réfléchi, soit seulement transmis, alors après le passage d'un grand nombre d'objets quantiques, on observerait 50% des objets en RR et 50% des objets en TT, et rien en RT ou TR.

Mais on observe qu'à chaque sortie, on a 25% d'objets à chaque sortie.

1.2.5 Expérience MZ3

Figure 1.2.6 : On a maintenant un interféromètre de Mach Zehnder : à chaque sortie du premier séparateur, on place maintenant un miroir parfait qui réfléchit tous les objets, les orientant vers un deuxième séparateur. Ainsi, une des sorties du deuxième séparateur correspond aux chemins

RT ou TR, l'autre aux chemins RR ou TT. On a donc à nouveau quatre chemins possibles, de longueur égale.

En vertu de la deuxième expérience, à la sortie RT ou TR, on observera $25\% + 25\% = 50\%$ d'objets quantiques, et à la sortie RR ou TT, 50% d'objets quantiques.

Cependant, on observe que **tous les objets quantiques se trouvent à la sortie RT ou TR** : le chemin RT est indiscernable du chemin TR après détection. On ne peut savoir quel chemin l'objet quantique détecté a pris !

On dit qu'il y a une **interférence constructive** à la sortie RT ou TR et une **interférence destructive** à la sortie TT ou RR. Puisqu'il y a une seule particule à la fois, on parle d'**interférence à une particule**. Concrètement, un pic d'intensité sur une des sorties correspond à un creux à l'autre sortie et inversement.

Le hasard quantique est vraiment étrange : lorsqu'on assemble d'une certaine manière deux diviseurs de faisceau ou beam-splitters (générateurs de hasard), on retrouve la certitude !

Posons-nous les deux questions suivantes qui admettent les réponses *oui* ou *non* :

Q1 : l'objet quantique a-t-il pris le chemin T après le premier séparateur ?

Q2 : l'objet quantique est-il détecté à la sortie RT ou TR ?

Dans la configuration de notre expérience MZ3, Q2 est toujours *oui*, mais ne pouvons pas répondre à Q1.

Si on modifie l'expérience en insérant des détecteurs aux chemins R et T après le premier séparateur, de sorte à pouvoir répondre à Q1, alors la réponse à la question Q2 est modifiée. Seule la moitié des objets quantiques donneront la réponse *oui*, conformément à l'expérience MZ1. Donc si l'objet quantique laisse une *trace* de son passage, on observe pas d'interférence.

*Il est donc impossible de savoir par quel chemin est passé l'objet quantique et observer les interférences. C'est le paradoxe connu sous le nom du **chat de Schrödinger**.*

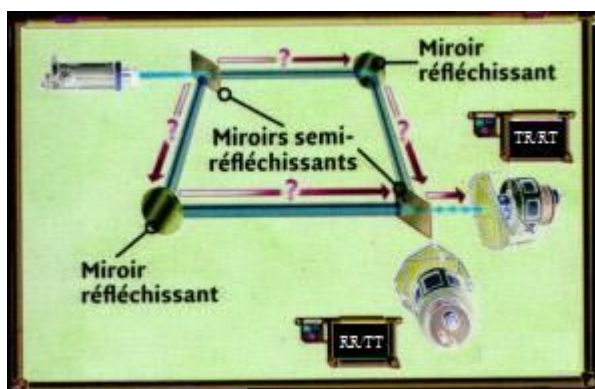


Figure 1.2.6 – Expérience MZ3 : Interféromètre de Mach Zehnder équilibré. Les chemins sont indiscernables.

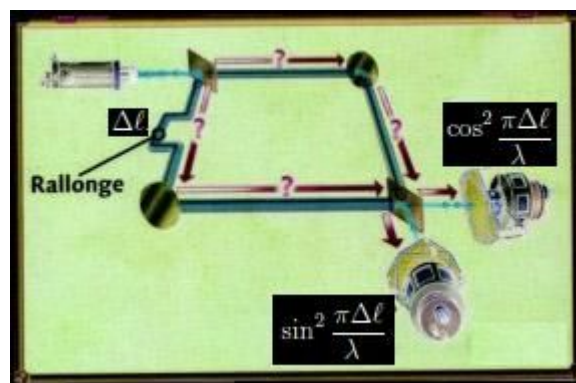


Figure 1.2.7 – Expérience MZ4 : Interféromètre de Mach Zehnder déséquilibré. Les chemins sont discernables et l'objet quantique explore tous les chemins possibles.

1.2.6 Expérience MZ4

Figure 1.2.7 : On modifie la longueur des chemins RT ou TR, en y introduisant par exemple une longueur supplémentaire $\Delta\ell$. On constate que les probabilités de détection des objets quantiques aux sorties (RT ou TR) et (RR ou TT) sont respectivement

$$\cos^2 \frac{\varphi}{2} \text{ et } \sin^2 \frac{\varphi}{2}, \quad \varphi = 2\pi \frac{\Delta\ell}{\lambda}. \quad (1.2.1)$$

Ainsi, lorsque par exemple,

- $\Delta\ell = \lambda$ (lame d'onde), tous les objets quantiques sont détectés à la sortie RT ou TR.
- $\Delta\ell = \frac{\lambda}{2}$ (lame demi-d'onde), tous les objets quantiques sont détectés à la sortie RR ou TT ;
- $\Delta\ell = \frac{\lambda}{4}$ (lame quart-d'onde), une moitié des objets quantiques est détectés à la sortie RR ou TT et l'autre moitié à la sortie RT ou TR ;

Donc, lorsqu'on modifie un seul des deux chemins, on modifie le comportement des tous les objets quantiques.

Comme on peut le voir sur les figures d'interférences 1.2.8, les différences de longueurs d'onde pour lesquelles toute la lumière est détectée dans RT ou TR correspondent à des pics d'intensité maximale (franges brillantes, interférences constructives) dans le montage des fentes d'Young. Les différences de longueurs d'onde pour lesquelles toute la lumière est détectée dans RR ou TT correspondent à des creux d'intensité nulle (franges sombres, interférences destructives) dans le montage des fentes d'Young.



Figure 1.2.8 – Figures d'interférences obtenues au détecteur RT ou TR et RR ou TT. La complémentarité des franges est remarquable.

En résumé

1. Chaque objet quantique est indivisible lors de la détection, comme un **corpuscule**.
2. Dans les expériences MZ1 et MZ2, il y a un seul chemin qui conduit à chaque détecteur ; chaque objet quantique détecté a emprunté un chemin connu : *c'est la situation de **discernabilité**, il n'y a pas d'interférence.*
3. Dans les expériences MZ3 et MZ4, on ne peut dire quel chemin chaque objet quantique détecté a emprunté, puisque que deux chemins sont possibles. *Ces deux chemins sont indiscernables et les effets d'interférence sont présents.* On peut donc énoncer le principe suivant :

Principe 1.2.1 (Indiscernabilité des chemins) *Les interférences apparaissent lorsqu'un objet quantique peut emprunter plusieurs chemins pour arriver au même détecteur, et que ces chemins sont **indiscernables** après la détection.*

On peut dire que le comportement des objets quantiques dépend de toutes les possibilités indiscernables.

- Chaque objet quantique explore tous les chemins possibles (**délocalisation**) comme une onde, cependant elle est indivisible à la détection. Si cette exploration de tous les chemins n'était pas possible, toutes les objets quantiques ne seraient pas influencés par le changement de longueur d'un seul chemin.

*Un objet quantique n'a donc pas **une trajectoire** bien définie.*

- Dans l'expérience MZ3, lorsqu'on cherche à savoir par quel chemin est passé l'objet quantique, on n'observe plus de figure d'interférence. On dit alors que

la mesure perturbe le système : il y a une perturbation incontrôlable de l'objet quantique par la mesure. La description quantique des phénomènes doit englober l'effet de l'appareil de mesure.

L'interposition d'un instrument de mesure modifie le chemin emprunté et la discernabilité apparaît.

Ce phénomène est d'ailleurs à la base de la *cryptographie quantique*⁵ car toute tentative d'espionnage est immédiatement détectée par la perturbation qu'elle introduit.

Soulignons que depuis les années '70, on a pu observer des figures d'interférences avec des objets quantiques aussi divers que photons, les neutrons, les atomes et même de molécules comme les fullèrenes ou footballènes⁶ C_{60} qui ont 1080 particules quantiques élémentaires : 360 protons, 360 neutrons et 360 électrons.

Achevons cette section en introduisant le terme **quanton** pour désigner les objets quantiques que sont les photons, électrons, neutrons, atomes, molécules, ..., qui dans certaines conditions, à savoir pour les valeurs de l'action caractéristique très supérieures à \hbar , peuvent présenter l'un ou l'autre des deux aspects particuliers, et être approximativement décrits, soit comme des particules (lorsqu'il y a échange d'énergie), soit comme des ondes (lorsqu'il y a transmission d'énergie).

Sortons du laboratoire et reprenons le chemin de la salle de cours.

1.3 Notion d'amplitude de probabilité

1.3.1 Vecteurs d'état et amplitudes de probabilité

L'objet de cette section n'est pas d'expliquer *pourquoi* il y a étrangeté au niveau quantique, mais plutôt de définir les règles permettant de comprendre ce comportement étrange. Il s'agit par exemple de comprendre par quel mécanisme, un quanton provenant de S choisit d'être transmis ou réfléchi sur un miroir semi-transparent BS. Cela exige un formalisme nouveau, que nous avons introduit à la **section 1.1**, à travers le qubit et l'espace de Hilbert, de façon à dépasser l'antinomie entre les notions d'onde et de corpuscule. A cet effet, étudions l'interféromètre de Mach-Zehnder déséquilibré de la figure 1.3.1.

⁵Le sécurité de la communication de la Coupe du Monde 2010 a été confiée à société de cryptographie quantique *ID Quantique* fondée par Nicolas Gisin de l'Université de Genève.

⁶[Zeilinger et al. *Nature* **401**, 680 (1999); *J. Mod. Opt.* **47**, 2811 (2000).; *Am. J. Phys.* **71**, 4 (2003)]

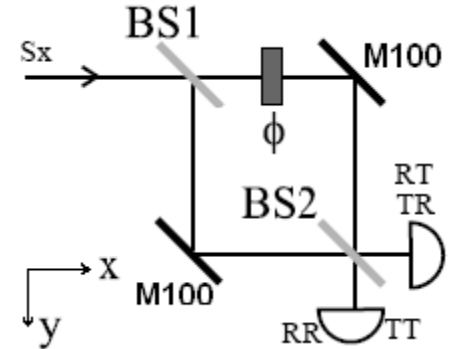
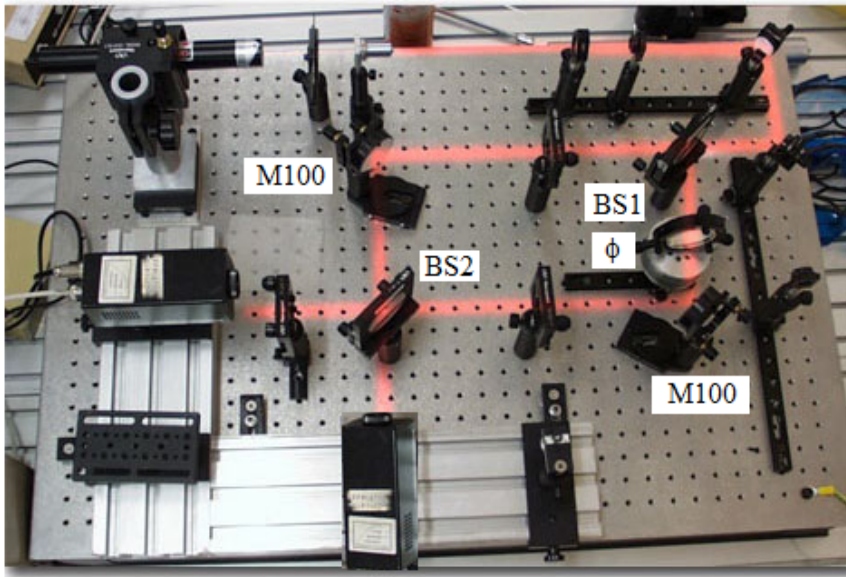


Figure 1.3.1 – Interféromètre de Mach-Zehnder déséquilibré (Image de laboratoire et schéma de principe). La phase ϕ introduit une différence de marche ou de longueur entre les deux bras. BS (Beam-Splitter) représente un miroir semi-transparent. M100 est le miroir parfait.

Définition 1.3.1 Pour une expérience donnée, une **transition** est un ensemble d'états **initiale** et **finale**.

Dans l'expérience des fentes de Young, le passage d'un électron de la source S pour arriver au détecteur à la position x est **une transition**. Sur l'interféromètre de Mach-Zehnder déséquilibré, c'est par exemple le passage d'un quanton du séparateur BS1 à un des détecteurs. L'objet de la théorie quantique est de prédire si cette transition a eu lieu ou non.

On désigne par

- $|x\rangle$ le **vecteur d'état** qui représente le quanton qui se propage dans la direction de x ;
- $|y\rangle$ le **vecteur d'état** qui représente le quanton qui se propage dans la direction de y .

Les coefficients de réflexion r et de transmission t des quantons sur un miroir semi-réfléchissant (BS) s'interprètent comme **les amplitudes de probabilité (ou ondes de probabilité) de réflexion et de transmission**. Ainsi, la **probabilité** de trouver le quanton transmis par un BS unique vaut alors $T = |t|^2$ et celle de le trouver réfléchi vaut $R = |r|^2$. Ces probabilités doivent bien évidemment satisfaire à la **condition de complétude**

$$|t|^2 + |r|^2 = 1. \quad (1.3.1)$$

Puisque les BS de l'interféromètre de Mach-Zehnder sont équilibrés, on a, en vertu de l'expérience MZ1,

$$|t|^2 = |r|^2 = \frac{1}{2} \Rightarrow t = r = \frac{1}{\sqrt{2}}. \quad (1.3.2)$$

Ainsi, l'action d'un BS est

$$\begin{cases} |x\rangle \xrightarrow{BS} |\psi_x\rangle = t|x\rangle + ir|y\rangle = \frac{1}{\sqrt{2}}(|x\rangle + i|y\rangle) \\ |y\rangle \xrightarrow{BS} |\psi_y\rangle = t|y\rangle + ir|x\rangle = \frac{1}{\sqrt{2}}(|y\rangle + i|x\rangle) \end{cases} \quad (1.3.3)$$

1. Le facteur i devant la partie réfléchi est due au fait que la réflexion entraîne un déphasage de $\frac{\pi}{2}$ (entre le chemin incident et le chemin réfléchi), soit un facteur de phase⁷ $e^{i\pi/2} = i$. Ce facteur donne un comportement symétrique aux entrées suivant x et suivant y .
2. $|\psi_x\rangle$ et $|\psi_y\rangle$ sont des **vecteurs d'état** de même nature que $|x\rangle$ et $|y\rangle$: ce sont des vecteurs obtenu comme combinaison linéaires de deux vecteurs. Le vecteur $|\psi_x\rangle$ (ou $|\psi_y\rangle$) décrit la **délocalisation** du quanton dans deux chemins indiscernables, due au BS.
3. Le principe physique correspondant à la possibilité de traiter les états comme des vecteurs, et donc à pouvoir en prendre des combinaisons linéaires, est appelé **principe de superposition des états**.

Un miroir complètement réfléchissant (M100) réfléchi ou *projette* un quanton se déplaçant suivant un axe, sur l'axe orthogonal, avec une amplitude de probabilité ou de projection r' de sorte que la probabilité de trouver le quanton réfléchi M100 sur l'axe orthogonal est $|r'|^2 = 1$:

$$\begin{aligned} |x\rangle &\xrightarrow{M100} i|y\rangle \\ |y\rangle &\xrightarrow{M100} i|x\rangle \end{aligned} \quad (1.3.4)$$

La lame placée sur l'un des bras introduit une différence de chemin $\phi = 2\pi\frac{L}{\lambda}$ entre les deux bras qui se traduit un facteur de phase $e^{i\phi}$, de module 1, sur le vecteur représentant le chemin le plus long :

$$|x\rangle \xrightarrow{\phi} e^{i\phi}|x\rangle. \quad (1.3.5)$$

Ainsi, les amplitudes de probabilité ou ondes de probabilité des quatre chemins possibles que peut emprunter le quanton envoyé suivant x et détecter après BS2 sont :

$$\begin{aligned} A(TR) &= te^{i\phi}i(ir) = -tre^{i\phi} & A(TT) &= te^{i\phi}it = i|t|^2e^{i\phi} \\ A(RT) &= (ir)it = -rt & A(RR) &= (ir)i(ir) = -i|r|^2 \end{aligned} \quad (1.3.6)$$

et les amplitudes de probabilité de détecter les quantons dans les sorties

$$\begin{aligned} x \text{ (TR ou RT)} : & A(x) = A(TR) + A(RT) = -rt(1 + e^{i\phi}) = -\frac{1}{2}(1 + e^{i\phi}) \\ y \text{ (TT ou RR)} : & A(y) = A(TT) + A(RR) = i(|t|^2e^{i\phi} - |r|^2) = \frac{i}{2}(e^{i\phi} - 1) \end{aligned} \quad (1.3.7)$$

et les probabilités correspondantes (voir la figure 1.3.2)

$$\begin{aligned} \mathcal{P}(x) &= |A(TR) + A(RT)|^2 = |t|^2|r|^2|1 + e^{i\phi}|^2 = \frac{1}{2}(1 + \cos \phi) = \cos^2 \frac{\phi}{2} \\ \mathcal{P}(y) &= |A(TT) + A(RR)|^2 = |t|^2|r|^2|e^{i\phi} - 1|^2 = \frac{1}{2}(1 - \cos \phi) = \sin^2 \frac{\phi}{2} \end{aligned} \quad (1.3.8)$$

On vérifie bien que

$$\mathcal{P}(x) + \mathcal{P}(y) = 1. \quad (1.3.9)$$

Pour $\phi = 2n\pi$, $n \in \mathbb{N}$, tous les quantons sont détectés en x ; pour $\phi = (2n + 1)\pi$, $n \in \mathbb{N}$, tous les quantons sont détectés en y .

Il est donc clair que les quantons n'interfèrent jamais entre eux, seuls interfèrent les champs ou amplitudes qui déterminent où et quand on peut les trouver et avec quelle probabilité.

⁷En optique ondulatoire, dans l'étude des interfaces, on suppose (hypothèse qui est toujours formulée implicitement) que l'origine du temps sur le rayon réfléchi est mesurée par le même observateur qui mesure le rayon incident.

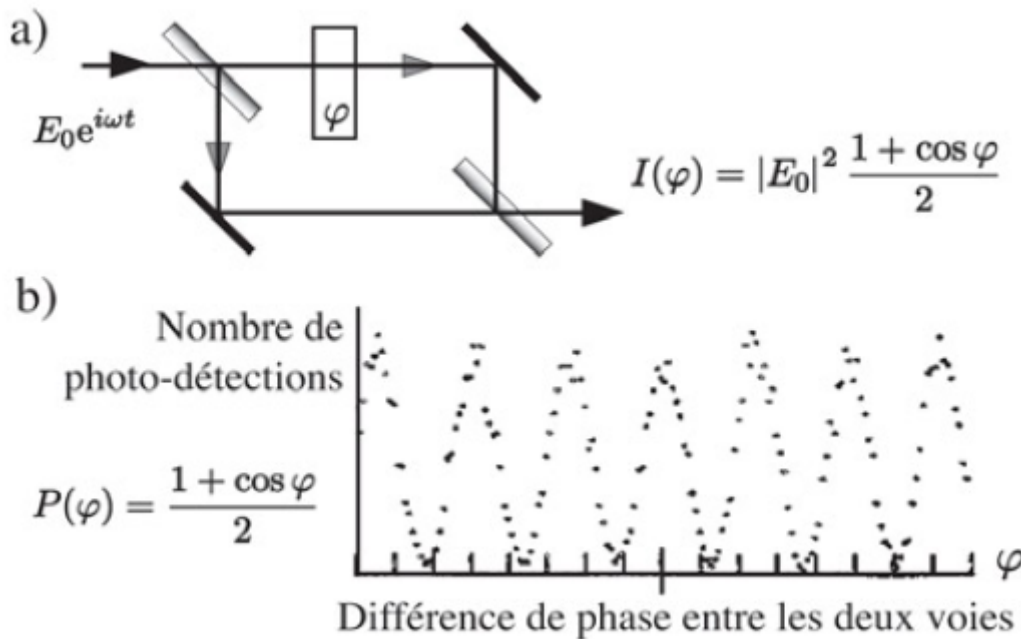


Figure 1.3.2 – a) Dans un interféromètre alimenté par un champ classique, l'intensité lumineuse $I(\varphi)$ en sortie oscille avec la différence de phase φ entre les deux chemins. b) Lorsqu'un photon unique est envoyé dans l'interféromètre, la probabilité de photo-détection $P(\varphi)$ en sortie varie avec φ comme l'intensité qui serait obtenue pour un champ classique. En traçant l'histogramme du nombre de photo-détections en fonction de φ lorsque l'expérience est répétée un grand nombre de fois, on retrouve le système de franges attendu dans le cas classique [Après P. Grangier et al. Europhys. Lett., **1**, 173 (1986)]

Cette interprétation que nous venons de faire est très générale :

*il y a interférence chaque fois qu'un système physique peut prendre plusieurs chemins distincts, pour évoluer vers un même état final, sans qu'il soit possible, par quelque mesure que ce soit, de savoir quel chemin a été emprunté (des chemins indiscernables). A chaque chemin est associée une amplitude de probabilité A et le carré du module de la somme de ces amplitudes donne la probabilité \mathcal{P} de trouver le système dans l'état final considéré. Ainsi, dans un interféromètre à deux ondes comme un interféromètre de Mach Zehnder, **ce ne sont pas les quantons qui interfèrent un à un**; pour chaque quanton, ce sont les amplitudes de probabilité associées aux deux chemins qu'il peut prendre qui interfèrent.*

1.3.2 Règles de calcul des amplitudes de probabilité

Il apparaît que pour calculer les amplitudes de probabilités et les probabilités quantiques, il faut définir des règles précises.

Définition 1.3.2 *L'amplitude quantique, qui détermine où et quand on peut trouver un objet quantique et avec quelle probabilité, n'est définie que lorsque l'état initial $|i\rangle$ et l'état final $|f\rangle$ du système quantique considéré sont spécifiés de façon unique, c'est-à-dire décrivent exhaustivement le système tout entier. Ces états $|i\rangle$ et $|f\rangle$ définissent une **transition quantique**.*

1. L'amplitude de probabilité de la transition $f \leftarrow i$ s'écrit

$$A(f \leftarrow i) = \langle f | i \rangle, \quad (1.3.10a)$$

et la **probabilité** correspondante s'écrit

$$\mathcal{P}(f \leftarrow i) = |\langle f | i \rangle|^2. \quad (1.3.10b)$$

La relation (1.3.10b) est connue sous le nom de la **règle de Born**.

- Dans le dispositif des fentes d'Young (DFY), on a

$$A(x \leftarrow S) = \langle x | S \rangle. \quad (1.3.11)$$

- Dans l'interféromètre de Mach-Zehnder (IMZ), partant du quanton qui se propage suivant S_x , on a la transition quantique menant au détecteur suivant x (TR ou RT) et la transition quantique menant au détecteur suivant y (TT ou RR). On a donc

$$A(x \leftarrow S_x) = \langle x | S_x \rangle \quad (1.3.12a)$$

$$A(y \leftarrow S_x) = \langle y | S_x \rangle \quad (1.3.12b)$$

2. Pour obtenir la probabilité $\mathcal{P}(f \leftarrow i)$ d'observer l'état final $|f\rangle$, on additionne toutes les amplitudes quantiques conduisant au résultat $|f\rangle$ en partant de $|i\rangle$:

$$A(f \leftarrow i) = \sum_n A_n(f \leftarrow i), \quad (1.3.13)$$

où les amplitudes A_n correspondent aux divers chemins physiquement indiscernables. D'où le principe suivant :

Principe 1.3.1 Superposition. *On somme les amplitudes quantiques correspondant à tous les chemins indiscernables (par exemple TR ou RT; RR ou TT) ou à des états finaux identiques.*

- Dans DFY

$$A(x \leftarrow S_x) = A_{F_1}(x \leftarrow S) + A_{F_2}(x \leftarrow S), \quad (1.3.14a)$$

$$\langle x | S \rangle = \langle x | F_1 \rangle \langle F_1 | S \rangle + \langle x | F_2 \rangle \langle F_2 | S \rangle. \quad (1.3.14b)$$

- Dans IMZ,

$$A(x \leftarrow S_x) = A(TR)(x \leftarrow S_x) + A(RT)(x \leftarrow S_x) \quad (1.3.15a)$$

$$\langle x | S_x \rangle = \langle x | R_2 \rangle \langle R_2 | M_x \rangle \langle M_x | T_1 \rangle \langle T_1 | S_x \rangle + \langle x | T_2 \rangle \langle T_2 | M_y \rangle \langle M_y | R_1 \rangle \langle R_1 | S_x \rangle \quad (1.3.15b)$$

$$A(y \leftarrow S_x) = A(TT)(y \leftarrow S_x) + A(RR)(y \leftarrow S_x) \quad (1.3.15c)$$

$$\langle y | S_x \rangle = \langle y | T_2 \rangle \langle T_2 | M_x \rangle \langle M_x | T_1 \rangle \langle T_1 | S_x \rangle + \langle y | R_2 \rangle \langle R_2 | M_y \rangle \langle M_y | R_1 \rangle \langle R_1 | S_x \rangle \quad (1.3.15d)$$

Le fait d'ajouter les amplitudes de transition intermédiaires (l'électron passe par F_1 ou F_2 par exemple) signifie qu'**on ne peut attribuer au quanton une trajectoire bien définie**. Cependant, quelle que soit la position x du détecteur, l'amplitude $\langle x | S \rangle$ est **complètement déterminée** par les amplitudes de transition **vers** et **provenant** des deux fentes, celles-ci étant les seules transitions possibles.

La superposition d'états quantiques ouvre la voie vers des applications très sophistiquées comme

- la **cryptographie quantique** qui garantirait aux utilisateurs une intimité absolue dans leur communication grâce au **qubit**, superposition des états $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ qui a une infinité de valeurs alors que le **bit** classique ne peut prendre que deux valeurs, symbolisées par 0 et 1 ;
- la **téléportation quantique** qui permet la transmission d'information *instantanée* sur des distances illimitées ;
- l'**ordinateur quantique** dont le temps de calcul sera radicalement inférieur comparé à celle des ordinateurs classiques actuels. On pense qu'en superposant les états quantiques qui réalisent des opérations parallèles simultanément, les ordinateurs quantiques peuvent rompre des codes de chiffrement et exercer d'autres miracles technologiques impossibles avec un ordinateur classique.

Soulignons qu'à travers la superposition des états, la cryptographie quantique repose sur le principe d'indétermination d'Heisenberg qui induit que *toute mesure perturbe nécessairement l'état des électrons*. Donc toute tentative d'interception est détectée, même si on intercepte et que l'on réinjecte un électron dans le système après lecture.

3. Lorsqu'une transition peut se faire par des voies intermédiaires en principe discernables, chacun de ces états peut être considéré comme final pour une partie de la transition.

Principe 1.3.2 Addition des probabilités. *Lorsqu'on a pour un état initial plusieurs états finaux différents ou disjoints, et donc plusieurs transitions quantiques, la probabilité de transition vers l'ensemble de ces états est la somme des probabilités vers chacun de ces états :*

$$\mathcal{P}(f \leftarrow i) = \sum_n \mathcal{P}(f_n \leftarrow i). \quad (1.3.16)$$

Lorsque la somme des probabilité de transition est l'unité, on dit que ces états forment un ensemble complet. C'est la propriété de **complétude** (voir l'Eq. (1.3.9)) :

$$\sum_n \mathcal{P}(f_n \leftarrow i) = 1. \quad (1.3.17)$$

4. Pour évaluer les amplitudes de l'Eq. (1.3.6), nous avons utilisé le principe suivant :

Principe 1.3.3 Factorisation séquentielle. *Lorsqu'une transition quantique peut se décomposer en plusieurs sous-transitions ou états intermédiaires, l'amplitude de probabilité de la transition se factorise en produit des amplitudes correspondant aux sous-transitions de la transitions :*

$$A_n(f \leftarrow i) = A_n(f \leftarrow j)A_n(j \leftarrow k) \cdots A_n(\ell \leftarrow i). \quad (1.3.18)$$

L'expression (1.3.18) s'énonce en lisant de droite à gauche, puisque alors les différents états consécutifs occupés seront énoncés dans l'ordre : état initial - état intermédiaire - état final.

Les sous-transitions ou états intermédiaires des divers transitions indiscernables sont,

- dans DFY,

$$A_{F_1}(x \leftarrow S) = A_{F_1}(x \leftarrow F_1)A_{F_1}(F_1 \leftarrow S) = \langle x | F_1 \rangle \langle F_1 | S \rangle, \quad (1.3.19a)$$

$$A_{F_2}(x \leftarrow S) = A_{F_2}(x \leftarrow F_2)A_{F_2}(F_2 \leftarrow S) = \langle x | F_2 \rangle \langle F_2 | S \rangle; \quad (1.3.19b)$$

- dans IMZ,

$$\begin{aligned} A(TR)(x \leftarrow S_x) &= A(TR)(x \leftarrow R_2)A(TR)(R_2 \leftarrow M_x)A(TR)(M_x \leftarrow T_1)A(TR)(T_1 \leftarrow S_x) \\ &= \langle x | R_2 \rangle \langle R_2 | M_x \rangle \langle M_x | T_1 \rangle \langle T_1 | S_x \rangle \end{aligned} \quad (1.3.20a)$$

$$\begin{aligned} A(RT)(x \leftarrow S_x) &= A(RT)(x \leftarrow T_2)A(RT)(T_2 \leftarrow M_y)A(RT)(M_y \leftarrow R_1)A(RT)(R_1 \leftarrow S_x) \\ &= \langle x | T_2 \rangle \langle T_2 | M_y \rangle \langle M_y | R_1 \rangle \langle R_1 | S_x \rangle \end{aligned} \quad (1.3.20b)$$

$$\begin{aligned} A(TT)(y \leftarrow S_x) &= A(TT)(y \leftarrow T_2)A(TT)(T_2 \leftarrow M_x)A(TT)(M_x \leftarrow T_1)A(TT)(T_1 \leftarrow S_x) \\ &= \langle y | T_2 \rangle \langle T_2 | M_x \rangle \langle M_x | T_1 \rangle \langle T_1 | S_x \rangle \end{aligned} \quad (1.3.20c)$$

$$\begin{aligned} A(RR)(y \leftarrow S_x) &= A(RR)(y \leftarrow R_2)A(RR)(R_2 \leftarrow M_y)A(RR)(M_y \leftarrow R_1)A(RR)(R_1 \leftarrow S_x) \\ &= \langle y | R_2 \rangle \langle R_2 | M_y \rangle \langle M_y | R_1 \rangle \langle R_1 | S_x \rangle \end{aligned} \quad (1.3.20d)$$

où

- (a) R_1, R_2, T_1 et T_2 désignent les réflexions et les transmissions sur $BS1$ et $BS2$;
- (b) M_x et M_y désignent respectivement les miroirs complètement réfléchissant situés suivant x et y sur la figure (1.3.1).

5. Dans (1.3.14b), les termes $\langle x | F_1 \rangle \langle F_2 | S \rangle$ et $\langle x | F_2 \rangle \langle F_1 | S \rangle$ sont implicitement nuls. En effet, quelle est l'amplitude de transition pour qu'un électron parte de S , passe par la fente F_1 (resp. F_2), sorte par la fente F_2 (resp. F_1) ? La réponse à cette question devrait inclure la transition de la fente F_1 (resp. F_2) à la fente F_2 (resp. F_1), i.e., l'amplitude $\langle F_1 | F_2 \rangle$ (resp. $\langle F_2 | F_1 \rangle$) :

$$\langle x | F_1 \rangle \langle F_1 | F_2 \rangle \langle F_2 | S \rangle \text{ ou } \langle x | F_2 \rangle \langle F_2 | F_1 \rangle \langle F_1 | S \rangle. \quad (1.3.21)$$

Cependant, on peut vérifier expérimentalement qu'on ne peut détecter un électron qui entre par une fente et qui sort par une autre fente. Ainsi, les transitions quantiques observées présentent la *propriété de disjonction mutuelle* :

$$\langle F_1 | F_2 \rangle = \langle F_2 | F_1 \rangle = 0. \quad (1.3.22)$$

Signalons aussi que l'amplitude de transition (et la probabilité) entre un état initial et un état final identiques est égale à l'unité :

$$\langle F_1 | F_1 \rangle = \langle F_2 | F_2 \rangle = 1, \quad (1.3.23a)$$

$$\mathcal{P}(i \leftarrow i) = 1. \quad (1.3.23b)$$

6. Si on considère un ensemble disjoint et complets d'états f_n , on peut écrire

$$1 = \langle i | i \rangle = \sum_n \langle i | f_n \rangle \langle f_n | i \rangle \quad (1.3.24a)$$

$$1 = \sum_n \mathcal{P}(f_n \leftarrow i) = \sum_n |\langle f_n | i \rangle|^2 \quad (1.3.24b)$$

Ces relations suggèrent que

$$\langle f_n | i \rangle = \langle i | f_n \rangle^*. \quad (1.3.25)$$

*D'où la **règle de conjugaison des amplitudes de probabilité quantiques** : les amplitudes de probabilité quantiques de deux transitions inverses l'une de l'autre sont complexes conjuguées*

$$\langle f | i \rangle = \langle i | f \rangle^* \text{ ou } A(f \leftarrow i) = A^*(i \leftarrow f). \quad (1.3.26)$$

*La conséquence immédiate est la **symétrie des probabilités** : les probabilités des deux transitions quantiques inverses sont égales*

$$\mathcal{P}(f \leftarrow i) = \mathcal{P}(i \leftarrow f). \quad (1.3.27)$$

Soulignons que

$$|\langle f | i \rangle|^2 = \langle f | i \rangle^* \langle f | i \rangle = \langle i | f \rangle \langle f | i \rangle. \quad (1.3.28)$$

Ainsi, en vertu de l'Eq. (1.3.15), on a

$$\begin{aligned} \mathcal{P}(x \leftarrow S_x) &= |\langle x | S_x \rangle|^2 = |A(TR)(x \leftarrow S_x)|^2 + |A(RT)(x \leftarrow S_x)|^2 \\ &\quad + A(TR)^*(x \leftarrow S_x)A(RT)(x \leftarrow S_x) + A(RT)^*(x \leftarrow S_x)A(TR)(x \leftarrow S_x) \end{aligned} \quad (1.3.29a)$$

$$\begin{aligned} \mathcal{P}(y \leftarrow S_x) &= |\langle y | S_x \rangle|^2 = |A(TT)(y \leftarrow S_x)|^2 + |A(RR)(y \leftarrow S_x)|^2 \\ &\quad + A(TT)^*(y \leftarrow S_x)A(RR)(y \leftarrow S_x) + A(RR)^*(y \leftarrow S_x)A(TT)(y \leftarrow S_x) \end{aligned} \quad (1.3.29b)$$

Les produits $A(TR)^*(x \leftarrow S_x)A(RT)(x \leftarrow S_x)$, $A(RT)^*(x \leftarrow S_x)A(TR)(x \leftarrow S_x)$, $A(TT)^*(y \leftarrow S_x)A(RR)(y \leftarrow S_x)$ et $A(RR)^*(y \leftarrow S_x)A(TT)(y \leftarrow S_x)$ sont les **termes d'interférences quantiques**.

C'est donc à la superposition des amplitudes de probabilité et la règle de conjugaison des amplitudes de probabilité quantiques qu'on doit les figures d'interférence.

Quand on dit que chaque quanton interfère avec lui-même, il s'agit en fait d'interférences d'amplitudes de probabilité.

Achevons ce chapitre, porte d'entrée dans le merveilleux monde quantique, en notant que classiquement, on est habitué à un *déterminisme* rigide et à la relation de *causalité* : quand on

connaît les conditions initiales, on sait parfaitement ce qui va se passer. En théorie quantique, ces certitudes sont abandonnées. La possibilité de prévoir le comportement d'un système quantique n'est qu'une prédictibilité probabiliste (un seul événement) et statistique (grand nombre d'événements). L'objet quantique est en quelque sorte une *juxtaposition de possibles* : on parle d'*indéterminisme*. On dit aussi que *Dieu joue au dés en théorie quantique*⁸.

Tant que la mesure sur lui n'est pas faite, la grandeur censée quantifier la propriété physique recherchée n'est pas strictement définie. Mais dès que cette mesure est engagée, elle détruit la superposition quantique.

1.3.3 Chat de Schrödinger

Nous avons déjà annoncé la fin du chapitre, alors pourquoi cette section ? Eh bien, pour raconter une histoire au coin du feu !

C'est l'histoire du fameux **paradoxe du chat de Schrödinger** dont nous avons fait allusion à la **section 1.2.2**.

En effet, dans les années 1930, ce célèbre physicien Autrichien avait, en pensée, enfermé un chat dans une boîte en acier contenant un flacon de gaz mortel, un compteur de radioactivité et un atome radioactif. Si le compteur détecte de la radioactivité, un mécanisme casse le flacon, et le chat meurt. Le compteur, appareil macroscopique, ne peut que mesurer l'un des deux états classiques possibles de l'atome : *désintégré* et *non-désintégré*. On suppose qu'après un temps $t_{1/2}$, l'atome se désintègre avec une probabilité (quantique) $\frac{1}{2}$ (voir la figure 1.3.3). Tant qu'aucune mesure n'est effectuée, cet atome se trouve dans un état superposé, à la fois *désintégré* et *non-désintégré*. Par conséquent, tant que la boîte reste fermée, le chat est dans un **état superposé, à la fois mort et vivant** ! Attention, le chat **n'est pas mort-vivant**, il est soit mort, soit vivant, mais tant que la boîte n'est pas ouverte, notre information sur son état est nécessairement constituée de ces deux possibilités. C'est en l'observant que l'on constate que le chat est mort ou vivant. Donc, on réduit le paquet d'ondes, transformant le chat de l'état superposé $\frac{1}{\sqrt{2}}(|vivant\rangle + |mort\rangle)$ à l'état $|vivant\rangle$ ou $|mort\rangle$ ⁹.



Figure 1.3.3 — Le chat de Schrödinger dans la boîte d'acier. Tant que la boîte reste fermée, le chat est dans un état superposé mort et vivant.

⁸Einstein n'a jamais accepté le caractère probabiliste lié à la discontinuité des quanta alors même qu'il avait prouvé en 1905 l'existence des atomes à partir d'une interprétation probabiliste des fluctuations d'entropie dans le mouvement brownien.

⁹En fait il n'y a pas paradoxe, puisque le principe de superposition n'est valable que pour les états quantiques. Or le chat est macroscopique.

Soulignons que depuis quelques années, la tendance en électronique quantique est plutôt d'utiliser les mots *chat de Schrödinger* d'une façon différente, pour caractériser une superposition cohérente de possibilités macroscopiquement distinctes. La cohérence du chat est évidemment une condition suffisante pour qu'il soit dans un état flou à la Schrödinger (la superposition cohérente sous entend nécessairement l'existence des deux possibilités); mais elle n'est pas nécessaire.

Achevons cette histoire au coin du feu en nous demandant si le chat peut être considéré comme un observateur : *le chat peut-il avoir conscience d'être mort ou vivant ?* Le chat ne peut avoir conscience par définition que d'être vivant. Cependant, cela ne l'empêche pas de constituer un observateur acceptable : vivant, il peut laisser dans la boîte des traces de son état, mort, il laisse d'autres types de traces, de sorte que la *mesure* de son état vivant ou mort serait également l'inscription rétroactive (en remontant le temps!) des traces laissées.

Wolai!! Effectuer la mesure dans le monde quantique est une histoire compliquée!!

Remarque 1.3.1 *Bien que le dispositif de Schrödinger soit, il a l'intérêt de mettre en évidence, qu'en principe au moins, l'étrangeté quantique des systèmes microscopiques se communique aux systèmes macroscopiques. Et il pose une question de fond : pourquoi les gens ne voient-ils que des chats soit vivants, soit morts et pas de chats morts-vivants ?*

*D'après la vision actuelle, si le monde semble si bien décrit par la physique classique, c'est parce que les interactions complexes d'un objet avec son environnement font très vite disparaître les particularités quantiques. L'information relative à l'état de santé d'un chat, par exemple, gagne rapidement son environnement sous la forme de photons et d'échanges de chaleur. Chaque phénomène quantique peut impliquer des états superposés du système en jeu (mort ou vivant), mais ces états tendent à disparaître. La fuite permanente d'information vers l'environnement est le mécanisme essentiel par lequel les états quantiques de superposition se détruisent, processus nommé **décohérence**. Les gros systèmes sont davantage sujets à la décohérence que les petits, tout simplement parce qu'ils laissent échapper plus d'informations. C'est pourquoi les physiciens tendent à associer la théorie quantique au monde microscopique. Dans de nombreux cas, toutefois, la perte d'information par un gros système peut être ralentie ou stoppée, ce qui met alors en évidence l'omniprésence des phénomènes quantiques.*

1.4 Exercices et problèmes

1.4.1 Interféromètre de Mach-Zehnder à deux lames

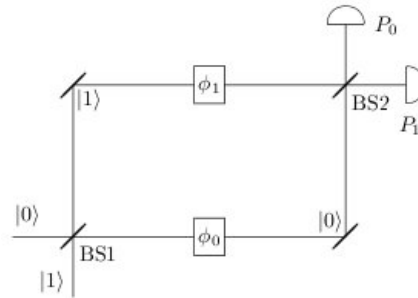


Figure 1.4.1 – MZ à deux lames.

On considère l'interféromètre de la figure 1.4.1. Le quanton qui y pénètre est soit dans l'état $|0\rangle$, soit dans l'état $|1\rangle$. Quelles sont les probabilités \mathcal{P}_0 et \mathcal{P}_1 ce quanton aux détecteurs D_0 et D_1 ?

1.4.2 Amplitudes de probabilité de transition

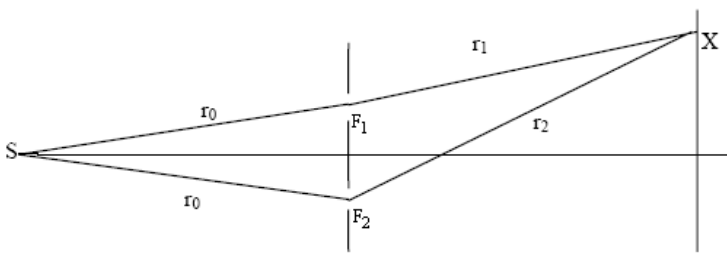


Figure 1.4.2 – Dispositif des fentes d'Young. Les fentes F_1 et F_2 sont à la même distance r_0 de la source S .

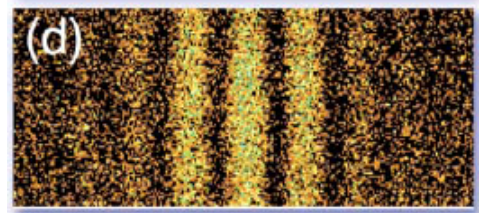


Figure 1.4.3 – Figure d'interférences photon par photon [École Normale Supérieure de Cachan (France, 2005)].

Pour un photon d'énergie bien définie, $E = \hbar\omega$, l'amplitude de probabilité de transition d'un point A à un point B est donnée par :

$$\langle B | A \rangle = \varphi(AB)e^{-i\omega t}, \quad (1.4.1)$$

où t est le temps de parcours et $\varphi(AB)$ est une fonction qui dépend uniquement de la distance entre les points A et B . Dans le cas où la divergence d'un faisceau de lumière peut être négligée tous les photons partant de A arrivent en B . La probabilité de transition pour un photon est égale à l'unité. L'amplitude de probabilité est alors de la forme :

$$\langle B | A \rangle = e^{i\alpha}e^{-i\omega t}, \quad (1.4.2)$$

L'amplitude étant indéterminée à un facteur de phase près on peut poser $\alpha = 0$.

Grâce à un dispositif spécial, la source S ne produit que des photons uniques qui passent soit par F_1 , soit par F_2 et peuvent être détectés au point X (voir la figure 1.4.2). Il existe deux chemins en principe indiscernables.

1. Appliquer le principe de superposition pour exprimer l'amplitude de probabilité $|\psi\rangle = \langle X | S \rangle$ du photon détecté au point X . Expliciter cette expression à l'aide du principe de factorisation séquentielle. En déduire l'expression de la probabilité $\mathcal{P}(X \leftarrow S)$ pour qu'un photon émis par la source S arrive en X en passant par l'une ou l'autre fente en faisant apparaître explicitement les termes d'*interférences quantiques*, en supposant que les amplitudes de probabilité de transition de la source S aux fentes F_1 et F_2 sont les mêmes.
2. Soient t_0 le temps de parcours de la source à l'une des fentes, t_1 le temps de parcours de la fente F_1 au point X , t_2 le temps de parcours de la fente F_2 au point X . Exprimer, en vertu de l'Eq. (1.4.1), chaque amplitude de probabilité de transition intermédiaire en fonction r_i et t_i et en déduire l'expression de $|\psi\rangle$.
3. Aux grandes distances, c'est-à-dire lorsque r_1 et r_2 sont beaucoup plus grands que la distance entre des fentes les amplitudes $\varphi(r_1)$ et $\varphi(r_2)$ sont à peu près égales et on peut écrire $\varphi(r_1) = \varphi(r_2) = C'$. Montrer que la probabilité pour qu'un photon émis par la source S arrive en X en passant par l'une ou l'autre fente est de la forme

$$\mathcal{P}(X \leftarrow S) = 2|C|^2 \left[1 + \cos \frac{\omega}{c}(r_2 - r_1) \right]. \quad (1.4.3)$$

4. Pour quelles valeurs de la différence de marche $r_2 - r_1$, en fonction de λ , a-t-on les franges brillantes et des franges sombres (voir la figure (1.4.3)) ?

1.4.3 Chat de Schrödinger

Nous reprenons dans cette exercice, la célèbre expérience de pensée de Schrödinger en considérant un chat enfermé dans une boîte avec un poison (substance radioactive) qui va déclencher la mort du chat à un moment ou un autre. Classiquement, le chat est soit mort, soit vivant. Quantiquement, on dit que le chat est dans une *superposition d'états mort ou vivant*.

1. Quelle base conceptuelle de la physique classique se trouve remise en cause par cette expérience ?
2. On se place dans la situation quantique. On désigne l'état mort et l'état vivant par les kets respectifs $|m\rangle$ et $|v\rangle$.
 - (a) Exprimer dans la base $\{|m\rangle, |v\rangle\}$ un état quelconque $|\psi\rangle$ du chat.
 - (b) Quelle condition doit être remplie pour que cet état traduise une onde de probabilité ?
 - (c) Quels sont les deux états *limites* ? Quand les obtient-on ?
 - (d) Soit t_1 le temps au bout duquel le chat a une chance sur deux d'être vivant et t_2 celui au bout duquel il a une chance sur quatre d'être vivant. Exprimer les états $|\psi_1\rangle$ et $|\psi_2\rangle$ du chat correspondant à ces instants.
3. En utilisant QuTiP, représenter sur une sphère de Bloch les états $|m\rangle$, $|v\rangle$, $|\psi_1\rangle$ et $|\psi_2\rangle$.

CHAPITRE 2

MESURE ET OPÉRATEURS LINÉAIRES

Sommaire

- 2.1 Mesure de grandeurs physiques et opérateurs
- 2.2 Opérateurs linéaires et représentation matricielle
- 2.3 Décomposition spectrale des opérateurs hermitiens
- 2.4 Inégalités d'Heisenberg
- 2.5 Exercices et problèmes

Maintenant que nous sommes entré dans le monde quantique, il est légitime de se demander comment on y extrait l'information ou comment on y effectue la mesure sur un système. On le fait grâce aux **opérateurs** qui sont des représentations mathématiques, des grandeurs physiques (**section 2.1**). L'essentiel de ce chapitre, très mathématique, est donc consacrée à l'algèbre des opérateurs linéaires (**section 2.2**) et à l'étude des propriétés des opérateurs hermitiens, opérateurs associés aux grandeurs physiques (**section 2.3**).

2.1 Mesure de grandeurs physiques et opérateurs

La théorie quantique est avant tout une théorie des phénomènes microscopiques ou plus exactement nanoscopiques (10^{-9}). Mais la physique est macroscopique (les microscopes, accélérateurs de particules, etc., sont des objets macroscopiques), et il est donc indispensable que les résultats simples de la théorie classique puissent se retrouver en théorie quantique. D'autre part, contrairement à la situation classique, il y a **indéterminisme** dans la mesure, vu que nous ne saurons dire **exactement** où est passé le quanton lorsqu'on observe une interférence avec des fentes de Young ou un interféromètre de Mach Zehnder. De ce fait, il est donc important de se munir d'une théorie de la mesure, afin d'éviter de transposer au monde nanoscopique notre expérience journalière qui est macroscopique¹.

¹Mais où est la limite entre le monde macroscopique et le monde microscopique ?

Définition 2.1.1 Une mesure est le résultat d'une interaction temporaire entre le système et un appareil de mesure (qui peut être un homme). Or comme il y a un quantum d'action minimale, $\frac{\hbar}{2}$ (**il y a un minimum de changement dans la nature**), on ne peut éviter que l'observation influence ou perturbe le système quantique. C'est pourquoi toute description précise de l'observation doit inclure une description de cette perturbation qui est modélisée par un changement d'état.

2.1.1 Mesure de grandeurs physiques

Reprenons le chemin du laboratoire où d'une source nous faisons sortir un jet monocinétique d'atomes électriquement neutres argent (Ag), paramagnétiques, porteurs d'un moment magnétique intrinsèque de spin. Nous avons ainsi préparé N quantons indépendamment dans le même état $|\psi\rangle$. Ces atomes traversent l'entrefer d'un aimant où règne un fort gradient d'induction magnétique $\frac{\partial B}{\partial z}$. Chaque atome est alors soumis à une force $F_z = \mu_z \frac{\partial B}{\partial z}$, où μ_z est la projection du moment magnétique de spin de l'atome sur le vecteur unitaire \mathbf{z} . Lorsque l'induction magnétique est nulle, on observe, sur une plaque de verre placée perpendiculairement au jet à une certaine distance de la sortie de l'entrefer, une tache unique de dimension finie en raison de la dispersion des vitesses. En présence du gradient d'induction magnétique, la théorie classique prévoit un élargissement de la tache précédente du fait de l'orientation à priori aléatoire des moments magnétiques $\boldsymbol{\mu}$ lors de la production des atomes².

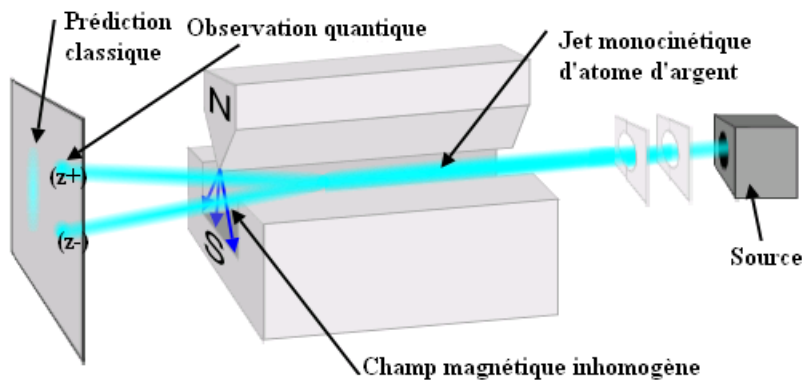


Figure 2.1.1 — *Expérience de Stern et Gerlach : classiquement, on devrait avoir une tache unique de dimension finie, mais on observe plutôt deux taches symétriques d'égales intensités aux points (z_+) et (z_-) .*

Cependant, on observe (voir la figure 2.1.1), que les impacts des atomes, pourtant identiques, se répartissent en deux taches quasi-ponctuelles d'égales intensités I_+ et I_- (de moment magnétique de spin $\mu_+ = +\frac{\hbar}{2}$ et $\mu_- = -\frac{\hbar}{2}$), de part et d'autre du point d'impact en absence d'induction magnétique, à égale distance, i.e., $\mathcal{P}_+ = \mathcal{P}_- = \frac{1}{2}$. On notera $|+\rangle$ (*up*) et $|-\rangle$ (*down*) l'état des atomes de moment magnétique de spin $\mu_+ = +\frac{\hbar}{2}$ et $\mu_- = -\frac{\hbar}{2}$.

Il apparaît que l'appareil de Stern et Gerlach instaure une *corrélation* dans le faisceau émergent entre l'état de spin et sa situation spatiale. On reconnaît alors un spin *up* à ce qu'il a comme point d'impact la position (z_+) et un spin *down* à ce qu'il y a comme point d'impact la

²Les atomes de moment magnétique $\boldsymbol{\mu}$ antiparallèle à Oz devraient subir une déviation maximale vers le haut pour $\frac{\partial B}{\partial z} < 0$. Ceux de $\boldsymbol{\mu}$ parallèle à Oz , une déviation maximale vers le bas. Toutes les déviations intermédiaires étant possibles.

position (z_-). La distance entre ces deux points étant proportionnelle au gradient $\frac{\partial B}{\partial z}$. Ainsi, un atome initialement dans un état de spin quelconque $|\psi\rangle$ (orientation des moments magnétiques *à priori* quelconque), donne après une mesure de la **grandeur physique spin \mathcal{S}** , une valeur $\mu_+ = +\frac{\hbar}{2}$ ou $\mu_- = -\frac{\hbar}{2}$, signifiant qu'*après la mesure* l'atome est dans l'état $|+\rangle$ ou $|-\rangle$. Ainsi, ***lors de son interaction avec l'appareil de mesure, le quanton change d'état.*** On dit qu'il y a **réduction du paquet d'ondes**, autrement, **la mesure a perturbé le système.** ***Cette réduction force l'émergence classique d'un résultat unique.***

Principe 2.1.1 Réduction du paquet d'ondes. *Après une mesure sur un système quantique, on modifie en général l'état de ce système.*

L'ensemble $\{\mu_+, \mu_-\}$ est l'ensemble **complet** des résultats de la mesure de \mathcal{S} puisque ce sont les seules modalités qu'on peut obtenir lors de cette mesure. Cet ensemble complet de résultats est obtenu avec N atomes paramagnétiques dans le même état $|\psi\rangle$. Donc *avant la mesure*, le système est dans l'état superposé (exploration de tous les chemins possibles)

$$|\psi\rangle = \sum_i |i\rangle \langle i|\psi\rangle = \alpha_+ |+\rangle + \alpha_- |-\rangle. \quad (2.1.1)$$

Les amplitudes $\alpha_{\pm} = \langle \pm | \psi \rangle$ décrivent l'*orientation* du spin dans l'espace tridimensionnel : ce sont des *coordonnées ou amplitudes de projections* dans la base des états de spin $\{|+\rangle, |-\rangle\}$.

Du point de vue classique, cette situation est paradoxale puisque le comportement de chaque atome ne peut être prédit, bien qu'il soit tous préparés de la même façon et indépendamment. *Dans chaque atome individuel, il existe l'alternative dichotomique d'être dans l'état spin up ou spin down.*

Les probabilités d'obtenir les moments magnétiques de spin μ_+ et μ_- sont donc

$$\mathcal{P}_+ = |\langle + | \psi \rangle|^2 = |\alpha_+|^2 \text{ et } \mathcal{P}_- = |\langle - | \psi \rangle|^2 = |\alpha_-|^2, \quad (2.1.2)$$

avec

$$\alpha_+ = \alpha_- = \frac{1}{\sqrt{2}}. \quad (2.1.3)$$

Par suite, la probabilité totale est (complétude du système)

$$\mathcal{P} = |\alpha_+|^2 + |\alpha_-|^2 = 1. \quad (2.1.4)$$

L'effet de l'appareil de mesure est décrit par l'**opérateur S** qui opère sur l'état $|\psi\rangle$ pour donner $|+\rangle$ ou $|-\rangle$, **états propres** de S avec les **valeurs propres** $+\frac{\hbar}{2}$ ou $-\frac{\hbar}{2}$:

$$S|\psi\rangle = \begin{cases} +\frac{\hbar}{2} |+\rangle, \\ \text{ou} \\ -\frac{\hbar}{2} |-\rangle. \end{cases} \quad (2.1.5)$$

On dit que l'opérateur transforme un vecteur d'état de l'espace de Hilbert en un autre vecteur d'état du même espace de Hilbert.

Autrement, le lien entre ce qu'on peut observer du système, une grandeur physique \mathcal{A} , et le système, se fait à travers le lien entre l'opérateur A associé à cette grandeur physique et le vecteur d'état.

Autant que possible, nous utiliserons des lettres majuscules (droites) pour les opérateurs.

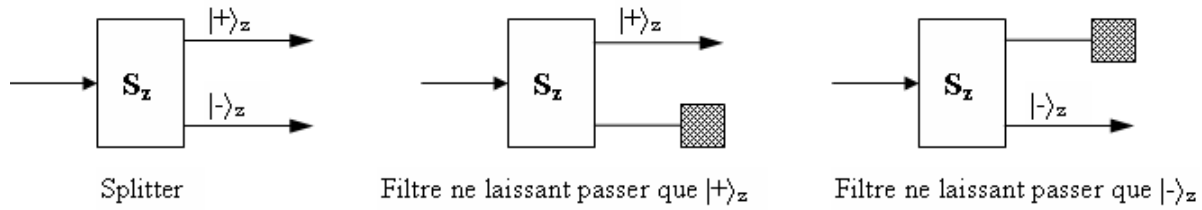


Figure 2.1.2 – Stern et Gerlach comme séparateur du jet atomique ou splitter et comme filtres.

2.1.2 Autres Expériences

Nous allons maintenant réaliser diverses expériences sur le spin en utilisant les symboles de la figure 2.1.2 pour les divers rôles des appareils de Stern et Gerlach.

Première expérience SG1

A la sortie du filtre de la figure 2.1.3, chaque atome est dans un état propre de l'opérateur S_z que l'on mesure. Le résultat de la mesure est donc **certain** : on trouve à coup sûr la valeur propre correspondante $+\frac{\hbar}{2}$

$$\mathcal{P}(+\frac{\hbar}{2}) = |\langle + | + \rangle|^2 = 1. \quad (2.1.6)$$

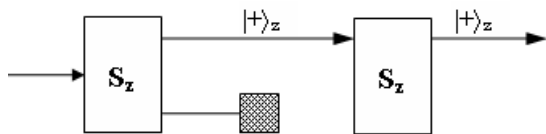


Figure 2.1.3 – Mesure de S_z dans l'état $|+\rangle$.

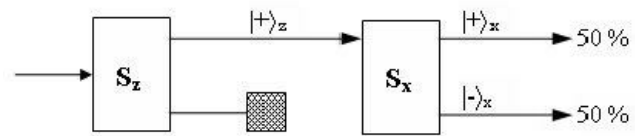


Figure 2.1.4 – Mesure de S_x dans l'état $|+\rangle$.

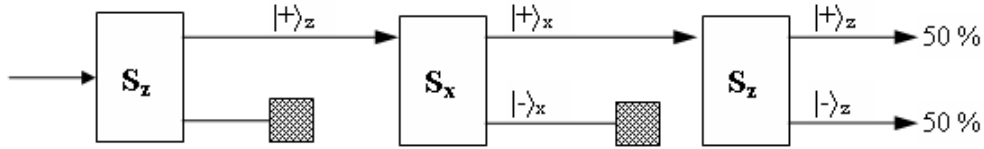
Deuxième expérience SG2

A la sortie du filtre de la figure 2.1.4, chaque atome qui entre dans le splitter orienté dans la direction Ox est dans l'état $|+\rangle$. Lors du processus de mesure de la grandeur S_x , **il y a indétermination dans le comportement de chaque atome** puisque $|+\rangle$ n'est pas un état propre de l'opérateur S_x . Cet opérateur a pour valeurs propres $+\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$ associées respectivement aux états propres $|+\rangle_x$ et $|-\rangle_x$. C'est parce que $|+\rangle$ se projette dans la base $\{|+\rangle_x, |-\rangle_x\}$ qui diagonalise S_x qu'on observe à la sortie deux faisceaux d'égales intensités, i.e.,

1. un faisceau où les atomes ont un spin $+\frac{\hbar}{2}$ avec la probabilité ${}_x\langle + | + \rangle|^2 = \frac{1}{2}$;
2. un faisceau où les atomes ont un spin $-\frac{\hbar}{2}$ avec la probabilité ${}_x\langle - | + \rangle|^2 = \frac{1}{2}$.

Troisième expérience SG3

On filtre maintenant $|+\rangle$ que fait pénétrer dans S_x . On filtre la sortie de ce SG pour ne laisser sortir que $|+\rangle_x$ qui va pénétrer dans un S_z . On constate avec surprise qu'on a à la sortie des atomes dans les états propres $|+\rangle$ et $|-\rangle$ de S_z , alors que $|-\rangle$ a été exclus à la sortie du premier SG, S_z .

Figure 2.1.5 – Incompatibilité des mesures de S_z et S_x .

Cette expérience met en exergue le fait qu'en théorie quantique, *l'état final du système dépend seulement de l'état de l'atome qui entre dans le dernier SG et de son action avec cet appareil*. Autrement, il n'y a pas de mémoire sur l'histoire passée du système.

En clair, comme le faisceau qui entre dans le dernier SG, S_z est dans l'état $|+\rangle_x$ qui n'est pas état propre de S_z , il va se projeter dans la base $\{|+\rangle, |-\rangle\}$ des états propres de S_z . C'est pourquoi on a

1. un faisceau où les atomes ont un spin $+\frac{\hbar}{2}$ avec la probabilité $|\langle + | + \rangle_x|^2 = \frac{1}{2}$;
2. un faisceau où les atomes ont un spin $-\frac{\hbar}{2}$ avec la probabilité $|\langle - | + \rangle_x|^2 = \frac{1}{2}$.

2.1.3 Point sur la mesure

Il découle de ce qui précède que :

1. L'acte de mesure modifie généralement d'une manière *instantanée* le système de façon *irréversible* : c'est la **réduction du paquet d'onde**.
2. **Le résultat complet de la mesure expérimentale** de la grandeur physique \mathcal{A} sur le système consiste à déterminer les modalités a_i (résultats de la mesure) et les amplitudes de probabilité α_i ou les probabilités $\mathcal{P}_i = |\alpha_i|^2$. Autrement dit, il s'agit d'extraire des nombres contenus dans le vecteur d'état $|\psi\rangle$.
3. Les modalités a_i dépendent de la *nature* du système et les amplitudes de probabilité α_i dépendent de l'*état* du système ou du vecteur d'état $|\psi\rangle$.
4. L'**opérateur** A extrait de $|\psi\rangle$ l'information physique sur la grandeur physique \mathcal{A} . $|\psi\rangle$ décrit la réalité physique d'un système quantique individuel.
5. Lorsqu'on a *un seul* système dans l'état $|\psi\rangle$, si *une seule* mesure de \mathcal{A} donne la modalité a_i , le système est après cette mesure dans l'état $|\varphi_i\rangle$ associé à a_i

$$|\varphi_i\rangle = |A\psi\rangle = A|\psi\rangle, \quad (2.1.7)$$

A est l'*opérateur (hermitien)*³ associé à la grandeur physique \mathcal{A} . Si on répète cette mesure de \mathcal{A} **immédiatement après** sur le système, qui est alors dans l'état $|\varphi_i\rangle$, on obtiendra de façon certaine la même modalité a_i avec la probabilité 1 :

$$A|\varphi_i\rangle = a_i|\varphi_i\rangle \text{ ou } A = |\varphi_i\rangle a_i \langle \varphi_i| \quad (2.1.8a)$$

$$\mathcal{P}(a_i) = |\langle \varphi_i | \varphi_i \rangle|^2 = |\langle \varphi_i | \varphi_i \rangle|^2 = 1. \quad (2.1.8b)$$

³Les propriétés d'un opérateur hermitien sont étudiées à la **section (2.2)**

Autrement dit, à chaque résultat possible a_i de la mesure correspond un état $|\varphi_i\rangle$ possédant la propriété ci-dessus, que nous appellerons **état propre**⁴ ou **vecteur propre** de l'opérateur A ; a_i est appelée **valeur propre** de l'opérateur A .

*Donc, la **mesure de \mathcal{A} sur un seul système** dans l'état $|\psi\rangle$ donne l'information sur l'état du système **après la mesure**.*

6. Pour obtenir l'information sur l'état du système **avant la mesure** il faut effectuer N **mesures de \mathcal{A} sur N systèmes identiques**⁵ dans l'état $|\psi\rangle$ afin d'obtenir toutes les modalités possibles a_i :

$$|\psi\rangle = \sum_i |\varphi_i\rangle \langle \varphi_i | \psi \rangle = \sum_i \alpha_i |\varphi_i\rangle, \quad (2.1.9a)$$

$$A|\psi\rangle = \sum_i \alpha_i A|\varphi_i\rangle = \sum_i \alpha_i a_i |\varphi_i\rangle. \quad (2.1.9b)$$

L'ensemble des états propres $|\varphi_i\rangle$ de la grandeur physique forme une base orthonormée

$$\langle \varphi_i | \varphi_j \rangle = \begin{cases} 1, & \text{si } i = j. \\ 0, & \text{sinon.} \end{cases} \quad (2.1.10)$$

D'où les propriétés suivantes de leurs probabilités de transition

$$\begin{aligned} \mathcal{P}(\langle \varphi_i | \varphi_j \rangle) &= 0, \quad \forall i, j \quad i \neq j \quad (\text{disjonction}), \\ \sum_i \mathcal{P}(\langle \varphi_i | \psi \rangle) &= 1, \quad \forall |\psi\rangle \quad (\text{complétude}). \end{aligned} \quad (2.1.11)$$

2.2 Opérateurs linéaires et représentation matricielle

Principe 2.2.1 *A chaque grandeur physique \mathcal{A} , l'on peut associer un **opérateur A , qui est linéaire hermitien** agissant dans l'espace de Hilbert \mathcal{H} , tel que la valeur moyenne $\langle a \rangle_\psi$ des résultats d'une mesure de la grandeur \mathcal{A} pour un quanton dans l'état $|\psi\rangle$ soit*

$$\langle a \rangle = \langle \psi | A | \psi \rangle. \quad (2.2.1)$$

Les opérateurs de la théorie quantique sont linéaires et cette linéarité est intimement liée au **principe de superposition**.

2.2.1 Linéarité et représentation matricielle

On appelle **opérateur linéaire** A de \mathcal{H} , toute application linéaire

$$\begin{aligned} A: \mathcal{H} &\longrightarrow \mathcal{H} \\ |\psi\rangle &\longrightarrow |\varphi\rangle = |A\psi\rangle \equiv A|\psi\rangle \end{aligned} \quad (2.2.2)$$

⁴C'est un état simple qui peut être qualifié de "déterministe".

⁵On peut par exemple réaliser une expérience de Stern et Gerlach avec N voies de sorties au lieu de deux voies $|+\rangle$ et $|-\rangle$ et un détecteur associé à chaque voie.

vérifiant la propriété

$$|A(\lambda_1 \psi_1 + \lambda_2 \psi_2)\rangle = \lambda_1 |A\psi_1\rangle + \lambda_2 |A\psi_2\rangle = \lambda_1 |\varphi_1\rangle + \lambda_2 |\varphi_2\rangle. \quad (2.2.3)$$

Un exemple simple d'opérateur linéaire est l'opérateur identité \mathbb{I} :

$$|\mathbb{I}\psi\rangle = |\psi\rangle. \quad (2.2.4)$$

L'algèbre sur ces opérateurs est la suivante,

$$|(\lambda A)\psi\rangle = \lambda |A\psi\rangle, \quad (2.2.5a)$$

$$|(A+B)\psi\rangle = |A\psi\rangle + |B\psi\rangle, \quad (2.2.5b)$$

$$|(AB)\psi\rangle = |A(B\psi)\rangle. \quad (2.2.5c)$$

Afin de déterminer l'effet de l'opérateur linéaire A sur n'importe quel état $|\psi\rangle$ dans une base $\{|i\rangle\}$, utilisons la décomposition (2.1.9a)

$$\begin{cases} |\varphi\rangle = A|\psi\rangle = \sum_i |i\rangle \langle i| A|\psi\rangle, \\ |\psi\rangle = \sum_j |j\rangle \langle j|\psi\rangle, \end{cases} \Rightarrow |\varphi\rangle = \sum_{i,j} |i\rangle \langle i| A|j\rangle \langle j|\psi\rangle. \quad (2.2.6)$$

Il apparaît ainsi que si l'on connaît les **matrices d'amplitudes** ou **éléments de matrice**

$$A_{ij} = \langle i| A|j\rangle = \langle i| A_j\rangle, \quad (2.2.7)$$

entre tous les états $\{|i\rangle\}$ de cette base, on peut déterminer l'effet de l'opérateur A sur n'importe quel état $|\psi\rangle$.

Si la base $\{|i\rangle\}$ à n états, alors les amplitudes $(n \times n)$ de l'équation (2.2.7) définissent complètement l'opérateur A .

Les opérateurs sont donc définis par les matrices d'amplitudes $(n \times n)$ dans une représentation particulière

$$A \longrightarrow \langle i| A|j\rangle = \langle i| A_j\rangle = A_{ij} \Longleftrightarrow \langle i| \downarrow \begin{matrix} |A_j\rangle \longrightarrow \\ \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1j} & \cdots \\ A_{21} & A_{22} & \cdots & A_{2j} & \cdots \\ \vdots & \vdots & & \vdots & \\ A_{i1} & A_{i2} & \cdots & A_{ij} & \cdots \\ \vdots & \vdots & & \vdots & \end{pmatrix} \end{matrix}. \quad (2.2.8)$$

Les amplitudes dans une matrice définissant l'opérateur A dépendent de la représentation. La transformation des éléments de matrices lors d'un changement de base est

$$\langle \nu| A| \mu\rangle = \sum_{ij} \langle \nu|i\rangle \langle i| A|j\rangle \langle j|\mu\rangle, \quad (2.2.9)$$

où $\langle \nu|i\rangle$ et $\langle j|\mu\rangle$ sont les éléments de la transformation de la base $\{|i\rangle\}$ à la base $\{|\mu\rangle\}$ et vice-versa.

Exemple 2.2.1 Soient les opérateurs $X = \sqrt{\alpha}x$ et $P = \frac{1}{\sqrt{\alpha}}\frac{d}{dx}$. L'action des opérateurs x et $\frac{d}{dx}$ sur les états $|n\rangle$ d'un oscillateur harmonique donne les fonctions d'Hermite suivantes :

$$\sqrt{2\alpha}x|n\rangle = \sqrt{n+1}|n+1\rangle + \sqrt{n}|n-1\rangle, \quad (2.2.10a)$$

$$\sqrt{\frac{2}{\alpha}}\frac{d}{dx}|n\rangle = -\sqrt{n+1}|n+1\rangle + \sqrt{n}|n-1\rangle. \quad (2.2.10b)$$

Les matrices des opérateurs X et P sur les états $|n\rangle$ sont

$$\begin{aligned} X_{mn} &= \langle m|X|n\rangle = \frac{1}{\sqrt{2}}\langle m|\sqrt{2\alpha}x|n\rangle \\ &= \frac{1}{\sqrt{2}}(\sqrt{n+1}\langle m|n+1\rangle + \sqrt{n}\langle m|n-1\rangle) \\ &= \frac{1}{\sqrt{2}}(\sqrt{n+1}\delta_{m,n+1} + \sqrt{n}\delta_{m,n-1}), \end{aligned} \quad (2.2.11)$$

et

$$\begin{aligned} P_{mn} &= \langle m|P|n\rangle = \frac{1}{\sqrt{2}}\langle m|\sqrt{\frac{2}{\alpha}}\frac{d}{dx}|n\rangle \\ &= \frac{1}{\sqrt{2}}(-\sqrt{n+1}\langle m|n+1\rangle + \sqrt{n}\langle m|n-1\rangle) \\ &= \frac{1}{\sqrt{2}}(-\sqrt{n+1}\delta_{m,n+1} + \sqrt{n}\delta_{m,n-1}). \end{aligned} \quad (2.2.12)$$

Pour $n, m \in [0, 3]$ on a les représentations matricielles du tableau 2.2.1.

X_{mn}	$ X0\rangle$	$ X1\rangle$	$ X2\rangle$	$ X3\rangle$	P_{mn}	$ P0\rangle$	$ P1\rangle$	$ P2\rangle$	$ P3\rangle$
$\langle 0 $	0	$\frac{1}{\sqrt{2}}$	0	0	$\langle 0 $	0	$\frac{1}{\sqrt{2}}$	0	0
$\langle 1 $	$\frac{1}{\sqrt{2}}$	0	1	0	$\langle 1 $	$-\frac{1}{\sqrt{2}}$	0	1	0
$\langle 2 $	0	1	0	$\sqrt{\frac{3}{2}}$	$\langle 2 $	0	-1	0	$\sqrt{\frac{3}{2}}$
$\langle 3 $	0	0	$\sqrt{\frac{3}{2}}$	0	$\langle 3 $	0	0	$-\sqrt{\frac{3}{2}}$	0

Table 2.2.1 – Matrices des opérateurs X et P sur les états $|n\rangle$ d'un oscillateur harmonique.

2.2.2 Hermiticité et fonction d'un opérateur

L'opérateur **adjoint** ou **hermitien conjugué** A^\dagger de A est défini par

$$\langle \varphi|A^\dagger\psi\rangle = \langle A\varphi|\psi\rangle = \langle \psi|A\varphi\rangle^*, \quad |\psi\rangle, |\varphi\rangle \in \mathcal{H}. \quad (2.2.13)$$

On montre facilement que

$$(A^\dagger)^\dagger = A, \quad (2.2.14a)$$

$$(\lambda A + \mu B)^\dagger = \lambda^* A^\dagger + \mu^* B^\dagger, \quad (2.2.14b)$$

$$(AB)^\dagger = B^\dagger A^\dagger. \quad (2.2.14c)$$

Algorithme pour prendre le conjugué hermitien d'une expression donnée :

1. renverser l'ordre des termes ;
2. remplacer
 - (a) les opérateurs par leurs adjoints ;
 - (b) les kets par les bras et réciproquement ;
 - (c) les nombres par leurs complexes conjugués.

Exemple 2.2.2

$$(\lambda \langle \varphi | AB | \psi \rangle \langle \chi | C^\dagger)^\dagger = C | \chi \rangle \langle \psi | B^\dagger A^\dagger | \varphi \rangle \lambda^*. \quad (2.2.15)$$

$$(2 | 0 \rangle \langle 1 | - i | 1 \rangle \langle 0 |)^\dagger = +i | 0 \rangle \langle 1 | + | 1 \rangle \langle 0 |. \quad (2.2.16)$$

Pas du tout compliqué n'est-ce pas ?!!!!

Dans la base $\{|i\rangle\}$, l'opérateur adjoint A^\dagger vérifie

$$(A^\dagger)_{ij} = A_{ji}^* = (A_{ij}^t)^* \Rightarrow A^\dagger = (A^t)^*. \quad (2.2.17)$$

Ainsi, les matrices représentant A et A^\dagger dans une représentation sont hermitiennes conjuguées l'une de l'autre, au sens des matrices : *on passe de l'une à l'autre par une conjugaison complexe suivie d'une symétrie par rapport à la diagonale principale.*

Il va de soi que lorsque A est une matrice réelle, $A^\dagger = A^t$.

Exemple 2.2.3

$$\begin{pmatrix} 2+i & -i \\ 4-i & 2+i \end{pmatrix}^\dagger = \begin{pmatrix} 2-i & 4+i \\ i & 2-i \end{pmatrix}; \quad (2.2.18a)$$

$$\begin{pmatrix} i & 2+i \\ 4i & 3-2i \end{pmatrix}^\dagger = \begin{pmatrix} -i & -4i \\ 2-i & 3+2i \end{pmatrix}; \quad (2.2.18b)$$

$$\begin{pmatrix} a+ib & c+id \\ e+if & g+ih \end{pmatrix}^\dagger = \begin{pmatrix} a-ib & e-if \\ c-id & g-ih \end{pmatrix}; \quad (2.2.18c)$$

$$\begin{bmatrix} -85 & -55 & -37 \\ -35 & 97 & 50 \\ 79 & 56 & 49 \end{bmatrix}^\dagger = \begin{bmatrix} -85 & -35 & 79 \\ -55 & 97 & 56 \\ -37 & 50 & 49 \end{bmatrix}. \quad (2.2.18d)$$

Un opérateur A est **hermitien** ou **auto-adjoint**, s'il coïncide avec son adjoint :

$$A^\dagger = A. \quad (2.2.19)$$

Par conséquent

$$\begin{cases} A_{ij}^\dagger = A_{ij} = A_{ji}^* & \text{si } i \neq j, \\ A_{ii}^\dagger = A_{ii} = A_{ii}^*. \end{cases} \quad (2.2.20)$$

Ainsi, dans une matrice hermitienne

1. deux éléments quelconques symétriques par rapport à la diagonale principale sont complexes conjugués l'un de l'autre,
2. les éléments diagonaux sont toujours réels.

Ceci nous permet de comprendre aisément pourquoi Zurek affirme que *la réalité serait quantique mais aurait une apparence classique par le fait que les éléments non diagonaux sont très petits et leurs effets inobservables de façon pratique.*

La forme générale d'une matrice hermitienne 2×2 est

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{12}^* & a_{22} \end{pmatrix}, \quad (2.2.21)$$

où $a_{11}, a_{22} \in \mathbb{R}$ et a_{12} à priori complexe.

Les opérateurs de la théorie quantique sont hermitiens. Les importantes conséquences sur leurs spectres seront étudiées à la **section 2.3**.

La fonction d'un opérateur $f(A)$ peut être développée comme une série entière

$$f(A) = \sum_n c_n A^n. \quad (2.2.22)$$

Par exemple,

$$e^A = \mathbb{I} + A + \frac{1}{2}A^2 + \dots + \frac{1}{n!}A^n + \dots \quad (2.2.23)$$

Si $|\psi\rangle$ est vecteur propre de A avec la valeur propre a , $|\psi\rangle$ est aussi vecteur propre de $f(A)$ avec la valeur propre $f(a)$

$$f(A) |\psi\rangle = \sum_n c_n A^n |\psi\rangle = \sum_n c_n a^n |\psi\rangle = f(a) |\psi\rangle. \quad (2.2.24)$$

Exemple 2.2.4 Pour $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, on a l'opérateur $e^A = \begin{pmatrix} e^1 & 0 \\ 0 & e^{-1} \end{pmatrix}$.

Pour $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, on a pour tout entier n , $B^{2n} = \mathbb{I}_2$, la matrice unité de rang 2, et $B^{2n+1} = B$, et par conséquent,

$$\begin{aligned} e^{i\alpha B} &= \sum_{n=0}^{\infty} \frac{(i\alpha B)^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{(i\alpha B)^{2n+1}}{(2n+1)!} = \mathbb{I}_2 \sum_{n=0}^{\infty} \frac{(i\alpha)^{2n}}{(2n)!} + B \sum_{n=0}^{\infty} \frac{(i\alpha)^{2n+1}}{(2n+1)!} \\ &= (\cos \alpha) \mathbb{I}_2 + i(\sin \alpha) B. \end{aligned} \quad (2.2.25)$$

Si les a_i sont les valeurs propres de l'opérateur A dans la base $\{|\varphi_i\rangle\}$, la **trace** de cet opérateur est la somme de ses éléments diagonaux

$$\text{tr } A = \sum_i \langle \varphi_i | A | \varphi_i \rangle = \sum_i a_i = \sum_i A_{ii}. \quad (2.2.26)$$

La trace est invariante dans un changement de base et on a

$$\begin{aligned} \text{tr}(A + B) &= \text{tr } A + \text{tr } B, & (\text{linéarité}), \\ \text{tr}(cA) &= c \text{tr } A, & (c \in \mathbb{C}) \\ \text{tr } AB &= \text{tr } BA, & (\text{propriété cyclique}). \end{aligned} \quad (2.2.27)$$

Exemple 2.2.5 Dans la base $\{|0\rangle, |1\rangle\}$, la trace de l'opérateur

$$A = 2i |0\rangle \langle 0| + 3 |0\rangle \langle 1| - 2 |1\rangle \langle 0| + 4 |1\rangle \langle 1| \quad (2.2.28a)$$

est

$$\text{tr}(A) = \langle 0| A |0\rangle + \langle 1| A |1\rangle = 2i + 4. \quad (2.2.28b)$$

2.2.3 Unitarité

Un opérateur S est dit **unitaire** s'il est l'inverse de son adjoint, i.e.,

$$S^\dagger = S^{-1}, \text{ i.e., } SS^\dagger = S^\dagger S = \mathbb{I}, \quad (2.2.29)$$

et par conséquent **conserve la norme** de tout vecteur d'état,

$$\|S|\psi\rangle\|^2 = \langle\psi| S^\dagger S |\psi\rangle = \|\psi\rangle\|^2. \quad (2.2.30)$$

Preuve. Si $|\psi_i\rangle$ et $|\varphi_i\rangle$ sont deux bases orthonormées complètes, et si

$$S|\psi_i\rangle = |\varphi_i\rangle, \quad (2.2.31)$$

alors

$$S = S\mathbb{I} = S \sum_i |\psi_i\rangle \langle\psi_i| = \sum_i |\varphi_i\rangle \langle\psi_i|, \quad (2.2.32)$$

et

$$S^\dagger = \sum_i |\psi_i\rangle \langle\varphi_i|. \quad (2.2.33)$$

Et par suite,

$$SS^\dagger = \sum_{i,j} |\varphi_i\rangle \langle\psi_i|\psi_j\rangle \langle\varphi_j| = \sum_{i,j} |\varphi_i\rangle \delta_{ij} \langle\varphi_j| = \mathbb{I}. \quad (2.2.34)$$

■

On peut construire des opérateurs unitaires par exponentiation d'opérateurs hermitiens A

$$S(\lambda) = e^{-i\lambda A}, \quad (2.2.35)$$

avec λ un paramètre continu réel. De plus, $S(\lambda)$ vérifie la propriété de groupe abélien

$$S(\lambda_1 + \lambda_2) = S(\lambda_1)S(\lambda_2), \quad (2.2.36a)$$

$$S(0) = \mathbb{I}. \quad (2.2.36b)$$

La réciproque de cette propriété est le théorème de Stone.

Théorème 2.2.1 Stone. Soit un ensemble d'opérateurs unitaires dépendant d'un paramètre continu λ et vérifiant la loi du groupe abélien. Il existe alors un opérateur hermitien G , appelé **générateur infinitésimal** du groupe de transformations $S(\lambda)$ tel que $S(\lambda) = e^{-i\lambda G}$.

Preuve. Si $\delta\lambda \rightarrow 0$,

$$S(\lambda + \delta\lambda) = S(\lambda)S(\delta\lambda) \simeq (\mathbb{I} - i\delta\lambda G)S(\lambda), \quad (2.2.37)$$

avec

$$B = i \left| \frac{dS}{d\lambda} \right|_{\lambda=0}. \quad (2.2.38)$$

Alors

$$\frac{dS(\lambda)}{d\lambda} = -iBS(\lambda). \quad (2.2.39)$$

Par intégration on trouve, en tenant compte de $S(0) = \mathbb{I}$ et en posant $G = B$, $S(\lambda) = e^{-i\lambda G}$. ■

Un opérateur A est une **isométrie** si

$$A^\dagger A = \mathbb{I}, \quad (2.2.40)$$

puisque le produit scalaire est préservé

$$\langle \varphi A^\dagger | A \psi \rangle = \langle \varphi | \psi \rangle. \quad (2.2.41)$$

Il est à noter qu'il existe des opérateurs isométriques non unitaire ou anti-unitaire.

2.2.4 Projection

Une classe importante des opérateurs linéaires hermitiens est celle des **opérateurs projecteurs** P caractérisés par les propriétés de normalisation, d'orthogonalité et d'hermiticité suivantes

$$P_i^2 = P_i, \quad (2.2.42a)$$

$$P_i P_j = \delta_{ij} P_i, \quad (2.2.42b)$$

$$P_i^\dagger = P_i. \quad (2.2.42c)$$

L'opérateur projecteur

$$P_i = \sum_{i=1}^{m \leq n} |i\rangle \langle i|, \quad (2.2.43)$$

projette l'état $|\psi\rangle$ sur la base orthonormée $\{|i\rangle\}$ de dimension m du sous-espace \mathcal{H}' de \mathcal{H} (qui est de dimension n) :

$$P_i |\psi\rangle = \sum_i |i\rangle \langle i| \psi\rangle = \sum_i \langle i | \psi \rangle |i\rangle = \sum_i \alpha_i |i\rangle. \quad (2.2.44)$$

On montre facilement que P_i est hermitien

$$P_i^\dagger = \left(\sum_i |i\rangle \langle i| \right)^\dagger = \sum_i |i\rangle \langle i| = P_i, \quad (2.2.45)$$

et qu'il vérifie la relation de normalisation

$$P_i^2 = \sum_i |i\rangle \langle i| |i\rangle \langle i| = \sum_i |i\rangle \langle i| = P_i. \quad (2.2.46)$$

Les seules valeurs propres d'un opérateur projecteur sont 0 et 1. En effet, si $|p\rangle$ est vecteur propre de l'opérateur P avec la valeur propre p , $P|p\rangle = p|p\rangle$, la condition nécessaire et suffisante $P^2 = P$ entraîne

$$P^2 |p\rangle - P |p\rangle = 0 \Rightarrow p^2 - p = p(p-1) = 0, \text{ i.e., } p = 0 \text{ ou } p = 1. \quad (2.2.47)$$

Lorsque $m = n$ dans l'équation (2.2.43), on obtient la décomposition de l'opérateur **identité** \mathbb{I}

$$\mathbb{I} = \sum_{i=1}^n |i\rangle \langle i|. \quad (2.2.48)$$

C'est la **relation de fermeture**. Elle exprime le fait que l'ensemble $\{|i\rangle\}$ est une base hilbertienne.

2.3 Décomposition spectrale des opérateurs hermitiens

Comme nous l'avons vu à la **section 2.2.2**, les opérateurs de théorie quantique associés aux grandeurs physiques sont hermitiens. **Leur spectre est par conséquent réel et l'ensemble de leurs vecteurs propres est complet.** Certains opérateurs, comme par exemple l'hamiltonien de l'oscillateur harmonique, ont un spectre discret. *Il est alors possible de construire une base hilbertienne à partir de l'ensemble de leurs vecteurs propres.*

L'étude de ces propriétés importantes des opérateurs hermitiens est l'objet de cette section.

2.3.1 Diagonalisation d'un opérateur hermitien

Un vecteur $|\psi\rangle$ est dit **vecteur propre** de A si

$$A|\psi\rangle = a|\psi\rangle, \quad (2.3.1)$$

le nombre a étant la **valeur propre** associée à ce vecteur propre.

1. Lorsqu'il correspond à a un vecteur propre unique à un facteur multiplicatif près, on dit que a est **non-dégénéré**. **Tous les vecteurs d'état associés sont colinéaires.**
2. Si au contraire, il existe plusieurs kets indépendants qui soient vecteurs propres de A , a est dit **dégénéré**. Son *degré de dégénérescence* est le nombre de vecteurs propres linéairement indépendant qui lui sont associés.

On appelle **spectre** d'un opérateur A , l'ensemble de ses valeurs propres. On obtient ses valeurs propres en résolvant l'équation (2.3.1) : on dit qu'on **diagonalise** la matrice représentant A . Les éléments diagonaux de cette matrice diagonale sont les valeurs propres.

L'algorithme pour la diagonalisation explicite d'une matrice hermitienne A de dimension finie n est la suivante :

1. Résoudre l'équation caractéristique ou séculaire $\det(A - \lambda\mathbb{I}) = 0$ afin de trouver les n valeurs propres λ de A .
2. Résoudre $A_{ij}\alpha_j = \lambda\alpha_i$ ($A|\psi\rangle = \lambda|\psi\rangle$) pour chaque vecteur propre de A (les α_i sont les composantes ou amplitudes de projection de ces vecteurs propres de A). Ce qui revient à résoudre un système de n équations à n inconnues.

L'ensemble des vecteurs propres $\{|\varphi_i\rangle\}$ d'un opérateur hermitien A forme une base orthonormée dans \mathcal{H} .

Dans un espace de Hilbert fini \mathcal{H} , lorsque les valeurs propres a_i sont *non-dégénérées*

$$A|\varphi_i\rangle = a_i|\varphi_i\rangle, \quad (2.3.2)$$

la **décomposition spectrale** de la matrice hermitienne A est

$$A = \sum_i a_i P_i = \sum_i a_i |\varphi_i\rangle \langle \varphi_i| = \sum_i |\varphi_i\rangle a_i \langle \varphi_i|. \quad (2.3.3)$$

Des équations (2.1.9a) et (2.3.3) il apparaît que l'opérateur projecteur

$$P_i = |\varphi_i\rangle \langle \varphi_i|, \quad (2.3.4)$$

permet soit

1. **de faire passer un test** $|\varphi_i\rangle$ à un système quantique (Eq.(2.1.9a)) lorsqu'on est intéressé par la probabilité de trouver le système dans un *état propre* de l'opérateur A : la mesure de P_i vaut 1 si le test réussit et vaut 0 si le test échoue ;
2. **de mesurer la grandeur physique** \mathcal{A} lorsqu'on est plutôt intéressé par une valeur propre a_i de l'opérateur A .

Par exemple, lors de la mesure de la composante suivant Oz du spin avec l'appareil de Stern et Gerlach, on obtient les valeurs $\pm \frac{\hbar}{2}$ de la grandeur physique \mathcal{S}_z . On peut aussi dire qu'on fait passer aux atomes le test $|+\rangle$ et $|-\rangle$ avec les probabilités respectives $|\langle +|\psi\rangle|^2$ et $|\langle -|\psi\rangle|^2$ de déviations vers le haut et vers le bas.

Remarque 2.3.1 Dans une mesure idéale ou un test idéal, on suppose que le système physique n'est pas détruite par la mesure. Lorsqu'on répète plusieurs fois une même mesure idéale, on a **mesure quantique sans démolition** ou mesure Quantum Non Demolition (QND).

Théorème 2.3.1 Les valeurs propres d'un opérateur hermitien sont réelles et les vecteurs propres d'un opérateur hermitien correspondants à deux valeurs propres différentes sont orthogonaux.

Preuve.

$$A = A^\dagger \Rightarrow \langle \varphi_i | A | \varphi_i \rangle = \langle \varphi_i | A^\dagger | \varphi_i \rangle = \langle \varphi_i | A | \varphi_i \rangle^*.$$

$$\text{Si } A | \varphi_i \rangle = a_i | \varphi_i \rangle, \text{ alors } \begin{cases} \langle \varphi_i | A | \varphi_i \rangle = a_i, \\ \langle \varphi_i | A | \varphi_i \rangle^* = a_i^*, \end{cases} \Rightarrow a_i = a_i^*, \text{ i.e., } a_i \in \mathbb{R}. \quad (2.3.5)$$

D'autre part,

$$\begin{cases} A | \varphi_i \rangle = a_i | \varphi_i \rangle, \\ A | \varphi_j \rangle = a_j | \varphi_j \rangle, \\ a_i \neq a_j, \end{cases} \Rightarrow \begin{cases} \langle \varphi_j | A | \varphi_i \rangle = a_i \langle \varphi_j | \varphi_i \rangle, \\ \langle \varphi_j | A | \varphi_i \rangle = a_j \langle \varphi_j | \varphi_i \rangle, \end{cases} \quad (2.3.6a)$$

$$\Rightarrow (a_i - a_j) \langle \varphi_j | \varphi_i \rangle = 0, \quad (2.3.6b)$$

$$\Rightarrow \langle \varphi_j | \varphi_i \rangle = 0, \text{ puisque par hypothèse } a_i \neq a_j.$$

$$\Rightarrow \langle \varphi_j | \varphi_i \rangle = \delta_{ij}. \quad (2.3.6c)$$

■

Par conséquent, les vecteurs propres normalisés à l'unité d'un opérateur hermitien forment une base orthonormée de \mathcal{H} lorsque toutes les valeurs propres sont différentes. Physiquement, cela entraîne que toute amplitude peut être décomposée suivant les amplitudes qui sont les projections des vecteurs propres de la grandeurs physique (donc suivant les amplitudes de base). Le principe de superposition des états est donc lié au caractère mathématique fermé du systèmes des vecteurs propres d'un opérateur hermitien.

Théorème 2.3.2 *Si un opérateur A est hermitien, il est toujours possible de trouver une matrice unitaire S (non unique) telle que $S^{-1}AS$ soit une matrice diagonale, dont les éléments diagonaux sont les valeurs propres qui apparaissent sur la diagonale un nombre de fois égal à leur dégénérescence.*

$$S^{-1}AS = \begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & \vdots \\ 0 & 0 & a_3 & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & a_n \end{pmatrix} \quad (2.3.7)$$

Exemple 2.3.1 *On considère la matrice*

$$H = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \quad (2.3.8)$$

Les valeurs propres de cette matrice déterminées par l'équation caractéristique

$$\det(H - \lambda \mathbb{I}) = \det \begin{pmatrix} -\lambda & 1 & 0 \\ 1 & -\lambda & 1 \\ 0 & 1 & -\lambda \end{pmatrix} = -\lambda^3 + 2\lambda = 0, \quad (2.3.9)$$

sont, $\lambda_1 = 0, \lambda_2 = \sqrt{2}, \lambda_3 = -\sqrt{2}$. Ainsi la matrice diagonalisée est

$$\tilde{H} = \begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -\sqrt{2} \end{pmatrix}. \quad (2.3.10)$$

L'ordre dans lequel on introduit les valeurs propres quand on écrit H est arbitraire. Mais très souvent, on les introduit par ordre décroissant.

Les vecteurs propres $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ de cette matrice sont telles que

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \quad (2.3.11)$$

d'où le système d'équations

$$\begin{cases} b = \lambda a, \\ a + c = \lambda b, \\ b = \lambda c, \\ |a|^2 + |b|^2 + |c|^2 = 1. \end{cases} \quad (2.3.12)$$

La quatrième équation est due à la condition de normalisation des vecteurs d'état. La résolution de ce système d'équation conduit facilement aux vecteurs propres

$$\frac{1}{2} \begin{pmatrix} 1 \\ \sqrt{2} \\ 1 \end{pmatrix}_{\lambda=\sqrt{2}}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}_{\lambda=0}, \quad \frac{1}{2} \begin{pmatrix} 1 \\ -\sqrt{2} \\ 1 \end{pmatrix}_{\lambda=-\sqrt{2}}. \quad (2.3.13)$$

Exemple 2.3.2 Dans la base des états de spin $\{|+\rangle, |-\rangle\}$,

$$|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (2.3.14)$$

sont vecteurs propres de la matrice de Pauli

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |+\rangle \langle +| - |-\rangle \langle -|, \quad (2.3.15)$$

avec les valeurs propres $+1$ et -1 respectivement. Dans la même base, la matrice de Pauli σ_x s'écrit

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle \langle -| + |-\rangle \langle +|. \quad (2.3.16)$$

Elle n'est pas diagonale dans cette base, mais elle est hermitienne :

$$\sigma_x^\dagger = (|+\rangle \langle -| + |-\rangle \langle +|)^\dagger = |+\rangle \langle -| + |-\rangle \langle +| = \sigma_x, \quad (2.3.17)$$

et unitaire :

$$\begin{aligned} \sigma_x \sigma_x^\dagger &= \sigma_x^2 = (|+\rangle \langle -| + |-\rangle \langle +|)(|+\rangle \langle -| + |-\rangle \langle +|) \\ &= |-\rangle \langle -| + |+\rangle \langle +| = \mathbb{I}. \end{aligned} \quad (2.3.18)$$

L'opérateur σ_x est diagonale dans la base

$$|+\rangle_x = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |-\rangle_x = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad (2.3.19)$$

dans laquelle sa décomposition spectrale est donnée par

$$\sigma_x = |+\rangle_{xx} \langle +| + |-\rangle_{xx} \langle -|. \quad (2.3.20)$$

Cette nouvelle base $\{|+\rangle_x, |-\rangle_x\}$ est reliée à la base $\{|+\rangle, |-\rangle\}$ des vecteurs propres de σ_z à travers la transformation unitaire

$$S = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (2.3.21)$$

Lorsqu'on a en général $\{a_i\}$ modalités avec des probabilités \mathcal{P}_i , la **valeur moyenne** des résultats de la grandeur physique \mathcal{A} dans l'état $|\psi\rangle$ est

$$\langle a \rangle_\psi = \sum_i a_i \mathcal{P}_i = \int a \, d\mathcal{P}(a), \quad (2.3.22a)$$

$$= \langle A \rangle_\psi = \sum_i \langle \psi | \varphi_i \rangle a_i \langle \varphi_i | \psi \rangle = \langle \psi | A | \psi \rangle. \quad (2.3.22b)$$

Ainsi, la valeur moyenne du moment de spin est

$$\langle \mu_z \rangle = \sum_i \mu_i \mathcal{P}_i = \left(+\frac{\hbar}{2} \right) \left(\frac{1}{2} \right) + \left(-\frac{\hbar}{2} \right) \left(\frac{1}{2} \right) = 0. \quad (2.3.23)$$

Ce résultat est conforme aux attentes de la théorie classique lorsque l'orientation des dipôles magnétiques n'a aucune direction privilégiée dans un champ d'induction magnétique inhomogène.

L'équation (2.3.22) représente la connexion générale entre le théorie quantique et le théorie quantique classique. Il s'agit du **principe de correspondance**.

Principe 2.3.1 Correspondance. Les valeurs moyennes des grandeurs physiques obéissent aux lois de la théorie classique. En d'autres termes, ce n'est que la statistique des résultats sur les éléments individuels ou microscopiques qui peut être comparée au résultat macroscopique (collectif d'éléments microscopiques)..

Aussi, dirons-nous que le principe de correspondance fournit l'expression des principales grandeurs de la théorie classique. En définitive, retenons le théorème suivant :

Théorème 2.3.3 Copenhagen. *Si le rôle de la physique est de bien décrire la nature, le rôle de la théorie quantique est d'étudier comment les contraintes de l'information troublent cette description. Et, un système physique n'a pas de réalité physique en dehors de ce qui est extrait par l'opérateur.*

Notons cependant, que ce point de vue restrictif de *Copenhagen*, est remis en cause par le théorème EPR :

Théorème 2.3.4 EPR. *Si les prédictions de la théorie quantique concernant les résultats de mesure sont correctes et si la réalité physique peut être décrite de façon locale (ou séparable), alors la théorie quantique n'est pas complète ; il existe des éléments de réalité dont elle ne rend pas compte.*

Les applications de ce théorème sorte du cadre de cet ouvrage. Nous limiterons donc à celui de Copenhagen.

Exercice 2.3.1 *An operator acts on the qutrit basis states in the following way :*

$$A|0\rangle = |1\rangle, \quad A|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad A|2\rangle = |0\rangle. \quad (2.3.24)$$

Find the expectation value $\langle A \rangle$ in the state

$$|\psi\rangle = \frac{1}{2}|0\rangle - \frac{i}{2}|1\rangle + \frac{1}{\sqrt{2}}|2\rangle. \quad (2.3.25)$$

Solution 2.3.1 *Using the matrix representation, one easy find*

$$\langle A \rangle = \langle \psi | A | \psi \rangle = \begin{pmatrix} \frac{1}{2} & +\frac{i}{2} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & 1 \\ 1 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ -\frac{i}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{3\sqrt{2} + i(2 - \sqrt{2})}{8} \quad (2.3.26)$$

2.3.2 Ensemble complet d'opérateurs compatibles (ECOC)

On appelle **commutateur** de A et B , l'opérateur

$$[A, B] = AB - BA. \quad (2.3.27)$$

Lorsque $[A, B] = 0$ ou $AB = BA$, on dit que A et B *commutent* ou *forme une paire d'Heisenberg*. Dans ce cas, faire d'abord un test sur une grandeur physique \mathcal{B} et ensuite faire un test sur la grandeur physique \mathcal{A} est équivalent à faire d'abord un test sur une grandeur physique \mathcal{A} et ensuite faire un test sur la grandeur physique \mathcal{B} . Autrement, l'ordre des tests sur les grandeurs physiques \mathcal{A} et \mathcal{B} n'est plus important.

L'**anticommutation** de deux opérateurs A et B est définie par

$$\{A, B\} = AB + BA. \quad (2.3.28)$$

On dit que A et B **anticommutent** lorsque $\{A, B\} = 0$. L'ordre des tests sur les grandeurs physiques \mathcal{A} et \mathcal{B} est très important.

Théorème 2.3.5 *Si deux opérateurs hermitiens A et B commutent, et si $|\varphi_i\rangle$ est un vecteur propre de A , $B|\varphi_i\rangle$ est aussi un vecteur propre de A , avec la même valeur propre.*

Preuve.

$$\begin{cases} A|\varphi_i\rangle = a_i|\varphi_i\rangle \Rightarrow AB|\varphi_i\rangle = a_iB|\varphi_i\rangle, \\ [A, B]|\varphi_i\rangle = 0 \Rightarrow A(B|\varphi_i\rangle) = BA|\varphi_i\rangle = a_i(B|\varphi_i\rangle), \end{cases} \quad (2.3.29)$$

$B|\varphi_i\rangle$ est vecteur propre de A avec la valeur propre a_i . ■

- Si a_i est non-dégénérée, les vecteurs propres qui lui sont associés sont colinéaires et $B|\varphi_i\rangle$ est nécessairement proportionnel à $|\varphi_i\rangle$. Donc $|\varphi_i\rangle$ est aussi vecteur propre de B .
- Si a_i est dégénérée, on peut seulement dire que $B|\varphi_i\rangle$ appartient au sous-espace propre \mathcal{H}_a de A , correspondant à la valeur propre a_n . On dit que \mathcal{H}_a est globalement invariant sous l'action de B .

Théorème 2.3.6 *Si deux opérateurs hermitiens A et B commutent, et si $|\psi_1\rangle$ et $|\psi_2\rangle$ sont deux vecteurs propres de A avec des valeurs propres différentes, l'élément de matrice $\langle\psi_1|B|\psi_2\rangle$ est nul (i.e., $|\psi_1\rangle$ et $B|\psi_2\rangle$ sont orthogonaux).*

Preuve.

$$\begin{cases} [A, B] = 0, \\ A|\psi_1\rangle = a_1|\psi_1\rangle, \\ A|\psi_2\rangle = a_2|\psi_2\rangle, \\ a_1 \neq a_2, \end{cases} \Rightarrow \begin{cases} \langle\psi_1|[A, B]|\psi_2\rangle = \langle\psi_1|AB|\psi_2\rangle - \langle\psi_1|BA|\psi_2\rangle = 0, \\ \Rightarrow a_1\langle\psi_1|B|\psi_2\rangle - a_2\langle\psi_1|B|\psi_2\rangle = 0, \\ \Rightarrow (a_1 - a_2)\langle\psi_1|B|\psi_2\rangle = 0, \\ \Rightarrow \langle\psi_1|B|\psi_2\rangle = 0 \text{ puisque } a_1 \neq a_2. \end{cases} \quad (2.3.30)$$

Autre démonstration :

$$\begin{cases} A|\psi_1\rangle = a_1|\psi_1\rangle, \\ A|\psi_2\rangle = a_2|\psi_2\rangle, \\ a_1 \neq a_2, \end{cases} \Rightarrow \begin{cases} [A, B] = 0 \Rightarrow AB|\psi_2\rangle = BA|\psi_2\rangle = a_2B|\psi_2\rangle, \text{ (voir Th. 2.3.5),} \\ \Rightarrow \langle\psi_1|B|\psi_2\rangle = 0, \text{ (voir Prop. 2.3.1),} \end{cases} \quad (2.3.31)$$

puisque $B|\psi_2\rangle$ et $|\psi_1\rangle$ sont vecteurs propres de A avec des valeurs propres différentes ($a_1 \neq a_2$). ■

Autrement, la matrice B n'a d'éléments de matrice non nuls que dans les sous-espaces propres de A et se présente sous forme de *blocs diagonaux*.

Exemple 2.3.3 La matrice représentant l'opérateur L_z dans la base $\{|u_1\rangle, |u_2\rangle, |u_3\rangle\}$ est

$$L_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \quad (2.3.32)$$

D'après le théorème 2.3.6, si A est un opérateur qui commute avec L_z , alors A ne peut avoir des éléments de matrices non-nuls entre $|u_1\rangle$ et $|u_2\rangle$; $|u_2\rangle$ et $|u_3\rangle$; $|u_1\rangle$ et $|u_3\rangle$. La matrice représentant A est donc forcément diagonale, i.e., est de la forme

$$A = \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix}. \quad (2.3.33)$$

De même, si M est une matrice qui commute avec

$$L_z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (2.3.34)$$

elle ne peut avoir des éléments de matrice non-nuls entre $|u_1\rangle$ et $|u_2\rangle$; $|u_1\rangle$ et $|u_3\rangle$ seulement. Ainsi la forme générale de M est

$$M = \begin{pmatrix} m_{11} & 0 & m_{13} \\ 0 & m_{22} & 0 \\ m_{31} & 0 & m_{33} \end{pmatrix}. \quad (2.3.35)$$

Le théorème (2.3.5) peut se mettre sous la forme suivante :

Théorème 2.3.7 Si deux opérateurs hermitiens A et B commutent, tout sous-espace propre \mathcal{H}_a de A est globalement invariant sous l'action de B . Donc lorsque $[A, B] = 0$, les opérateurs hermitiens A et B sont simultanément diagonalisables.

Cette propriété est très souvent utilisée pour rechercher le spectre de H . Si le spectre de A est connu, et si $[A, H] = 0$, alors la dynamique quantique générée par H laisse invariant chaque sous-espace propre de l'opérateur A .

Théorème 2.3.8 Si deux opérateurs hermitiens A et B commutent, on peut construire une base orthonormée de l'espace des états \mathcal{H} constituée par les vecteurs propres communs à A et B et réciproquement.

Preuve. Démontrons la réciproque. Considérons $\{|abn\rangle\}$ ⁶ une base de vecteurs propres communs à A et B :

$$\begin{cases} A|abn\rangle = a|abn\rangle \\ B|abn\rangle = b|abn\rangle \end{cases} \Rightarrow \begin{cases} BA|abn\rangle = aB|abn\rangle = ab|abn\rangle \\ AB|abn\rangle = bA|abn\rangle = ab|abn\rangle \end{cases} \Rightarrow [A, B]|abn\rangle = 0. \quad (2.3.36)$$

⁶L'indice n sert à éventuellement distinguer les différents vecteurs de base qui correspondent aux mêmes valeurs propres a et b (dégénérescence).

■

Ainsi, si deux opérateurs hermitiens A et B commutent, il existe une base orthonormée dans laquelle elles sont diagonalisées simultanément. En effet, il est toujours possible d'effectuer des diagonalisations partielles de B à l'intérieur de chacun des blocs diagonaux correspondant à des sous-espaces propres de A .

Théorème 2.3.9 *Un ensemble d'opérateurs A, B, C, \dots , est appelé **ensemble complet d'opérateurs compatibles (ECOC)** s'il existe une base unique orthonormée de vecteurs propres communs (aux facteurs de phase près).*

Le théorème équivalent s'énonce comme suit :

Un ensemble d'opérateurs A, B, C, \dots est appelé ensemble complet d'opérateurs compatibles (ECOC) si :

- *tous les opérateurs (hermitiens) A, B, C, \dots commutent deux à deux,*
- *la donnée des valeurs propres de tous les opérateurs $A, B, C \dots$ suffit à déterminer un vecteur propre commun unique (aux facteurs de phase près).*

En d'autres termes, la diagonalisation simultanée de A et B peut faire apparaître des sous-espaces propres de dimension supérieure à 1 commun à ces deux opérateurs hermitiens. Il est alors possible d'introduire un opérateur hermitien C qui commute avec A et B et qui n'a donc les éléments de matrice que dans le sous espace propre commun à A et B . Il est par conséquent possible de diagonaliser C à l'intérieur de chaque bloc sans toutefois altérer la diagonalisation de A et B .

Si après cette opération, il n'existe plus de sous espace propre commun à A, B et C de dimension supérieure à 1, on dit que A, B et C forment un ECOC. Si ce n'est pas le cas, on cherche un opérateur D qui commute avec A, B et C etc.

La mesure simultanée d'un système complet de grandeurs physiques compatibles $\{A, B, C \dots\}$ constitue un *test maximal* du vecteur d'état. Ceci dit, si l'espace est à N dimensions, un test maximal doit avoir N résultats différents possibles. Alors, on connaît exactement le vecteur d'état du système quantique : on dit qu'on a préparé le système quantique dans un état déterminé.

Exemple 2.3.4 *On considère un système physique dont l'espace des états, qui est à trois dimensions, est rapporté à la base orthonormée formée par les trois kets $|\varphi_1\rangle, |\varphi_2\rangle, |\varphi_3\rangle$. Dans la base de ces trois vecteurs pris dans cet ordre, les deux opérateurs H et B sont définis par*

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \quad (2.3.37)$$

1. *Les opérateurs H et B sont hermitiens car ils sont représentés par des matrices symétriques, réelles. Comme en plus, l'espace est de dimension finie, elles sont diagonalisables et représentent donc des grandeurs physiques.*
2. *On peut montrer que H et B commutent par un calcul direct du produit des matrices HB et BH et en constatant l'égalité. Mais procédons autrement afin de déduire aisément les vecteurs propres communs à H et B .*

- (a) Soit \mathcal{H}_1 le sous-espace (de dimension 1) associé à $|\varphi_1\rangle$. Dans ce sous-espace, $[H, B] = 0$ puisque $HB|\varphi_1\rangle = BH|\varphi_1\rangle$. Ainsi, $|\varphi_1\rangle$ est un vecteur propre commun à H et B de valeur propre 1.
- (b) Considérons maintenant le sous-espace \mathcal{H}_2 associé à $\{|\varphi_2\rangle, |\varphi_3\rangle\}$. Dans ce sous-espace, les restrictions de H et B sont

$$H_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbb{I}_2 \text{ et } B_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.3.38)$$

Puisque H_2 est proportionnelle à la matrice unité, il commute avec toutes les matrices carrées de rang 2, i.e., $[H_2, B_2] = 0$.

- (c) Finalement, $[H, B] = 0$ dans la base $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$.
- (d) Pour avoir une base de vecteurs propres communs à H et B , il faut diagonaliser B_2 . Les valeurs propres de B_2 sont $\lambda = \pm 1$ et les vecteurs propres

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|\varphi_2\rangle + |\varphi_3\rangle) \text{ et } |\psi_3\rangle = \frac{1}{\sqrt{2}}(|\varphi_1\rangle - |\varphi_2\rangle), \quad (2.3.39)$$

Ces vecteurs sont aussi vecteurs propres de H_2 avec la valeur propre -1 (deux fois dégénérés).

- (e) En définitive, les vecteurs propres communs à H et B sont

Vecteur propre	Valeur propre de H	Valeur propre de B
$ \psi_1\rangle = \varphi_1\rangle$	1	1
$ \psi_2\rangle = \frac{1}{\sqrt{2}}(\varphi_2\rangle + \varphi_3\rangle)$	-1	1
$ \psi_3\rangle = \frac{1}{\sqrt{2}}(\varphi_2\rangle - \varphi_3\rangle)$	-1	-1

Il n'y a pas deux lignes semblables dans ce tableau des valeurs propres de H et B : ces deux opérateurs forment donc un ECOC. Ce qui n'est pas le cas pour chacun d'entre eux pris individuellement.

2.4 Inégalités d'Heisenberg

Nous examinons de façon qualitative le concept de grandeurs physiques incompatibles et ses conséquences sur la mesure. En général, il ne sera pas possible de trouver des états où les valeurs des grandeurs physiques \mathcal{A} et \mathcal{B} soient toutes deux bien déterminées.

Supposons qu'on ait $[A, B] \neq 0$ et qu'une première mesure de A ait donné une valeur a et projeté le vecteur d'état initial sur le vecteur propre $|a\rangle$ de A : $A|a\rangle = a|a\rangle$. Si on effectue une mesure \mathcal{B} immédiatement après celle de \mathcal{A} , en général, $|a\rangle$ ne sera pas vecteur propre de B et le résultat de la mesure ne sera pas connu qu'avec une certaine probabilité. En effet, si b est une valeur propre de B correspondant au vecteur propre $|b\rangle$, $B|b\rangle = b|b\rangle$, la probabilité de mesurer b sera

$$\mathcal{P}(b \leftarrow a) = |\langle b|a\rangle|^2. \quad (2.4.1)$$

Il existe donc des dispersions ou écarts quadratiques moyens des mesures effectuées à partir d'un état initial $|\psi\rangle$ arbitraire :

$$\Delta_\psi A = \sqrt{\langle A^2 \rangle_\psi - \langle A \rangle_\psi^2} = \sqrt{\langle (A - \langle A \rangle_\psi \mathbb{I})^2 \rangle_\psi}, \quad (2.4.2a)$$

$$\Delta_\psi B = \sqrt{\langle B^2 \rangle_\psi - \langle B \rangle_\psi^2} = \sqrt{\langle (B - \langle B \rangle_\psi \mathbb{I})^2 \rangle_\psi}. \quad (2.4.2b)$$

Nous savons que nous pouvons écrire $[A, B] = iC$, avec $C^\dagger = C$. Considérons les opérateurs hermitiens P et Q de valeur moyenne nulle, définis par

$$P = A - \langle A \rangle_\psi \mathbb{I} \text{ et } Q = B - \langle B \rangle_\psi \mathbb{I}, \quad (2.4.3)$$

et dont le commutateur est aussi iC :

$$[P, Q] = iC, \quad (2.4.4)$$

puisque $\langle A \rangle_\psi$ et $\langle B \rangle_\psi$ sont des nombres. Le vecteur $(P + i\lambda Q) |\psi\rangle$, où $\lambda \in \mathbb{R}$, a une norme au carré positive :

$$\begin{aligned} \|(P + i\lambda Q) |\psi\rangle\|^2 &= \|P |\psi\rangle\|^2 + i\lambda \langle [P, Q] \rangle_\psi + \lambda^2 \|Q |\psi\rangle\|^2 \\ &= \langle P^2 \rangle_\psi - \lambda \langle C \rangle_\psi + \lambda^2 \langle Q^2 \rangle_\psi \geq 0 \end{aligned} \quad (2.4.5)$$

Le discriminant de ce polynôme de deuxième degré en λ est négatif ou nul :

$$\langle C \rangle_\psi^2 - 4\langle P^2 \rangle_\psi \langle Q^2 \rangle_\psi \leq 0, \quad (2.4.6)$$

et nous avons, en vertu de (2.4.3),

$$\Delta_\psi A \cdot \Delta_\psi B \geq \frac{1}{2} |\langle C \rangle_\psi|, \quad (2.4.7)$$

qui est **l'inégalité de Heisenberg**.

En effectuant un grand nombre de mesures de \mathcal{A} , un grand nombre de mesures de \mathcal{B} et un grand nombre de mesure de \mathcal{C} sur des systèmes tous préparés dans le même état $|\psi\rangle$, on pourra en déduire avec une bonne précision les dispersions $\Delta_\psi A$ et $\Delta_\psi B$ ainsi que la valeur moyenne $\langle C \rangle_\psi$, qui obéiront alors à (2.4.7).

Cependant, il faut préciser que c'est le quanton ou le système quantique lui-même qui ne peut avoir simultanément une grandeur physique \mathcal{A} et une grandeur physique \mathcal{B} bien déterminées. Et c'est de cette indétermination que découle naturellement les incertitudes des mesures. La relation (2.4.7) est donc une conséquence du caractère spécifique des quantons et non du jeu de la Nature en vertu duquel on ne saurait étendre nos connaissances à tout ce qui existe.

2.5 Exercices et problèmes

2.5.1 Représentation matricielle

1. L'espace des états d'un certain système physique est à trois dimensions. Soit $\{|\varphi_1\rangle, |\varphi_2\rangle, |\varphi_3\rangle\}$, une base orthonormée de cet espace. On définit les kets $|\psi_0\rangle$ et $|\psi_1\rangle$ par

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}|\varphi_1\rangle + \frac{i}{2}|\varphi_2\rangle + \frac{1}{2}|\varphi_3\rangle, \quad |\psi_1\rangle = \frac{1}{\sqrt{3}}(|\varphi_1\rangle + i|\varphi_3\rangle). \quad (2.5.1)$$

Ces kets sont-ils normés ? Calculer les matrices P_0 et P_1 représentant dans la base $\{|\varphi_i\rangle\}$ les projecteurs sur les états $|\psi_0\rangle$ et $|\psi_1\rangle$ respectivement. Vérifier que ces matrices sont hermitiennes.

2. Dans un espace à deux dimensions, on considère l'opérateur dont la matrice dans une base orthonormée $\{|\varphi_1\rangle, |\varphi_2\rangle\}$ s'écrit

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (2.5.2)$$

La matrice Y est-elle hermitienne ? Calculer ses valeurs propres et ses vecteurs propres. Calculer les matrices représentant les projecteurs sur ces vecteurs propres. Vérifier que celles-ci satisfont à des relations d'orthogonalité et de fermeture.

2.5.2 QuTiP - Opérateurs

Cet exercice a pour objet de familiariser l'étudiant à l'utilisation des différentes classes `qutip.Qobj` associées aux fonctions **operator** et **state** avoir obtenir des informations sur les opérateurs.

On considère un espace de Hilbert \mathcal{H} d'un état de spin 1/2. Une base de cet espace est $\{|0\rangle, |1\rangle\}$. On considère en outre les trois matrices de Pauli $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ et $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ dont les Qobj prédéfinis sont `sigmax()`, `sigmay()`, `sigmaz()`.

1. En utilisant la commande `Q.eigenstates()` appropriée, calculer les valeurs propres et vecteurs propres de σ_x . On notera `vec1` et `vec2` lesdits vecteurs propres.
2. Évaluer $\sigma_z * \text{vec1}$ et $\sigma_z * \text{vec2}$ et commenter.
3. Calculer les valeurs propres et vecteurs propres de l'opérateur $H = \frac{2}{\sqrt{2}}(\sigma_x + \sigma_y)$.
4. En utilisant la commande `Q.isherm` appropriée (Qobj attribue), vérifier que H est hermitienne. Évaluer H^2 et le comparer à \mathbb{I}_2 . En déduire que H est une matrice unitaire.
5. Définir les projecteurs P_1 et P_2 sur les états propres de H . Vérifier les propriétés d'un opérateur projecteur sur P_1 (i.e., $P_1^\dagger = P_1$, $P_1^2 = P_1$).

2.5.3 Formule de Baker-Campbell-Hausdorff

Soient A et B deux opérateurs qui commutent avec leur commutateur $[A, B]$. On définit l'opérateur $F(t)$ par la fonction de la variable t , $F(t) = e^{At}e^{Bt}$.

1. Démontrer que $\frac{dF}{dt} = (A + B + t[A, B])F(t)$.
2. Intégrer cette équation et vérifier la formule de **Baker-Campbell-Hausdorff** (BCH)

$$e^A e^B = e^{A+B} e^{\frac{1}{2}[A, B]}. \quad (2.5.3)$$

Il est donc clair que si A et B commutent $e^A e^B = e^B e^A$.

2.5.4 Opérateur de Hausdorff

On considère l'opérateur

$$f(t) = e^{tA} B e^{-tA}, \quad (2.5.4)$$

où A et B sont des opérateurs.

1. Montrer que

$$\frac{df(t)}{dt} = [A, f(t)], \quad \frac{d^2 f(t)}{dt^2} = [A, [A, f(t)]]. \quad (2.5.5)$$

2. En déduire

$$e^A B e^{-A} = B + \frac{t}{1!} [A, B] + \frac{t^2}{2!} [A, [A, B]] + \dots \quad (2.5.6)$$

2.5.5 ECOC

Dans la base orthonormée $\{|u_1\rangle, |u_2\rangle, |u_3\rangle\}$, la matrice représentant le hamiltonien en eV est

$$H = \begin{pmatrix} 2 & -3\sqrt{2} & 3\sqrt{2} \\ -3\sqrt{2} & -1 & -3 \\ 3\sqrt{2} & -3 & -1 \end{pmatrix} \quad (2.5.7)$$

1. Déterminer les énergies E_1, E_2, E_3 du système quantique, avec $E_1 \geq E_2 \geq E_3$.
2. Vérifier que les vecteurs propres normés correspondant sont respectivement

$$\begin{cases} |E_1\rangle = \frac{1}{2}(-\sqrt{2}|u_1\rangle + |u_2\rangle - |u_3\rangle) \\ |E_2\rangle = \frac{1}{\sqrt{2}}(|u_2\rangle + |u_3\rangle) \\ |E_3\rangle = \frac{1}{2}(\sqrt{2}|u_1\rangle + |u_2\rangle - |u_3\rangle) \end{cases} \quad (2.5.8)$$

3. A $t = 0$, le système est dans l'état $|\psi(t=0)\rangle = |u_1\rangle$. Quel est l'état du système à un instant ultérieur t ?
4. Évaluer en eV la valeur moyenne $\langle H \rangle$ et la déviation standard ΔH de la variable dynamique H dans l'état $|\psi(t)\rangle$? Que peut-on conclure?
5. Soit K l'opérateur défini par

$$K = |E_1\rangle \langle E_1| + |E_2\rangle \langle E_2|. \quad (2.5.9)$$

- (a) Quels sont les valeurs propres et les vecteurs propres de K ?
- (b) Montrer que H et K forment un ECOC (Ensemble Complet d'Opérateurs Compatibles).

2.5.6 QuTiP - ECOC

Il s'agit ici d'utiliser les fonctions **state** et **operator** de QuTiP pour résoudre l'exercice (??). Il est conseillé, de rédiger un programme (script) en python en utilisant la commande **print()** pour visionner les attributs Qobj.

Avec la classe des objets `qutip.Odedata`, QuTiP permet de résoudre l'équation de Schrödinger $i\hbar \frac{\partial}{\partial t} |\psi\rangle = H |\psi\rangle$, de calculer les états $|\psi(t)\rangle$ pour un intervalle de temps données et les valeurs moyennes des opérateurs voulus, avec la commande `mesolve(operator, state, tlist, [], [exp-op-list])`.

- **operator**=opérateur hamiltonien H ;
- **state**=état $|\psi\rangle$;
- **tlist**=utilise la commande `linspace(temps-initial, temps-final, pas)` pour définir l'intervalle de temps ;
- **[exp-op-list]**=liste des opérateurs dont évaluera les valeurs moyennes pendant **tlist**.

On utilise les commandes `odedata.state` et `odedata.expect` pour extraire les informations sur l'état du système la valeur moyenne calculés.

1. Définir les états $|u1\rangle$, $|u2\rangle$, $|u3\rangle$ ainsi que le hamiltonien H .
2. En utilisant la commande `Q.eigenstates()` appropriée, calculer les énergies $E1$, $E2$, $E3$ et les vecteurs propres $|E1\rangle$, $|E2\rangle$, $|E3\rangle$ associés.
3. Calculer pour $t \in [0, 10]$, avec 10 pas, les états $|\psi(t)\rangle$ lorsque l'état initial du système est $|u1\rangle$.
4. Calculer la déviation standard de H , $\sqrt{\langle H^2 \rangle - \langle H \rangle^2}$ pour $t = 10$ s.
5. Définir les projecteurs P_1 , P_2 et P_3 sur les états propres de H .
6. Exprimer K en fonction de P_1 , P_2 et P_3 .
7. Calculer les valeurs propres et les vecteurs propres de K .
8. Vérifier que les vecteurs propres de K sont vecteurs propres de H . $\{H, K\}$ forme-t-il un ECOC ?

2.5.7 Propriétés des matrices de Pauli

On appelle **matrices de Pauli** σ_i , les matrices

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.5.10)$$

Elles sont telles que

$$\sigma_i \sigma_j = i \varepsilon_{ijk} \sigma_k + \delta_{ij} \mathbb{I}, \quad (2.5.11)$$

où le symbole de Levi-Civita ε_{ijk} est un tenseur de rang 3 complètement anti-symétrique (dans l'échange de n'importe quelle paire indices) :

$$\varepsilon_{ijk} := \begin{cases} 1, & \text{pour les permutations circulaires droite de } (i, j, k), \\ -1, & \text{pour les permutations circulaires de 2 indices de } (i, j, k), \\ 0, & \text{sinon.} \end{cases} \quad (2.5.12)$$

1. Montrer que les matrices σ_i anti-commutent entre elles et en déduire

$$\sigma_x \sigma_y \sigma_z = -\sigma_y \sigma_x \sigma_z = i\mathbb{I}. \quad (2.5.13)$$

2. Montrer que si \mathbf{A} et \mathbf{B} sont deux vecteurs dont les composantes sont des nombres ou des opérateurs qui commutent avec σ_i , alors

$$(\boldsymbol{\sigma} \cdot \mathbf{A})(\boldsymbol{\sigma} \cdot \mathbf{B}) = \mathbf{A} \cdot \mathbf{B} \mathbb{I} + i\boldsymbol{\sigma} \cdot (\mathbf{A} \wedge \mathbf{B}). \quad (2.5.14)$$

En déduire $(\boldsymbol{\sigma} \cdot \mathbf{P})^2$ et $(\boldsymbol{\sigma} \cdot \boldsymbol{\pi})^2$.

3. On pose $\sigma_0 = \mathbb{I}$. Une matrice carrée quelconque M peut s'écrire

$$M = \sum_{i=0}^3 \lambda_i \sigma_i. \quad (2.5.15)$$

Montrer que

$$\lambda_i = \frac{1}{2} \text{tr}(M \sigma_i). \quad (2.5.16)$$

A quelle condition doivent obéir les coefficients λ_i lorsque la matrice M est hermitienne ?

2.5.8 Porte logique quantique élémentaire

Une porte quantique logique \mathbf{U} , $|\psi_e\rangle \xrightarrow{\mathbf{U}} |\psi_s\rangle$ est un dispositif expérimental agissant de manière linéaire sur un 1-qubit d'entrée $|\psi_e\rangle$, en fournissant un 1-qubit de sortie $|\psi_s\rangle = \mathbf{U} |\psi_e\rangle$, où \mathbf{U} est pour une matrice carrée.

On rappelle que la relation duale de $|\psi_s\rangle = \mathbf{U} |\psi_e\rangle$ s'écrit $\langle \psi_s| = \langle \psi_e| \mathbf{U}^\dagger$, où $\langle \psi_e| = \alpha^* \langle 0| + \beta^* \langle 1|$.

Les matrices de Pauli définies dans la base $\{|0\rangle, |1\rangle\}$, par

$$\mathbf{X} = |1\rangle \langle 0| + |0\rangle \langle 1|, \mathbf{Y} = i(|1\rangle \langle 0| - |0\rangle \langle 1|), \mathbf{Z} = |0\rangle \langle 0| - |1\rangle \langle 1|, \quad (2.5.17)$$

permettent de construire des portes quantique logiques élémentaires.

1. Pour $|\psi_e\rangle = \alpha |0\rangle + \beta |1\rangle$, donner l'expression des sorties $|\psi_{sx}\rangle = \mathbf{X} |\psi_e\rangle$, $|\psi_{sy}\rangle = \mathbf{Y} |\psi_e\rangle$ et $|\psi_{sz}\rangle = \mathbf{Z} |\psi_e\rangle$.
2. Montrer que la normalisation simultanée de $|\psi_e\rangle$ et de $|\psi_s\rangle$ impose que \mathbf{U} soit, en toute généralité, une matrice **unitaire**, i.e., telle que $\mathbf{U}^\dagger \mathbf{U} = \mathbb{I}$. **Tout dispositif expérimental implémentant une porte quantique logique devra respecter cette condition dite d'unitarité.**
3. Vérifier, en utilisant la forme vectorielle (2.5.17), que les opérateurs $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ sont unitaires.
4. $\{\mathbf{X}, \mathbf{Z}\}$ est-il un ECOC ? Justifier.

2.5.9 Délocalisation et recombinaison d'un spin 1/2

On considère un dispositif expérimental de la figure 2.5.1 où un faisceau de quantons de spin $\frac{1}{2}$, dans l'état $|+\rangle_z$ se propagent suivant l'axe Oy . Le faisceau pénètre dans un premier appareil de Stern et Gerlach, SG1, dont champ magnétique est tourné d'un angle θ autour de Oy . Sur les deux sortant de SG1, on place deux détecteurs A et B .

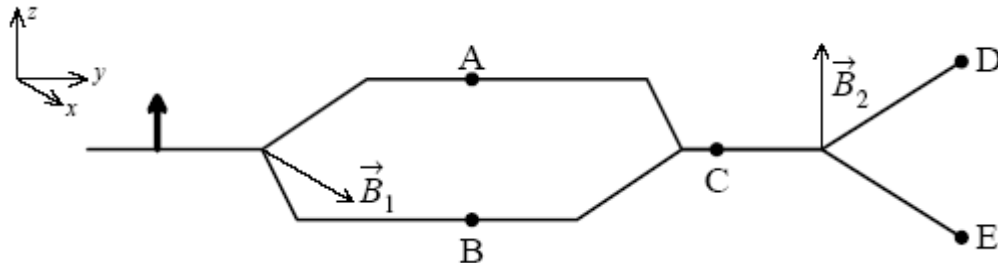


Figure 2.5.1 – Mesure du spin 1/2

On considérera que le faisceau A , tout comme le faisceau D des questions 3. et 4. ci-dessous, a la plus grande valeur du spin.

1. Donner dans la base $\{|+\rangle_z, |-\rangle_z\}$, la matrice de l'opérateur $R_y(\theta)$ de rotation d'angle θ autour de Oy d'un spin $\frac{1}{2}$.
2. Expliquer clairement pourquoi on obtient deux faisceaux à la sortie de SG1, en donnant l'état du spin en A et B et les probabilités de détection \mathcal{P}_A et \mathcal{P}_B .
3. On enlève les détecteurs A et B précédents, et les deux faisceaux sont recombinaés en un seul faisceau avant de pénétrer à nouveau dans un deuxième appareil de Stern-Gerlach, SG2, orienté selon Oz . A la sortie de SG2, on place deux détecteurs D et E .

Quel est l'état de spin des quantons détectés en D et E et quelles sont les probabilités \mathcal{P}_D et \mathcal{P}_E ?

4. On place un absorbeur en A , c'est-à-dire que SG1 agit comme un filtre qui ne laisse passer que le faisceau B .

Quel est l'état de spin des quantons détectés en D et E et quelles sont les probabilités \mathcal{P}_D et \mathcal{P}_E ? Considérer en particulier le cas de $\theta = \frac{\pi}{2}$.

5. Quelles commentaires pouvez-vous faire par rapport aux probabilités obtenues aux questions 3. et 4. ?

CHAPITRE 3

POSTULATS ET ÉVOLUTION TEMPORELLE

Sommaire

- 3.1 Postulats de la théorie quantique
- 3.2 Évolution temporelle
- 3.3 Manipulations de qubits - Oscillations de Rabi
- 3.4 Exercices et problèmes

Nous sommes maintenant suffisamment éclairés sur la *magie* du monde quantique pour procéder à une généralisation des résultats et principes établis jusqu'alors à travers les postulats de base de la théorie quantique (**section 3.1**). Ces postulats fixent cadre conceptuel général de la dite théorie. A la **section 3.2**, on s'intéresse à l'évolution temporelle des états quantiques en mettant l'accent sur les états stationnaires ou états propres de l'énergie. Le chapitre s'achève avec la **section 3.3** avec les oscillations de Rabi, exemples de manipulations des qubits.

3.1 Postulats de la théorie quantique

3.1.1 Postulat 1 : Espace des états

*L'état physique d'un système est **entièrement ou complètement** défini, à chaque instant, par un élément $|\psi\rangle$ d'un espace de Hilbert \mathcal{H} approprié.*

Toute superposition linéaire d'états

$$|\psi\rangle = \sum_n |\varphi_n\rangle \langle \varphi_n | \psi \rangle = \sum_n \alpha_n |\varphi_n\rangle, \quad (3.1.1)$$

est un élément de \mathcal{H} , avec $\alpha_n \in \mathbb{C}$, $|\varphi_n\rangle \in \mathcal{H}$. Les $|\varphi_n\rangle$ sont donc également des vecteurs d'état et la base $\{|\varphi_n\rangle\}$ est orthonormée. Ce sont les amplitudes de projections ou de transition $\alpha_n = \langle \varphi_n | \psi \rangle$ de l'état $|\psi\rangle$ sur l'ensemble des états $|\varphi_n\rangle$ du système qui caractérisent l'état du

système. Autrement, $|\psi\rangle$ est l'être mathématique qui décrit la réalité physique d'un état quantique individuel¹.

Dans l'expérience de Stern et Gerlach de la section 2.1.1, $|\psi\rangle = \alpha_+ |+\rangle + \alpha_- |-\rangle$, $|+\rangle$ et $|-\rangle$ étant les différents états physiques (de spin) des atomes d'argent qui forme le système quantique.

3.1.2 Postulat 2 : Amplitudes de probabilité et probabilités

Si $|\psi\rangle$ et $|\varphi_n\rangle$ représente les états physiques d'un système quantique, la probabilité $\mathcal{P}(\varphi_n \leftarrow \psi)$ pour l'état $|\psi\rangle$ de passer le test $|\varphi_n\rangle$ est (3.1.4), avec $\langle\varphi_n|\psi\rangle$ est l'amplitude de probabilité ou de transition pour que le système qui était dans l'état $|\psi\rangle$ se trouve dans l'état $|\varphi_n\rangle$.

Dans l'expérience de Stern et Gerlach, l'amplitude de probabilité de trouver $|\psi\rangle$ dans l'état $|+\rangle$ est $\alpha_+ = \langle+|\psi\rangle$, et la probabilité pour l'état $|\psi\rangle$ de passer donc le test $|+\rangle$ est $\mathcal{P}(+) = |\langle+|\psi\rangle|^2 = |\alpha_+|^2$.

3.1.3 Postulat 3 : Grandeurs physiques et opérateurs

*A toute grandeur physique mesurable \mathcal{A} (position, vitesse, polarisation, etc,) est associé un **opérateur linéaire hermitien** A agissant dans \mathcal{H} : A est le représentant mathématique de cette grandeur \mathcal{A} .*

On note que contrairement à la théorie classique, la théorie quantique décrit de façon fondamentalement différente l'état physique d'un système et les grandeurs physiques associées. Un état est représenté par un vecteur d'état normé, une grandeur physique par un opérateur hermitien.

3.1.4 Postulat 4 : Principe de quantification et de décomposition spectrale

La mesure d'une grandeur physique \mathcal{A} ne peut donner comme résultat qu'une des valeurs propres de l'opérateur hermitien A correspondante.

*Si $\{|\varphi_n\rangle\}$ est la base des **vecteurs propres** de A , i.e.,*

$$A|\varphi_n\rangle = a_n|\varphi_n\rangle, \quad (3.1.2)$$

alors on peut écrire A sous la décomposition spectrale

$$A = \sum_n |\varphi_n\rangle a_n \langle\varphi_n|, \quad (3.1.3)$$

avec a_n une valeur propre de A ou valeur résultant d'une mesure idéale faite sur \mathcal{A} .

¹On peut aussi dire que c'est l'être mathématique qui décrit l'information disponible sur un système quantique.

La probabilité $\mathcal{P}(a_n)$ d'obtenir comme résultat la valeur propre a_n de l'opérateur hermitien A est

$$\mathcal{P}(a_n) = |\langle \varphi_n | \psi \rangle|^2 = \langle \psi | \varphi_n \rangle \langle \varphi_n | \psi \rangle = |P_n | \psi \rangle|^2, \quad (3.1.4)$$

où $P_n = |\varphi_n\rangle \langle \varphi_n|$ est l'opérateur projection sur la base orthonormée $\{|\varphi_n\rangle\}$.

Ce principe signifie l'ensemble de ces vecteurs propres d'un opérateur hermitien forme une base complète de l'espace de Hilbert. La description d'un état en terme d'une grandeur physique \mathcal{A} quantifiée, prenant N valeurs distinctes a_n , repose sur la connaissance de N nombres, avec lesquels on peut calculer la probabilité d'obtenir la valeur a_n . L'ensemble des a_n forme le **spectre** de \mathcal{A} .

Dans l'expérience de Stern et Gerlach, l'opérateur S associé à la grandeur physique spin S peut s'écrire

$$S = |+\rangle \left(+\frac{\hbar}{2} \right) \langle +| + |-\rangle \left(-\frac{\hbar}{2} \right) \langle -|. \quad (3.1.5)$$

Les vecteurs propres $|+\rangle$ et $|-\rangle$, associés respectivement aux valeurs propres $+\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$ forme une base complète de l'espace de Hilbert et les $\{+\frac{\hbar}{2}, -\frac{\hbar}{2}\}$ forme le spectre de S .

Remarque 3.1.1 1. Les vecteurs $|\varphi_n\rangle$ et $|\varphi'_n\rangle = e^{i\delta} |\varphi_n\rangle$ représente le même état physique, puisque ce ne sont que les probabilités d'amplitude qui peuvent être mesurées :

$$|\langle \varphi'_n | \psi \rangle|^2 = |\langle \varphi_n | \psi \rangle|^2, \quad \forall |\psi\rangle \in \mathcal{H}. \quad (3.1.6)$$

Autrement, il n'est pas possible de distinguer deux états qui diffèrent seulement par un facteur de phase global $e^{i\delta}$.

2. Cependant, l'état physique $\lambda |\varphi_1\rangle + \mu |\varphi_2\rangle$ est différent de l'état $\lambda |\varphi_1\rangle + \mu |\varphi'_2\rangle$.

3.1.5 Postulat 5 : Principe de réduction du paquet d'onde

Si la mesure d'une grandeur physique \mathcal{A} sur le système dans l'état $|\psi\rangle$ donne le résultat a_n , l'état du système immédiatement après la mesure est

$$|\varphi_n\rangle = \frac{P_n |\psi\rangle}{\|P_n |\psi\rangle\|} = \frac{P_n |\psi\rangle}{\sqrt{\langle \psi | P_n | \psi \rangle}}, \quad (3.1.7)$$

la projection normée de $|\psi\rangle$ sur le sous-espace propre associé à a_n . **Donc la mesure est une projection orthogonale.**

Ce postulat, qui suppose qu'on est dans un cas de mesure QND, est l'énoncé quantitatif de l'affirmation "**la mesure perturbe le système**". Si on effectue une mesure sur le système qui est alors dans l'état propre $|\varphi_n\rangle$, on trouvera de façon certaine, i.e., avec une probabilité unité, la valeur propre a_n . Ce principe sous-entend que l'appareil de mesure agit comme un objet classique et ne se préoccupe pas des détails du processus de la mesure (*point de vue de Copenhague*).

Dans le cas du spin, si le système $|\psi\rangle$ passe avec succès le test $|+\rangle$,

$$\frac{P_+ |\psi\rangle}{\|P_+ |\psi\rangle\|} = \frac{|+\rangle \langle + | \psi \rangle}{\sqrt{\langle \psi | + \rangle \langle + | \psi \rangle}} = |+\rangle, \quad (3.1.8)$$

une mesure du spin immédiatement après donnera de façon certaine $+\frac{\hbar}{2}$: $S|+\rangle = +\frac{\hbar}{2}|+\rangle$.

Soulignons que si A et B commutent, la mesure de B ne fait pas perdre les informations préalables fournies par une mesure de A (et réciproquement), mais au contraire les complète ; de plus, l'ordre dans lequel on mesure les deux opérateurs A et B est sans importance. Pour que l'état du système après la mesure soit déterminé, dans tous les cas, uniquement pour le résultat obtenu, il faut que cette mesure porte sur un ECOC.

Ajoutons que *si la valeur d'une grandeur physique peut être prédite avec certitude sans perturber en rien le système, alors il existe une réalité physique attachée à cette grandeur* : c'est la **réalité** EPR (Einstein-Podolsky-Rosen).

Exercice 3.1.1 *A system is in the state*

$$|\psi\rangle = \frac{1}{\sqrt{19}}(2|u_1\rangle + 2|u_2\rangle + |u_3\rangle + 2|u_4\rangle + \sqrt{6}|u_5\rangle) \quad (3.1.9)$$

where $\{|u_i\rangle, i = 1 - 5\}$, are a complete and orthonormal set of vectors. Each $|u_i\rangle$ is an eigenstate of the system's Hamiltonian corresponding to the possible measurement result $H|u_i\rangle = i\varepsilon|u_i\rangle$.

1. Describe the set of projection operators corresponding to the possible measurement results.
2. Determine the probability of obtaining each measurement result. What is the state of the system after measurement if we measure the energy to be 3ε ?
3. What is the average energy of the system?

Solution 3.1.1 1. The possible measurement results are $\varepsilon, 2\varepsilon, 3\varepsilon, 4\varepsilon$ and 5ε . These measurement results correspond to the basis states $|u_1\rangle, |u_2\rangle, |u_3\rangle, |u_4\rangle$, and $|u_5\rangle$ respectively. Hence the projection operators corresponding to each measurement result are

$$P_1 = |u_1\rangle\langle u_1|, P_2 = |u_2\rangle\langle u_2|, P_3 = |u_3\rangle\langle u_3|, P_4 = |u_4\rangle\langle u_4|, P_5 = |u_5\rangle\langle u_5|. \quad (3.1.10)$$

Since the $|u_i\rangle$'s are a set of orthonormal basis vectors, the completeness relation is satisfied and

$$\sum_i P_i = \mathbb{I}. \quad (3.1.11)$$

2. We can calculate the probability of obtaining each measurement result using the Born rule. First we need to check and see if the state is normalized. This is done by calculating $\sum_{i=1}^5 |c_i|^2$ and seeing if the result is 1. We have

$$\begin{aligned} \sum_{i=1}^5 |c_i|^2 &= \frac{1}{19}(|2|^2 + |2|^2 + |1|^2 + |2|^2 + |\sqrt{6}|^2) \\ &= \frac{1}{19}(4 + 4 + 1 + 4 + 6) = 1. \end{aligned} \quad (3.1.12)$$

The state is normalized, so we can proceed. Before doing so, recall that the fact that the basis states are orthonormal means that $\langle u_i | u_j \rangle = \delta_{ij}$. So, in the first case, applying the Born rule we have

$$\varepsilon = |\langle u_1 | \psi \rangle|^2 = \langle \psi | u_1 \rangle \langle u_1 | \psi \rangle = \frac{|2|^2}{19} = \frac{4}{19}, \quad (3.1.13a)$$

$$\varepsilon = |\langle u_2 | \psi \rangle|^2 = \langle \psi | u_2 \rangle \langle u_2 | \psi \rangle = \frac{|2|^2}{19} = \frac{4}{19}, \quad (3.1.13b)$$

$$\varepsilon = |\langle u_3 | \psi \rangle|^2 = \langle \psi | u_3 \rangle \langle u_3 | \psi \rangle = \frac{|1|^2}{19} = \frac{1}{19}, \quad (3.1.13c)$$

$$\varepsilon = |\langle u_4 | \psi \rangle|^2 = \langle \psi | u_4 \rangle \langle u_4 | \psi \rangle = \frac{|2|^2}{19} = \frac{4}{19}, \quad (3.1.13d)$$

$$\varepsilon = |\langle u_5 | \psi \rangle|^2 = \langle \psi | u_5 \rangle \langle u_5 | \psi \rangle = \frac{|\sqrt{6}|^2}{19} = \frac{6}{19}. \quad (3.1.13e)$$

If a measurement is made and we find the energy to be 3ε , then the state of the system after measurement is,

$$\frac{P_3 |\psi\rangle}{\sqrt{\langle\psi| P_3 |\psi\rangle}} = \frac{\frac{1}{\sqrt{19}} |u_3\rangle}{\sqrt{\frac{1}{19}}} = |u_3\rangle \quad (3.1.14)$$

3. The average energy of the system is

$$\begin{aligned} \langle H \rangle &= \sum_{i=1}^5 E_i \langle\psi| P_i |\psi\rangle \\ &= \varepsilon \langle\psi| P_1 |\psi\rangle + 2\varepsilon \langle\psi| P_2 |\psi\rangle + 3\varepsilon \langle\psi| P_3 |\psi\rangle + 4\varepsilon \langle\psi| P_4 |\psi\rangle + 5\varepsilon \langle\psi| P_5 |\psi\rangle \\ &= \varepsilon \frac{4}{19} + 2\varepsilon \frac{4}{19} + 3\varepsilon \frac{1}{19} + 4\varepsilon \frac{4}{19} + 5\varepsilon \frac{6}{19} = \frac{61}{19}\varepsilon \end{aligned} \quad (3.1.15)$$

3.2 Évolution temporelle

3.2.1 Postulat 6 : Évolution temporelle du système

L'évolution temporelle du vecteur d'état $|\psi(t)\rangle$ est régie par l'équation de Schrödinger ou équation d'évolution

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle, \quad (3.2.1)$$

où $H(t)$ est l'opérateur hermitien associé à l'énergie totale du système ou **hamiltonien** du système.

Ce postulat montre que lorsque le système physique est isolé², la théorie quantique est **déterministe** : elle est capable de prévoir l'évolution de l'état du système grâce à l'équation de Schrödinger. Pour un état initial $|\psi(t_0)\rangle$, l'état $|\psi(t)\rangle$ à un instant ultérieur $t > t_0$ est complètement et uniquement déterminé par l'équation (3.2.1), lorsque H est connu.

Seulement, lorsqu'une mesure est effectuée, la théorie quantique devient **indéterministe** : elle n'est plus capable de prévoir exactement ce qui va se produire. Elle permet seulement de connaître les probabilités des différentes occurrences en vertu du postulat de la réduction du paquet d'onde.

La nécessaire **conservation de la norme du vecteur d'état au cours du temps** est assurée par l'hermiticité de H . En effet,

$$\frac{d}{dt} \|\psi(t)\|^2 = \frac{d}{dt} \langle\psi(t)|\psi(t)\rangle \quad (3.2.2a)$$

$$= \frac{d\langle\psi(t)|}{dt} |\psi(t)\rangle + \langle\psi(t)| \frac{d|\psi(t)\rangle}{dt}. \quad (3.2.2b)$$

Or, en vertu de l'équation (3.2.1)

$$\begin{cases} \frac{d|\psi(t)\rangle}{dt} = -\frac{i}{\hbar} H |\psi(t)\rangle, \\ \frac{d\langle\psi(t)|}{dt} = +\frac{i}{\hbar} \langle\psi(t)| H^\dagger. \end{cases} \quad (3.2.3)$$

²Un système quantique est isolé

- s'il est dynamiquement indépendant d'un autre système, i.e., s'il n'y a pas un hamiltonien d'interaction ;
- et s'il est probabilistiquement indépendant (ou séparable) de tout autre système.

Par conséquent,

$$\frac{d}{dt} \| |\psi(t)\rangle \|^2 = \frac{i}{\hbar} \langle \psi(t) | H^\dagger | \psi(t) \rangle - \frac{i}{\hbar} \langle \psi(t) | H | \psi(t) \rangle. \quad (3.2.4)$$

Comme H est un opérateur hermitien, $H^\dagger = H$ et

$$\frac{d}{dt} \| |\psi(t)\rangle \|^2 = 0 \Rightarrow \langle \psi(t) | \psi(t) \rangle = Cst. \quad (3.2.5)$$

3.2.2 Opérateur d'évolution et états stationnaires

L'équation (3.2.1) suggère la correspondance

$$H \rightarrow i\hbar \frac{d}{dt}. \quad (3.2.6)$$

qui indique que l'hamiltonien H est le **générateur de l'évolution temporelle** du système. **L'opérateur de translation dans le temps** est donc

$$U(t) = e^{-iHt/\hbar}, \quad (3.2.7)$$

Il est unitaire

$$U^\dagger(t) = U(-t) = U^{-1}(t), \quad (3.2.8)$$

Le vecteur d'état $|\psi(t)\rangle$ au temps t se déduit du vecteur d'état $|\psi(t_0)\rangle$ au temps t_0 de la façon suivante

$$|\varphi(t)\rangle = U(t, t_0) |\psi(t_0)\rangle = \exp\left(-i\frac{t-t_0}{\hbar}H\right) |\psi(t_0)\rangle. \quad (3.2.9)$$

La propriété d'unitarité (3.2.8) assure la conservation (3.2.5) de la norme

$$\langle \varphi(t) | \varphi(t) \rangle = \langle \varphi(t_0) | U^\dagger(t, t_0) U(t, t_0) | \varphi(t_0) \rangle = \langle \varphi(t_0) | \varphi(t_0) \rangle = 1. \quad (3.2.10)$$

Intéressons nous au cas particulier où $|\varphi\rangle$ est un vecteur propre de l'énergie du système, i.e.,

$$H |\varphi\rangle = E |\varphi\rangle, \quad (3.2.11)$$

Notons $\{|\varphi_E\rangle\}$ ces états propres de l'énergie. Les probabilités de projection de $|\langle u | \varphi_E(t) \rangle|^2$ gardent la même valeur au cours du temps, quel que soit le vecteur de projection $|u\rangle$: elles sont **stationnaires**.

$$|\langle u | \varphi_E(t) \rangle|^2 = |\langle u | \varphi_E(0) \rangle|^2. \quad (3.2.12)$$

Ce qui traduit l'invariance par translation dans le temps des états propres de l'énergie. Autrement dit, l'enveloppe de l'onde ne change pas au cours du temps, seule sa phase complexe change à vitesse constante. Cette vitesse dépend de E .

Afin de distinguer entre elles les diverses valeurs possibles de l'énergie E et les états propres correspondants, nous leurs affecterons un indice n

$$H |\varphi_n\rangle = E_n |\varphi_n\rangle, \quad (3.2.13)$$

les énergies E_n étant réels.

Pour qu'un état évolue, il doit être une *superposition* d'états stationnaires,

$$|\psi(t)\rangle = \alpha_1 |\varphi_1\rangle e^{-iE_1 t/\hbar} + \alpha_2 |\varphi_2\rangle e^{-iE_2 t/\hbar} + \dots = \sum_n \alpha_n |\varphi_n\rangle e^{-iE_n t/\hbar}, \quad (3.2.14)$$

ou

$$|\psi(t)\rangle = \sum_n \alpha_n(t) |\varphi_n\rangle, \text{ avec } \alpha_n(t) = \langle \varphi_n | \psi(t) \rangle = e^{-i(\frac{t-t_0}{\hbar} H)} \alpha_n(t_0). \quad (3.2.15)$$

Ainsi, les termes d'interférence dans $|\langle u | \psi(t) \rangle|^2$ dépend du temps.

L'état stationnaire de plus basse énergie est appelé **état fondamental**. A température presque nulle, un système isolé se met dans son état fondamental. Par exemple, dans les expériences de spectroscopie, grâce à une force stationnaire qu'on impose au système³, on le fait transiter d'un état stationnaire à un autre.

3.2.3 Système à deux états

Représentons un état quelconque d'un quanton comme la superposition des états de base $|\psi_1\rangle$ et $|\psi_2\rangle$:

$$|\psi\rangle = \alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle. \quad (3.2.16)$$

Les amplitudes α_1 et α_2 doivent, en vertu de (3.2.1), satisfaire au système d'équations

$$\begin{cases} i\hbar \frac{d}{dt} \alpha_1 = h_{11} \alpha_1 + h_{12} \alpha_2, \\ i\hbar \frac{d}{dt} \alpha_2 = h_{21} \alpha_1 + h_{22} \alpha_2. \end{cases} \quad (3.2.17)$$

Nous devons considérer deux cas.

Les éléments non-diagonaux h_{12} et h_{21} sont nuls

La matrice de H est diagonalisée. Le système d'équations (3.2.17)

$$\begin{cases} i\hbar \frac{d}{dt} \alpha_1 = h_{11} \alpha_1, \\ i\hbar \frac{d}{dt} \alpha_2 = h_{22} \alpha_2. \end{cases} \quad (3.2.18)$$

Ainsi, si un quanton est, à un instant donné, dans l'état $|\phi_1\rangle$ par exemple, il ne se trouvera jamais dans l'état $|\psi_2\rangle$. Les états $|\psi_1\rangle$ et $|\psi_2\rangle$ sont alors des états stationnaires du quanton, caractérisés par les valeurs h_{11} et h_{22} de l'énergie,

$$\begin{cases} \alpha_1(t) = \alpha_1(0) e^{-ih_{11}t/\hbar} \Rightarrow |\alpha_1(t)|^2 = |\alpha_1(0)|^2 \\ \alpha_2(t) = \alpha_2(0) e^{-ih_{22}t/\hbar} \Rightarrow |\alpha_2(t)|^2 = |\alpha_2(0)|^2 \end{cases} \quad (3.2.19)$$

Si à $t = 0$, le quanton est dans l'état $|\psi_1\rangle$, les probabilités de le détecter dans l'un ou l'autre état à instant t ultérieur sont $|\alpha_1(t)|^2 = 1$ et $|\alpha_2(t)|^2 = 0$.

³Une onde laser sur une molécule par exemple.

Les éléments non-diagonaux h_{12} et h_{21} sont non-nuls

Les deux équations du système (3.2.17) sont alors mutuellement liées. Si à un instant, le quanton se trouve dans l'état $|\phi_1\rangle$, à un autre instant, il peut se trouver dans l'état $|\psi_2\rangle$.

*La présence dans la matrice du hamiltonien H des éléments de matrice non-diagonaux non nuls marque la possibilité de **transitions** du quanton entre ces deux états de base stationnaires.*

3.3 Manipulations de qubits - Oscillations de Rabi

Il est légitime de chercher à savoir comment évolue un qubit au cours du temps. Nous allons rentrer à nouveau au laboratoire pour examiner cela avec un qubit réaliser grâce au spin $\frac{1}{2}$ que nous plongeons dans un champ magnétique uniforme $\mathbf{B}(0, 0, B)$.

Nous allons d'abord considérer le phénomène d'un point de vue classique, puis, à travers la notion de valeur moyenne d'une grandeur physique, nous allons montrer que les résultats obtenus à partir ces considérations classiques se retrouvent aisément avec le formalisme quantique.

Il apparaîtra que le moment magnétique d'un quanton plongé dans un tel champ décrit un mouvement de précession analogue à celui d'une toupie. Ce mouvement de précession, caractérisé par une pulsation ω , donne lieu à des phénomènes de résonance, dite **résonance magnétique**, lorsqu'on module le champ magnétique \mathbf{B} en amplitude, à une pulsation ω_0 proche de ω .

3.3.1 Formalisme classique

En toute rigueur, le formalisme classique est inadapté à l'étude d'un quanton possédant un spin. Cependant, nous allons voir que les résultats obtenus illustrent l'allure générale du phénomène mis en jeu, la **résonance magnétique**.

En considérant que le moment angulaire de la particule est exclusivement dû au moment angulaire de spin, une particule placée dans un champ magnétique subit un moment

$$\Gamma = \boldsymbol{\mu}_s \times \mathbf{B} = \gamma \mathbf{S} \times \mathbf{B} = \boldsymbol{\omega} \times \mathbf{S}, \quad (3.3.1)$$

où $\omega = -\gamma B$ est la **fréquence de Larmor**. En vertu du théorème du moment angulaire,

$$\frac{d\mathbf{S}}{dt} = \Gamma = \gamma \mathbf{S} \times \mathbf{B}. \quad (3.3.2)$$

Cette équation caractérise le mouvement de précession du spin \mathbf{S} autour de l'axe du champ magnétique \mathbf{B} .

En effet, puisque $\mathbf{B}(0, 0, B)$, on a

$$\frac{dS_x}{dt} = \Gamma_x = -\omega S_y \quad (3.3.3a)$$

$$\frac{dS_y}{dt} = \Gamma_y = \omega S_x \quad (3.3.3b)$$

$$\frac{dS_z}{dt} = \Gamma_z = 0 \quad (3.3.3c)$$

Par intégration de l'équation (3.3.3c), on trouve sans peine

$$S_z = Cte, \quad (3.3.4)$$

qui indique que le mouvement de la particule est rectiligne uniforme le long de l'axe Oz .

Dans le plan Oxy , le système d'équations couplées (3.3.3a) et (3.3.3b) peut s'écrire

$$\frac{d(S_x + iS_y)}{dt} = i\omega(S_x + iS_y), \quad (3.3.5)$$

soit après intégration,

$$S_x(t) + iS_y(t) = e^{i(\omega t + \phi)}(S_x(0) + iS_y(0)), \quad (3.3.6a)$$

ou

$$S_x(t) = \cos(\omega t + \phi)S_x(0), \quad (3.3.6b)$$

$$S_y(t) = \sin(\omega t + \phi)S_y(0). \quad (3.3.6c)$$

Dans le plan Oxy , la particule effectue un mouvement circulaire à la vitesse angulaire ω , de phase initiale ϕ .

On dit que la particule effectue un mouvement de précession à la pulsation $\omega = -\gamma B$ autour de l'axe Oz .

3.3.2 Formalisme quantique

États stationnaires

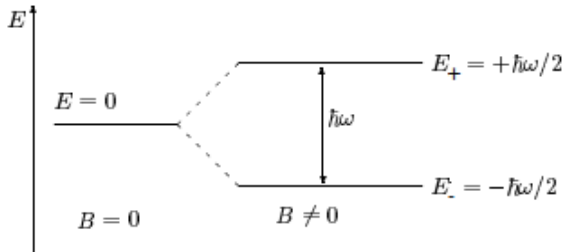


Figure 3.3.1 – Séparation du niveau fondamental en deux sous-niveaux en présence du champ magnétique \mathbf{B} .

comme on peut le voir sur la figure 3.3.1.

L'hamiltonien qui décrit dans l'espace des états l'évolution du quanton dans le champ \mathbf{B} est

$$H = -\gamma B S_z = \omega S_z. \quad (3.3.7)$$

Il est clair que $[H, S_z] = 0$, donc les états propres de S_z sont des états stationnaires

$$H|+\rangle = \frac{\hbar\omega}{2}|+\rangle, \quad H|-\rangle = -\frac{\hbar\omega}{2}|-\rangle. \quad (3.3.8)$$

Le champ magnétique \mathbf{B} provoque donc l'apparition de deux niveaux d'énergie séparés par $\hbar\omega$

Rotation et état de spin d'orientation arbitraire

Afin de fabriquer un qubit dans état de spin d'orientation arbitraire (comme $|\psi\rangle$ sur la figure 3.3.2) faisons tourner la direction du champ magnétique du filtre de Stern et Gerlach et alignons le dans la direction arbitraire

$$\hat{\mathbf{u}}(\theta, \varphi) = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta). \quad (3.3.9)$$

Ainsi, seule la composante $B_u = \mathbf{B} \cdot \hat{\mathbf{u}}$ du champ magnétique est non nulle. Avec cette nouvelle orientation, le filtre de Stern et Gerlach va fabriquer des états $|\pm_u\rangle$, obtenus en sélectionnant les atomes déviés respectivement dans les sens $\pm \hat{\mathbf{u}}$. Ces états sont vecteurs propres de l'opérateur

$$\begin{aligned} \sigma_u &= \vec{\sigma} \cdot \hat{\mathbf{u}} = \sigma_x \sin \theta \cos \varphi + \sigma_y \sin \theta \sin \varphi + \sigma_z \cos \theta \\ &= \begin{pmatrix} \cos \theta & e^{-i\varphi} \sin \theta \\ e^{i\varphi} \sin \theta & -\cos \theta \end{pmatrix}. \end{aligned} \quad (3.3.10)$$

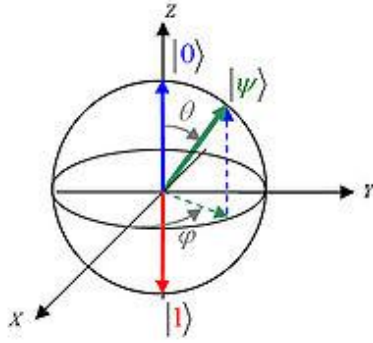


Figure 3.3.2 – Représentation 3D d'un spin $\frac{1}{2}$ sur une sphère de Bloch : $|\psi\rangle = e^{-i\varphi/2} \cos \frac{\theta}{2} |+\rangle + e^{i\varphi/2} \sin \frac{\theta}{2} |-\rangle$, avec $|+\rangle \equiv |0\rangle$, $|-\rangle \equiv |1\rangle$.

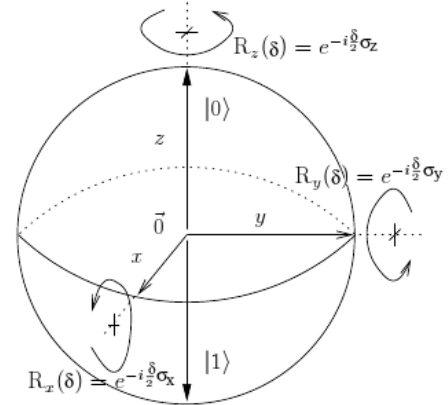


Figure 3.3.3 – Opérateurs rotations d'un single-qubit.

Autrement,

$$|+\rangle_u = \begin{pmatrix} e^{-i\varphi/2} \cos \frac{\theta}{2} \\ e^{i\varphi/2} \sin \frac{\theta}{2} \end{pmatrix}, \quad |-\rangle_u = \begin{pmatrix} -e^{-i\varphi/2} \sin \frac{\theta}{2} \\ e^{i\varphi/2} \cos \frac{\theta}{2} \end{pmatrix}. \quad (3.3.11)$$

Les états $|+\rangle_u$ et $|-\rangle_u$ sont les transformés des états par une rotation qui amène l'axe Oz sur l'axe \hat{u} . Un choix possible consiste à faire une première rotation de θ autour de l'axe Oy , suivie d'une rotation de φ autour de l'axe Oz .

En effet, sur la sphère de Bloch qu'illustre la figure 3.3.3, les rotations d'angle δ autour des axes Ox , Oy et Oz sont générées, en vertu de l'équation (2.2.25), par les opérateurs,

$$R_x(\delta) = e^{-i\frac{\delta}{2}\sigma_x} = \mathbb{I} \cos \frac{\delta}{2} - i\sigma_x \sin \frac{\delta}{2} = \begin{pmatrix} \cos \frac{\delta}{2} & -i \sin \frac{\delta}{2} \\ -i \sin \frac{\delta}{2} & \cos \frac{\delta}{2} \end{pmatrix}, \quad (3.3.12a)$$

$$R_y(\delta) = e^{-i\frac{\delta}{2}\sigma_y} = \mathbb{I} \cos \frac{\delta}{2} - i\sigma_y \sin \frac{\delta}{2} = \begin{pmatrix} \cos \frac{\delta}{2} & -\sin \frac{\delta}{2} \\ \sin \frac{\delta}{2} & \cos \frac{\delta}{2} \end{pmatrix}, \quad (3.3.12b)$$

$$R_z(\delta) = e^{-i\frac{\delta}{2}\sigma_z} = \mathbb{I} \cos \frac{\delta}{2} - i\sigma_z \sin \frac{\delta}{2} = \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix}. \quad (3.3.12c)$$

Pour un axe de rotation quelconque de vecteur unitaire $\hat{u} = (\hat{u}_x, \hat{u}_y, \hat{u}_z)$, on a

$$R_{\hat{u}}(\delta) = e^{-i\frac{\delta}{2}(\hat{u} \cdot \sigma)} = \mathbb{I} \cos \frac{\delta}{2} - (\hat{u} \cdot \sigma) i \sin \frac{\delta}{2}, \quad (3.3.13)$$

où $\hat{u} \cdot \sigma = u_x \sigma_x + u_y \sigma_y + u_z \sigma_z$.

Les matrices de Pauli étant hermitiennes, les opérateurs de rotation $R_{\hat{u}}(\delta)$ sont unitaires :

$$R_{\hat{u}}^\dagger(\delta) = R_{\hat{u}}(-\delta) = R_{\hat{u}}^{-1}(\delta). \quad (3.3.14)$$

Dans la base standard $\{|+\rangle, |-\rangle\}$, la matrice générale de rotation du spin $\frac{1}{2}$ d'une rotation de θ autour de l'axe Oy suivie d'une rotation de φ autour de l'axe Oz est alors

$$\mathcal{D}^{1/2}(\theta, \varphi) = e^{-i\frac{\varphi}{2}\sigma_z} e^{-i\frac{\theta}{2}\sigma_y} = \begin{pmatrix} e^{-i\varphi/2} \cos \frac{\theta}{2} & -e^{-i\varphi/2} \sin \frac{\theta}{2} \\ e^{i\varphi/2} \sin \frac{\theta}{2} & e^{i\varphi/2} \cos \frac{\theta}{2} \end{pmatrix}. \quad (3.3.15)$$

Le fait le plus remarquable à propos dans l'expression de $\mathcal{D}^{1/2}(\theta, \varphi)$ est qu'elle est multivoque : la représentation d'une rotation de $\theta = 2\pi$ est la matrice $-\mathbb{I}$, alors que la rotation équivalente de $\theta = 0$ ou $\theta = 4\pi$ donne \mathbb{I} . C'est une caractéristique des représentations de spin demi-entier.

L'ensemble des matrices $\mathcal{D}^{1/2}(\theta, \varphi)$ forme le **groupe** $SU(2)$:

- S : Spécial, i.e., $\det \mathcal{D}^{1/2} = +1$;
- U : Unitaire, i.e., $(\mathcal{D}^{1/2})^\dagger = [\mathcal{D}^{1/2}]^{-1}$;
- 2 : matrice 2×2 .

Évolution du qubit

Supposons maintenant qu'à l'instant $t = 0$, le quanton soit dans l'état propre $|+\rangle_u$ de S_u ,

$$|\psi(0)\rangle = |+\rangle_u = e^{-i\varphi/2} \cos \frac{\theta}{2} |+\rangle + e^{i\varphi/2} \sin \frac{\theta}{2} |-\rangle. \quad (3.3.16)$$

qui n'est visiblement pas un état stationnaire. A un instant $t > 0$, le quanton est, d'après le *postulat d'évolution*, dans l'état,

$$\begin{aligned} |\psi(t)\rangle &= e^{-iHt/\hbar} |\psi(0)\rangle = e^{-i\omega t/2} e^{-i\varphi/2} \cos \frac{\theta}{2} |+\rangle + e^{+i\omega t/2} e^{i\varphi/2} \sin \frac{\theta}{2} |-\rangle \\ &= e^{-i(\varphi+\omega t)/2} \cos \frac{\theta}{2} |+\rangle + e^{i(\varphi+\omega t)/2} \sin \frac{\theta}{2} |-\rangle. \end{aligned} \quad (3.3.17)$$

Il apparaît que si à $t = 0$ le spin est orienté suivant la direction $\mathbf{u}_0(\theta, \varphi)$, à l'instant t , il est orienté dans la direction $\mathbf{u}_t(\theta, \varphi + \omega t)$. Au cours du temps, la direction du spin tourne, dans le sens trigonométrique, autour de l'axe de quantification Oz à la vitesse angulaire $\omega = -\gamma B$, proportionnelle au champ magnétique. Ce mouvement qui coïncide avec le mouvement du moment magnétique classique porte le nom de **précession de Larmor**. On remarque que c'est après $t_{etat} = \frac{4\pi}{\omega}$ que le quanton retrouve son état initial.

D'après (3.3.17) lors d'une mesure de \mathcal{S}_z à l'instant t on obtient

1. $+\frac{\hbar}{2}$ avec une probabilité $|\langle + | \psi(t) \rangle|^2 = \cos^2 \frac{\theta}{2}$;
2. $+\frac{\hbar}{2}$ avec une probabilité $|\langle - | \psi(t) \rangle|^2 = \sin^2 \frac{\theta}{2}$.

Ces probabilités sont bien évidemment indépendantes du temps puisque $|+\rangle$ et $|-\rangle$ sont des états stationnaires.

La probabilité pour que, à l'instant t , le système retrouve son état de spin initial $|\psi(0)\rangle \equiv |+\rangle_u$ est

$$\begin{aligned} \mathcal{P}_+(t) &= |{}_u \langle + | \psi(t) \rangle|^2 = |e^{-i\omega t/2} \cos^2 \frac{\theta}{2} + e^{+i\omega t/2} \sin^2 \frac{\theta}{2}|^2 \\ &= \cos^4 \frac{\theta}{2} + \sin^4 \frac{\theta}{2} + \frac{1}{2} \cos^2 \frac{\theta}{2} \sin^2 \frac{\theta}{2} \cos \omega t. \end{aligned} \quad (3.3.18)$$

Les probabilités oscillent à une fréquence proportionnelle à la fréquence de Larmor $\omega = \frac{E_+ - E_-}{\hbar} = \frac{\Delta E}{\hbar}$. ΔE est la dispersion sur l'énergie : le quanton passe d'un niveau à l'autre avec un temps caractéristique $\Delta t \simeq \frac{\hbar}{2\Delta E}$.

Si $|+\rangle_u \equiv |+\rangle_x$, alors $\theta = \frac{\pi}{2}$ et $\varphi = 0$ et cette probabilité devient

$$\mathcal{P}_+(t) = |{}_x \langle + | \psi(t) \rangle|^2 = \left| \frac{1}{2} (e^{-i\omega t/2} + e^{+i\omega t/2}) \right|^2 = \cos^2 \left(\frac{\omega t}{2} \right). \quad (3.3.19)$$

Afin de comprendre cette précession du spin ou les oscillations des probabilités, déterminons les valeurs moyennes des trois composantes du spin $\frac{1}{2}$ dans l'état $|\psi(t)\rangle$:

$$\langle\psi(t)|S_z|\psi(t)\rangle = \left(\frac{\hbar}{2}\right) \cos^2 \frac{\theta}{2} + \left(-\frac{\hbar}{2}\right) \sin^2 \frac{\theta}{2} = \frac{\hbar}{2} \cos \theta. \quad (3.3.20)$$

Cette valeur moyenne est sans surprise indépendante du temps puisque $[H, S_z] = 0$. En utilisant les expressions matricielles de S_x et S_y , on trouve sans difficulté

$$\langle\psi(t)|S_x|\psi(t)\rangle = \hbar \cos \frac{\theta}{2} \sin \frac{\theta}{2} \cos(\varphi + \omega t) = \frac{\hbar}{2} \sin \theta \cos(\varphi + \omega t), \quad (3.3.21a)$$

$$\langle\psi(t)|S_y|\psi(t)\rangle = \hbar \cos \frac{\theta}{2} \sin \frac{\theta}{2} \sin(\varphi + \omega t) = \frac{\hbar}{2} \sin \theta \sin(\varphi + \omega t). \quad (3.3.21b)$$

S_x et S_y ne sont visiblement pas des constantes de mouvement. Les équations (3.3.21) peuvent encore s'écrire

$$\langle\psi(t)|S_x + iS_y|\psi(t)\rangle = \frac{\hbar}{2} \sin \theta e^{i(\varphi + \omega t)} = e^{i\omega t} (\langle\psi(0)|S_x + iS_y|\psi(0)\rangle), \quad (3.3.22)$$

montrant que $\langle\mathbf{S}(t)\rangle$ précesse autour de Oz à la fréquence ω :

$$\frac{d\langle\mathbf{S}\rangle}{dt} = \boldsymbol{\omega} \wedge \langle\mathbf{S}\rangle. \quad (3.3.23)$$

Après $t_{prec} = \frac{2\pi}{\omega}$, le quanton retrouve sa direction initiale.

A travers la valeur moyenne du spin, on retrouve le même comportement que le moment magnétique classique.

Cette propriété, la précession, est à la base des techniques de **résonance magnétique**.

3.4 Exercices et problèmes

3.4.1 Moment magnétique du deutéron

Un noyau de deutérium plongé dans un champ magnétique \mathbf{B} possède trois états $|+\rangle$, $|0\rangle$, $|-\rangle$ d'énergie $+E_0$, 0 , $-E_0$ respectivement, avec $E_0 = \hbar\omega$. Ce noyau a un moment magnétique et on suppose que l'opérateur M associé à la projection de ce moment sur une direction fixe perpendiculaire au champ \mathbf{B} a la forme $M = \mu_0 A$, avec $\mu_0 > 0$ et A défini par

$$A|+\rangle = \frac{1}{\sqrt{2}}|0\rangle, A|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), A|-\rangle = \frac{1}{\sqrt{2}}|0\rangle. \quad (3.4.1)$$

1. Écrire la matrice représentant A dans la base $\{|+\rangle, |0\rangle, |-\rangle\}$. A est-il hermitien ?
2. Calculer les valeurs propres m_1 , m_2 et m_3 de M (avec $m_1 > m_2 > m_3$) et déterminer les vecteurs propres normalisés correspondant $|m_1\rangle$, $|m_2\rangle$, $|m_3\rangle$.
3. On suppose qu'à l'instant $t = 0$, le noyau est dans l'état $|\psi(0)\rangle = |m_1\rangle$. Calculer $\langle E \rangle$ et ΔE dans cet état.
4. Calculer $\langle M \rangle$ dans l'état $|\psi(t)\rangle$ en fonction de ω .
5. Quelles sont, en fonction de ω , les probabilités de trouver m_1 , m_2 et m_3 lors d'une mesure de M sur l'état $|\psi(t)\rangle$?
6. Interpréter physiquement l'évolution de la composante transverse du moment magnétique.

3.4.2 Précession de Larmor

On considère un quanton de spin $\frac{1}{2}$ dont les états propres de S_z sont notés $|+\rangle_z$ et $|-\rangle_z$. On considère un état de spin quelconque $|\psi\rangle$ caractérisé par les amplitudes de transition $\alpha = {}_z\langle +|\psi\rangle$ et $\beta = {}_z\langle -|\psi\rangle$.

1. Quelle sont les probabilités des transitions $|+\rangle_z \leftarrow |\psi\rangle$ et $|-\rangle_z \leftarrow |\psi\rangle$? Quelle relation doit lier ces deux quantités ?
2. On suppose que le quanton possède un moment magnétique $\boldsymbol{\mu}$ et qu'il est placé dans un champ magnétique $\mathbf{B} = (0, 0, B)$. Le hamiltonien étant $H = -\boldsymbol{\mu} \cdot \mathbf{B} = \omega S_z$ avec $\omega = -\gamma B$, quels sont les états stationnaires de ce quanton ? Préciser les énergies associées à ces états.
3. Si à l'instant $t = 0$ le quanton est dans un état de spin qui soit état propre d'une composante de \mathbf{S} orthogonale à \mathbf{B} , par exemple S_x . Notons $|+\rangle_x$ cet état.
 - (a) Cet état est-il stationnaire ?
 - (b) Quelle est à l'instant $t > 0$ et dans la base $\{|+\rangle_z, |-\rangle_z\}$, l'amplitude de probabilité ${}_x\langle +|\varphi(t)\rangle$ si $\varphi(0) = |+\rangle_x$?
 - (c) Quelle est la probabilité $\mathcal{P}_+(t) = |{}_x\langle +|\varphi(t)\rangle|^2$ pour que, à l'instant $t > 0$, le quanton se retrouve dans son état initial $|+\rangle_x$? Même question pour $\mathcal{P}_-(t) = |{}_x\langle -|\varphi(t)\rangle|^2$.

4. Les variations temporelles de ces probabilités sont le plus souvent interprétées par référence à l'évolution des valeurs moyennes des composantes du spin. Calculer ces valeurs moyennes dans l'état $|\varphi(t)\rangle$ et conclure.
5. Le quanton est un neutron de longueur d'onde $\lambda = 1.55 \text{ \AA}$ et masse $mc^2 = 939.566 \text{ MeV}$. On rappelle que $\hbar c = 1973 \text{ eV\AA}$.
 - (a) Calculer la vitesse du neutron.
 - (b) Dédire de la figure (3.4.1) la valeur de la vitesse angulaire de précession du spin.
 - (c) Le champ magnétique vaut $B = 15.5 \times 10^{-4} \text{ T}$. En déduire la valeur du moment magnétique du neutron.

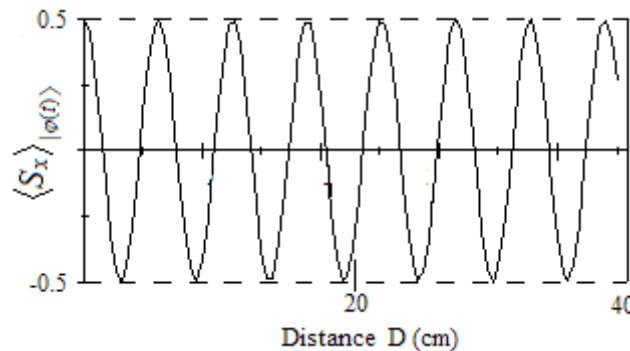


Figure 3.4.1 – *Précession de Larmor des neutrons. Variation de $\langle S_x \rangle_{|\psi(t)\rangle}$ en fonction de la distance (c'est-à-dire du temps de parcours).*

3.4.3 Détection des électrons

Des électrons polarisés, avec des spins $\frac{1}{2}$ polarisés (+) dans la direction Oz pénètrent dans une région où règne un champ magnétique statique $\mathbf{B} = (B_0, 0, 0)$. Les électrons se déplacent dans la direction Oy . Après un temps T , les électrons atteignent un appareil de Stern-Gerlach où le gradient de champ est orienté suivant Oz .

1. Écrire, dans la base qui diagonalise la matrice de Pauli σ_z , la matrice du hamiltonien d'interaction H_0 dans la région où règne le champ $\mathbf{B} = (B_0, 0, 0)$. On posera $\omega_0 = -\gamma B_0$.
2. Sur un détecteur D placé après l'appareil de Stern-Gerlach, on ne peut détecter que les électrons de spin (−) dans la direction Oz . Trouver les valeurs de B_0 qui permettent à tous les électrons d'atteindre le détecteur D .
3. Pour la valeur minimale de B_0 , de la question 2, quel est le pourcentage des électrons qui atteignent D si le temps de parcours dans la région où règne B_0 est $\frac{T}{2}$ et non T ?

3.4.4 Réalisation expérimentale d'une porte logique 1-qubit

On rappelle que le spin de l'électron génère un moment magnétique $\boldsymbol{\mu} = \gamma \mathbf{S}$, où $\gamma = g \frac{q}{2m}$ est le rapport gyromagnétique et g est le facteur de Landé.

L'hamiltonien qui décrit dans l'espace des états l'évolution de l'électron dans le champ $\mathbf{B} = (0, 0, B_0)$ est $H = -\boldsymbol{\mu} \cdot \mathbf{B}$. On posera $\omega_0 = \gamma B_0$, la pulsation de Larmor ou pulsation de résonance.

On rappelle que l'opérateur de rotation autour de Ou est

$$\mathbf{R}_u(\theta) = e^{-i\theta\sigma_u/2} = (\cos \frac{\theta}{2})\mathbb{I} - i(\sin \frac{\theta}{2})\sigma_u. \quad (3.4.2)$$

1. Donner, dans la base qui diagonalise \mathbf{S}_z , l'expression de la matrice de \mathbf{H} en fonction de ω_0 . Quels sont les niveaux d'énergie du système ?
2. Le vecteur d'état du spin, $|\psi(t)\rangle$ se décompose dans la base des états propres de \mathbf{S}_z sous la forme

$$|\psi(t)\rangle = \alpha_0(t)|0\rangle + \alpha_1(t)|1\rangle. \quad (3.4.3)$$

- (a) En résolvant matriciellement l'équation de Schrödinger, $i\hbar \frac{d}{dt} |\psi(t)\rangle = \mathbf{H}(t) |\psi(t)\rangle$, donner les expressions de $\alpha_{0,1}(t)$, en fonction de $\alpha_{0,1}(0)$ et $\mathbf{R}_z(\theta)$. On précisera l'expression de θ .
 - (b) Combien de temps faut-il laisser agir le champ magnétique statique \mathbf{B}_0 sur le spin de l'électron pour réaliser, à un facteur de phase globale près sur $\alpha_{0,1}(t)$, une porte q-logique Z, $|k\rangle \xrightarrow{\mathbf{Z}} (-1)^k |k\rangle$? Pourquoi ce facteur de phase globale est-il non-significatif du point de vue de la mesure ?
3. Afin de réaliser une porte q-logique X, $|k\rangle \xrightarrow{\mathbf{X}} |1-k\rangle$, on ajoute au champ statique \mathbf{B}_0 un champ $\mathbf{B}_1(t)$ situé dans le plan xOy tournant dans le sens trigonométrique avec la vitesse angulaire ω ,

$$\mathbf{B}_1(t) = B_1(\mathbf{e}_x \cos \omega t + \mathbf{e}_y \sin \omega t). \quad (3.4.4)$$

On posera $\omega_1 = \gamma B_1$ la *fréquence ou pulsation de Rabi* et $\delta = \omega + \omega_0$ le *désaccord à la résonance*.

- (a) Écrire la nouvelle matrice du hamiltonien $\mathbf{H}(t)$ du système dans la base où \mathbf{S}_z est diagonale, puis le système d'équations différentielles auquel obéissent $\alpha_{0,1}(t)$.
- (b) Pour résoudre ce système, on se place dans le référentiel tournant avec le champ en posant

$$\alpha_0(t) = \beta_0(t)e^{-i\omega t/2}, \quad \alpha_1(t) = \beta_1(t)e^{+i\omega t/2}, \quad |\tilde{\psi}(t)\rangle = \beta_0(t)|0\rangle + \beta_1(t)|1\rangle. \quad (3.4.5)$$

- i. Écrire $|\tilde{\psi}(t)\rangle$ en fonction de l'opérateur rotation \mathbf{R}_z et $|\psi(t)\rangle$ afin de justifier l'expression *référentiel tournant*.
- ii. Montrer que

$$i\hbar \begin{pmatrix} \dot{\beta}_0(t) \\ \dot{\beta}_1(t) \end{pmatrix} = \tilde{\mathbf{H}} \begin{pmatrix} \beta_0(t) \\ \beta_1(t) \end{pmatrix}, \quad (3.4.6)$$

où $\tilde{\mathbf{H}}$ est fonction des matrices de Pauli et indépendant du temps.

- iii. A partir de $|\tilde{\psi}(t)\rangle = \tilde{\mathbf{U}}(t)|\tilde{\psi}(0)\rangle$, déduire la relation entre $\alpha_{0,1}(t)$ et $\alpha_{0,1}(0)$ en fonction des matrices de Pauli.
4. Lorsque $\delta = 0$, combien de temps faut-il laisser agir le champ tournant pour réaliser, à un facteur de phase globale près, une porte q-logique X ?
 5. A l'instant $t = 0$, le spin est dans l'état pur $|0\rangle$.
 - (a) Quelle est la probabilité $\mathcal{P}_{1 \leftarrow 0}(t)$ de trouver au temps t le spin dans l'état $|1\rangle$?
 - (b) À quel instant cette probabilité est-elle maximale ? Montrer que la porte q-logique X consiste à faire basculer le spin de l'état $|0\rangle$ à $|1\rangle$ et vice-versa. Quel est l'équivalent *classique* de cette opération logique quantique ?

3.4.5 QuTiP - Evolution d'un état de spin 1/2

Écrire un programme (script) en Python utilisant QuTiP pour répondre aux questions suivantes.

L'évolution d'un quanton de spin 1/2, de moment magnétique μ , dans un champ magnétique $\mathbf{B}(0, 0, B)$, peut être décrit par l'hamiltonien $H = -\mu \cdot \mathbf{B} = \omega S_z$. Le quanton pénètre dans le champ magnétique dans l'état $|+\rangle_x$. On prendra : $\hbar\omega = 0.5$.

1. Définir l'hamiltonien H , ainsi que ses états propres $|+\rangle_z$ et $|-\rangle_z$.
2. Exprimer les états $|+\rangle_x$ et $|-\rangle_x$ en fonction des états propres du hamiltonien H .
3. Définir les projecteurs P_+ et P_- respectivement sur les états $|+\rangle_x$ et $|-\rangle_x$.
4. Le quanton initialement dans l'état $|+\rangle_x$ pénètre dans le champ magnétique à $t = 0$. Résoudre l'équation de Schrödinger, pour $t \in [0, 30]$. Calculer en même temps les valeurs moyennes de P_+ , P_- , H et H^2 .
Note : la valeur moyenne $\langle \psi(t) | P_+ | \psi(t) \rangle = \langle \psi(t) | + \rangle_x \langle + | \psi(t) \rangle = \mathcal{P}_+(t)$, est la probabilité de trouver le quanton à l'instant t dans l'état $|+\rangle_x$. De même pour P_- .
5. Représenter, pour $t \in [0, 30]$, les probabilités de trouver le quanton dans l'état $|+\rangle_x$ et $|-\rangle_x$. Que remarque-t-on ?
6. Calculer pour $t = 30s$ la déviation standard de ΔH .

CHAPITRE 4

CORRÉLATIONS QUANTIQUES

Sommaire

- 4.1 Produit tensoriel et états intriqués
- 4.2 Théorème de Bell et interférences des états corrélés
- 4.3 Information quantique
- 4.4 Exercices

Nos incursions dans le monde quantique ce sont jusqu'à présent limitées aux états à un quanton. L'objet de ce chapitre est la description d'états à deux quantons qui conduisent à des configurations très riches dites **intriquées** ou **corrélées**. Ces corrélations sont à la base du calcul quantique. Une fois assimilé le cas à deux quantons, la généralisation à un nombre quelconque de quantons est facile.

Dans la vie courante, on a par exemple des *corrélations par échange du signal* tel que le feu rouge correspond à l'arrêt des véhicules et au passage des piétons. Mais on a pas de corrélation entre particules classiques.

Le chapitre commence avec la **section 4.1** qui introduit les notions de produit tensoriel et d'états intriqués indispensables à la description des états à plusieurs quantons. La **section 4.2** est consacrée à l'étude des importantes conséquences physiques telles les inégalités de Bell et les interférences des états corrélés, qui permettent de mettre en exergue le caractère non local et non séparable de la théorie quantique. En effet, il apparaît que

1. les corrélations quantiques ne disparaissent pas lorsqu'on augmente la distance entre les quantons, et leur origine ne peut être la réception d'un signal commun ;
2. les corrélations quantiques violent les inégalités de Bell et donc leur origine ne peut non plus être une décision commune prise à la source.

La dernière section, **section 4.3**, est réservée aux applications en information quantique comme la cryptographie et la téléportation quantique.

4.1 Produit tensoriel et états intriqués

4.1.1 États

Soient deux systèmes physiques isolés (S_1) et (S_2), d'espaces d'états correspondants respectifs \mathcal{H}_1 et \mathcal{H}_2 . Si on considère l'ensemble de ces deux états comme un système unique (S), quel est l'espace des états \mathcal{H} associé ?

Définition 4.1.1 Par définition, l'espace d'états \mathcal{H} est appelé **produit tensoriel** de \mathcal{H}_1 et \mathcal{H}_2 , et noté $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, si à tout couple de vecteurs, $(|\psi_1\rangle, |\psi_2\rangle) \in \mathcal{H}_1 \times \mathcal{H}_2$, on associe un vecteur de \mathcal{H} , noté $|\psi_1\rangle \otimes |\psi_2\rangle$ et appelé produit tensoriel de $|\psi_1\rangle$ et $|\psi_2\rangle$, tel que cette correspondance soit linéaire par rapport à la multiplication par des scalaires, et distributive par rapport à l'addition vectorielle :

$$[|\psi_1\rangle + \lambda |\psi'_1\rangle] \otimes |\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle + \lambda |\psi'_1\rangle \otimes |\psi_2\rangle, \quad (4.1.1a)$$

$$|\psi_1\rangle \otimes [|\psi_2\rangle + \lambda |\psi'_2\rangle] = |\psi_1\rangle \otimes |\psi_2\rangle + \lambda |\psi_1\rangle \otimes |\psi'_2\rangle, \quad (4.1.1b)$$

et tel que si $\{|\psi_1^i\rangle\}$ et $\{|\psi_2^j\rangle\}$ sont respectivement des bases de \mathcal{H}_1 et \mathcal{H}_2 , alors $\{|\psi_1^i\rangle \otimes |\psi_2^j\rangle\}$ est une base de \mathcal{H} .

Pour des raisons de simplicité, on note le plus souvent

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle |\psi_2\rangle = |\psi_1 \psi_2\rangle. \quad (4.1.2)$$

Définition 4.1.2 Le **produit scalaire** sur $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ se définit de la manière suivante

$$\langle \psi'_1 \psi'_2 | \psi_1 \psi_2 \rangle = \langle \psi'_1 | \psi_1 \rangle \langle \psi'_2 | \psi_2 \rangle. \quad (4.1.3)$$

Si $\{|n\rangle\}$ est une base orthonormée de \mathcal{H}_1 et $\{|m\rangle\}$ une base orthonormée de \mathcal{H}_2 telles que

$$|\psi_1\rangle = \sum_{n=1}^N \alpha_n |n\rangle, \quad |\psi_2\rangle = \sum_{m=1}^M \alpha_m |m\rangle, \quad (4.1.4)$$

alors

$$|\psi_1 \psi_2\rangle = \sum_{n,m} \alpha_n \alpha_m |nm\rangle, \quad (4.1.5)$$

avec

$$\langle n'm' | nm \rangle = \delta_{n'n} \delta_{m'm}. \quad (4.1.6)$$

Exemple 4.1.1 On considère dans la base $\{|0\rangle, |1\rangle\}$ les vecteurs d'état $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ et $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Dans la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ le produit tensoriel $|\psi_1\rangle \otimes |\psi_2\rangle$ a pour matrice

$$|\psi_1\rangle \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1. |\psi_2\rangle \\ -1. |\psi_2\rangle \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}. \quad (4.1.7)$$

On peut considérer qu'un état produit $|\psi_1\rangle \otimes |\psi_2\rangle$ représente la simple juxtaposition de deux systèmes, l'un dans l'état $|\psi_1\rangle$ et l'autre dans l'état $|\psi_2\rangle$. On dit encore que, dans un tel état, les deux systèmes sont **sans corrélations** : les résultats de deux types de mesures pourtant soit sur un système, soit sur l'autre, correspondent à des variables aléatoires indépendantes. Une telle situation est réalisée lorsque les deux systèmes ont été préparés indépendamment et séparément dans les états $|\psi_1\rangle$ et $|\psi_2\rangle$ et qu'on les réunit ensuite, sans qu'ils interagissent.

4.1.2 Opérateurs

Soient A et B deux opérateurs agissant respectivement dans \mathcal{H}_1 et \mathcal{H}_2 . On peut construire un opérateur $A \otimes B$ agissant dans $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ tel que

$$(A \otimes B) |\psi_1 \psi_2\rangle = A |\psi_1\rangle \otimes B |\psi_2\rangle. \quad (4.1.8)$$

Si A et B sont des opérateurs hermitiens, alors $A \otimes B$ est un opérateur hermitien.

Une classe simple des opérateurs de \mathcal{H} est

$$A \otimes \mathbb{I}_B \text{ et } \mathbb{I}_A \otimes B. \quad (4.1.9)$$

Il est à noter que

$$(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD). \quad (4.1.10)$$

Ainsi

$$[A \otimes \mathbb{I}_B, \mathbb{I}_A \otimes B] = (A \otimes \mathbb{I}_B) \cdot (\mathbb{I}_A \otimes B) - (\mathbb{I}_A \otimes B) \cdot (A \otimes \mathbb{I}_B) = 0. \quad (4.1.11)$$

Si $|\psi_1\rangle$ est un vecteur propre de l'opérateur A avec la valeur propre a , $A |\psi_1\rangle = a |\psi_1\rangle$, alors $|\psi_1 \otimes \psi_2\rangle$ est aussi vecteur propre de $A \otimes \mathbb{I}_B$ avec la valeur propre a :

$$A \otimes \mathbb{I}_B |\psi_1 \otimes \psi_2\rangle = a |\psi_1 \otimes \psi_2\rangle. \quad (4.1.12)$$

On omet très souvent d'écrire explicitement les opérateurs identités \mathbb{I}_A et \mathbb{I}_B pour écrire simplement

$$A |\psi_1 \otimes \psi_2\rangle = a |\psi_1 \otimes \psi_2\rangle, \quad (4.1.13a)$$

ou

$$A |\psi_1 \psi_2\rangle = a |\psi_1 \psi_2\rangle, \quad (4.1.13b)$$

en supprimant le produit tensoriel.

Exemple 4.1.2 La matrice représentant le produit tensoriel des matrices de Pauli $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ est

$$\sigma_x \otimes \sigma_z = \begin{pmatrix} 0 \cdot \sigma_z & 1 \cdot \sigma_z \\ 1 \cdot \sigma_z & 0 \cdot \sigma_z \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}. \quad (4.1.14)$$

Exercice 4.1.1 Évaluer $\sigma_z \otimes \sigma_x$ et conclure.

Exercice 4.1.2 Suppose that A is a projector in \mathcal{H}_1 where $A = |0\rangle \langle 0|$ and B is a projector in \mathcal{H}_2 where $B = |1\rangle \langle 1|$. Find

$$A \otimes B \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}} \right) \quad (4.1.15)$$

Solution 4.1.1

$$\begin{aligned}
A \otimes B \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}} \right) &= \frac{1}{\sqrt{2}} [|A0\rangle |B1\rangle + |A1\rangle |B0\rangle] \\
&= \frac{1}{\sqrt{2}} [|0\rangle \langle 0| 0\rangle |1\rangle \langle 1| 1\rangle + |0\rangle \langle 0| 1\rangle |1\rangle \langle 1| 0\rangle] = \frac{1}{\sqrt{2}} |01\rangle.
\end{aligned} \tag{4.1.16}$$

Exercice 4.1.3 *A system is in the state*

$$|\psi\rangle = \frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle \tag{4.1.17}$$

1. What is the probability that measurement finds the system in the state $|\phi\rangle = |01\rangle$?
2. What is the probability that measurement finds the first qubit in the state $|0\rangle$? What is the state of the system after measurement ?

Solution 4.1.2 1. Given that the system is in the state $|\psi\rangle$, the probability of finding it in the state $|\phi\rangle = |01\rangle$ is calculated using the Born rule, which is $\mathcal{P} = |\langle\phi|\psi\rangle|^2$. Since $\langle 0|1\rangle = \langle 1|0\rangle = 0$, we have

$$\begin{aligned}
\langle\phi|\psi\rangle &= \langle 01| \left(\frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle \right) \\
&= \sqrt{\frac{3}{8}} \langle 0|0\rangle \langle 1|1\rangle = \sqrt{\frac{3}{8}}.
\end{aligned} \tag{4.1.18}$$

Therefore the probability is

$$\mathcal{P} = |\langle\phi|\psi\rangle|^2 = \frac{3}{8}. \tag{4.1.19}$$

2. To find the probability that measurement finds the first qubit in the state $|0\rangle$, we can apply $P_0 \otimes \mathbb{I} = |0\rangle \langle 0| \otimes \mathbb{I}$ to the state. So the projection operator P_0 is applied to the first qubit and the identity operator to the second qubit, leaving the second qubit unchanged.

This obtains

$$\begin{aligned}
P_0 \otimes \mathbb{I} |\psi\rangle &= |0\rangle \langle 0| \otimes \mathbb{I} \left(\frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle \right) \\
&= \frac{1}{\sqrt{8}} |0\rangle \langle 0| 0\rangle \otimes |0\rangle + \sqrt{\frac{3}{8}} |0\rangle \langle 0| 0\rangle \otimes |1\rangle = \frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle
\end{aligned} \tag{4.1.20}$$

The probability of obtaining this result is

$$\begin{aligned}
\mathcal{P} &= \langle\psi| P_0 \otimes \mathbb{I} |\psi\rangle = \left(\frac{1}{\sqrt{8}} \langle 00| + \sqrt{\frac{3}{8}} \langle 01| + \frac{1}{2} \langle 10| + \frac{1}{2} \langle 11| \right) \left(\frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle \right) \\
&= \frac{1}{8} + \frac{3}{8} = \frac{1}{2}.
\end{aligned} \tag{4.1.21}$$

The state of the system after measurement using (3.1.7) is found to be

$$\frac{\frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle}{\sqrt{\langle\psi| P_0 \otimes \mathbb{I} |\psi\rangle}} = \sqrt{2} \left(\frac{1}{\sqrt{8}} |00\rangle + \sqrt{\frac{3}{8}} |01\rangle \right) = \frac{1}{2} |00\rangle + \frac{\sqrt{3}}{2} |01\rangle \tag{4.1.22}$$

4.1.3 États corrélés ou intriqués

Soient deux qubits de \mathcal{H}_A et \mathcal{H}_B ,

$$|\varphi_A\rangle = a_0 |0_A\rangle + a_1 |1_A\rangle, \quad |a_0|^2 + |a_1|^2 = 1, \quad (4.1.23a)$$

$$|\varphi_B\rangle = b_0 |0_B\rangle + b_1 |1_B\rangle, \quad |b_0|^2 + |b_1|^2 = 1. \quad (4.1.23b)$$

Le produit tensoriel $|\varphi_A \otimes \varphi_B\rangle$ est donné suivant (4.1.5) par

$$|\varphi_A \otimes \varphi_B\rangle = a_0 b_0 |0_A \otimes 0_B\rangle + a_0 b_1 |0_A \otimes 1_B\rangle + a_1 b_0 |1_A \otimes 0_B\rangle + a_1 b_1 |1_A \otimes 1_B\rangle. \quad (4.1.24)$$

Un vecteur arbitraire $|\Psi\rangle$ de \mathcal{H} est

$$|\Psi\rangle = \alpha |0_A \otimes 0_B\rangle + \beta |0_A \otimes 1_B\rangle + \gamma |1_A \otimes 0_B\rangle + \delta |1_A \otimes 1_B\rangle. \quad (4.1.25)$$

Ce vecteur n'est en général pas de la forme (4.1.24) : en comparant (4.1.24) et (4.1.25), on note que pour que $|\Psi\rangle$ soit de la forme $|\varphi_A \otimes \varphi_B\rangle$ (produit tensoriel), une condition nécessaire et suffisante est que

$$\alpha = a_0 b_0, \quad \beta = a_0 b_1, \quad \gamma = a_1 b_0, \quad \delta = a_1 b_1 \Rightarrow \alpha \delta = \beta \gamma, \quad (4.1.26)$$

ce qui *à priori* n'a aucune raison d'être valide. Lorsque $|\Psi\rangle$ n'est pas de la forme (4.1.24), on dit qu'il est dans un état **intriqué** ou **corrélé** (*entangled* en anglais). C'est par exemple le cas de

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0_A \otimes 1_B\rangle + |1_A \otimes 0_B\rangle), \quad (4.1.27)$$

qui est manifestement intriqué puisque

$$\alpha = 0, \quad \beta = \gamma = \frac{1}{\sqrt{2}}, \quad \delta = 0 \Rightarrow \alpha \delta \neq \beta \gamma. \quad (4.1.28)$$

Un état intriqué n'est donc pas factorisable !

Il est clair que lorsqu'un système est dans un état intriqué, les propriétés du système global sont définies, mais celles de chacun des sous-systèmes ne le sont pas.

Par exemple, lorsqu'on a un système composé d'une paire d'électrons, il est possible de préparer ce système de sorte que les deux électrons aient *des spins opposés* et donc un état de spin total nul (propriété de la paire), sans que l'on puisse dire dans quelle direction pointe chaque spin individuel (pas de propriétés pour chaque sous-système). Quand on mesure le spin de l'un des électrons de la paire, on trouve toujours que l'autre est dans l'orientation opposée. Tout se passe comme si une mesure d'un des spins, opérée le long d'un axe, obligeait l'autre spin à prendre la valeur opposée. Comment les deux spins se *concertent-ils* ? Cela reste mystérieux. En outre, la mesure du spin de l'un des quantons dans la direction horizontale n'empêche pas d'obtenir aussi un résultat dans la direction verticale, ce qui suggère que les quantons n'ont pas d'axes de rotation déterminés. En un mot, les résultats des mesures effectuées sur les deux électrons sont corrélés d'une façon que la physique classique n'explique pas.

L'intrication des états est une spécificité de la théorie quantique.

Il est cependant important de souligner que comme un système composé de nombreux quantons est difficile à isoler de l'environnement, ses constituants ont une probabilité bien plus grande de s'intriquer avec des particules non contrôlées de l'environnement, ce qui détruit leurs interconnexions originelles. Autrement dit, dans les termes servant à décrire la décohérence,

trop d'informations s'échappent du système dans l'environnement, ce qui confère au système un comportement classique, non quantique. On comprend donc que lorsqu'on cherche à exploiter l'intrication, par exemple pour construire des ordinateurs quantiques, le principal défi est la difficulté de préserver l'intrication.

L'état intriqué (4.1.27) n'est pas anodin. En effet, $|\Psi^+\rangle$ a une importance en information quantique. C'est l'un des quatre états de Bell

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (4.1.29a)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (4.1.29b)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (4.1.29c)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (4.1.29d)$$

Ces états forment une base orthonormée de \mathcal{H}^2 . En effet, pour tout $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \in \mathcal{H}^2$ peut être exprimé comme

$$\begin{aligned} |\psi\rangle &= |\Phi^+\rangle \langle \Phi^+ | \psi \rangle + |\Phi^-\rangle \langle \Phi^- | \psi \rangle + |\psi^+\rangle \langle \psi^+ | \psi \rangle + |\psi^-\rangle \langle \psi^- | \psi \rangle \\ &= \frac{1}{\sqrt{2}} [(\alpha + \delta) |\Phi^+\rangle + (\alpha - \delta) |\Phi^-\rangle + (\beta + \gamma) |\psi^+\rangle + (\beta - \gamma) |\psi^-\rangle]. \end{aligned} \quad (4.1.30)$$

Exemple 4.1.3 Construction d'un état corrélé. On considère deux spins $\frac{1}{2}$ dont l'interaction est représentée par

$$H = \frac{1}{2} \hbar \omega \vec{\sigma}_1 \cdot \vec{\sigma}_2. \quad (4.1.31)$$

avec $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ et $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. On vérifie facilement que

$$\begin{array}{lll} \text{Bit flip} & \text{Bit+sign flip} & \text{Sign flip} \\ \left\{ \begin{array}{l} \sigma_x |0\rangle = |1\rangle \\ \sigma_x |1\rangle = |0\rangle \end{array} \right. & \left\{ \begin{array}{l} \sigma_y |0\rangle = i |1\rangle \\ \sigma_y |1\rangle = -i |0\rangle \end{array} \right. & \left\{ \begin{array}{l} \sigma_z |0\rangle = |0\rangle \\ \sigma_z |1\rangle = -|1\rangle \end{array} \right. \end{array} \quad (4.1.32)$$

2. Soient les qubits

$$|\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle). \quad (4.1.33)$$

Sachant que (vous devez le vérifier),

$$\frac{1}{2}(\mathbb{I} + \vec{\sigma}_1 \cdot \vec{\sigma}_2) |ij\rangle = |ji\rangle, \quad (4.1.34)$$

on a

$$\begin{aligned} (\vec{\sigma}_1 \cdot \vec{\sigma}_2) |\psi_+\rangle &= |\psi_+\rangle, \\ (\vec{\sigma}_1 \cdot \vec{\sigma}_2) |\psi_-\rangle &= -3 |\psi_-\rangle \end{aligned} \quad (4.1.35)$$

Autrement, $|\psi_+\rangle$ et $|\psi_-\rangle$ sont vecteurs propres de $\vec{\sigma}_1 \cdot \vec{\sigma}_2$ avec les valeurs propres $+1$ et -3 respectivement, et donc vecteurs propres de H avec les valeurs propres $E_+ = +\frac{1}{2}\hbar\omega$ et $E_- = -\frac{3}{2}\hbar\omega$.

3. Si à l'instant $t = 0$ on a un état non corrélé $|\psi(0)\rangle = |10\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle + |\psi_-\rangle)$, alors son évolution temporelle est

$$\begin{aligned}
 e^{-iHt/\hbar} |\psi(0)\rangle &= \frac{1}{\sqrt{2}}(e^{-iHt/\hbar} |\psi_+\rangle + e^{-iHt/\hbar} |\psi_-\rangle) \\
 &= \frac{1}{\sqrt{2}}(e^{-i\omega t/2} |\psi_+\rangle + e^{+3i\omega t/2} |\psi_-\rangle) \\
 &= \frac{e^{+i\omega t/2}}{\sqrt{2}}(e^{-i\omega t} |\psi_+\rangle + e^{+i\omega t} |\psi_-\rangle) \\
 &= e^{+i\omega t/2}(\cos \omega t |10\rangle - i \sin \omega t |01\rangle)
 \end{aligned} \tag{4.1.36}$$

4. Il suffit de prendre $\omega t = \frac{\pi}{4}$ pour obtenir l'état corrélé

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - i |01\rangle). \tag{4.1.37}$$

Pratiquement, la difficulté de construction vient de ce que H est en général une interaction interne au système, qui, contrairement aux interactions de type externe utilisées pour les qubits individuels, ne peut pas être branchée et débranchée facilement pour ajuster t . Si l'interaction est à courte distance, il est possible de rapprocher puis d'éloigner les deux qubits. On peut aussi appliquer aux deux qubits des interactions externes différentes, ce qui est la technique utilisée dans le cas de la RMN, où l'interaction interne est plus simple, en $\sigma_{1z}\sigma_{2z}$.

4.2 Théorème de Bell et interférences des états corrélés

4.2.1 L'analyse EPR - Dieu ne joue pas au dés

Cette analyse est celle d'Einstein, Podolsky et Rosen en 1935. Ils utilisèrent la notion d'état corrélés pour montrer l'opposition entre la théorie quantique et une théorie réaliste et locale du monde physique. L'analyse s'appuie sur deux principes.

Principe 4.2.1 Réalité. Si, sans perturber **localement** un système, on peut prévoir avec certitude la valeur d'une de ses grandeurs physiques, alors il existe un élément de réalité associé à cette grandeur.

Principe 4.2.2 Localité. Au moment de la mesure, les deux systèmes n'interagissent plus et sont dans des régions locales de l'espace-temps¹, qui ne peuvent pas être causalement reliées, alors rien de ce que l'on fait au premier système ne peut modifier le second.

A la suite de ces hypothèses, ils font les constats suivants :

- Une théorie complète doit prédire les valeurs précises de tous les éléments de réalité.
- Les deux orientations du spin sont des éléments de réalité.
- Pourtant, la théorie quantique ne peut pas prédire ces orientations de spins.

¹Si par exemple Alice et Bob sont distants de L dans un référentiel où ils sont tous deux au repos et que les mesures prennent un temps τ , on exigera que $\tau \ll \frac{L}{c}$.

- La théorie quantique est donc INCOMPLÈTE!

Il faut donc, sans contester la validité du formalisme quantique, la compléter en introduisant un niveau supplémentaire de description plus détaillé. Cependant, en 1964, John Bell montre qu'il n'est pas possible de **comprendre** dans leur totalité les corrélations EPR en complétant le formalisme quantique dans l'esprit suggéré par Einstein.

4.2.2 Théorème de Bell

L'objet de ce théorème est de fournir un critère pour tester expérimentalement l'hypothèse que l'information qui détermine les corrélations quantiques est établie à la source. *La conséquence de cette hypothèse est que la corrélation entre les quantons établie à la source ne doit pas dépendre des mesures que l'on choisit d'effectuer sur chacun des quantons.* Autrement, les quantons ne **savent** pas à quel type de mesures elles vont être soumises.

Théorème 4.2.1 Bell. *Il existe un nombre positif X , calculable à partir des corrélations observées, tel que*

1. *X est toujours inférieur ou égal à 2 si les corrélations sont établies à la source ;*
2. *X peut dépasser 2 lorsque les corrélations sont dues à l'intrication.*

*$X \leq 2$ est appelée **inégalité de Bell** ; si $X > 2$, on dit que les corrélations violent l'inégalité de Bell. Les corrélations qui violent une inégalité de Bell ne peuvent être produites à la source.*

Démontrons le théorème². Pour cela, on a besoin de deux conditions supplémentaires :

- Sur chaque quanton qu'elle reçoit, Alice choisit parmi deux mesures, $A \equiv A_+$ et $A' \equiv A_-$; de même Bob choisit entre $B \equiv B_+$ et $B' \equiv B_-$. On a donc quatre possibilités de mesures sur chaque paire de quantons : (A, B) , (A', B) , (A, B') et (A', B') .
- Chacune des mesures A, A', B, B' ne peut donner que deux résultats $+1$ et -1 . Donc chaque paire ne peut valoir que $+2$ ou -2 .

On définit le nombre

$$X = A(B + B') + A'(B - B'). \quad (4.2.1)$$

Supposons, c'est l'hypothèse qu'on veut tester on le rappelle, que tout est établi à la source, notamment les résultats de chaque mesure. Alors X peut prendre les valeurs $+2$ et -2 : en effet, si $B' = B$, $B + B' = \pm 2$; si $B' = -B$, $B - B' = \pm 2$. Malheureusement, on ne peut pas mesurer X sur chaque paire de quantons, car Alice mesure soit A soit A' , jamais les deux à la fois (*la mesure perturbe le système*).

Mais on peut mesurer la valeur moyenne de X sur un grand nombre de paires de quantons, car

$$\langle X \rangle = \langle AB \rangle + \langle AB' \rangle + \langle A'B \rangle - \langle A'B' \rangle, \quad (4.2.2)$$

et AB , AB' , $A'B$ et $A'B'$ sont des expériences que l'on peut faire. Selon l'hypothèse, $|\langle X \rangle| \leq 2$.

²La formulation proposée ici n'est la version originale de Bell, mais celle due à John Clauser, Michael Horne, Abner Shimony et Dick Holt, connue comme CHSH. Elle a l'avantage de prouver le théorème de manière directe.

Or pour les états corrélés comme $|\varepsilon_a \varepsilon_b\rangle$ (deux spins $\frac{1}{2}$), la théorie quantique prédit des valeurs moyennes de corrélations de la forme

$$\begin{aligned}\langle AB \rangle &= \sum \varepsilon_a \varepsilon_b \mathcal{P}_{\varepsilon_a \varepsilon_b} = (\mathcal{P}(x, x) + \mathcal{P}(y, y)) - (\mathcal{P}(x, y) + \mathcal{P}(y, x)) \\ &= -\cos(\alpha + \beta)\end{aligned}\quad (4.2.3)$$

Or il est facile de trouver des valeurs de $\alpha, \alpha', \beta, \beta'$ tel que $X > 2$. Par exemple, pour $\alpha = 0$, $\alpha' = \frac{\pi}{2}$, $\beta = -\frac{\pi}{4}$ et $\beta' = \frac{\pi}{4}$, on trouve

$$X = 2\sqrt{2} > 2, \quad (4.2.4)$$

en manifeste violation de l'inégalité de Bell.

Les corrélations quantiques ne sont donc pas établies à la source.

Aucune corrélation de type classique n'est capable de reproduire les corrélations quantiques : les corrélations quantiques sont trop fortes pour une explication classique. Même si les qubits A et B sont éloignés de plusieurs années lumière, on ne peut pas les considérer comme des entités séparées et il n'existe pas d'algorithme probabiliste classique local susceptible de reproduire leurs corrélations. Les qubits A et B forment une entité unique, ils sont **non séparables**, en un mot ils sont **intriqués**, et cela quelle que soit la distance qui les sépare. On parle alors de **non-localité quantique** ou **non-localité EPR**.

4.2.3 Interférences à deux quantons

Il est apparu à la **section 1.3** que le hasard quantique était assez curieux en ce sens que l'assemblage d'une certaine façon de deux *générateurs de hasard* ou *BS* (MZ3 ou MZ équilibré), générerait une certitude ! Nous allons maintenant appliquer le principe d'indiscernabilité à un système d'états corrélés et voir quelles en sont les prédictions.

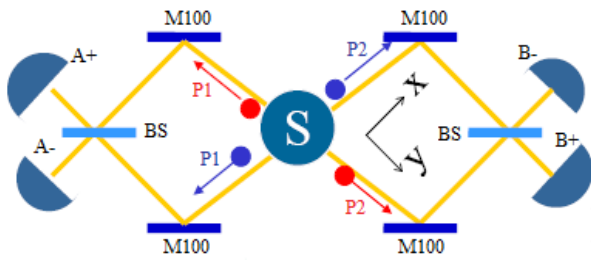


Figure 4.2.1 – Interféromètre équilibré. La source S produit deux quantons qui partent dans des directions indéterminées mais certainement opposées. Attention, il n'y a que 2 quantons, pas 4 !

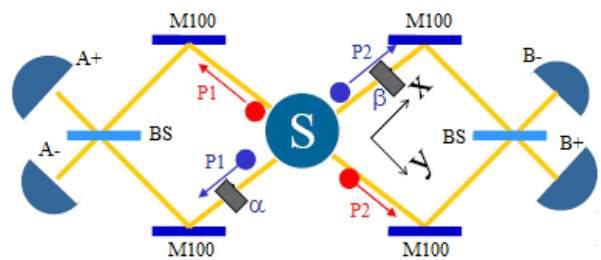


Figure 4.2.2 – Interféromètre déséquilibré. Modifier un seul chemin influence toutes les corrélations !

On considère une source S qui simultanément produit deux quantons suivant deux possibilités indiscernables : les deux quantons sont émis en sens opposés, soient dans la direction x , soient dans la direction y (figures 4.2.1 et 4.2.2). Cela signifie qu'il est absolument *impossible* de savoir dans quelle direction la paire a été émise sans devoir mettre des détecteurs juste après la source, c'est-à-dire sans modifier le montage. Par absolument impossible on doit comprendre exactement que ni dans les atomes qui forment la source, ni ailleurs dans l'univers, n'a été stockée une quelconque information sur la direction d'émission. Tout ce que l'on sait

est qu'il y a une **corrélation parfaite** : si un quanton a été émis selon x , alors l'autre l'est aussi (et de même pour y).

Nous allons admettre que la source est construite de sorte à assurer cette *indétermination quantique*. Une fois la paire émise, chaque quanton rencontre les mêmes éléments décrits pour le MZ à la **section 1.3**.

Dans l'expérience de la figure 4.2.1, on note que

- Lorsqu'on observe individuellement le quanton P_1 (ou le quanton P_2), il est détecté tantôt en A_- , tantôt en A_+ avec une probabilité $\frac{1}{2}$ pour chaque alternative (de même en B_- et B_+). Il n'y a donc pas d'interférence à un quanton. Il s'agit juste du hasard en A et en B , mais le même hasard !
- Lorsqu'on compare les résultats de A et B , on s'aperçoit que les détecteurs (A_+, B_+) ou (A_-, B_-) se sont activés au même moment ou simultanément. Il y a donc corrélation parfaite.

$$\begin{cases} \mathcal{P}(A_+, B_+) = \mathcal{P}(A_-, B_-) = \frac{1}{2} \\ \mathcal{P}(A_+, B_-) = \mathcal{P}(A_-, B_+) = 0 \end{cases} \implies \begin{cases} \mathcal{P}(A = B) = 1 \\ \mathcal{P}(A \neq B) = 0 \end{cases} \quad (4.2.5)$$

Dans l'expérience de la figure 4.2.2, examinons ce qui se passe formellement. La source produit un état intriqué

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|x\rangle_1 |x\rangle_2 + |y\rangle_1 |y\rangle_2). \quad (4.2.6)$$

L'évolution de $|x\rangle_1 |x\rangle_2$ dans l'interféromètre est

$$\begin{aligned} & |x\rangle_1 |x\rangle_2 \xrightarrow{\alpha, \beta} [e^{i\alpha} |x\rangle_1][e^{i\beta} |x\rangle_2] \xrightarrow{M100} [ie^{i\alpha} |y\rangle_1][ie^{i\beta} |y\rangle_2] \\ & \xrightarrow{BS} \left[ie^{i\alpha} \frac{1}{\sqrt{2}}(|y\rangle_1 + i|x\rangle_1) \right] \left[ie^{i\beta} \frac{1}{\sqrt{2}}(|y\rangle_2 + i|x\rangle_2) \right] \\ & = -\frac{1}{2}e^{i(\alpha+\beta)}(|y\rangle_1 |y\rangle_2 - |x\rangle_1 |x\rangle_2 + i|x\rangle_1 |y\rangle_2 + i|y\rangle_1 |x\rangle_2) \end{aligned} \quad (4.2.7)$$

De même, l'évolution de $|y\rangle_1 |y\rangle_2$ dans l'interféromètre est

$$\begin{aligned} & |y\rangle_1 |y\rangle_2 \xrightarrow{M100} [i|x\rangle_1][i|x\rangle_2] \\ & \xrightarrow{BS} \left[i \frac{1}{\sqrt{2}}(|x\rangle_1 + i|y\rangle_1) \right] \left[i \frac{1}{\sqrt{2}}(|x\rangle_2 + i|y\rangle_2) \right] \\ & = -\frac{1}{2}(|x\rangle_1 |x\rangle_2 - |y\rangle_1 |y\rangle_2 + i|y\rangle_1 |x\rangle_2 + i|x\rangle_1 |y\rangle_2) \end{aligned} \quad (4.2.8)$$

Ainsi, l'évolution de $|\Psi\rangle$ dans l'interféromètre est, en posant $\theta = \frac{\alpha+\beta}{2}$,

$$\begin{aligned} |\Psi\rangle &= \frac{1}{\sqrt{2}} \left[\frac{e^{i(\alpha+\beta)} - 1}{2}(|x\rangle_1 |x\rangle_2 - |y\rangle_1 |y\rangle_2) - i \frac{e^{i(\alpha+\beta)} + 1}{2}(|x\rangle_1 |y\rangle_2 + |y\rangle_1 |x\rangle_2) \right] \\ &= \frac{ie^{i\theta}}{\sqrt{2}} [\sin \theta (|x\rangle_1 |x\rangle_2 - |y\rangle_1 |y\rangle_2) + \cos \theta (|x\rangle_1 |y\rangle_2 + |y\rangle_1 |x\rangle_2)] \end{aligned} \quad (4.2.9)$$

On en déduit les probabilités

$$\mathcal{P}(x, x) = \mathcal{P}(y, y) = \frac{1}{2} \sin^2 \theta = \frac{1}{4} [1 - \cos(\alpha + \beta)] \quad (4.2.10a)$$

$$\mathcal{P}(x, y) = \mathcal{P}(y, x) = \frac{1}{2} \cos^2 \theta = \frac{1}{4} [1 + \cos(\alpha + \beta)] \quad (4.2.10b)$$

- Pour $\alpha = \beta = 0$, les deux quantons prennent toujours des sorties différentes : si l'un prend x , l'autre prend y et vice-versa. Pour $\alpha \pm \beta = \pi$, les deux quantons prennent toujours la même sortie. On dit qu'il y a corrélation, ou plutôt **anti-corrélation, parfaite**. On peut fixer $\beta = 0$ et ne faire varier que α , et quand même on passe d'une situation à l'autre : ***en variant un seul chemin d'un seul quanton, on modifie les corrélations !***
- On a donc des interférences dans les corrélations, mais des **interférences non-locales** puisqu'elles dépendent de la somme $\alpha + \beta$.
- Il est facile de vérifier que si l'on regarde chacun des deux quantons indépendamment de l'autre, le comportement est indépendant de α et β , et en fait

$$\mathcal{P}(1 = x) = \mathcal{P}(1 = y) = \frac{1}{2} \quad (4.2.11a)$$

$$\mathcal{P}(2 = x) = \mathcal{P}(2 = y) = \frac{1}{2} \quad (4.2.11b)$$

Effet,

$$\mathcal{P}(1 = x) = \mathcal{P}(x, x) + \mathcal{P}(y, y). \quad (4.2.12)$$

Cela implique que les corrélations quantiques ne peuvent pas être utilisées pour transmettre un message : si le physicien à droite modifie α , rien n'est modifié chez le physicien à gauche.

Exercice 4.2.1 A system of two qubits is in the state $|00\rangle$. We operate on this state with $W \otimes W$, where

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (4.2.13)$$

is the **Walsh-Hadamard** matrix. Is the state $W \otimes W |00\rangle$ entangled?

Solution 4.2.1

$$\begin{aligned} W \otimes W |00\rangle &= W |0\rangle \otimes W |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned} \quad (4.2.14)$$

So $W \otimes W |00\rangle$ is clearly a product state.

4.3 Information quantique

Nous allons maintenant examiner quelques applications pratiques des états corrélés à l'information quantique. L'idée directrice de l'information quantique est que l'on peut, en utilisant les spécificités du formalisme quantique, concevoir de nouvelles façon de traiter et transmettre l'information.

4.3.1 Non-clonage quantique

Théorème 4.3.1 Non-clonage. *Il n'est pas possible de construire une machine (Quantum Cloning Machine, QCM) qui opère des transformations unitaires et capable de dupliquer (cloner) parfaitement un qubit arbitraire.*

Preuve. On considère un système composé du qubit à dupliquer, un second qubit et une machine à dupliquer.

Le premier qubit est préparé dans un état arbitraire

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \text{ avec } |\alpha|^2 + |\beta|^2 = 1. \quad (4.3.1)$$

Initialement, le second qubit et la machine à cloner sont préparés dans les états de référence $|R\rangle$ et $|M\rangle$. $|R\rangle$ joue le rôle de support vierge.

La machine à cloner devrait être capable d'effectuer une transformation unitaire U telle que

$$\begin{aligned} U |\psi\rangle |R\rangle |M\rangle &= |\psi\rangle |\psi\rangle |M(\psi)\rangle \\ &= (\alpha |0\rangle + \beta |1\rangle)(\alpha |0\rangle + \beta |1\rangle) |M(\psi)\rangle \\ &= (\alpha^2 |00\rangle + \alpha\beta(|01\rangle + |10\rangle) + \beta^2 |11\rangle) |M(0+1)\rangle \end{aligned} \quad (4.3.2)$$

où $|M(\psi)\rangle$ est l'état final de la machine. Elle pourrait dépendre de l'état à dupliquer.

Montrons maintenant que U ne peut exister.

$$U |0\rangle |R\rangle |M\rangle = |0\rangle |0\rangle |M(0)\rangle \quad (4.3.3a)$$

$$U |1\rangle |R\rangle |M\rangle = |1\rangle |1\rangle |M(1)\rangle \quad (4.3.3b)$$

En vertu de la linéarité,

$$U |\psi\rangle |R\rangle |M\rangle = \alpha |0\rangle |0\rangle |M(0)\rangle + \beta |1\rangle |1\rangle |M(1)\rangle \quad (4.3.4)$$

qui est clairement différent de (4.3.2), le qubit cloner que l'on souhaite obtenir. ■

Il est essentiel de considérer un état arbitraire. En effet, si l'on sait au départ que le qubit est dans l'un des états orthogonaux, par exemple $|0\rangle$ ou $|1\rangle$, alors on peut mesurer avec certitude l'état du qubit et effectuer autant de copie que souhaité. Dans ce cas, le qubit agit comme le bit classique et nous savons qu'il existe des machines à dupliquer classiques (les photocopieurs).

Preuve. Soient $|\chi\rangle$ et $|\varphi\rangle$ deux qubits à un état que l'on souhaite cloner

$$U |\chi\rangle |R\rangle |M\rangle = |\chi\rangle |\chi\rangle |M\rangle \quad (4.3.5a)$$

$$U |\varphi\rangle |R\rangle |M\rangle = |\varphi\rangle |\varphi\rangle |M\rangle \quad (4.3.5b)$$

Le produit scalaire $X = \langle\chi| \langle R| \langle M| U^\dagger U |\varphi\rangle |R\rangle |M\rangle$ peut s'évaluer de deux façons différentes :

$$X = \langle\chi| \langle R| \langle M| \varphi\rangle |R\rangle |M\rangle = \langle\chi|\varphi\rangle \quad (4.3.6a)$$

$$X = \langle\chi| \langle\chi| \langle M| \varphi\rangle |\varphi\rangle |M\rangle = (\langle\chi|\varphi\rangle)^2 \quad (4.3.6b)$$

Il s'ensuit que soit $|\chi\rangle = |\varphi\rangle$ (états identiques), soit $\langle\chi|\varphi\rangle = 0$ (états orthogonaux). ■

Comme le principe d'indétermination d'Heisenberg, le théorème de non-clonage définit une impossibilité intrinsèque, pas seulement une limitation de laboratoire.

Pour évaluer la qualité d'un clonage et connaître le clonage le moins parfait possible, on utilise un paramètre appelé **fidélité**

$$F_j = \langle \psi | \rho_j | \psi \rangle \leq 1, \quad (4.3.7)$$

qui mesure le recouvrement entre l'état d'entrée $|\psi\rangle$ et l'état de sortie caractérisé par son opérateur densité partiel ρ_j .

- Une QCM est dite **universelle** (UQCM) si elle copie parfaitement tous les états, i.e., si F_j est indépendante de $|\psi\rangle$.
- Une QCM est dite **symétrique** lorsque les états de tous les clones ont la même fidélité, i.e., $F_j = F_{j'}$, $j = j' = 1, 2, \dots, M$.
- Une QCM est dite **optimale** lorsque pour une fidélité donnée d'un état original, les fidélités des états de clones sont les maxima permis par la formulation quantique. Spécifiquement, si \mathcal{S} est l'ensemble des états à cloner, l'optimalité peut être définie en maximisant soit la moyenne de la fidélité sur les états,

$$\bar{F} = \int_{\mathcal{S}} F(\psi) d\psi, \quad (4.3.8)$$

soit le minimum de la fidélité sur les états

$$F_{\min} = \min_{\psi \in \mathcal{S}} F(\psi). \quad (4.3.9)$$

4.3.2 Cryptographie quantique

SSL (Secure Socket Layer), RSA (Rivest-Shamir-Adleman), DES (Data Encryption standard), sont les acronymes (barbares!?) que nous utilisons au quotidien pour nos communications sur internet. Il s'agit de systèmes de cryptographie ³ qui repose sur un principe vieux de plus d'un siècle : l'algorithme, c'est-à-dire la manière dont est **chiffrer ou coder** l'information, peut-être connu de tous, mais la **clé**, sésame qui permet d'appliquer l'algorithme et de lire le message, doit rester secrète. Il en existe deux grands types (voir l'**annexe C** pour plus de détails.).

1. Le premier, dit **à clé privée**, fonctionne sur le modèle du coffre-fort. La même clé sert à chiffrer et déchiffrer l'information, ouvrir et fermer le coffre. Le protocole de Vernam ou *One-time pad*, qui permet une cryptographie absolument sûre, en est un.
2. Le second, dit **à clé publique**, s'apparente plutôt à une boîte aux lettres. La clé publique, comme l'adresse sur une enveloppe, permet à n'importe qui d'envoyer des messages cryptés, mais seul le destinataire peut ouvrir la boîte, autrement dit possède la clé privée qui permet de déchiffrer. Le célèbre protocole RSA⁴ en est un exemple.

Plus la clé privée est longue, moins un éventuel espion a de chances de la deviner par tâtonnement. Le DES⁵, créée en 1970 par IBM utilise une clé de 56 bits, ce qui offre $2^{56} \simeq$

³Écriture secrète en grec

⁴L'algorithme RSA peut être utilisé soit comme algorithme de chiffrement, soit comme algorithme de signature. Sa sécurité repose sur celle de la factorisation des nombres entiers.

⁵C'est certainement l'algorithme cryptographique le plus connu dans le monde, il fut établi en 1976 comme standard pour les communications gouvernementales américaines non classifiées.

7×10^{16} possibilités de clés différentes. Ce qui a été fait en 1998 en une journée avec des ordinateurs mis en parallèles.

L'opération de cryptage à clé publique ne s'effectue pas avec un *ou exclusif* mais avec des fonctions dites **à sens unique**. *Une fonction est à sens unique si elle se calcule rapidement et que sa réciproque se calcule en un temps très long.* Par exemple, $y = x^3$ serait à sens unique si $x = \sqrt[3]{y}$ était très long à calculer. Pour l'instant, l'existence de fonctions à sens unique n'a pas été démontrée, mais certaines fonctions le sont probablement, comme les exponentielles modulaires du type $a^p \bmod n$, où \bmod est la fonction modulo, qui renvoie le reste de la division par n . C'est précisément ces fonctions qui sont utilisées dans les protocoles à clé publique.

One-time pad

Il a été proposé en 1917 par G. Vernam et son inviolabilité a été prouvé 30 ans plus tard par Shannon. Il peut se résumer de la façon suivante :

Alice (A) souhaite envoyer à Bob (B) un message \mathcal{M} codée en binaire et de longueur N . On suppose qu'Alice et Bob partagent une liste \mathcal{K} de \mathcal{N} bits aléatoires appelée **clé**, qui est secrète, c'est-à-dire connue d'eux seuls.

1. Alice forme la liste de N bits $\mathcal{X} = \mathcal{M} \oplus \mathcal{K}$, où \oplus indique la somme binaire bit par bit (XOR), qu'elle envoie à Bob. La liste \mathcal{X} est **aléatoire**, c'est-à-dire qu'elle ne contient aucune information. Un espion qui écoute la ligne ne peut tirer aucune information.

Algorithm 4.3.1 Chiffrement (M, K)

- 1: Message à coder en binaire $M = m_1 m_2 \cdots m_n$.
 - 2: Clé binaire de chiffrement $K = k_1 k_2 \cdots k_n$.
 - 3: Renvoyer le message chiffré $C = c_1 c_2 \cdots c_n$, avec $c_i = m_i \oplus k_i, \forall i \in \{1, 2, \dots, n\}$.
-

2. Bob va **déchiffrer ou décoder**⁶ le message car il possède la clé,

$$\mathcal{X} \oplus \mathcal{K} = \mathcal{M} \quad (4.3.10)$$

Algorithm 4.3.2 Déchiffrement (C, K)

- 1: Message binaire chiffré $C = c_1 c_2 \cdots c_n$.
 - 2: Clé binaire de déchiffrement associé $K = k_1 k_2 \cdots k_n$.
 - 3: Renvoyer le message déchiffré $M = m_1 m_2 \cdots m_n$, avec $m_i = c_i \oplus k_i, \forall i \in \{1, 2, \dots, n\}$.
-

Proposition 4.3.1 Dans le **one-time pad**, si la clé est aussi longue que le message à chiffrer, et si elle n'est utilisée qu'une seule fois, alors il est impossible de décrypter le message.

Preuve. $K \rightarrow \text{dechiffrement}(C, K)$ étant une bijection de $\{0, 1\}^n$, sans aucune information sur la clé de chiffrement, il est impossible de décrypter un message en utilisant le one-time pad. ■

⁶On parle de **décryptage** lorsqu'on *crack* ou *attaque* une information chiffrée, c'est-à-dire le recouvrement de l'information, sans connaissance de la clé secrète.

La cryptographie à clé secrète est absolument sûre, pourvu qu’Alice et Bob partagent une clé secrète. Il faut donc qu’ils puissent se transmettre cette clé sans qu’elle soit interceptée par un espion. La cryptographie quantique est une méthode pour **distribuer secrètement la clé**.

Protocole BB84

Bennett et Brassard ont proposé en 1984 un protocole, le **protocole BB84**, qui permet à Alice et Bob, qui n’ont initialement en commun aucune information secrète, **d’échanger publiquement une clé, mais qui reste connue d’eux seules**. Cette clé servira par la suite au chiffrement des messages suivant le code de Vernam. Ce protocole, qui nécessite qu’Alice et Bob aient accès à un canal quantique et un canal classique, repose sur le fait que le qubit,

- ne peut-être cloné,
- autorise la superposition des états,
- change d’état lors de la mesure,

et se résumer en phases suivantes :

1. **Envoie.** Alice prépare des photons uniques polarisés suivant⁷ Oz ou Ox . Les états associés aux résultats de la mesures sont

Base Z	Base X
$ 0_z\rangle = H\rangle$	$ 0_x\rangle = +\rangle = \frac{1}{\sqrt{2}}(H\rangle + V\rangle)$
$ 1_z\rangle = V\rangle$	$ 1_x\rangle = -\rangle = \frac{1}{\sqrt{2}}(H\rangle - V\rangle)$

Pour chaque photon qu’elle a envoyée, Alice relève la base Z ou X dans laquelle le photon a été polarisée. Bob aussi relevé la base dans laquelle il a effectué sa mesure⁸.

2. **Sifting ou accord des bases.** Alice et Bob se communiquent publiquement les bases dans lesquelles ils ont effectué les mesures. Ils gardent les cas où ils ont utilisé la même base et jettent les autres. Sans espions ni erreurs, à ce stade, Alice et Bob devraient avoir deux listes identiques de bits secrets (voir la table 4.3.1).
3. **Estimation de l’erreur.** Alice communique publiquement quelques-uns des bits de sa clé à Bob. Celui compare et estime le taux d’erreurs R . Ces erreurs peuvent être dues à la présence d’un espion ou aux bruits⁹. Les bits qui n’ont pas été révélés publiquement dans cette étape vont former la **clé**.
4. **Traitement ultérieur.** Lorsque le taux d’erreur est assez faible, Alice et Bob appliquent des procédures qui corrigent presque toutes les erreurs et diminuent l’information d’un espion éventuel. On parle alors de **clé transmise** (voir la table 4.3.2). Lorsque par contre ce taux est élevé, Alice et Bob rejette la clé car l’espion pourrait avoir trop d’information. **Jamais une clé non-secrète n’est utilisée.**

Numéro du quanton	1	2	3	4	5	6	7	8
Axe choisi par Alice (secret)	Z	Z	X	Z	Z	X	X	Z
État choisi par Alice (secret)	0	1	0	1	1	1	0	1
Axe choisi par Bob (Publique)	Z	X	X	Z	X	Z	X	X
État choisi par Bob (Publique)	0	1	0	1	1	0	0	0
Mesure utile ?	Oui	Non	Oui	Oui	Non	Non	Oui	Non

Table 4.3.1 – Détection éventuelle d’une espion : Alice recherche parmi les mesures effectuées avec le même choix d’axes par Bob et par elle-même (quantons 1, 3, 4 et 7) une éventuelle différence dans les états, qui signalerait la présence d’un espion. Aucune anomalie ne se produit ici. Pour s’assurer de l’absence d’un espion avec une probabilité raisonnable, il faut utiliser en pratique un nombre de mesures bien supérieur à 8.

Numéro du quanton	9	10	11	12	13	14	15	16
Axe choisi par Alice (secret)	X	Z	X	Z	Z	X	Z	Z
État choisi par Alice (secret)	0	1	0	0	1	1	0	1
Axe choisi par Bob (Publique)	Z	Z	X	X	Z	Z	Z	X
État choisi par Bob (Publique)	0	1	0	1	1	0	0	0
Mesure utile ?	Non	Oui	Oui	Non	Oui	Non	Oui	Non

Table 4.3.2 – Après s’être assurée de l’absence d’un espion, Alice choisit parmi les mesures utiles celles qui lui permettent de communiquer son message. Par exemple, pour communiquer le message «0,0», elle demande (publiquement) à Bob de considérer les résultats de ses mesures 11 et 15.

Il est à noter lorsqu’une espionne Eve (E) intercepte l’information envoyée à Bob, elle fait la même chose que Bob, en choisissant de mesurer soit Z soit X. Ensuite, elle prépare un nouveau photon polarisé suivant le résultat de sa mesure qu’elle envoie à Bob. On appelle cette attaque **intercept-resend**. Le clonage du photon émis par Alice n’étant pas possible.

Puisqu’Eve ne sait pas dans quelle base Alice a préparé les photons, Eve ne peut imiter Alice au mieux que dans la moitié des cas. Alors les résultats d’Alice et Bob sont différents dans 25% des cas lorsqu’ils ont la même base. Ils concluent donc qu’il y a un espion sur la ligne quantique.

Faisons un résumé sur les unités d’informations :

- 50% échangés entre Alice et Bob par le canal classique
 - 25% inutilisables car Alice et Bob n’ont pas choisi le même axe
 - 25% utilisées pour détecter la présence d’Eve
- 50% gardées par Bob
 - 25% inutilisables car Alice et Bob n’ont pas choisi le même axe
 - 25% utilisées pour le véritable message (d’une importance gigantesque vu tout le mal que l’on s’est donné pour lui transmettre)

⁷Deux bases sont **conjuguées** lorsqu’un système représenté dans une des bases, se comporte de façon aléatoire lorsqu’il est soumis à une mesure faite dans l’autre base, et si l’information codée par le système est alors irréversiblement détruite.

⁸Lorsque la mesure de Bob est effectuée dans la même base que celle d’Alice, les résultats sont identiques (la probabilité de détection de chaque photon est 1). Lorsque les bases sont différentes, les résultats ne sont identiques que dans 50% des cas (la probabilité de détection de chaque photon est $\frac{1}{2}$).

⁹Mauvaises préparations des états, détecteurs imparfaits, interactions des qubits avec l’environnement.

La probabilité que Eve ne soit pas détecté est de

$$\left(\frac{3}{4}\right)^{\frac{N}{4}}. \quad (4.3.11)$$

Par exemple si Bob annonce publiquement 1 000 résultats, 500 en moyenne seront utilisables par Alice, et Eve aura introduit une erreur pour 125 d'entre eux (25%), toujours en moyenne. La probabilité pour qu'un espion effectivement présent ne soit pas détecté par une telle procédure est de $(\frac{3}{4})^{500} \simeq 3 \times 10^{-63}$, ce qui est complètement négligeable.

4.3.3 Fax quantique ou téléportation quantique

Définition 4.3.1 La *téléportation quantique* est un protocole de communications quantiques consistant à **transférer** l'état quantique d'un système vers un autre système similaire et séparé spatialement du premier en mettant à profit l'intrication quantique.

Contrairement à ce que le nom laisse entendre, *il ne s'agit donc pas de transfert de matière*. Le terme de téléportation quantique est utilisé pour souligner le fait que le processus est destructif : à l'issue de la téléportation, le premier système ne sera plus dans le même état qu'initialement.

La téléportation quantique pourrait être intéressant pour le calcul quantique en ce sens qu'elle peut servir pour le transfert de l'information quantique entre différentes unités indépendantes du calculateur quantique.

On peut formuler la problématique de la téléportation quantique de la façon suivante :

Problème 4.3.1 Il était une fois, Alice et Bob qui, avant de se séparer, prirent chacun un qubit d'une même paire EPR, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Puis Bob s'en alla, vers une galaxie ignorée d'Alice.

C'est alors que, bien plus tard, un qubit dans un état inconnu, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, arriva chez Alice. Mission d'Alice, transmettre l'état de $|\psi\rangle$ à Bob.

Mais Alice ne pouvait pas,

- porter ce qubit à Bob,
- ni cloner pour en disperser des copies dans l'univers,
- ni connaître α et β pour diffuser leurs valeurs sur les ondes dans l'espace intergalactique. Une mesure de α (ou β) réduira malheureusement $|\psi\rangle$ à $|0\rangle$ (ou $|1\rangle$).

Le protocole de téléportation quantique est le suivant :

- Alice et Bob utilisent un canal EPR composé d'une paire de qubits maximalement intriqués :

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}}(|00\rangle_{23} + |11\rangle_{23}). \quad (4.3.12)$$

Le qubit 2 est pris par Alice et le qubit 3 est pris par Bob.

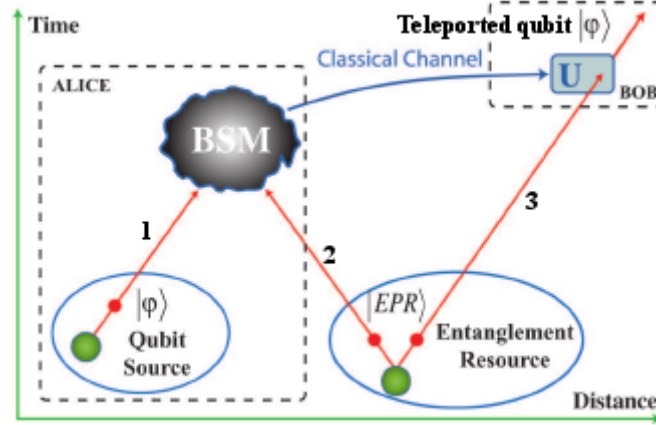


Figure 4.3.1 – Schéma de principe de la téléportation quantique. Alice effectue une mesure de Bell (BSM, Bell State Measurement) sur les qubits $|\psi\rangle$ et un des qubits EPR et informe Bob du résultat par un canal classique (bits classiques) afin que ce dernier finalise la téléportation en appliquant une transformation unitaire U adéquate qui lui permet de reconstruire le qubit $|\psi\rangle$ envoyé par Alice. [Après N. Gisin and R. Trew, Quantum Communication, <http://arxiv.org/abs/quant-ph/0703255v1>]

- Alice souhaite transmettre ou transférer à Bob l'information sur l'état d'un qubit

$$|\psi\rangle_1 = \alpha |0\rangle_1 + \beta |1\rangle_1 \quad (4.3.13)$$

qui lui est *à priori* inconnu, sans lui transmettre directement ce qubit.

- Alice mesure l'état quantique de la nouvelle paire de qubits 1 et 2 (non intriqués) en utilisant la **base de Bell** constituée des états intriqués

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (4.3.14a)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (4.3.14b)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (4.3.14c)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (4.3.14d)$$

On vérifie facilement que l'état des trois qubits est alors

$$\begin{aligned} |\psi\rangle_{123} &= |\psi\rangle_1 \otimes |\Phi^+\rangle_{23} = (\alpha |0\rangle + \beta |1\rangle)_1 \otimes |\Phi^+\rangle_{23} \\ &= \frac{1}{2} [|\Phi^+\rangle_{12} (\alpha |0\rangle + \beta |1\rangle)_3 + |\Phi^-\rangle_{12} (\alpha |0\rangle - \beta |1\rangle)_3 \\ &\quad + |\psi^+\rangle_{12} (\alpha |1\rangle + \beta |0\rangle)_3 + |\psi^-\rangle_{12} (\alpha |1\rangle - \beta |0\rangle)_3] \end{aligned} \quad (4.3.15)$$

La mesure par Alice de l'état de la paire de qubits intriqués 12 projette cet état sur l'un des quatre états de base (4.3.14), ce qui projette l'état du qubit 3 sur l'état correspondant dans (4.3.15). Le tableau 4.3.3 récapitule les différentes *mesures de Bell* : On constate que l'état du qubit d'Alice est téléporté sur le qubit de Bob avec une probabilité de 25%.

- Alice transmet à Bob par un canal classique le résultat de sa mesure (mesure de Bell), et Bob sait que le qubit 3 lui arrive dans l'état inconnu de départ (4.3.13), mais qui reste tout aussi inconnu ! L'état du qubit 1 a été téléporté, mais il n'y a jamais eu une mesure de cet état.

Résultat de la mesure de 12	État préparé en 3	probabilité
$ \Phi^+\rangle$	$\alpha 0\rangle + \beta 1\rangle$	$\frac{1}{4}$
$ \Phi^-\rangle$	$\alpha 0\rangle - \beta 1\rangle$	$\frac{1}{4}$
$ \psi^+\rangle$	$\alpha 0\rangle + \beta 1\rangle$	$\frac{1}{4}$
$ \psi^-\rangle$	$\alpha 0\rangle - \beta 1\rangle$	$\frac{1}{4}$

Table 4.3.3 – Mesure de Bell qui distingue les quatre états de Bell

- Si le résultat de la mesure d'Alice n'est pas $|\Phi^+\rangle_{12}$, Bob en sait assez pour faire la correction en appliquant la transformation unitaire U convenable qui permet de ramener le qubit 3 dans l'état (4.3.13).

Remarque 4.3.1 1. A aucun moment, les coefficients α et β ne sont mesurés, et l'état $|\psi\rangle_1$ est détruit au cours de la mesure effectuée par Alice. Il n'y a pas contradiction avec le théorème de non-clonage.

2. Bob ne connaît l'état du qubit 3 que lorsqu'il a reçu le résultat de la mesure d'Alice. La transmission de cette information doit se faire par un canal classique, à une vitesse au plus égale à la vitesse de la lumière. Il n'y a donc pas transfère instantanée de l'information à distance.
3. Il y a jamais transport de la matière dans la téléportation.

4.4 Exercices

4.4.1 Inégalités de Bell avec des photons

On considère deux photons partant en sens inverse, l'un (1) suivant Oz et l'autre (2) suivant $-Oz$ comme indiqué sur la figure 4.4.1, dans un état de polarisation intriqué

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|xy\rangle - |yx\rangle). \quad (4.4.1)$$

Les états $|x\rangle$ et $|y\rangle$ sont des états de polarisation linéaire suivant Ox et Oy .

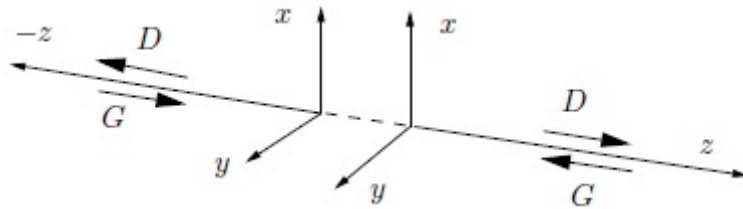


Figure 4.4.1 – Configuration des polarisations des photons intriqués.

1. L'état de polarisation linéaire suivant la direction \hat{n}_θ du plan xOy est

$$|\theta\rangle = \cos \theta |x\rangle + \sin \theta |y\rangle, \quad (4.4.2)$$

et l'état de polarisation orthogonale est

$$|\theta_\perp\rangle = -\sin \theta |x\rangle + \cos \theta |y\rangle. \quad (4.4.3)$$

Montrer que

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\theta\theta_\perp\rangle - |\theta_\perp\theta\rangle). \quad (4.4.4)$$

L'état $|\Psi\rangle$ est donc invariant par rotation autour de Oz .

2. Montrer que $|\Psi\rangle$ s'écrit, en fonction des états de polarisation circulaire

$$|D\rangle = -\frac{1}{\sqrt{2}}(|x\rangle + i|y\rangle), \quad (4.4.5a)$$

$$|G\rangle = \frac{1}{\sqrt{2}}(|x\rangle - i|y\rangle), \quad (4.4.5b)$$

en prenant garde au sens de propagation des axes $+Oz$ et $-Oz$ comme indiqué sur la figure 4.4.1,

$$|\Psi\rangle = \frac{i}{\sqrt{2}}(|DD\rangle - |GG\rangle). \quad (4.4.6)$$

3. Soient \mathcal{P}_D et \mathcal{P}_G les projecteurs sur les états de polarisation circulaire. On peut associer à la grandeur physique polarisation circulaire l'opérateur

$$\Sigma_z = \mathcal{P}_D - \mathcal{P}_G. \quad (4.4.7)$$

(a) Montrer cet opérateur est hermitien et que ses vecteurs propres sont $|D\rangle$ et $|G\rangle$.

(b) En utilisant (4.4.7), vérifier que (4.4.6) est invariant par rotation autour de Oz .

4. Alice et Bob analysent la polarisation des photons à l'aide de polariseurs linéaires orientés suivant les directions \hat{n}_α pour le photon 1 et \hat{n}_β pour le photon 2 dans le plan xOy . On définit

- $p_{++}(\alpha, \beta)$, la probabilité pour que le photon 1 soit polarisé suivant \hat{n}_α et le photon 2 suivant \hat{n}_β ;
- $p_{+-}(\alpha, \beta)$, la probabilité pour que le photon 1 soit polarisé suivant \hat{n}_α et le photon 2 suivant \hat{n}_{β^\perp} ;
- $p_{-+}(\alpha, \beta)$ et $p_{--}(\alpha, \beta)$ étant définis de façon analogue.

On définit le coefficient de corrélation de polarisation

$$E(\alpha, \beta) = [p_{++}(\alpha, \beta) + p_{--}(\alpha, \beta)] - [p_{+-}(\alpha, \beta) + p_{-+}(\alpha, \beta)]. \quad (4.4.8)$$

(a) En utilisant l'invariant par rotation de $|\Psi\rangle$ pour simplifier les calculs, trouver l'expression des probabilités précédentes et montrer que

$$E(\alpha, \beta) = -\cos[-2(\alpha - \beta)]. \quad (4.4.9)$$

(b) Quelles valeurs de α , α' , β et β' doit-on utiliser pour obtenir comme dans le cas des spins $\frac{1}{2}$,

$$X = E(\alpha, \beta) + E(\alpha, \beta') + E(\alpha', \beta') - E(\alpha', \beta) = -2\sqrt{2}? \quad (4.4.10)$$

5. Montrer que

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|xx\rangle + |yy\rangle), \quad (4.4.11)$$

est également invariant par rotation autour de Oz . Donner son expression en fonction des états de polarisation circulaire.

4.4.2 Distribution quantique des clefs 1

BB4 sans espion

1. Compléter le tableau 4.4.1 qui décrit la phase **Envoie**.
2. Vérifier qu'après la phase **sifting**, Alice et Bob partagent une liste identique de bits secrets. Pourquoi ces bits sont-ils secrets ?

BB4 avec espion

On suppose qu'une espionne Eve (E) fait la même chose que Bob, en choisissant de mesurer soit Z soit X . Ensuite, elle prépare un nouveau photon polarisé suivant le résultat de sa mesure qu'elle envoie à Bob. On appelle cette attaque **intercept-resend**.

Pour le tableau 4.4.2 de la phase **Envoie**, nous ne considérons que les cas où Alice et Bob mesurent dans la même base, car les autres cas seront de toute façon écartés lors de la phase **sifting**. Aussi nous ne considérons que la base Z , la situation pour la base X étant symétrique.

A envoie	B mesure et trouve	Probabilité	A envoie	B mesure et trouve	Probabilité
$ 0_z\rangle$	$Z \rightarrow 0_z\rangle$	1	$ 0_x\rangle$	$Z \rightarrow 0_z\rangle$	
$ 0_z\rangle$	$Z \rightarrow 1_z\rangle$		$ 0_x\rangle$	$Z \rightarrow 1_z\rangle$	
$ 0_z\rangle$	$X \rightarrow 0_x\rangle$	$\frac{1}{2}$	$ 0_x\rangle$	$X \rightarrow 0_x\rangle$	
$ 0_z\rangle$	$X \rightarrow 1_x\rangle$		$ 0_x\rangle$	$X \rightarrow 1_x\rangle$	
$ 1_z\rangle$	$Z \rightarrow 0_z\rangle$		$ 1_x\rangle$	$Z \rightarrow 0_z\rangle$	
$ 1_z\rangle$	$Z \rightarrow 1_z\rangle$		$ 1_x\rangle$	$Z \rightarrow 1_z\rangle$	
$ 1_z\rangle$	$X \rightarrow 0_x\rangle$		$ 1_x\rangle$	$X \rightarrow 0_x\rangle$	
$ 1_z\rangle$	$X \rightarrow 1_x\rangle$		$ 1_x\rangle$	$X \rightarrow 1_x\rangle$	

Table 4.4.1 – Phase *envoi* d'une situation idéale sans espion ni erreurs du protocole BB84 sans espion

1. Compléter les probabilités du tableau 4.4.2. On notera qu'Alice et Bob n'ont pas le même bit en présence de l'attaque d'Eve, malgré le fait qu'ils ont effectué les mesures dans la même base.
2. Pourquoi dans le protocole BB4 est-il nécessaire d'utiliser deux bases ? Que se passerait-il si Alice et Bob décidaient de n'utiliser qu'une seule base pour coder leurs bits ?
3. Comment Alice et Bob font pour détecter la présence de l'espion Eve ?

A envoie	E mesure et trouve	B mesure et trouve	Proba	A envoie	E mesure et trouve	B mesure et trouve	Probab
$ 0_z\rangle$	$Z \rightarrow 0_z\rangle$	$Z \rightarrow 0_z\rangle$	$\frac{1}{2}$	$ 1_z\rangle$	$Z \rightarrow 0_z\rangle$	$Z \rightarrow 0_z\rangle$	
$ 0_z\rangle$	$Z \rightarrow 0_z\rangle$	$Z \rightarrow 1_z\rangle$	0	$ 1_z\rangle$	$Z \rightarrow 0_z\rangle$	$Z \rightarrow 1_z\rangle$	
$ 0_z\rangle$	$Z \rightarrow 1_z\rangle$	$Z \rightarrow 0_z\rangle$		$ 1_z\rangle$	$Z \rightarrow 1_z\rangle$	$Z \rightarrow 0_z\rangle$	
$ 0_z\rangle$	$Z \rightarrow 1_z\rangle$	$Z \rightarrow 1_z\rangle$		$ 1_z\rangle$	$Z \rightarrow 1_z\rangle$	$Z \rightarrow 1_z\rangle$	
$ 0_z\rangle$	$X \rightarrow 0_x\rangle$	$Z \rightarrow 0_z\rangle$	$\frac{1}{8}$	$ 1_z\rangle$	$X \rightarrow 0_x\rangle$	$Z \rightarrow 0_z\rangle$	
$ 0_z\rangle$	$X \rightarrow 0_x\rangle$	$Z \rightarrow 1_z\rangle$		$ 1_z\rangle$	$X \rightarrow 0_x\rangle$	$Z \rightarrow 1_z\rangle$	
$ 0_z\rangle$	$X \rightarrow 1_x\rangle$	$Z \rightarrow 0_z\rangle$		$ 1_z\rangle$	$X \rightarrow 1_x\rangle$	$Z \rightarrow 0_z\rangle$	
$ 0_z\rangle$	$X \rightarrow 1_x\rangle$	$Z \rightarrow 1_z\rangle$		$ 1_z\rangle$	$X \rightarrow 1_x\rangle$	$Z \rightarrow 1_z\rangle$	

Table 4.4.2 – Phase *envoi* d'une situation avec espion du protocole BB84

4.4.3 Distribution quantique des clefs 1

Deux personnes qui veulent communiquer dans l'intimité ou la discrétion doivent prévoir une clef et la garder secrète. Le code de Vernam est le seul qui soit mathématiquement reconnu comme inviolable, mais il impose d'utiliser une clef différente pour chaque chiffrement. C'est problème de distribution des clefs secrètes. Le présent exercice montre comment la théorie quantique peut fournir une procédure répondant à ce besoin.

On rappelle que $\cos^4 x + \sin^4 x = \frac{1}{2}(1 + \cos^2 2x)$ et $\int (1 + \cos^2 x) dx = \frac{3}{2}x + \frac{1}{4} \sin 2x$.

1. On considère un quanton de spin $\frac{1}{2}$. L'opérateur de spin est $\mathbf{S} = \frac{\hbar}{2} \boldsymbol{\sigma}$, où les $\boldsymbol{\sigma}$ sont les matrices de Pauli, qui dans la base $\{|z+\rangle, |z-\rangle\}$ qui diagonalise \mathbf{S}_z s'écrivent,

$$\sigma_x = |z-\rangle \langle z+| + |z+\rangle \langle z-|, \quad \sigma_y = i(|z-\rangle \langle z+| - |z+\rangle \langle z-|), \quad \sigma_z = |z+\rangle \langle z+| - |z-\rangle \langle z-|. \quad (4.4.12)$$

On suppose que l'état du spin du quanton est $|z+\rangle$. On effectue la mesure de la composante du spin suivant un axe orienté le long du vecteur unitaire $\hat{\mathbf{u}}(\sin \theta, 0, \cos \theta)$. Les

états propre de \mathbf{S}_u , $|u+\rangle$ et $|u-\rangle$ sont les transformés des états $|z\pm\rangle$ par une rotation qui amène l'axe Oz sur l'axe $\hat{\mathbf{u}}$. Un choix possible consiste à faire une rotation de θ autour de l'axe Oy . On rappelle que l'opérateur de rotation autour de Ou est $\mathbf{R}_u(\theta) = e^{-i\theta\sigma_u/2} = (\cos \frac{\theta}{2})\mathbb{I} - i(\sin \frac{\theta}{2})\sigma_u$.

- (a) Donner l'expression de $|u\pm\rangle$ en fonction de θ . En déduire les probabilités $\mathcal{P}_{u\leftarrow z+}^{\pm}(\theta)$ de trouver $\pm\frac{\hbar}{2}$ suivant u , l'état mesuré étant $|z+\rangle$.
- (b) Quels sont les états de spins après une mesure ayant donné $+\frac{\hbar}{2}$ ou $-\frac{\hbar}{2}$?

2. Immédiatement après cette mesure, on mesure la composante du spin suivant l'axe z .

- (a) Donner les résultats possibles et leurs probabilités en fonction du résultat obtenu précédemment le long de u .
- (b) Montrer que la probabilité de retrouver la même valeur $+\frac{\hbar}{2}$ que dans l'état initial $|z+\rangle$ est,

$$\mathcal{P}_{++}(\theta) = \frac{1}{2}(1 + \cos^2 \theta). \quad (4.4.13)$$

- (c) En supposant, maintenant que l'état initial soit $|z-\rangle$, quelle est, dans la même séquence de mesures, la probabilité $\mathcal{P}_{--}(\theta)$ de retrouver $-\frac{\hbar}{2}$ dans la dernière mesure? On se contentera d'une brève justification!

3. On dispose d'une source O qui produit une paire (a, b) de quantons de spins $\frac{1}{2}$, préparé dans l'état $|\psi\rangle = \phi(\mathbf{r}_a, \mathbf{r}_b) |\Sigma\rangle$ où l'état du spin des 2 quantons est

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}(|z+\rangle |z+\rangle + |z-\rangle |z-\rangle) = \frac{1}{\sqrt{2}}(|z+z+\rangle + |z-z-\rangle), \quad (4.4.14)$$

c'est-à-dire que les variables spatiales et les variables de spin sont indépendantes. Dans la suite, on ne s'intéresse qu'aux mesures du spin.

- (a) Montrer que l'état (4.4.14) peut également s'écrire

$$|\Sigma\rangle = \frac{1}{\sqrt{2}}(|x+x+\rangle + |x-x-\rangle). \quad (4.4.15)$$

- (b) La paire de quanton (a, b) étant préparé dans l'état (4.4.14) ou (4.4.15), ces quanton sont spatialement séparés (voir la figure 4.4.2) sans que l'état de spin ne soit affecté (avant qu'une mesure n'intervienne).

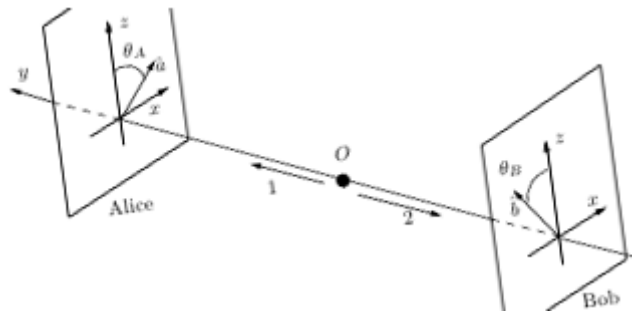


Figure 4.4.2 – Configuration des axes pour l'expérience de mesure de deux spins.

- i. Alice mesure d'abord la composante du spin de a suivant un axe u_a d'angle θ_a . Quels sont les résultats de mesure et les probabilités correspondantes dans les deux cas $\theta_a = 0$ (z) et $\theta_a = \frac{\pi}{2}$ (x) ?
- ii. Après cette mesure d'Alice l'état de spin des deux quantons est

Axe	Résultat	État
z	$+\frac{\hbar}{2}$	$ z + z+\rangle$
z	$-\frac{\hbar}{2}$	$ z - z-\rangle$
x	$+\frac{\hbar}{2}$	$ x + x+\rangle$
x	$-\frac{\hbar}{2}$	$ x - x-\rangle$

En déduire qu'on peut désormais ignorer le quanton a pour ce qui concerne les mesures de spin sur b .

- (c) Après cette mesure d'Alice, Bob mesure la composante du spin de b suivant un axe u_b d'angle θ_b . Déterminer les résultats de mesure possible de Bob et leurs probabilités, en fonction du résultat d'Alice, dans les quatre configurations suivantes :

(θ_a, θ_b)	Résultat Alice	Résultat Bob	Probabilité
$(0, 0)$			
$(0, \frac{\pi}{2})$			
$(\frac{\pi}{2}, 0)$			
$(\frac{\pi}{2}, \frac{\pi}{2})$			

Dans quel(s) cas la mesure sur a et celle sur b donnent-elles certainement le même résultat ?

- (d) On se place dans la situation $\theta_a = 0$. On suppose qu'un *espion*, situé entre la source O et Bob, fait une mesure de la composante du spin b suivant un axe u_e d'angle θ_e .
- Quels sont, en fonction de θ_e et du résultat de mesure d'Alice, les résultats de mesure de l'espion et leurs probabilités ?
 - Après cette mesure de l'espion, Bob mesure le spin de b suivant l'axe défini par $\theta_b = 0$, que trouve-t-il, avec quelle probabilité, en fonction du résultat trouvé par l'espion ?
 - Quelle est la probabilité $\mathcal{P}(\theta_e)$ qu'Alice et Bob trouvent le même résultat ?
 - Quelle est la moyenne de $\mathcal{P}(\theta_e)$ si l'espion choisit au hasard θ_e avec une probabilité uniforme sur $[0, 2\pi]$ ($\frac{1}{2\pi} \int_0^{2\pi} \mathcal{P}(\theta_e) d\theta_e$) ? Quelle est cette même moyenne s'il choisit équitablement seulement les deux valeurs $\theta_e = 0$, et $\theta_e = \frac{\pi}{2}$?

4. On souhaite utiliser les résultats qui précèdent à la transmission confidentielle d'information. Alice et Bob utilisent alors la procédure ci-dessous :

- Alice et Bob décident d'un choix d'axes x et z qui leurs servent de direction d'analyse.
- Alice, qui dispose de la source O prépare une séquence ordonnée de $N \gg n$ paires de spins $\frac{1}{2}$ dans l'état (4.4.14) (n est le nombre de bits du message). Elle envoie les spins b à Bob, et garde les spins a .
- Alice et Bob font, pour chacun des spins dont ils disposent, la mesure de la composante x ou z . Le choix entre x et z se fait de manière aléatoire et équiprobable pour chaque spin, et il n'y a pas de corrélation, pour un spin donné, entre la composante choisie par Alice et celle choisie par Bob. Ils stockent chacun l'ensemble de leurs résultats.

- Bob sélectionne une partie FN de ses mesures et il les communique publiquement à Alice, par un canal classique, la direction d'analyse choisie et le résultat obtenu pour chacune des mesures de cet ensemble. En pratique $F \sim 0.5$.
 - Alice compare pour cet ensemble FN ses directions et ses résultats avec ceux que vient de lui communiquer Bob. Elle peut alors détecter la présence éventuelle d'un espion. Si un espion est repéré, la procédure s'arrête et une recherche *physique* de l'espion doit avoir lieu. Sinon,
 - Alice annonce publiquement qu'elle est convaincue de ne pas avoir été écoutée, et Bob lui transmet, toujours publiquement, ses directions d'analyse pour les $(1 - F)N$ spins restants. En revanche, il ne communique pas ses résultats correspondants.
- (a) Comment Alice peut-elle se convaincre de la présence d'un espion dans le cas idéal des détecteurs parfaits ?
- (b) Quelle est la probabilité qu'un espion présent ne soit pas détecté ? A.N. : $FN = 200$.
- (c) L'espion gagne-t-il en *invisibilité* s'il connaît le système d'axe Oxz retenu par Alice et Bob et déterminant les directions d'analyse ?
- (d) Discuter sur les deux expériences décrites ci-dessous par les tables 4.4.3 et 4.4.4, l'existence d'un espion. On montrera que la communication 2 a certainement été espionnée. On calculera la probabilité qu'un espion ait opéré sans être détecté dans la communication 1.
- (e) Donner la dernière phase de la procédure en indiquant comment Alice peut envoyer son message (1) à Bob, sans utiliser d'autres paires de spins que les N paires déjà produites et analysées par Bob et elle-même. En utilisant les colonnes grisées de la table 4.4.3, indiquer comment dans l'expérience 1 ci-dessus, Alice peut transmettre à Bob le message $\{+, -\}$.

Numéro Spin	1	2	3	4	5	6	7	8	9	10	11	12
Axe choisi par Alice (secret)	X	X	Z	X	Z	Z	X	Z	Z	Z	X	X
Résultat d'Alice (secret)	+	-	+	+	-	-	+	+	+	-	+	-
Axe choisi par Bob (public)	X		X	Z			X			X	X	
Résultat de Bob (public)	+		-	-			+			+	+	

Table 4.4.3 – Expérience 1 réalisée avec $N = 12$ paires de spins.

Numéro Spin	1	2	3	4	5	6	7	8	9	10	11	12
Axe choisi par Alice (secret)	X	Z	Z	Z	X	X	Z	X	X	Z	X	Z
Résultat d'Alice (secret)	+	+	-	+	+	-	+	+	-	-	+	+
Axe choisi par Bob (public)		X			X			X	Z		Z	Z
Résultat de Bob (public)		+			+			-	+	+	+	-

Table 4.4.4 – Expérience 2 réalisée avec $N = 12$ paires de spins.

Sommaire

- 5.1 Notion de calculateur
- 5.2 Circuits quantiques
- 5.3 Portes quantiques universelles
- 5.4 Algorithme de Deutsch-Jozsa
- 5.5 Transformation de Fourier quantique
- 5.6 Réalisations physiques
- 5.7 Conclusion
- 5.8 Exercices

Qu'est-ce qu'un calculateur quantique, ou comme on le dit abusivement, un ordinateur quantique ? Ce chapitre nous permettra d'en acquérir les éléments de base à travers les notions de circuits quantiques (**section 5.2**), de portes logiques quantiques universelles (**section 5.3**). Pour effectuer des calculs de façon automatique, il faut des algorithmes. Bien qu'il n'existe pour le moment que très peu d'algorithmes quantiques, elles mettent toutes en exergue la supériorité des calculs quantiques par rapport aux calculs classiques. A la **section 5.4**, nous présentons l'un des tous premiers de ces algorithmes, l'algorithme de Deutsch-Jozsa. Mais commençons par revisiter la notion de calculateur à la **section 5.1**.

5.1 Notion de calculateur

Un état de n bits d'un calculateur classique ou **registre classique** de taille n , ne peut stocker, en instant donné, qu'un **seul entier** $i \in [0, 2^n - 1]$ décrit en notation binaire par

$$i = i_{n-1}2^{n-1} + \cdots + i_12^1 + i_02^0 = \sum_{m=0}^{n-1} i_m2^m, \quad (5.1.1)$$

où $i_m \in [0, 1]$. Ainsi, 3 bits physiques peuvent être préparés dans $2^3 = 8$ configurations différentes, représentant les nombres de 0 à 7. Par exemple, les chaînes binaires

$$011, \quad (5.1.2a)$$

$$111, \quad (5.1.2b)$$

représentent respectivement les nombres 3 et 7.

Un calculateur quantique est une collection de n qubits qui représente un **registre quantique** de taille n . L'état de n qubits d'un calculateur quantique est

$$\begin{aligned} |\psi\rangle &= \sum_{i=0}^{2^n-1} c_i |i\rangle \\ &= \sum_{i_{n-1}=0}^1 \cdots \sum_{i_1=0}^1 \sum_{i_0=0}^1 c_{i_{n-1}, \dots, i_1, i_0} |i_{n-1}\rangle \otimes \cdots \otimes |i_1\rangle \otimes |i_0\rangle \\ &= \sum_{i_{n-1}, \dots, i_1, i_0=0}^1 c_{i_{n-1}, \dots, i_1, i_0} |i_{n-1} \cdots i_1 i_0\rangle \end{aligned} \quad (5.1.3)$$

avec la contrainte (complétude)

$$\sum_{i=0}^{2^n-1} |c_i|^2 = 1. \quad (5.1.4)$$

Ainsi, en vertu du principe de superposition clairement visible dans l'Eq. (5.1.3), un registre quantique de n qubits peut être préparé non seulement dans l'état $|i\rangle$ de la base de calcul, mais aussi dans une superposition d'états et donc stocker 2^n nombres, qui augmente exponentiellement avec le nombre de qubits. Par conséquent, le principe de superposition offre de nouvelles possibilités de calculs comme le **parallélisme** qui permet le calcul en parallèle d'un grand nombre d'opérations.

Un état de n qubits d'un calculateur quantique est un vecteur d'état d'un espace de Hilbert de 2^n dimensions, construit comme produit tensoriel de n espaces de Hilbert de 2 dimensions, une pour chaque qubit. En prenant en compte la relation de complétude (5.1.4) et le fait que l'état de tout système quantique n'est défini qu'à un facteur de phase global près sans signification physique, l'état d'un calculateur est déterminé par $2(2^n - 1)$ paramètres indépendants. Par exemple, pour $n = 2$, un état générique de 2 qubits d'un calculateur quantique s'écrit

$$\begin{aligned} |\psi\rangle &= c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle \\ &= c_{0,0} |0\rangle |0\rangle + c_{0,1} |0\rangle |1\rangle + c_{1,0} |1\rangle |0\rangle + c_{1,1} |1\rangle |1\rangle \\ &= c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle \end{aligned} \quad (5.1.5)$$

Dans la suite, $i \in \{0, 1\}^n$, i.e., i est une chaîne binaire de taille n , implique que $|i\rangle$ appartient à l'espace de Hilbert à 2^n dimensions $\mathcal{H}^{\otimes n}$.

Pour effectuer un calcul quantique, il faut effectuer les trois étapes de base suivantes (voir la figure 5.1.1) :

- La **préparation** de n qubits dans l'état initial $|\psi_i(t_0)\rangle$ (input state) au temps t_0 . Le vecteur d'état initial est un vecteur de l'espace de Hilbert à 2^n dimensions $\mathcal{H}^{\otimes n}$.
- L'**implémentation** de la transformation unitaire désirée ou souhaitée $U(t, t_0)$ qui agira sur l'état initial en évitant toute interaction avec l'environnement, $|\psi_f(t)\rangle = U(t, t_0) |\psi_i(t_0)\rangle$.

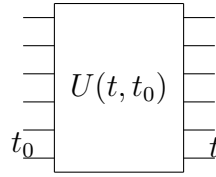


Figure 5.1.1 — Schéma de principe d'un calcul quantique : n qubits sont préparés dans l'état initial $|0\rangle$. Ils subissent une évolution unitaire dans l'espace $\mathcal{H}^{\otimes n}$ de l'instant t_0 à l'instant t , décrite par un opérateur unitaire $U(t, t_0)$ agissant dans $\mathcal{H}^{\otimes n}$. Une mesure des qubits est effectuée au temps t .

- La **mesure** à l'instant t sur les n qubits afin d'obtenir l'état final (output state).

Il est à noter que l'évolution unitaire $U(t, t_0)$ est **réversible** : connaissant le vecteur d'état au temps t , on peut remonter à celui au temps t_0 par $U^-(t, t_0) = U(t_0, t)$.

Un calcul quantique est évolution quantique.

5.2 Circuits quantiques

5.2.1 Énergie - information - réversibilité

L'information, malgré son caractère abstrait est portée par un support physique. Il est donc intéressant de se demander s'**il est possible de calculer sans dissiper de l'énergie**.

Principe 5.2.1 Landauer. *Chaque fois qu'un bit d'information est effacé, la quantité d'énergie dissipée dans l'environnement vaut au moins $k_B T \ln 2$. De façon équivalente, on dit que l'entropie de l'environnement décroît d'au moins de $k_B \ln 2$. k_B est la constante de Boltzmann et T est la température absolue de l'environnement (ordinateur).*

La valeur $k_B T \ln 2$ représente donc la limite inférieure théorique de l'énergie dissipée d'une porte logique irréversible. Cependant, malgré l'énorme réduction de l'énergie dissipée par porte logique tout au long des décennies passées du fait des progrès techniques, les ordinateurs actuels dissipent encore jusqu'à environ $500k_B T$ par bit effacé, en raison de la consommation de l'énergie électrique.

Puisque le principe de Landauer est lié à l'irréversibilité, il est légitime de se poser la question de savoir si les opérations logiques habituelles peuvent être conduites de façon réversible, et donc sans dissipation de l'énergie, afin de transposer au calcul quantique des algorithmes classiques¹.

En effet, toute fonction irréversible $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$ peut être transformée en fonction réversible en définissant une fonction

$$\tilde{f} : \{0, 1\}^{m+n} \rightarrow \{0, 1\}^{m+n} \quad (5.2.1)$$

telle que

$$\tilde{f}(x, y) = (x, y \oplus^n f(x)), \quad (5.2.2)$$

¹La plupart des portes logiques classiques, nous le savons, sont irréversibles car elles correspondent à un passage de 2 bits à 1 bit, et l'état final d'un bit ne permet pas de remonter à l'état initial de deux bits.

où \oplus^n est l'addition modulo 2^n , x représente m bits lors que y et $f(x)$ représentent n bits. Puisque \tilde{f} transforme des entrées distinctes en sorties distinctes, elle est une fonction $(m+n)$ -bits inversible.

En effet, puisque $f(x) \oplus f(x) = 0, \forall f(x)$,

$$(x, y) \mapsto (x, y \oplus f(x)) \mapsto (x, (y \oplus f(x)) \oplus f(x)) = (x, y). \quad (5.2.3)$$

Il est donc possible de trouver une porte logique universelle.

Comme la porte **NAND** et l'opération **COPY** suffisent à construire tous les circuits logiques classiques, la transposition au calcul quantique des algorithmes classiques nécessite le remplacement de l'opérateur **NAND** par une opération réversible et de trouver l'équivalent de l'opérateur **COPY** sans entrer en conflit avec le théorème de non clonage quantique. La solution de ce problème est l'objet de la **Section 5.3**.

5.2.2 Parallélisme quantique

Dans la notation $|x\rangle$, où le nombre x est un des huit nombres (en binaire)

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle, \quad (5.2.4)$$

un registre quantique de taille 3 peut stocker les entiers individuels comme 3 ou 7

$$|0\rangle \otimes |1\rangle \otimes |1\rangle \equiv |011\rangle \equiv |3\rangle, \quad (5.2.5a)$$

$$|1\rangle \otimes |1\rangle \otimes |1\rangle \equiv |111\rangle \equiv |7\rangle, \quad (5.2.5b)$$

mais, aussi les stocker simultanément. On parle alors de **parallélisme quantique**. En effet, si au lieu de prendre le premier single-qubit dans l'état $|0\rangle$ ou $|1\rangle$, on le prend plutôt dans l'état superposé $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, alors

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle) = \frac{1}{\sqrt{2}}(|3\rangle + |7\rangle). \quad (5.2.6)$$

On peut évidemment préparer ce registre de taille 3 dans une superposition d'état des huit entiers, en mettant chaque single-qubit de (5.2.5) dans l'état superposé $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\ &= \frac{1}{\sqrt{2^3}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle) = \frac{1}{\sqrt{2^3}} \sum_{x=0}^{2^3-1} |x\rangle \end{aligned} \quad (5.2.7)$$

Ces préparations, et toutes autres manipulations sur les qubits, doivent être effectués par des opérations unitaires et donc des portes réversibles. L'opération unitaire la plus générale est une transformation dans l'espace de Hilbert de dimension 2^n des n -qubits, $\mathcal{H}^{\otimes n}$, et la porte logique la plus générale est une matrice $2^n \times 2^n$ opérant dans $\mathcal{H}^{\otimes n}$.

On appellera

- **porte logique quantique**, un dispositif qui réalise une opération unitaire fixe sur un qubit donné, pendant une période de temps donnée;

- **réseau ou circuit quantique**, un dispositif constitué de portes logiques quantiques dont les séquences de calculs sont synchronisées dans le temps.
 - La **taille du circuit** est le nombre de portes logiques quantiques qu'il contient.
 - La **largeur du circuit** est le nombre de fils qu'il contient.

Si $f : \{0,1\}^n \mapsto \{0,1\}^m$ est calculable par un circuit réversible de p portes et de largeur w alors il est calculable **proprement** par un circuit réversible de $2p + m$ portes et de largeur $w + m$.

5.2.3 Portes single-qubit

Les opérations sur un single-qubit (1-qubit) sont décrites par des matrices unitaires 2×2 . Les plus utilisées sont les matrices de Pauli, X , Y , Z , la porte de Walsh-Hadamard et la porte Phase-Shift.

Porte de Walsh-Hadamard

La porte de Walsh-Hadamard, ou de Walsh-Hadamard simplement, définie par la matrice

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (5.2.8)$$

permet de transformer les états de base $\{|0\rangle, |1\rangle\}$ en état superposés,

$$W|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad (5.2.9a)$$

$$W|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad (5.2.9b)$$

soit sous forme compacte,

$$W|k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k |1\rangle) = \frac{1}{\sqrt{2}}((-1)^k |k\rangle + |1-k\rangle), \quad k = \{0, 1\}, \quad (5.2.10)$$

ou schématiquement par le diagramme

$$|k\rangle \text{ --- } \boxed{W} \text{ --- } \frac{1}{\sqrt{2}}((-1)^k |k\rangle + |1-k\rangle)$$

Comme $W^2 = \mathbb{I}$, la transformation inverse $W^{-1} = W$. La forme de la matrice (5.2.8) montre que W est hermitien.

Le diagramme ci-dessous représente un circuit quantique de taille 3 qui affecte la transformation de Walsh-Hadamard à 3 single-qubits, $W^{\otimes 3} |0\rangle |0\rangle |0\rangle = W|0\rangle \otimes W|0\rangle \otimes W|0\rangle$:

$$|0\rangle \text{ --- } \boxed{W} \text{ --- } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|0\rangle \text{ --- } \boxed{W} \text{ --- } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \mapsto \frac{1}{\sqrt{2^3}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)$$

$$|0\rangle \text{ --- } \boxed{W} \text{ --- } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Le résultat (*output*) est une superposition de tous les huit entiers, de 0 à 7. Si les 3 single-qubits sont initialement dans un autre état que $|000\rangle$, le résultat de leur transformation par

Walsh-Hadamard est une superposition de tous les huit entiers, de 0 à 7, mais avec la moitié signée positivement. Par exemple,

$$W^{\otimes 3} |101\rangle = \frac{1}{2^{3/2}} (|0\rangle - |1\rangle + |2\rangle - |3\rangle + |4\rangle - |5\rangle + |6\rangle - |7\rangle) \quad (5.2.11)$$

En général, si initialement on a un registre de taille n dans un état $y \in \{0, 1\}^n$, alors

$$W^{\otimes n} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{yx} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{i\pi yx} |x\rangle, \quad (5.2.12)$$

où le produit de $y = (y_0 y_{n-2} \cdots y_1 y_0)$ et de $x = (x_{n-1} x_{n-2} \cdots x_1 x_0)$ est fait bit par bit,

$$yx = (y_0 x_{n-1} + y_{n-2} x_{n-2} + \cdots + y_1 x_1 + y_0 x_0). \quad (5.2.13)$$

Si l'on prend $|0_m\rangle$ comme état initial du registre de résultats, alors

$$U |x \otimes 0_m\rangle = |x \otimes f(x)\rangle. \quad (5.2.14)$$

Si on applique W sur le registre de données dans l'état $|0_n\rangle$ avant U , le vecteur d'état dans l'état final sera par linéarité

$$|\psi_{fin}\rangle = U |(W0_n) \otimes 0_m\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x \otimes f(x)\rangle. \quad (5.2.15)$$

Ce vecteur contient en principe 2^n valeurs de la fonction $f(x)$ obtenu en une seule action de U . Par exemple, si $n = 100$, il contient $\sim 10^{30}$ valeurs de $f(x)$: c'est le miracle du **parallélisme quantique**. Mais une mesure sur $|\psi_{fin}\rangle$ ne donnera qu'une et une seule de ces valeurs. Cependant, on peut extraire des informations utiles sur des relations entre valeurs de $f(x)$ pour un ensemble de valeurs de x différentes, mais bien sûr au prix de la perte de ces valeurs individuelles, alors qu'un ordinateur classique devrait évaluer $f(x)$ 2^n fois pour obtenir la même information. C'est là l'origine de l'accélération exponentielle d'un calcul quantique pour la résolution de certains problèmes.

Remarque 5.2.1 Les rotations de la sphère de Bloch autour d'un axe arbitraire $\hat{\mathbf{u}}$, que nous avons étudiée à la **section 3.3.2** sont une classe importante de transformations unitaires :

$$R_{\hat{\mathbf{u}}}(\delta) = e^{-i\frac{\delta}{2}(\hat{\mathbf{u}} \cdot \boldsymbol{\sigma})} = \mathbb{I} \cos \frac{\delta}{2} - (\hat{\mathbf{u}} \cdot \boldsymbol{\sigma}) i \sin \frac{\delta}{2}. \quad (5.2.16)$$

On note que la porte de **Walsh-Hadamard** est une opération de rotation d'angle $\delta = \pi$ autour de l'axe $\hat{\mathbf{u}}' = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$. En effet,

$$W = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = -iR_{\mathbf{u}'}(\pi). \quad (5.2.17)$$

Remarque 5.2.2 L'application de la porte W à un 1-qubit arbitraire $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ est un exemple de l'**interférence quantique** qui se manifeste mathématiquement par l'addition des amplitudes de probabilités. En effet,

$$W|\psi\rangle = \frac{\alpha + \beta}{2}|0\rangle + \frac{\alpha - \beta}{2}|1\rangle. \quad (5.2.18)$$

- La probabilité d'obtenir $|0\rangle$ après une mesure a augmentée par **interférence constructive** :

$$\alpha \rightarrow \frac{\alpha + \beta}{2} \quad (5.2.19)$$

- La probabilité d'obtenir $|1\rangle$ après une mesure a diminuée par **interférence destructive** :

$$\alpha \rightarrow \frac{\alpha - \beta}{2} \quad (5.2.20)$$

Si par exemple $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$, $x \in \{0, 1\}$,

$$|\psi\rangle = \frac{1 + (-1)^x}{2} |0\rangle + \frac{1 - (-1)^x}{2} |1\rangle. \quad (5.2.21)$$

Pour $x = 0$, on a

$$W\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle. \quad (5.2.22)$$

Ainsi, par interférence constructive, la mesure de $|0\rangle$ est certaine. Alors que par interférence destructive, on a aucune chance de trouver $|1\rangle$ la mesure.

Exercice 5.2.1 En utilisant $W = \frac{1}{\sqrt{2}}(X + Z)$ et les propriétés des matrices de Pauli, montrer que $W^2 = \mathbb{I}$, $WXW = Z$ et $WZW = X$.

Porte Phase-Shift

La **porte Phase-Shift** définie par la matrice

$$R_z(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}, \quad (5.2.23)$$

et symboliquement représentée par le diagramme de la figure 5.2.1, laisse inchangée l'état de base $|0\rangle$ et change la phase globale de l'état $|1\rangle$, $e^{i\delta} |1\rangle$.

$$|k\rangle \text{ --- } \boxed{R_z(\delta)} \text{ --- } e^{ik\delta} |k\rangle$$

Figure 5.2.1 – Représentation schématique de l'action de la porte **Phase-Shift** sur un single-qubit dans l'état $|k\rangle$, $k = \{0, 1\}$.

$$|0\rangle \text{ --- } \boxed{W} \text{ --- } \boxed{R_z(\theta)} \text{ --- } \boxed{W} \text{ --- } \boxed{R_z(\frac{\pi}{2} + \varphi)} \text{ --- } |\psi\rangle$$

Figure 5.2.2 – Construction du single-qubit générique $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$ à partir single-qubit $|0\rangle$.

La porte de **Walsh-Hadamard** et la porte **Phase-Shift** peuvent être combinées pour construire le circuit de taille 4 de la figure 5.2.2, qui génère, au facteur de phase globale $e^{i\frac{\theta}{2}}$ près, le single-qubit générique

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle. \quad (5.2.24)$$

Ce circuit quantique s'écrit vectoriellement sous la forme²

$$R_z(\frac{\pi}{2} + \varphi)WR_z(\theta)W|0\rangle = e^{i\frac{\theta}{2}}(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle). \quad (5.2.25)$$

²Le diagramme se lit de gauche à droite alors que le produit d'opérateurs se lit de droite à gauche.

Conséquemment, la porte de *Walsh-Hadamard* et la porte *Phase-Shift* suffisent pour construire **toute** opération unitaire sur un single-qubit.

Et d'une manière générale, ces deux portes peuvent être utilisées pour transformer l'état initial $|0_1\rangle |0_2\rangle \dots |0_n\rangle$ d'un registre de n qubits en n'importe quel état de type $|\psi_1\rangle |\psi_2\rangle \dots |\psi_n\rangle$, où $|\psi_i\rangle$ est un état superposé arbitraire de $|0\rangle$ et $|1\rangle$. Ce sont ces états n -qubits qu'on appelle **états produit tensoriel ou état séparables**.

Le tableau (5.2.1) présente les portes unitaires single-qubit les plus usuelles.

Nom	Diagramme	Matrice dans $\{ 0\rangle, 1\rangle\}$
Walsh-Hadamard W	$ k\rangle \text{ --- } \boxed{W} \text{ --- } \frac{1}{\sqrt{2}}((-1)^k k\rangle + 1-k\rangle)$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli X	$ k\rangle \text{ --- } \boxed{X} \text{ --- } 1-k\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	$ k\rangle \text{ --- } \boxed{Y} \text{ --- } i(-1)^k 1-k\rangle$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	$ k\rangle \text{ --- } \boxed{Z} \text{ --- } (-1)^k k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase	$ k\rangle \text{ --- } \boxed{S} \text{ --- } (i)^k k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Phase-Shift	$ k\rangle \text{ --- } \boxed{R_z(\delta)} \text{ --- } e^{ik\delta} k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{ik\delta} \end{pmatrix}$

Table 5.2.1 – Représentation symbolique et matricielle des portes unitaires les plus usuelles.

Exercice 5.2.2 On considère les états $|0\rangle$ et $|1\rangle$ orthonormés, élément de l'espace de Hilbert \mathcal{H} .

1. On appelle opérateur de **Hubbard**, les opérateurs X^{ik} ($i, k = 1, 2$) dont les matrices sont carrées et ont un élément de matrice unité à l'intersection de la i -ième ligne et de la k -ième colonne. Les autres éléments de matrices sont nuls. En notation de Dirac,

$$X^{ik} = |i-1\rangle \langle k-1|. \quad (5.2.26)$$

- (a) Écrire en notation de Dirac les quatre opérateurs X^{ik} et donner leur forme matricielle.
- (b) Évaluer $X^{12}|1\rangle$ et $X^{21}|0\rangle$ et conclure.
- (c) Donner l'expression générale de la multiplication de deux opérateurs X^{ik} , $X^{ik}X^{mn}$.

2. On définit l'opérateur porte logique **NOT** par

$$\text{NOT} = X^{12} + X^{21}. \quad (5.2.27)$$

- (a) Exprimer **NOT** en notation de Dirac et sous forme matricielle.
- (b) Vérifier que **NOT** est un opérateur hermitien et unitaire.
- (c) Évaluer $\text{NOT}|1\rangle$ et $\text{NOT}|0\rangle$ et conclure.
- (d) Soit un système représenté par le qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ avec } |\alpha|^2 + |\beta|^2 = 1. \quad (5.2.28)$$

Que représente $|\alpha|^2$ et $|\beta|^2$ avant et après l'action de l'opérateur porte logique **NOT** ?

5.2.4 Portes de contrôle et génération de l'intrication

En général, un registre de taille $n > 1$ peut être préparé dans des **états intriqués ou non séparables**. On rappelle que, par exemple pour $n = 2$, l'état

$$\alpha |00\rangle + \beta |01\rangle = |0\rangle \otimes (\alpha |0\rangle + \beta |1\rangle), \quad (5.2.29)$$

est séparable, en $|\psi_1\rangle = |0\rangle$ et $|\psi_2\rangle = \alpha |0\rangle + \beta |1\rangle$. Par contre, l'état

$$\alpha |00\rangle + \beta |11\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle, \quad (5.2.30)$$

est intriqué ($\alpha, \beta \neq 0$).

Afin d'intriquer au moins deux qubits, il nous faut étendre notre répertoire de portes logiques quantiques aux portes logiques 2-qubits qui réalise une dynamique conditionnelle. Ces portes sont des **portes de contrôle** U qui traduisent quantiquement **if (x) then y := Ux** par

$$|x\rangle |y\rangle \mapsto |x\rangle U^x |y\rangle, \quad (5.2.31)$$

qui correspond, pour $x, y \in \{0, 1\}$, à

$$|0\rangle |0\rangle \rightarrow |0\rangle |0\rangle \quad (5.2.32a)$$

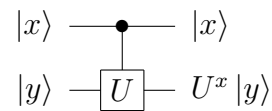
$$|0\rangle |1\rangle \rightarrow |0\rangle |1\rangle \quad (5.2.32b)$$

$$|1\rangle |0\rangle \rightarrow |1\rangle U |0\rangle \quad (5.2.32c)$$

$$|1\rangle |1\rangle \rightarrow |1\rangle U |1\rangle \quad (5.2.32d)$$

Usuellement, on l'appelle porte **Controlled-U** ou **CU** et on la représente sous formes de décomposition spectrale et matricielle, dans la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, par

$$|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U = \begin{pmatrix} \mathbb{I} & \mathbb{O} \\ \mathbb{O} & U \end{pmatrix}$$



Porte **CU**

où \mathbb{I} , \mathbb{O} et U sont des matrices 2×2 .

Le premier bit $|x\rangle$ agit comme **contrôle** et sa valeur reste inchangée à la sortie. Le second bit $|y\rangle$ est appelé **cible**. Sur le diagramme, le contrôle est représenté le point noir.

*Une porte **CU** applique la transformation identité \mathbb{I} au bit cible lorsque le bit de contrôle est dans l'état $|0\rangle$. Elle applique la transformation U au bit cible lorsque le bit de contrôle est dans l'état $|1\rangle$.*

Puisque pour $x \in \{0, 1\}$, $U^{2x} = \mathbb{I}$ et les opérateurs **CU** sont unitaires.

Pour une transformation unitaire quelconque $U : (x, y) \rightarrow (x, y \oplus f(x))$, on a

$$|\psi\rangle = \mathbf{CU}(\alpha |0\rangle + \beta |1\rangle) |0\rangle = \alpha |0f(0)\rangle + \beta |1f(1)\rangle, \quad (5.2.33)$$

qui contient **à la fois** l'information sur $f(0)$ et sur $f(1)$.

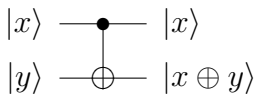
Porte **CNOT**

La plus populaire des portes **CU** est la porte **CNOT** ou **CX** qui opère la transformation décrite par

$$\mathbf{CNOT} = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \mathbf{X} = \begin{pmatrix} \mathbb{I} & \mathbb{O} \\ \mathbb{O} & \mathbf{X} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (5.2.34)$$

autrement qui inverse le bit cible $|y\rangle$ lorsque le bit de contrôle $|x\rangle$ est dans l'état $|1\rangle$. On l'a résumé par

$$\text{CNOT } |x\rangle |y\rangle = |x\rangle |x \oplus y\rangle, \quad x, y \in \{0, 1\},$$



x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Porte **CNOT**

On note sur la table de vérité que lorsque la cible est dans l'état $|1\rangle$, la porte **CNOT** devient la porte **COPY** :

$$|x\rangle |0\rangle \mapsto |x\rangle |x\rangle, \quad x \in \{0, 1\}. \quad (5.2.35)$$

Par conséquent,

$$\text{CNOT}(\alpha |0\rangle + \beta |1\rangle) |0\rangle = \alpha |00\rangle + \beta |11\rangle, \quad (5.2.36)$$

qui est non factorisable pour $\alpha, \beta \neq 0$. Donc, la porte **CNOT** génère des états intriqués.

On peut penser que cette porte pourrait aussi être utilisée pour copier un état superposé comme $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, si bien que

$$|\psi\rangle |0\rangle \mapsto |\psi\rangle |\psi\rangle. \quad (5.2.37)$$

Ceci n'est pas possible en vertu du théorème du non-clonage.

Théorème 5.2.1 Toute opération unitaire sur $\mathcal{H}^{\otimes n}$ peut se décomposer en produit d'opérations unitaires single qubit (1-qubit) et de **CNOT**.

Exercice 5.2.3 Implémenter, en utilisant QuTiP, la porte logique quantique CX .

Exercice 5.2.4 The most general separable state of the two qubits can be written, up to an overall phase, as

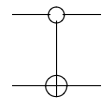
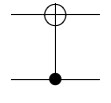
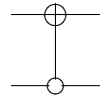
$$|\psi\rangle = a(|0\rangle + b_1 e^{i\varphi_1} |1\rangle) \otimes (|0\rangle + b_0 e^{i\varphi_0} |1\rangle), \quad (5.2.38)$$

where a is set to the completeness. What conditions should the real coefficients b_0, b_1, φ_0 and φ_1 satisfy in order that **CNOT** $|\psi\rangle$ be entangled?

Remarque 5.2.3 Il est possible de définir une porte **CNOT** généralisée, dépendante du fait que

- le bit de contrôle est le premier ou le second qubit,
- ou encore que la porte agit trivialement³ quand le bit de contrôle est $|0\rangle$ ou $\beta |1\rangle$.

Ainsi, les trois autres matrices **CNOT**, leurs représentations symboliques et actions sont :

$B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	$D = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
		
B inverse le 2 ^e qubit lorsque le 1 ^{er} est dans l'état $ 0\rangle$	C inverse le 1 ^{er} qubit lorsque le 2 ^e est dans l'état $ 1\rangle$	D inverse le 1 ^{er} qubit lorsque le 2 ^e est dans l'état $ 1\rangle$

³L'action de la porte se réduit à l'identité.

Base de Bell

Comme vu à la **Section 5.2.4**, la porte **CNOT** peut générer l'intrication, et en particulier les états intriqués de la base de Bell, définis par 4.3.14,

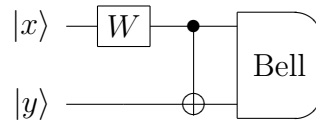
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (5.2.39a)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (5.2.39b)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (5.2.39c)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (5.2.39d)$$

peuvent être obtenus de la base de calcul $\{|0\rangle, |1\rangle\}$ à travers le circuit



Il est facile de vérifier que ce circuit produit les transformations

$$|00\rangle \rightarrow |\Phi^+\rangle; |10\rangle \rightarrow |\Phi^-\rangle; |01\rangle \rightarrow |\psi^+\rangle; |11\rangle \rightarrow |\psi^-\rangle. \quad (5.2.40)$$

On note que cette transformation peut être inversée simplement en exécutant le circuit de la droite vers la gauche, puisque les portes **CNOT** et de **Walsh-Hadamard** sont inversibles. Par conséquent, tout état de la base de Bell est transformé en état factorisable. Et il est donc possible, via une mesure standard dans la base de calcul, d'établir laquelle des quatre états de base de Bell était présente au début.

Porte Controlled Phase-Shift

La deuxième porte CU usuelle est la porte **Controlled Phase-Shift** définie, dans la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, par

$$\text{CPS}(\delta) = \begin{pmatrix} \mathbb{I} & \mathbb{O} \\ \mathbb{O} & R_z(\delta) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{pmatrix}$$

Porte CPS

Elle applique la phase global $e^{i\delta}$ lorsque le qubit de contrôle $|y\rangle$ est dans l'état $|1\rangle$, $\text{CPS}|11\rangle = e^{i\delta}|11\rangle$. La porte **Controlled Phase-Shift** n'a pas d'analogue classique.

Exercice 5.2.5 1. Find the action of the CW gate using (5.2.31) when the input state are $|01\rangle$ and $|11\rangle$.

2. Give the matrix representation and the Dirac notation representation of CW.

Solution 5.2.1 1. From (5.2.31) is this easy to obtain

$$\text{CW}|01\rangle = |0\rangle W^0|1\rangle = |0\rangle|1\rangle = |01\rangle, \quad (5.2.41a)$$

$$\text{CW}|11\rangle = |1\rangle W^1|1\rangle = |1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle). \quad (5.2.41b)$$

2. The matrix representation and the Dirac notation representation are respectively

$$C_W = \begin{pmatrix} \mathbb{I} & \mathbb{O} \\ \mathbb{O} & W \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \quad (5.2.42a)$$

$$C_W = |00\rangle\langle 00| + |01\rangle\langle 01| + \frac{1}{\sqrt{2}}(|10\rangle\langle 10| + |10\rangle\langle 11| + |11\rangle\langle 10| - |11\rangle\langle 11|). \quad (5.2.42b)$$

Remarque 5.2.4 La porte **CZ** ou **CMINUS** est définie par $CPS(\pi) = CZ$, soit

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \begin{array}{ccc} |x\rangle & \text{---} & |x\rangle \\ |y\rangle & \text{---} [W] \text{---} [X] \text{---} [W] \text{---} & (-1)^{xy} |y\rangle \end{array}$$

Porte **CZ**

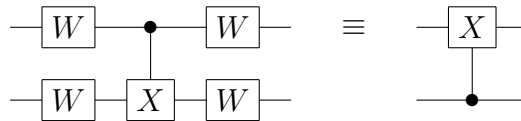
Cette porte est importante en ce sens qu'elle est plus facile à implémenter que la porte **CX**. Comme $CZ^{-1} = CZ$, l'action de **CZ** ne dépend pas de quel qubit est la cible ou le contrôle.

On a les relations suivantes entre **CX** et **CZ**

$$CZ = (\mathbb{I} \otimes W)CX(\mathbb{I} \otimes W) \quad (5.2.43a)$$

$$CX = (\mathbb{I} \otimes W)CZ(\mathbb{I} \otimes W) \quad (5.2.43b)$$

Exercice 5.2.6 Montrer que l'équivalence suivante :



Remarque 5.2.5 Nous utiliserons une notation abrégée pour exprimer les opérateurs agissant sur un ou plusieurs qubits d'un registre à n qubits.

- Si U agit sur $\mathcal{H}^{\otimes 2}$, alors $U_{[i]} = \mathbb{I}^{\otimes i-1} \otimes U \otimes \mathbb{I}^{\otimes n-i}$.
- Si U agit sur $\mathcal{H}^{\otimes 2} \otimes \mathcal{H}^{\otimes 2}$ alors $U_{[i,j]}$ agit dans l'ordre sur les qubits i et j sans toucher les autres qubits. Par exemple, $CNOT_{[2,1]} |x\rangle |y\rangle = |x \oplus y\rangle |y\rangle$.

Cette définition peut se généraliser à un nombre arbitraire de qubits.

5.3 Portes quantiques universelles

L'intérêt de ces portes universelles est de faciliter l'intégration à partir de portes pré-caractérisées.

Nous savons déjà que n'importe quelle fonction peut être synthétisée à l'aide de :

- porte **NAND**, constantes 0 et 1 dans le cas classique,
- porte **CNOT**, portes **single-qubit** ($W, R_u(\delta)$) dans le cas quantique. On dit que (**CNOT**, $W, R_u(\delta)$) forme un ensemble *infini* de portes quantiques universelles.

Il existe cependant d'autres ensembles de portes quantiques universelles.

5.3.1 Porte CV

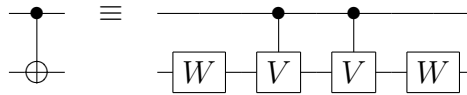
Proposition 5.3.1 *Toute porte quantique qui peut intriquer deux qubits peut être utilisée comme porte quantique universelle. Mathématiquement, un choix élégant consiste en une paire de portes de **Walsh-Hadamard** et des portes **CV**, où **V** est la matrice*

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \equiv R_z\left(\frac{\pi}{2}\right). \quad (5.3.1)$$

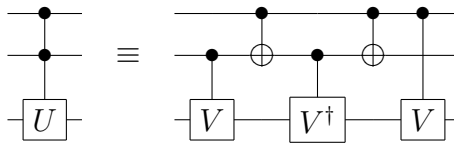
Ces deux portes forment un ensemble fini de portes quantiques universelles. Les circuits quantiques contenant alors un nombre fini des portes **W** et **CV** peuvent implémenter toute transformation unitaire sur $n \geq 2$ qubits.

Lorsqu'on applique quatre fois **CV**, on obtient l'identité, ainsi trois applications consécutives de **CV** donne l'inverse de **CV** ou V^\dagger .

On construit une porte **CNOT** à partir des portes **W** et **CV** de la manière suivante :



On montre que toute matrice 2×2 unitaire U , telle que $U = V^2$, peut être simulée par le circuit



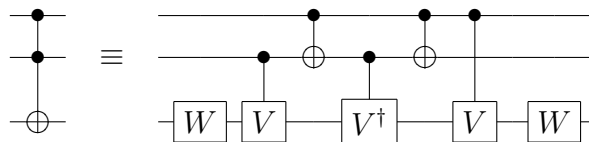
Construction de Sleator-Weinfurter

Il est noter que

$$CCU|xyz\rangle = |xy\rangle U^{xy}|z\rangle. \quad (5.3.2)$$

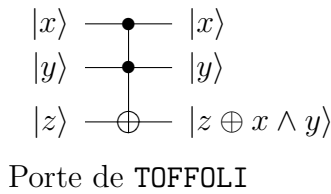
5.3.2 Porte de TOFFOLI

Les portes **W** et **CV** permettent aussi de construire une porte fort utile, à trois bits d'entrée et de sortie, appelée de **TOFFOLI** ou porte **Controlled-Controlled-NOT** (**CCNOT**, **C²NOT**).



Implémentation de la porte de **TOFFOLI**

Cette porte, dont les deux bits de contrôle x et y restent inchangés alors que le bit cible z est inversé lorsque les deux bits de contrôle sont à 1, c'est-à-dire $z' = z \oplus xy$, est représentée par la table de vérité suivante :



N°	x	y	z	x	y	$z \oplus x \wedge y$
1	0	0	0	0	0	0
2	0	0	1	0	0	1
3	0	1	0	0	1	0
4	0	1	1	0	1	1
5	1	0	0	1	0	0
6	1	0	1	1	0	1
7	1	1	0	1	1	1
8	1	1	1	1	1	0

La porte **CCNOT** nous donne la connectivité logique nécessaire à l'arithmétique.

- Lorsque le qubit cible $|z\rangle$ est dans l'état $|0\rangle$ (lignes 1, 3, 5, 7), la porte de **CCNOT** effectue l'opération **AND**

$$\text{CCNOT } |x\rangle |y\rangle |0\rangle = |x\rangle |y\rangle |x \wedge y\rangle. \quad (5.3.3)$$

- Lorsque le qubit cible $|z\rangle$ est dans l'état $|1\rangle$ (lignes 2, 4, 6, 7), la porte de **CCNOT** effectue l'opération **NAND**

$$\text{CCNOT } |x\rangle |y\rangle |1\rangle = |x\rangle |y\rangle |x \bar{\wedge} y\rangle. \quad (5.3.4)$$

- Lorsque le premier qubit de contrôle $|x\rangle$ est dans l'état $|1\rangle$ (lignes 5-8), la porte de **CCNOT** effectue l'opération **CNOT**

$$\text{CCNOT } |1\rangle |y\rangle |z\rangle = |1\rangle |y\rangle |z \oplus y\rangle. \quad (5.3.5)$$

- Lorsque le premier qubit de contrôle $|x\rangle$ est dans l'état $|1\rangle$ et le qubit cible $|z\rangle$ est dans l'état $|0\rangle$ (lignes 5 et 7), la porte de **CCNOT** effectue l'opération **COPY**

$$\text{CCNOT } |1\rangle |y\rangle |0\rangle = |1\rangle |y\rangle |y\rangle. \quad (5.3.6)$$

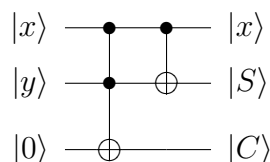
Ainsi donc, avec la porte de **CCNOT**, on peut reproduire de façon réversible tous les circuits logiques classiques.

*La porte de **CCNOT** est une porte universelle pour toutes les opérations réversibles de la logique booléenne.*

De ce qui précède, il apparaît que les portes logiques irréversibles comme **AND** et **OR** peuvent être transformées en portes réversibles. Cependant, le prix à payer est la production d'un bit ou de plusieurs **bits résiduels** qui ne peuvent être re-utilisés pour le calcul. Ils sont plutôt utiles pour le stockage de l'information à des fins de réversibilité. Par exemple, lorsque dans la porte **CCNOT** $z = 1$, on a $z' = x \wedge y$ et deux bits résiduels, $x' = x$ et $y' = y$. On peut penser que de l'énergie est nécessaire pour effacer ces résiduels et annuler l'effet avantageux de la réversibilité. Ce n'est point le cas puisque d'après Bennett, on peut effectuer le calcul ou l'opération voulu, imprimer le résultat et ensuite faire l'opération inverse, en utilisant à nouveau les portes logiques, afin de retrouver l'état initial du calculateur. Conséquemment, les bits résiduels reviennent à leur état initial sans dépense d'énergie.

Exercice 5.3.1 *Construct the **NOT** and **OR** gates from **CCNOT** gate.*

Exercice 5.3.2 Additionneur quantique. *Donner les expressions et les tables de vérité de S et C du circuit suivant :*



5.3.3 Résumé

On retient que

- Pour toute rotation U à un qubit, l'opération CU peut être décomposée en portes single-qubit et une porte $CNOT$;
- La porte $CCNOT$ peut être implémentée en utilisant les portes $CNOT$ et de *Walsh-Hadamard*;
- Toute porte C^k-U , $k > 2$, peut être décomposée en portes de $CCNOT$ et en portes CU ;
- Une opération unitaire générique $U^{(n)}$ agissant dans l'espace $\mathcal{H}^{\otimes n}$ peut être décomposée au moyen des portes C^k-U .

De façon réductrice, on peut dire qu'il suffit de savoir réaliser les rotations single-qubits et des $CNOT$ pour fabriquer le calculateur quantique !

Mais pourquoi donc est-ce si difficile ? Parce que

- Il faut pouvoir agir sur chaque qubit séparément des autres ;
- Il faut pouvoir intriquer n'importe quelle paire de qubits ;
- Chaque opération doit être très précise ;
- Le calcul doit être effectué rapidement (*décohérence*).

5.3.4 Évaluation quantique d'une fonction

Pour évaluer une fonction $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$, on a besoin d'au moins deux registres. Le premier, le registre de données (*input register*) de taille n pour stocker les arguments x de la fonction f , le second, le registre de résultat (*output register*) de taille m pour stocker les valeurs de $f(x)$. La fonction d'évaluation est une évolution unitaire des deux registres,

$$|x, y\rangle \mapsto |x, (y + f(x)) \bmod 2^m\rangle, \quad y \in \{0, 1\}^m. \quad (5.3.7)$$

Par exemple, le circuit calculant la fonction

$$\begin{aligned} f : \{0, 1\}^2 &\rightarrow \{0, 1\}^3 \\ x &\rightarrow f(x) = x^2 \end{aligned} \quad (5.3.8)$$

agit ainsi qu'il suit

$$\begin{aligned} |00\rangle |000\rangle &\mapsto |00\rangle |000\rangle & |10\rangle |000\rangle &\mapsto |01\rangle |100\rangle \\ |01\rangle |000\rangle &\mapsto |01\rangle |001\rangle & |11\rangle |000\rangle &\mapsto |11\rangle |001\rangle \end{aligned} \quad (5.3.9)$$

On peut l'écrire sous la forme

$$|x, 0\rangle \mapsto |x, x^2 \bmod 2^3\rangle. \quad (5.3.10)$$

Comme $3^2 \bmod 2^3 = 1$, on écrit $|11\rangle |000\rangle \mapsto |11\rangle |001\rangle$.

En réalité, pour ce genre d'opérations, on a aussi besoin d'un troisième registre qui stocke initialement dans l'input des qubits à l'état zéro et retourne des qubits à l'état zéro dans l'output, mais qui ont des valeurs non-nulles durant le calcul.

Ce qui rend intéressant l'évaluation quantique d'une fonction est son action sur la superposition d'état des différents inputs x . Par exemple,

$$\sum_x |x, 0\rangle \mapsto \sum_x |x, f(x)\rangle, \quad (5.3.11)$$

produit $f(x)$ pour x dans un cycle. Le bémol est que nous ne pouvons les avoir toutes dans l'état intriqué $\sum_x |x, f(x)\rangle$ puisque tout bit obtenu par mesure sur le premier registre donnera une valeur particulière $x' \in \{0, 1\}^n$ et le deuxième registre se trouvera donc avec la valeur $f(x') \in \{0, 1\}^m$.

5.4 Algorithme de Deutsch-Jozsa

L'**algorithme de Deutsch-Jozsa** est un algorithme quantique, proposé par David Deutsch et Richard Jozsa en 1992 avec des améliorations de R. Cleve *et al.* en 1998⁴. *Bien qu'il ne soit pas d'un grand intérêt pratique, il s'agit d'un des premiers algorithmes quantiques qui est plus efficace qu'un algorithme classique.*

5.4.1 Problème et solution classique

Dans le cas du problème de Deutsch-Jozsa, nous disposons d'une *boîte noire quantique*, connu sous le nom d'**oracle**, qui implémente une fonction mathématique $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Nous savons que cette fonction est soit *constante* ($f(0) = f(1) = 0$ ou $f(0) = f(1) = 1$) soit *équilibrée* ($f(0) = 0, f(1) = 1$ et $f(0) = 1, f(1) = 0$). Le but du problème est de savoir si la fonction est constante ou équilibrée par invocation de l'oracle.

- Si un algorithme *classique et déterministe* est utilisé, il faut $2^{n-1} + 1$ évaluation de la fonction mathématique f dans le pire des cas pour trouver la solution.
- Dans le cas de l'utilisation d'un algorithme *probabiliste*, un nombre constant d'évaluation est suffisant pour trouver la bonne réponse avec une forte probabilité, néanmoins $2^{n-1} + 1$ évaluation sont toujours nécessaire pour que la réponse soit toujours correcte.

L'algorithme quantique de Deutsch-Jozsa permet de trouver une réponse toujours correcte avec une seule évaluation de f .

5.4.2 Algorithme quantique de Deutsch-Jozsa

Le but est de tester la parité de la fonction $f : \{0, 1\} \rightarrow \{0, 1\}$ ou la condition $f(0) = f(1)$, ce qui équivaut à vérifier $f(0) \oplus f(1)$. Si cela vaut zéro alors f est constante, sinon f est équilibrée. Le circuit implémentant cet algorithme est donné par la figure 5.4.1.

1. L'algorithme commence avec deux qubit dans l'état $|0\rangle|1\rangle$.

⁴R. Cleve, A. Ekert, C. Macchiavello, et M. Mosca, *Quantum algorithms revisited*, *Proceedings of the Royal Society of London A*, vol. 454, 1998, p. 339-354

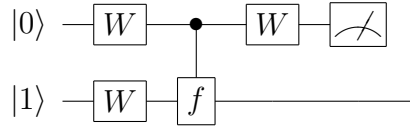


Figure 5.4.1 – *Algorithme quantique de Deutsch-Jozsa avec un 1-qubit en entrée.*

2. Une transformation de Walsh-Hadamard est d'abord appliquée à chaque qubit. Cela donne

$$W |0\rangle W |1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle). \quad (5.4.1)$$

3. Une implémentation quantique (oracle) de la fonction f permet de passer de $|x\rangle |y\rangle$ à $|x\rangle |y \oplus f(x)\rangle$, i.e., le second qubit est inversé si et seulement si $f(x) = 1$. Soit pour $x \in \{0, 1\}$,

$$U_f |x\rangle (|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle), \quad (5.4.2)$$

où le facteur $(-1)^{f(x)}$ s'est retropropagé (*kicked back*) devant le premier qubit. Ainsi, l'évaluation de la fonction nous donne

$$\begin{aligned} & \frac{1}{2} [(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle] (|0\rangle - |1\rangle) \\ &= (-1)^{f(0)} \frac{1}{2} (|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle) (|0\rangle - |1\rangle). \end{aligned} \quad (5.4.3)$$

Le second qubit n'est plus utile, de même que le facteur de phase global, on peut donc les ignorer. On a alors l'état

$$\frac{1}{\sqrt{2}} (|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle). \quad (5.4.4)$$

4. En appliquant une transformation de Walsh-Hadamard à cet état, on a

$$\begin{aligned} & \frac{1}{2} (|0\rangle + |1\rangle + (-1)^{f(0) \oplus f(1)} |0\rangle - (-1)^{f(0) \oplus f(1)} |1\rangle) \\ &= \frac{1}{2} ([1 + (-1)^{f(0) \oplus f(1)}] |0\rangle + [1 - (-1)^{f(0) \oplus f(1)}] |1\rangle). \end{aligned} \quad (5.4.5)$$

$f(0) \oplus f(1) = 0$, i.e., $f(0) = f(1)$ si et seulement si on observe $|0\rangle$.

5. Donc, l'état final du premier qubit est $|f(0) \oplus f(1)\rangle$ et la fonction est constante si et seulement si on mesure $|0\rangle$.

Comme on le constate, la parité de la fonction $f(x)$ a été encodé par un 1-qubit après une seule invocation de f . Ceci parce qu'un calculateur quantique peut évaluer simultanément $f(0)$ et $f(1)$. Les deux chemins alternatifs ou complémentaires sont recombinaés par la dernière porte de **Walsh-Hadamard**. L'interférence est constructive pour l'une des valeurs de $f(0) \oplus f(1)$ et destructive pour la valeur alternative.

Dans le cas général, on a $n + 1$ bit dans l'état $|0\rangle^{\otimes n} |1\rangle$ et la figure 5.4.2 représente l'implémentation de l'algorithme de Deutsch-Jozsa correspondant.

Les premiers n bits sont tous dans l'état $|0\rangle$ et les derniers bit dans l'état $|1\rangle$. Nous appliquons ensuite la transformation de Walsh-Hadamard à chaque qubit, pour obtenir

$$|\psi_1\rangle = W^{\otimes n} |0\rangle^{\otimes n} \otimes W |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^{\otimes n}} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (5.4.6)$$

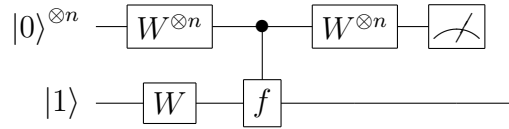


Figure 5.4.2 – Algorithme quantique de Deutsch-Jozsa avec un n -qubit entrée.

Après l'oracle, le système est dans l'état

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (5.4.7)$$

Comme l'application de W sur le n -qubit $|x\rangle$ donne

$$W^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y} |y\rangle, \quad (5.4.8)$$

on a à la sortie du circuit

$$|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x \sum_y (-1)^{x \cdot y + f(x)} |y\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \quad (5.4.9)$$

Les résultats possibles de la mesure sur $|y\rangle$ donnent

- seulement la valeur 0 et dans ce cas la fonction $f(x)$ est constante,
- au moins une valeur 1 et dans ce cas la fonction $f(x)$ est équilibrée.

Exercice 5.4.1 1. On considère une fonction à 2-qubit telle que $f(x) = 1$. Montrer explicitement que la sortie de l'algorithme de Deutsch-Jozsa donne $|y\rangle = |00\rangle$.

2. On suppose que $f(00) = f(10) = 0$ et $f(01) = f(11) = 1$. Montrer explicitement que des deux bits de la sortie y de l'algorithme de Deutsch-Jozsa au moins un à la valeur 1.

5.5 Transformation de Fourier quantique

La **transformation de Fourier discrète** d'un vecteur avec N composantes complexes $\{f(0), f(1), \dots, f(N-1)\}$ est un nouveau vecteur complexe $\{\tilde{f}(0), \tilde{f}(1), \dots, \tilde{f}(N-1)\}$, défini par

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2i\pi \frac{xy}{N}} f(x). \quad (5.5.1)$$

La transformation de Fourier quantique (**QFT, Quantum Fourier Transform**) fait exactement la même chose. Elle est définie sur un registre de n qubits ($N = 2^n$) comme une opération unitaire F_N dont l'action sur les états de la base de calcul est

$$F_N |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2i\pi \frac{xy}{N}} |y\rangle, \quad (5.5.2a)$$

ou

$$F_N = \frac{1}{\sqrt{N}} \sum_{x,y=0}^{N-1} |y\rangle e^{2i\pi \frac{xy}{N}} \langle x|. \quad (5.5.2b)$$

Par conséquent, un état arbitraire $|\psi\rangle = \sum_x f(x) |x\rangle$ est transformé en

$$|\tilde{\psi}\rangle = \sum_{k=0}^{N-1} \tilde{f}(y) |y\rangle, \quad (5.5.3)$$

où les coefficients $\{\tilde{f}(y)\}$ sont les transformées de Fourier discrètes des coefficients $\{f(y)\}$, en vertu de (5.5.1).

On vérifie facilement que F_N est unitaire. En effet,

$$F_N^\dagger F_N = \left(\frac{1}{\sqrt{N}} \sum_{y,x=0}^{N-1} |x\rangle e^{-2i\pi \frac{xy}{N}} \langle y| \right) \left(\frac{1}{\sqrt{N}} \sum_{y,x=0}^{N-1} |y\rangle e^{2i\pi \frac{xy}{N}} \langle x| \right) \quad (5.5.4a)$$

$$= \frac{1}{N} \sum_{y,x=0}^{N-1} \left(\sum_{y,x=0}^{N-1} |x\rangle e^{-2i\pi \frac{xy}{N}} \langle y| y \rangle e^{2i\pi \frac{xy}{N}} \langle x| \right) \quad (5.5.4b)$$

$$= \frac{1}{N} \sum_{x=0}^{N-1} \left(\sum_{x=0}^{N-1} |x\rangle \langle x| \right) = \mathbb{I} \quad (5.5.4c)$$

Exercice 5.5.1 Montrer que

$$F_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \quad (5.5.5)$$

Si on pose $\omega_N = e^{\frac{2i\pi}{N}}$,

$$F_N = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N & \omega_N^2 & \dots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \dots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \dots & \omega_N^{(N-1)(N-1)} \end{pmatrix}. \quad (5.5.6)$$

Utilisons maintenant une technique standard des transformées de Fourier rapides (**FFF** ou **Fast Fourier Transform**) pour montrer que la QFT ne génère pas d'intrication entre les qubits sur lesquels elle agit.

Adoptons la représentation binaire pour écrire x et y ,

$$x = x_{n-1}x_{n-2} \dots x_1x_0 = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \dots + x_12^1 + x_02^0, \quad (5.5.7a)$$

$$y = y_{n-1}y_{n-2} \dots y_1y_0 = y_{n-1}2^{n-1} + y_{n-2}2^{n-2} + \dots + y_12^1 + y_02^0. \quad (5.5.7b)$$

En vertu de ce que $\omega_N = e^{\frac{2i\pi}{N}}$ est une racine N-ième de l'unité, on peut ignorer dans le produit xy de l'exponentielle de (5.5.2), tous les termes divisibles par $N = 2^n$ puisqu'il ne contribuent pas à l'exponentielle⁵. Ainsi,

$$\frac{xy}{2^n} = y_{n-1}(.x_0) + y_{n-2}(.x_1x_0) + \dots + y_0(.x_{n-1}x_{n-2} \dots x_1x_0). \quad (5.5.8)$$

⁵Si $xy = aN + b$, avec $a, b \in \mathbb{N}$, $\omega_N^{xy} = \omega_N^b$.

Les termes entre parenthèses sont les fractions binaires, i.e.,

$$0.x_{n-1}x_{n-2}\cdots x_1x_0 = \frac{x_{n-1}}{2^1} + \frac{x_{n-2}}{2^2} + \cdots + \frac{x_1}{2^{n-1}} + \frac{x_0}{2^n}. \quad (5.5.9)$$

Ainsi pour, $y_i \in \{0, 1\}$, l'amplitude

$$\sum_{y=0}^{2^n-1} e^{2i\pi \frac{xy}{2^n}} = \left(\sum_y e^{2i\pi y_{n-1}(\cdot x_0)} \right) \cdots \left(\sum_y e^{2i\pi y_0(\cdot x_{n-1}x_{n-2}\cdots x_1x_0)} \right), \quad (5.5.10)$$

permet d'écrire l'équation (5.5.2) sous la forme d'un produit tensoriel

$$\mathbf{F}_N |x\rangle = \frac{1}{\sqrt{2^n}} [|0\rangle + e^{2i\pi(\cdot x_0)} |1\rangle]_{n-1} \otimes \cdots \otimes [|0\rangle + e^{2i\pi(\cdot x_{n-1}x_{n-2}\cdots x_1x_0)} |1\rangle]_0. \quad (5.5.11)$$

La QFT ne génère donc pas un état intriqué.

Exemple 5.5.1 Pour $n = 2$

$$\begin{aligned} \mathbf{F}_4 |x\rangle &= \mathbf{F}_4 |x_1x_0\rangle = \frac{1}{\sqrt{2^2}} [|0\rangle + e^{2i\pi(\cdot x_0)} |1\rangle]_1 [|0\rangle + e^{2i\pi(\cdot x_1x_0)} |1\rangle]_0 \\ &= \frac{1}{2} [|00\rangle + e^{2i\pi(\cdot x_1x_0)} |01\rangle + e^{2i\pi(\cdot x_0)} |10\rangle + e^{2i\pi(\cdot x_0 + x_1x_0)} |11\rangle]. \end{aligned} \quad (5.5.12)$$

Si en plus on prend $|x\rangle = |01\rangle$,

$$\begin{aligned} \mathbf{F}_4 |01\rangle &= \frac{1}{2} [|00\rangle + e^{2i\pi(\cdot 01)} |01\rangle + e^{2i\pi(\cdot 1)} |10\rangle + e^{2i\pi(\cdot 1+01)} |11\rangle] \\ &= \frac{1}{2} [|00\rangle + i |01\rangle - |10\rangle - i |11\rangle]. \end{aligned} \quad (5.5.13)$$

Ce résultat est conforme à (5.5.5).

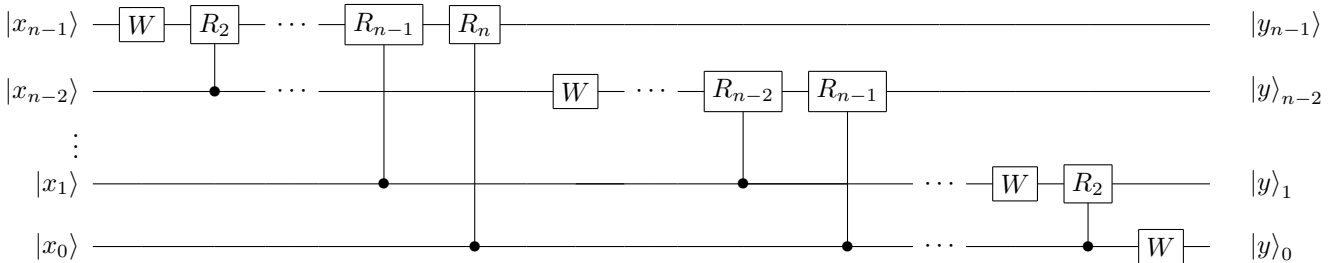


Figure 5.5.1 – Circuit implémentant la transformation de Fourier quantique, avec $|y\rangle_k = \frac{1}{\sqrt{2}} [|0\rangle + e^{2i\pi(\cdot x_k x_{k-1} \cdots x_1 x_0)} |1\rangle]$. Les portes *SWAP* qui inversent l'ordre des qubits de sortie ne sont pas représentées. On note que la transformation de Fourier d'un vecteur complexe de taille $N = 2^n$ peut être implémenté de manière efficace sur un registre de n qubits en utilisant n portes de W et $\frac{n(n-1)}{2}$ portes CR_k . Soit au total $\mathcal{O}(n^2)$ portes quantiques élémentaires. L'algorithme classique le plus efficace, la transformée de Fourier rapide (FFF), calcule la transformée de Fourier discrète en $\mathcal{O}(2^n n)$ opérations élémentaires.

Le produit tensoriel (5.5.11) rend aisée l'implémentation d'un circuit qui calcule la QFT de façon *efficace*. Un tel circuit, qu'illustre la figure 5.5.1, n'a besoin que des opérateurs de base W et **Controlled Phase Rotation** $\text{CR}_{k \geq 2}(\frac{2\pi}{2^k})$ avec

$$\mathbf{R}_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}. \quad (5.5.14)$$

Considérons l'action que circuit sur l'état $|x_{n-1}x_{n-2}\cdots x_1x_0\rangle$ de la base de calcul.

- La première porte de W agit sur le qubit le plus significatif $|x_{n-1}\rangle$ et, en vertu de $e^{2i\pi(\cdot x_{n-1})} = (-1)^{x_{n-1}}$, génère l'état

$$(W|x_{n-1}\rangle)|x_{n-2}\cdots x_1x_0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + e^{2i\pi(\cdot x_{n-1})}|1\rangle]_{n-1}|x_{n-2}\cdots x_1x_0\rangle. \quad (5.5.15)$$

- L'application de la porte CR_2 génère l'état

$$\frac{1}{\sqrt{2}}[|0\rangle + e^{2i\pi(\cdot x_{n-1})}e^{\frac{2i\pi x_{n-2}}{2^2}}|1\rangle]_{n-1}|x_{n-2}\cdots x_1x_0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + e^{2i\pi(\cdot x_{n-1}x_{n-2})}|1\rangle]_{n-1}|x_{n-2}\cdots x_1x_0\rangle \quad (5.5.16)$$

- Les portes $CR_{k \geq 3}$ subséquentes, CR_3 à CR_n ajoute les phases de $\frac{\pi}{2^2}$ à $\frac{\pi}{2^{n-1}}$ lorsque le qubit de contrôle a pour valeur 1. Après ces $n-1$ portes à 2 qubits, le calculateur quantique est dans l'état

$$\frac{1}{\sqrt{2}}[|0\rangle + e^{2i\pi(\cdot x_{n-1}x_{n-2}\cdots x_1x_0)}|1\rangle]_{n-1}|x_{n-2}\cdots x_1x_0\rangle. \quad (5.5.17)$$

- La même procédure est répétée aux autres qubits et on obtient finalement

$$\frac{1}{\sqrt{2^n}}[|0\rangle + e^{2i\pi(\cdot x_{n-1}x_{n-2}\cdots x_1x_0)}|1\rangle]_{n-1} \otimes \cdots \otimes [|0\rangle + e^{2i\pi(\cdot x_0)}|1\rangle]_0. \quad (5.5.18)$$

Cet état coïncide avec (5.5.11), excepté que le fait que l'ordre des qubits est inversé. Le bon ordre est obtenu, soit en utilisant $\mathcal{O}(n)$ portes $SWAP$, soit en renumérotant simplement les qubits à la sortie.

Exercice 5.5.2 Dessiner le circuit qui implémente la QFT du 3-qubit $|x\rangle = |x_2x_1x_0\rangle$ et évaluer pas à pas, l'état final de ce circuit.

Remarque 5.5.1 Il faut souligner qu'on ne peut pas vraiment parler d'une accélération exponentielle dans le calcul de la QFT, puisqu'un état arbitraire $|\psi\rangle = \sum_x f(x)|x\rangle$ ne peut pas être préparé de manière efficace et l'état transformé $|\tilde{\psi}\rangle = \sum_{k=0}^{N-1} \tilde{f}(y)|y\rangle$ n'est pas facilement accessible. En effet, une mesure standard donne simplement un résultat avec y probabilité $|\tilde{f}(y)|$. Le problème est que la transformée de Fourier quantique est effectuée sur les amplitudes de la fonction d'onde, qui ne sont pas directement accessibles. Ils ne peuvent être reconstitués avec une précision finie qu'après de itérations (chaque itération calcule la transformée de Fourier de l'état $|\psi\rangle$ et se termine avec une mesure standard projective).

5.6 Réalisations physiques

Les approches expérimentales proposées pour la réalisation d'un ordinateur quantique sont nombreuses et variées :

- les qubits supraconducteurs à base de jonctions Josephson,
- les qubits à boîtes quantiques semiconductrices,
- les ions piégés dans le vide,
- les spins nucléaires de molécules en solution, pilotés par résonance magnétique nucléaire (RMN),

- les atomes de Rydberg,
- les défauts optiques cristallins, les cavités résonantes relevant du domaine de l'optique quantique.

Dans un premier temps, il s'agit de réaliser une porte logique élémentaire, c'est-à-dire d'arriver à coupler deux systèmes quantiques de façon suffisamment forte pour que l'état de l'un puisse être modifié par l'état de l'autre avant que la décohérence n'entre en jeu.

L'étape suivante consiste à augmenter le nombre de qubits en interaction pour construire un vrai ordinateur. Des propositions ont été faites pour cette dernière étape, mais la plupart soulève des difficultés technologiques considérables.

Les points forts et faibles des différentes approches expérimentales sont résumés dans le tableau 5.6.1, qui reprend les cinq critères de Di Vincenzo avec en plus, deux critères de connectivité :

- C1** Capacité d'initialiser les qubits dans un état bien défini.
- C2** Capacité de mesurer les qubits avec fiabilité.
- C3** Temps de décohérence suffisamment long (beaucoup plus long que le temps d'opération des portes quantiques).
- C4** Disposer d'un jeu universel de portes quantiques.
- C5** Capacité d'accommoder un grand nombre de qubits.
- C6** Capacité de convertir les qubits fixes en qubits mobiles.
- C7** Capacité de transmettre efficacement les qubits mobiles entre plusieurs endroits.

Approche Expérimentale	Critères de Di Vincenzo					Connectivité	
	C1	C2	C3	C4	C5	C6	C7
Supraconducteur	♠	♠	♣	♣	♣	♣	♣
Semiconducteur	♣	♣	♣	♣	♣	▼	▼
RMN	♣	♣	♣	♠	▼	▼	▼
Ions piégés	♠	♠	♣	♠	♣	♣	♣
Cavités QED	♣	♠	♣	♠	♠	♣	♣
Atomes neutres	♠	♣	♣	♣	♣	♣	♣
Optique quantique	♠	♠	♣	♣	♣	♣	♣

Table 5.6.1 – Synthèse des réalisations physiques. ♠=approche viable ayant suffisamment fait ses preuves ; ♣=approche viable mais requérant plus de preuves expérimentales ; ▼=aucune approche viable connue actuellement. [Crédits : A quantum information science and technology roadmap, report of the quantum information science and technology experts panel, v2.0 Avril 2004, http://qist.lanl.gov/qcomp_map.shtml]

5.7 Conclusion

L'ordinateur quantique a pu apparaître un temps comme un calculateur magique, à l'origine de la révolution informatique du prochain millénaire. Ceci a été largement sur-évalué par l'imagination populaire, à cause principalement du mystère planant autour des concepts de théorie quantique, souvent mal compris et mal interprétés. Il est très peu probable en effet, que l'ordinateur quantique supplante intégralement l'ordinateur classique, pour la même raison que la physique quantique ne remplace pas la physique classique pour la grande majorité des problèmes quotidiens. Dans le monde macroscopique, personne ne s'aventure en effet dans la résolution de l'équation de Schrödinger pour concevoir un avion ou une voiture. De la même manière, l'ordinateur quantique sera réservé à la résolution de problèmes particuliers, pour lesquels le parallélisme quantique apporte un avantage décisif.

En particulier, l'ordinateur quantique donne l'espoir de pouvoir un jour résoudre efficacement (en temps polynomial) des problèmes complexes, qui sont insolubles avec des ordinateurs classiques, à cause de l'explosion exponentielle de leur temps de calcul. Des algorithmes quantiques efficaces ont déjà vu le jour, avec la découverte spectaculaire des **algorithmes de Shor et de Grover** dans les années '90, suivie de la mise au point de nombreuses variantes et améliorations. Malgré leur nombre encore restreint, ces algorithmes quantiques sont théoriquement très efficaces, et apporteront à terme des avantages calculatoires notables. S'ajoute à cela la mise au point de codes correcteurs d'erreur, autorisant une certaine dose de décohérence sans laquelle l'ordinateur quantique ne verrait certainement jamais le jour.

5.8 Exercices

5.8.1 Effets des erreurs d'amplitude et de phase

On définit *l'erreur d'amplitude* par la transformation

$$|\psi\rangle \rightarrow |\psi_a\rangle = \beta|0\rangle + \alpha|1\rangle, \quad (5.8.1)$$

et *l'erreur de phase* par la transformation

$$|\psi\rangle \rightarrow |\psi_p\rangle = \alpha|0\rangle - \beta|1\rangle. \quad (5.8.2)$$

Afin d'étudier les effets de ces deux transformations sur le qubit contrôle ou cible d'une porte logique CNOT, on considère l'état initial

$$(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (5.8.3)$$

1. Montrer que l'action de l'erreur de phase sur le qubit cible est transférée au qubit de contrôle après application de l'opérateur porte logique CNOT. On parle alors de *propagation régressive du signe*.
2. Qu'en est-il lorsque l'erreur de phase agit d'abord sur le qubit de contrôle et qu'on applique ensuite de l'opérateur porte logique CNOT ?
3. Étudier de la même façon l'effet de l'erreur d'amplitude.

5.8.2 Opérateur racine carrée NOT

On considère l'opérateur linéaire $H = i\hbar\omega(|0\rangle\langle 1| - |1\rangle\langle 0|)$ qui agit dans l'espace de Hilbert \mathbb{C}^2 , où $\{|0\rangle, |1\rangle\}$ est une base orthonormée dans \mathbb{C}^2 et $\omega \in \mathbb{R}$.

1. H est-il hermitien ?
2. Quels sont les valeurs propres et les vecteurs propres normalisés de H ?
3. Développer $U(t) = e^{-iHt/\hbar}$ sous la forme d'un cos et d'un sin et trouver les valeurs de t telles que U réalise l'opération FNOT (**F**ake **N**OT) :

$$\begin{cases} U(t)|0\rangle = -|1\rangle \\ U(t)|1\rangle = |0\rangle \end{cases} \quad (5.8.4)$$

4. Calculer $U(t = \frac{\pi}{4\omega})$ et $[U(t = \frac{\pi}{4\omega})]^2$. Que peut-on conclure ?
5. Sachant que traditionnellement en calcul quantique, l'opérateur NOT est

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (5.8.5)$$

utiliser l'opérateur $U(t) = e^{i\frac{\pi}{2}}e^{-iHt/\hbar}$, H étant à définir, pour montrer que l'opérateur **racine carrée NOT** est

$$V = \frac{1+i}{2}(\mathbb{I}_2 - iX) = \frac{1+i}{\sqrt{2}}e^{-i\frac{\pi}{4}X}. \quad (5.8.6)$$

5.8.3 Algorithme quantique

Soit $x_1, x_2, y_1, y_2 \in \{0, 1\}$ où Alice a x_1 et x_2 et Bob, y_1 et y_2 . Alice et Bob veulent calculer la fonction booléenne

$$g(x_1, x_2, y_1, y_2) = x_2 \oplus y_2 \oplus (x_1 \wedge y_1), \quad (5.8.7)$$

où \oplus désigne l'opération XOR et \wedge l'opération AND. En plus Alice et Bob échange la paire EPR

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \quad (5.8.8)$$

Alice applique la matrice unitaire $R(\theta_1) \otimes \mathbb{I}_2$ à son qubit EPR alors que Bob applique au sien $\mathbb{I}_2 \otimes R(\theta_2)$ avec $\theta_1 = -\frac{\pi}{16} + x_1 \frac{\pi}{4}$, $\theta_2 = -\frac{\pi}{16} + y_1 \frac{\pi}{4}$ et

$$R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}. \quad (5.8.9)$$

On note a le résultat de la mesure d'Alice sur son qubit EPR et b le résultat de la mesure de Bob sur le sien.

1. Donner l'expression de $|\psi\rangle = R(\theta_1) \otimes R(\theta_2) |\Phi^-\rangle$, l'état de la paire EPR après l'application de opérateurs de rotation unitaires par Alice et Bob.
2. Si $\mathcal{P}(a, b)$ est la probabilité de trouver a et b , remplir la table de vérité suivante :

a	b	$a \oplus b$	$\mathcal{P}(a, b)$
0	0		
0	1		
1	0		
1	1		

3. Remplir la table de vérité suivante

x_1	y_1	$x_1 \wedge y_1$	$\mathcal{P}(a \oplus b = x_1 \wedge y_1)$
0	0		
0	1		
1	0		
1	1		

et en déduire la probabilité pour que

$$a \oplus b = x_1 \wedge y_1. \quad (5.8.10)$$

5.8.4 Circuit intraportation

La **téléportation quantique** est un protocole de communications quantiques consistant à **transférer** l'état quantique d'un système vers un autre système similaire et séparé spatialement du premier en mettant à profit l'intrication quantique. Nous l'avons introduite à la section 4.3.3. Résumons la problématique.

Il était une fois Alice et Bob qui, avant de se séparer, prirent chacun un qubit d'une même paire EPR $|\Phi^+\rangle$. Puis Bob s'en alla, vers une galaxie ignorée d'Alice.

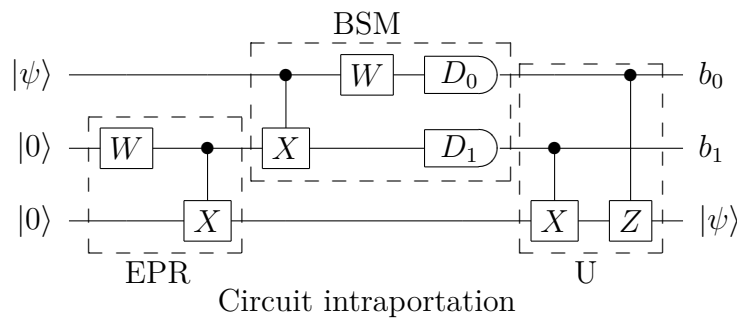
C'est alors que, bien plus tard, un qubit dans un état inconnu, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, arriva chez Alice. Mission d'Alice : transmettre l'état $|\psi\rangle$ à Bob. Mais Alice ne pouvait pas

- porter ce qubit à Bob,
- ni cloner $|\psi\rangle$ pour en disperser des copies dans l'univers,
- ni connaître α et β pour diffuser leurs valeurs sur les ondes dans l'espace intergalactique.

Alors Alice devait téléporter $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Ils avaient prévu tout ce qu'il fallait :

- Un *canal quantique*, la paire EPR $|\Phi^+\rangle$, dont ils avaient soigneusement gardé chacun un qubit avant de se séparer.
- Deux opérateurs, W et CX , qu'Alice avait chez elle, et deux détecteurs D_0, D_1 .
- Et quatre autres opérateurs unitaires $U \equiv \mathbb{I}, X, iY, Z$ que Bob avait pris dans son vaisseau.

Le circuit quantique ci-dessous qui présente cette téléportation⁶. La première ligne représente le qubit $|\psi\rangle$ à téléporter. La deuxième ligne appartient à Alice et la troisième ligne appartient à Bob. La mesure effectuée par Alice (BSM), à travers les détecteurs D_0 et D_1 , donne deux bits classiques b_0 et b_1 (communiqués par un canal classique (Téléphone, Internet) à Bob) qui conditionnent ou contrôlent la transformation unitaire U effectuée par Bob.



1. Donner l'expression de la paire EPR $|\Phi^+\rangle$ que Alice et Bob se sont partagés.
2. Alice fait interagir $|\psi\rangle$ avec sa moitié de l'EPR. Exprimer le 3-qubit $|\psi\rangle_{123} = |\psi\rangle \otimes |\Phi^+\rangle$ qu'elle obtient dans la base de Bell $\{|\Phi^+\rangle, |\Phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, avec $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$.
On posera $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\psi_1\rangle = \alpha|1\rangle + \beta|0\rangle$, $|\psi_2\rangle = \alpha|0\rangle - \beta|1\rangle$, $|\psi_3\rangle = \alpha|1\rangle - \beta|0\rangle$.
3. Lorsque Alice effectue des mesures de Bell (c'est-à-dire dans la base de Bell), quelles résultats peut-elle obtenir et avec quelles probabilités ?
4. Cependant, les états propres des appareils de mesure ou détecteurs d'Alice ne sont pas les états de Bell, mais états standards $|b_0 b_1\rangle \equiv \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
 - (a) Trouver la porte q-logique B qui permet le passage base de Bell \rightarrow base standard ($B|\Phi^+\rangle = |00\rangle, B|\Phi^-\rangle = |10\rangle, B|\psi^+\rangle = |01\rangle, B|\psi^-\rangle = |11\rangle$), en représentation matricielle et comme produit des opérateurs 1-qubit et CX .
 - (b) Quelle est maintenant l'expression de $|\psi\rangle_{123}$ (dans la base standard) ?

⁶Voir G. Brassard, S.L. Braunstein and R. Cleve, *Teleportation as a quantum computation*, Physica **D120**, 43, (1998). Ce circuit est très souvent appelé **intraportation** puisque la portes CX s'exécutent entre les premier-second et second-troisième qubits. Ainsi, pour implémenter ces portes CX , les deux premiers qubits ne peuvent être arbitrairement éloignés du troisième.

5. Alice mesure les deux bits classiques en sa possession dans la base standard. Cette mesure projette l'état du qubit de Bob dans un des états $|\psi_i\rangle$, $i = 0, 1, 2, 3$. Faire un tableau où apparaîtra les résultats possibles de la mesure d'Alice, l'état du qubit de Bob et les probabilités correspondantes.

Résultat de la mesure de Alice	État du qubit projeté reçu par Bob	Probabilité	U

6. Alice transmet à Bob par un canal classique le résultat de sa mesure, et Bob sait que le qubit $|\psi_i\rangle$ lui arrive dans l'état inconnu de départ, mais qui reste tout aussi inconnu !

En fonction de $|\psi_i\rangle$, dire quel opérateur unitaire U (que l'on exprimera en fonction des puissances de X, Z) Bob doit appliquer pour reconstituer $|\psi\rangle$. Ce résultat sera inclut dans le tableau de la question précédente.

L'état du qubit de départ $|\psi\rangle$ a été téléporté, mais il n'y a jamais eu une mesure de cet état.

7. Montrer, en parcourant le circuit, qu'on a effectivement à la sortie de la 3e ligne, $|\psi\rangle$.

5.8.5 Circuit intraportation avec QuTiP

En utilisant le logiciel QuTiP, simuler le circuit de l'exercice 5.8.4. Votre programme devrait faire ce qui suit :

1. Définir toutes les portes logiques du circuit intraportation.
2. Définir particulièrement l'opérateur B qui permet de générer la paire EPR $|\Phi^+\rangle$ partager par Alice et Bob.
3. Définir l'état d'entrée $|\psi\rangle_{in} = |\psi\rangle \otimes |\Phi^+\rangle$ du circuit.
4. Évaluer l'état de sortie $|\psi\rangle_{out}$ du circuit.
5. Évaluer ρ_{Bob} , en prenant la trace partielle de $|\psi\rangle_{out}$,
6. Calculer $\langle\psi|\rho_{Bob}|\psi\rangle$. Vous devez trouver le résultat 1.

5.8.6 Téléportation d'une paire EPR

Le circuit quantique ci-dessous qui présente la téléportation d'une paire EPR⁷. Les premières portes génèrent l'état intriqué

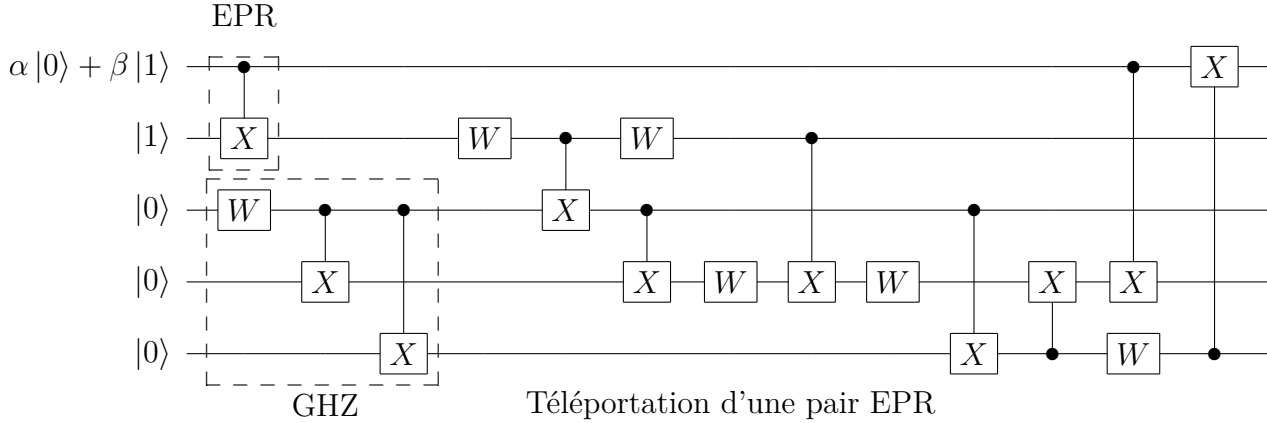
$$\alpha |01\rangle + \beta |10\rangle, \quad (5.8.11)$$

⁷voir V.N. Gorbachev and A.I. Trubilko, *Quantum teleportation of EPR pair by three-particle entanglement*, J. Exp. Phys. **91**, 894 (2000).

et l'état GHZ (Greenberger, Horne et Zeilinger)

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \quad (5.8.12)$$

1. Montrer qu'à la sortie, l'état EPR (5.8.11) est retrouvé aux deux dernières lignes du circuit.



2. Simuler ce circuit en utilisant QuTiP. Votre programme devrait :

- (a) Définir les portes logiques quantique du circuit.
- (b) Définir de l'état d'entrée du circuit $|EPR\rangle \otimes |GHZ\rangle$ (on prendra $|\alpha|^2 = |\beta|^2 = \frac{1}{2}$). Il faudra au préalable évaluer les états $|EPR\rangle$ et $|GHZ\rangle$.
- (c) Évaluer l'état de sortie du circuit, y extraire, à travers la trace partielle, l'état final de la dernière ligne,
- (d) Comparer avec l'état initial.

5.8.7 Transformée de Fourier Quantique

Évaluer la sortie du circuit quantique de la figure 5.8.1, où W la porte 1-qubit de Walsh-Hadamard, $\mathbf{CR}_k = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \mathbf{R}_k$, avec $\mathbf{R}_k = |0\rangle\langle 0| + e^{\frac{2\pi i}{2^k}} |1\rangle\langle 1|$.

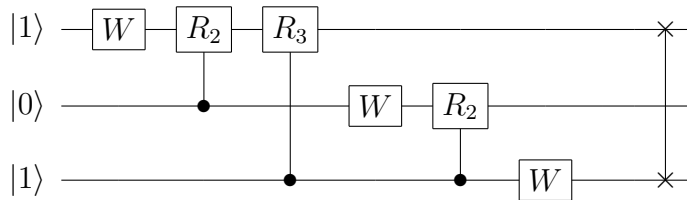


Figure 5.8.1 – Circuit implémentant la Transformation de Fourier Quantique (QFT) de $|101\rangle$.

ANNEXE A

INSTALLATION DE QUTIP ET COMMANDES USUELLES

QuTiP (**Q**uantum **T**oolbox **i**n **P**ython) est un logiciel *libre ou open-source* de calculs d'optique quantique avec des applications en information quantique. C'est un excellent outil d'appropriation et de simulation des concepts fondamentaux de la théorie quantique. Grâce à ce logiciel dont la maîtrise est aisée, l'étudiant peut facilement représenter un état quantique ou un opérateur, calculer une valeur moyenne, simuler l'évolution d'un système, implémenter des algorithmes de l'information quantique.

QuTiP étant rédigé en Python, il est nécessaire, pour utiliser optimalement, d'avoir quelques notions de base du langage de programmation Python. Pour cela nous vous conseillons le cours gratuit *Apprenez à programmer en Python* disponible sur le site du zéro <http://uploads.siteduzero.com/pdf/223267-apprenez-a-programmer-en-python.pdf>. Il est important de souligner que Python est un langage de programmation **interprété**, c'est-à-dire que les instructions que vous lui envoyez sont transcrites en langage machine au fur et à mesure de leur lecture. Les langages comme le C / C++ ou le fortran sont appelés **langages compilés** car, avant de pouvoir les exécuter, un logiciel spécialisé se charge de transformer le code du programme en langage machine par la *compilation*. À chaque modification du code, il faut rappeler une étape de compilation.

Nous présentons ici les étapes à suivre pour l'installation de QuTiP sous le système d'exploitation libre **Linux**. Il est à noter que QuTiP fonctionne aussi sous les systèmes d'exploitation **Mac OS X** et **Windows**.

A.1 Installation de QuTiP pour Ubuntu 12.04 et plus récente

Pour commencer, il faut déjà un ordinateur sur lequel est installée une variante de la distribution Linux Ubuntu (Ubuntu, Xubuntu, Kubuntu, Lubuntu, etc.). Se connecter à Internet pour télécharger les *paquets* nécessaires¹

¹Il faut aussi préciser qu'il y a deux possibilités d'installer QuTiP : manuellement et automatiquement. Nous allons présenter seulement l'installation automatique pour sa simplicité. Pour l'installation manuelle et l'installation sur d'autres systèmes d'exploitation veuillez consulter le manuel de QuTiP *QuTiP : The Quantum Toolbox in Python release 2.2.0* disponible sur le site <http://qutip.googlecode.com/files/QuTiP-2.2.0-DOC.pdf>.

Aller sur le terminal et entrez la commande suivante, pour ajouter le dépôt de QuTiP à la *sourcelist* :

```
sudo add-apt-repository ppa:jrjohansson/qutip-releases
```

Mettre ensuite cette liste de dépôt grâce à la commande

```
sudo apt-get update
```

et installer QuTiP avec la commande

```
sudo apt-get install python-qutip
```

Il est recommandé d'installer d'autres paquets afin de compléter l'installation. Pour cela dans votre terminal, tapez les commandes suivantes :

```
sudo apt-get install texlive-latex-extra
```

```
sudo apt-get install python-nose
```

La dernière étape de la procédure consiste à installer une console Python ou interpréteur. A cet effet nous suggérons IPython ou bpython qui permet une bonne complétion. Taper sur le terminal

```
sudo apt-get install ipython
```

ou

```
sudo apt-get install bpython
```

A.2 Vérification de l'installation

Il est possible de vérifier si votre installation de QuTiP s'est bien dérouler. Le temps de cette vérification est fonction de la puissance de votre ordinateur. Pour vérifier, il faut taper sur terminal les commandes :

```
ipython # ou bpython si vous l'avez installé
```

```
import qutip.testing as qt
```

```
qt.run()
```

Une fois la vérification faite vous pouvez utiliser QuTiP.

A.3 Commandes usuelles

A.3.1 Quantum object class

Expliquer clairement la notion de `Qobj()`

A.3.2 États et opérateurs

Donner ici les `Qobj` prédéfinis pour les états et les opérateurs qui seront utilisés dans les divers exercices de ce cours.

A.3.3 Les attribues d'une classe `Qobj`

Expliquer et donner le tableau.

A.3.4 `Qobj Math`

Expliquer à travers quelques exemples.

A.3.5 Fonction opérant sur une classe Qobj

En plus des attribues, une classe d'objet quantique à des fonctions qui agissent sur les instances Qobj. Les plus usuelles sont :

Donner le tableau et illustrer par quelques exemples.

A.4 Manipuler les états et opérateurs

A.4.1 États ket et bra

Expliquer en prenant des exemples compatibles avec le niveau de compréhension ou de connaissances des étudiants.

A.4.2 Qubit

Exemples simples.

A.4.3 Valeurs moyennes

Exemples simples.

A.5 Produit tensoriel et trace partielle

Présenter tenant compte du niveau de connaissances du cours.

A.5.1 Produit tensoriel

Exemples simples.

A.5.2 Trace partielle

Exemples simples.

A.6 Sphère de Bloch

A.6.1 Bloch class

Exemples simples.

A.6.2 Bloch3d class

Exemples simples.

A.6.3 Différences entre Bloch and Bloch3d

A.7 Évolution temporelle unitaire

ANNEXE B

THÉORIE DE L'INFORMATION CLASSIQUE

Claude Shannon a apporté en 1948 les solutions aux deux problèmes qui sont au cœur de la théorie de l'information classique :

1. De quel ordre peut être comprimé un message ou *quelle est la redondance d'une information* ?
2. A quel taux peut-on communiquer de manière sûre au travers d'un canal bruité ou *quelle redondance doit être incorporée à un message pour le protéger contre les erreurs* ?

Les réponses à ces questions se formulent en deux théorèmes :

Théorème B.0.1 The noiseless coding theorem. *Il existe de nombreuses façons de coder un message. Le code optimal est celui qui compresse en moyenne chaque lettre d'un message de n lettres d'un facteur $H(X)$ dans la limite $n \rightarrow \infty$.*

Théorème B.0.2 The noisy channel coding theorem. *Tout canal peut être utilisé pour une communication d'une qualité arbitrairement fiable à un taux fini (différent de zéro), tant qu'il existe une corrélation entre l'input (donnée) et l'output (résultat).*

Il est à noter que la **redondance** est le degré d'imprévisibilité en moyenne de la prochaine lettre d'un message. Et le problème se résume à déterminer le concept à utiliser pour quantifier la redondance. La clé a été trouvée par Shannon à travers la notion d'**entropie**.

B.1 Entropie de Shannon

Un message est une suite de lettres choisie dans un alphabet composé de k lettres

$$x_1, x_2, \dots, x_k \tag{B.1.1}$$

où l'on suppose que les lettres du message sont statistiquement indépendantes et que la probabilité d'avoir dans le message la lettre x_i est donnée par \mathcal{P}_i avec $\sum_{i=1}^k \mathcal{P}_i = 1$.

Considérons le cas simple d'un alphabet binaire, $\{0, 1\}$ par exemple, où 0 a lieu avec la probabilité $1 - p$ et 1 avec p ($0 \leq p \leq 1$). Soit un long message composé de n lettres, $n \gg 1$.

Est-il alors possible de compresser le message en une chaîne de lettres plus courte transmettant essentiellement la même information ?

Pour n très grand, la loi des nombres nous dit que les chaînes typiques contiendront, pour le cas binaire, environ $n(1-p)$ 0 et np 1. Le nombre de chaînes distinctes de cette forme est donné par le coefficient binomial $\binom{n}{np}$, et en utilisant l'approximation de Stirling $\log n! = n \log n - n$, on trouve

$$\begin{aligned} \log \binom{n}{np} &= \log \left(\frac{n!}{(np)![n(1-p)]!} \right) \\ &\simeq n \log n - n - (np \log np - np) - [n(1-p) \log n(1-p) - n(1-p)] \\ &= nH(p) \end{aligned} \quad (\text{B.1.2})$$

avec

$$H(p) = -p \log p - (1-p) \log(1-p), \quad (\text{B.1.3})$$

l'**entropie**. Ainsi, le nombre de chaînes typiques de lettres est de l'ordre de $2^{nH(p)}$.

Pour transmettre essentiellement toute information contenue dans une chaîne de n bits, il suffit de choisir un code (*block code*) qui assigne un index (un entier positif, une lettre, ...) à chacune des chaînes typiques. Ce code a donc environ $2^{nH(p)}$ index équiprobables, ce qui signifie que chacun d'eux (chacune des chaînes typiques) peut être spécifiés en utilisant une chaîne binaire d'une longueur de

$$\log 2^{nH(p)} = nH(p). \quad (\text{B.1.4})$$

Comme $0 \leq H(p) \leq 1$ pour $0 \leq p \leq 1$, et $H(p) = 1$ seulement pour $p = \frac{1}{2}$, le code raccourcit le message $\forall p \neq \frac{1}{2}$, i.e., chaque fois que 0 et 1 ne sont pas équiprobables. C'est le résultat de **Shannon**. Le point important est que l'on a pas besoin d'un code pour chaque séquence de lettres, seules les séquences typiques comptent. La probabilité d'avoir un message atypique devient négligeable dans la limite $n \rightarrow \infty$.

Ce raisonnement se généralise facilement au cas d'un alphabet de k lettres, où la lettre x_i apparaît avec une probabilité \mathcal{P}_i . Dans une chaîne de n lettres, x_i apparaît typiquement $n\mathcal{P}_i$ fois, et le nombre de chaînes typiques est de l'ordre de

$$\frac{n!}{\prod_{i=1}^k (n\mathcal{P}_i)!} \simeq 2^{nH(X)}, \quad (\text{B.1.5})$$

où l'approximation de Stirling est une fois de plus utilisée, et

$$H(X) = - \sum_{i=1}^k \mathcal{P}_i \log \mathcal{P}_i, \quad (\text{B.1.6})$$

est l'**entropie de Shannon** de l'ensemble $X = \{x_i, \mathcal{P}_i\}_{i \in \mathbb{N}}$. A noter que $0 \leq H(X) \leq \log k$ bits.

De même, en adoptant un code qui assigne une chaîne binaire aux séquences typiques, l'information d'une chaîne de n lettres peut être compressé d'un facteur $H(X)$ *bits* (logarithme base 2). Dans ce sens, une lettre x_i choisie dans l'ensemble porte en moyenne $H(X)$ bits d'information. Il est également possible d'exprimer la compression $H(X)$ en *nats* (logarithme base n), c'est-à-dire en utilisant non plus une chaîne binaire pour spécifier les chaînes typiques, mais un alphabet composé de n lettres. Ce qui justifie la formulation du théorème B.0.1.

Il est important de souligner que l'entropie $H(X)$ renseigne sur le **gain d'information** acquis une fois le message X reçu, et non sur la **signification de l'information**. Autrement, le sens de l'information n'est pas du tout pris en compte dans cette interprétation de l'entropie.

Exemple B.1.1 En français, le message $X = \text{“exzwctys”}$ a une entropie plus grande que le message $X' = \text{“beaucoup”}$. En effet, “beaucoup” est le seul mot français commençant par les lettres “beauc”. Ainsi, après la réception des cinq premières lettres du mot, on connaît à coup sûr les trois dernières. En revanche, la suite des mots composant X est complètement imprévisible, il renferme donc un gain d'information plus grand pour le même nombre de lettres que X' , même si en français X n'a pas de sens.

Exemple B.1.2 Soit un message X composé de n lettres équiprobables, i.e., $\mathcal{P}_i = \frac{1}{n}$. Alors une fois le message reçu,

$$H(X) = - \sum_{i=1}^n \frac{1}{n} \log \frac{1}{n} = - \log \frac{1}{n} = \log n \text{ (bits)}, \quad (\text{B.1.7a})$$

ou

$$H(X) = - \sum_{i=1}^n \frac{1}{n} \log_n \frac{1}{n} = \sum_{i=1}^n \frac{1}{n} = 1 \text{ (nat)}, \quad (\text{B.1.7b})$$

et le gain d'information (entropie) est maximum. Le message ne peut donc pas être compressé.

Exemple B.1.3 Soit un message X composé d'une seule lettre, i.e., $\mathcal{P}_1 = 1$ et $\mathcal{P}_{i \neq 1} = 0$. Alors,

$$H(X) = -1 \log 1 = 0, \quad (\text{B.1.8})$$

et le gain d'information est nul.

Exemple B.1.4 Soit $X = \{a, b, c, d\}$ avec les probabilités $\mathcal{P}_a = \frac{1}{2}$, $\mathcal{P}_b = \frac{1}{4}$, $\mathcal{P}_c = \mathcal{P}_d = \frac{1}{8}$. On suppose que l'on veut envoyer un message de n lettres $A = \{y_1, \dots, y_n\}$, $y_i \in X$.

Naïvement, on décide d'utiliser, pour coder les quatre lettres de l'alphabet,

$$\log_2 4 = 2 \text{ bits/lettre}, \quad (\text{B.1.9})$$

ce qui donne $a \rightarrow 00$, $b \rightarrow 01$, $c \rightarrow 10$, $d \rightarrow 11$. Ainsi on a le message A suivant et son codage,

$$\begin{array}{cccccccccccc} a & a & b & a & a & a & b & c & a & b & d \\ 00 & 00 & 01 & 00 & 00 & 00 & 01 & 10 & 00 & 01 & 11 \end{array} \quad (\text{B.1.10})$$

- Il faut donc logiquement, pour coder ce message,

$$n \left(\frac{1}{2} 2 + \frac{1}{4} 2 + \frac{1}{8} 2 + \frac{1}{8} 2 \right) = 2n \text{ bits}. \quad (\text{B.1.11})$$

- Le taux de compression maximal ici est

$$H(X) = - \sum_{i=1}^4 \mathcal{P}_i \log_2 \mathcal{P}_i = - \left(\frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 2 + \frac{1}{8} \log_2 2 + \frac{1}{8} \log_2 2 \right) = \frac{1}{2} 1 + \frac{1}{4} 2 + \frac{2}{8} 3 = \frac{7}{4}. \quad (\text{B.1.12})$$

- En choisissant un code qui tient compte des probabilités, $a \rightarrow 0$, $b \rightarrow 10$, $c \rightarrow 110$, $d \rightarrow 111$, et qui demande de coder le message A avec $nH(X) = \frac{7}{4}n$ bits, on parvient à atteindre la compression maximale. ce résultat inopiné est dû au fait que les probabilités \mathcal{P}_i sont des puissances de 2.

B.2 Information conditionnelle

L'entropie $H(X)$ quantifie en moyenne l'information transmise par une lettre tirée d'un ensemble X , pour laquelle elle nous dit combien de bits sont nécessaires pour codifier l'information, dans la limite $n \rightarrow \infty$, où n est le nombre de lettres tirées de l'ensemble.

De ce qui précède, on introduit la notion d'**information conditionnelle** $H(A|B)$ qui représente le gain d'information obtenu à la réception du message A , compte tenu du fait que B est connu. Donc $H(A|B)$ correspond au gain d'information contenu dans A qui ne se trouve pas déjà dans B .

Soit le message A composé des lettres x_i et soit le message B composé des lettres y_j associées aux poids¹ $\mathcal{P}(y_j) = q_j$. Alors,

$$H(A|B) = \sum_j q_j \left\{ - \sum_i \mathcal{P}(x_i|y_j) \log \mathcal{P}(x_i|y_j) \right\}, \quad (\text{B.2.1})$$

où $\mathcal{P}(x_i|y_j)$ est la probabilité de x_i conditionnellement à y_j .

B.3 Information mutuelle

L'**information mutuelle** $I(A : B)$ quantifie la corrélation de deux messages A et B . Autrement, elle représente la quantité d'information qu'ont en commun les messages A et B . Alors,

$$I(A : B) = H(A) - H(A|B) = \sum_i \sum_j \mathcal{P}(x_i, y_j) \log \left(\frac{\mathcal{P}(x_i, y_j)}{\mathcal{P}(x_i) \mathcal{P}(y_j)} \right), \quad (\text{B.3.1})$$

avec $I(A : B) = I(B : A)$. On peut encore dire que $I(A : B)$ est la réduction de l'entropie sur la variable aléatoire A qu'apporte la connaissance de la variable aléatoire B .

- Si $A = B$, alors

$$\mathcal{P}(x_i|y_j) = \delta_{ij} \rightarrow H(A|y_j) = 0, \forall j, \quad (\text{B.3.2a})$$

et

$$I(A : B) = H(A) - 0 = H(A). \quad (\text{B.3.2b})$$

En effet, si les deux messages sont identiques, toute l'information leur est commune.

- Si A et B n'ont rien de commun, alors

$$\mathcal{P}(x_i|y_j) = \mathcal{P}(x_i), \forall j, \quad (\text{B.3.3a})$$

et

$$I(A : B) = H(A) - H(A) = 0. \quad (\text{B.3.3b})$$

B.4 Probabilité conjointe

La **probabilité conjointe** $\mathcal{P}(x_i, y_j)$ représente la probabilité d'avoir la lettre x_i et la lettre y_j .

¹Probabilité de présence

Soit $\mathcal{P}(x_i)$ la probabilité d'avoir la lettre x_i et $\mathcal{P}(y_j|x_i)$ la probabilité conditionnelle d'avoir y_j si x_i a lieu. Alors,

$$\mathcal{P}(x_i, y_j) = \mathcal{P}(x_i)\mathcal{P}(y_j|x_i) = \mathcal{P}(y_j)\mathcal{P}(x_i|y_j) = \mathcal{P}(y_j, x_i). \quad (\text{B.4.1})$$

On peut alors énoncer le **théorème de Bayes**

$$\mathcal{P}(x_i|y_j) = \frac{\mathcal{P}(x_i, y_j)}{\mathcal{P}(y_j)} \quad (\text{B.4.2})$$

et en vertu de (B.2.1) l'information conditionnelle s'écrit

$$H(A|B) = - \sum_{ij} \mathcal{P}(y_j) \frac{\mathcal{P}(x_i, y_j)}{\mathcal{P}(y_j)} \log \frac{\mathcal{P}(x_i, y_j)}{\mathcal{P}(y_j)} \quad (\text{B.4.3a})$$

$$= - \sum_{ij} \mathcal{P}(x_i, y_j) \log \mathcal{P}(x_i, y_j) + \sum_{ij} \mathcal{P}(x_i, y_j) \log \mathcal{P}(y_j) \quad (\text{B.4.3b})$$

$$= H(A, B) + \sum_j \mathcal{P}(y_j) \log \mathcal{P}(x_i, y_j) \quad (\text{B.4.3c})$$

$$= H(A, B) - H(B) \quad (\text{B.4.3d})$$

Pour ce qui est de l'information mutuelle, on a

$$I(A : B) = H(A) + H(B) - H(A, B) \quad (\text{B.4.4})$$

où apparaît plus aisément la symétrie de l'information mutuelle.

Exemple B.4.1 Soit $A = \{00, 01, 10, 11\}$ un ensemble de quatre lettres équiprobables (i.e., une probabilité $\frac{1}{4}$ pour chaque lettre) et soit $B = \{0, 1\}$ un ensemble de deux lettres. On fait l'hypothèse que B est une fonction de A et que

$$\mathcal{P}(B = 0|A = 00) = \mathcal{P}(B = 0|A = 11) = 1 \quad (\text{B.4.5a})$$

$$\mathcal{P}(B = 0|A = 01) = \mathcal{P}(B = 0|A = 10) = 0 \quad (\text{B.4.5b})$$

ce qui signifie

$$\mathcal{P}(B = 0) = \sum_{x \in A} \mathcal{P}(B = 0|x) \mathcal{P}(x) \quad (\text{B.4.6a})$$

$$= 1 \cdot \frac{1}{4} + 1 \cdot \frac{1}{4} + 0 \cdot \frac{1}{4} + 0 \cdot \frac{1}{4} = \frac{1}{2} \quad (\text{B.4.6b})$$

et donc $\mathcal{P}(B = 1) = \frac{1}{2}$. Ainsi,

$$H(A) = - \sum_{i=1}^4 \frac{1}{4} \log 2^{-2} = \sum_{i=1}^4 \frac{1}{4} 2 = 2, \quad (\text{B.4.7a})$$

$$H(B) = - \sum_{i=1}^2 \frac{1}{2} \log 2^{-1} = \sum_{i=1}^2 \frac{1}{2} 2 = 1. \quad (\text{B.4.7b})$$

Comme par hypothèse B est entièrement déterminé par l'information de A

$$H(A, B) = 2 = H(A), \quad (\text{B.4.8})$$

toute l'information de B est connue dès qu'on connaît A . D'où

$$H(A|B) = H(A, B) - H(B) = 1, \quad (\text{B.4.9})$$

ou encore

$$H(A|B) = \mathcal{P}(B=0)H(A|B=0) + \mathcal{P}(B=1)H(A|B=1) \quad (\text{B.4.10a})$$

$$= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 1 = 1 \quad (\text{B.4.10b})$$

Ainsi, l'information mutuelle vaut

$$I(A : B) = H(A) - H(A|B) = 2 - 1 = 1. \quad (\text{B.4.11})$$

Par le théorème de Bayes, on peut encore calculer

$$\mathcal{P}(A=00|B=0) = \frac{\mathcal{P}(A=00, B=0)}{\mathcal{P}(B=0)} \quad (\text{B.4.12a})$$

$$= \frac{\mathcal{P}(B=0|A=00)\mathcal{P}(A=00)}{\mathcal{P}(B=0)} = \frac{1 \cdot \frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}. \quad (\text{B.4.12b})$$

De même, pour

$$\mathcal{P}(A=11|B=0) = \frac{1}{2} \quad (\text{B.4.13a})$$

$$\mathcal{P}(A=01|B=0) = \mathcal{P}(A=10|B=0) = 0. \quad (\text{B.4.13b})$$

Le terme de **cryptologie** recouvre un domaine qui ne se limite plus à la simple protection d'une communication au moyen d'une écriture conventionnelle secrète. Les objectifs de la cryptologie d'une part, les moyens qu'elle utilise d'autre part, ont beaucoup évolué depuis une soixantaine d'année. Le développement des transmissions électroniques, qui va en s'accéléralant, fait apparaître un grand nombre de besoins cryptologiques.

La cryptologie présente un double aspect :

1. la **cryptographie** qui consiste à construire des outils pour assurer un certain nombre de fonctionnalités ;
2. la **cryptoanalyse** qui s'attaque aux outils précédents pour en trouver les faiblesses.

C.1 Fonctionnalités de la cryptographie

Les dites fonctionnalités sont les suivantes :

1. **Le chiffrement.** L'application la plus ancienne de la cryptographie est la **confidentialité**. Elle consiste, au moyen d'une information appelée **clé**, à réaliser le **chiffrement** de l'information confidentielle. Le **déchiffrement** réalise l'opération inverse, connaissant la **clé secrète**. Le **décryptage** constitue l'attaque cryptanalytique du chiffrement, c'est-à-dire le recouvrement du message, sans connaissance de la clé secrète.
2. **L'intégrité.** Avec l'émergence des technologies informatiques, le problème de l'intégrité d'une donnée est apparu de façon nouvelle. En effet, autant la falsification d'un document papier laisse des traces de l'agression physique, autant la modification d'une donnée informatique mémorisée peut se faire de manière absolument invisible.

La cryptographie a donc développé des *fonctions de hachage* qui permettent d'obtenir d'un message un **haché** ou **condensat**, de taille réduite par rapport au message initial. La particularité de ces fonctions est qu'il est très difficile de modifier le message sans modifier le haché.

3. **L'authentification.** Elle consiste à prouver son identité ou plus généralement sa qualité. Autrement, elle vise à empêcher autrui de se faire passer pour qui il n'est pas. Un exemple

classique d'authentification est celui de la carte bancaire : dans un distributeur de billets (DAB), il y a avant toute chose, un *protocole d'authentification* qui vise à s'assurer qu'il s'agit bien d'une carte bancaire. L'autre authentification en elle-même est obtenue par la preuve de possession d'un secret, en l'occurrence le code du porteur de carte.

4. **La signature.** Elle consiste à associer de manière sûre une *identité* à un message et à empêcher toute *répudiation* ultérieure. Une signature suppose une action volontaire de la part de la personne qui signe. Le besoin de signature numérique est lui aussi apparu récemment.

C.2 Principe du chiffrement symétrique

Supposons qu'Alice souhaite envoyer un message m à Bob, de telle façon que Bob soit le seul à pouvoir prendre connaissance du message. Pour cela, Alice peut utiliser un système de chiffrement C symétrique, et utiliser une clé de chiffrement secrète K_s . Le système de chiffrement symétrique permet à Alice de fabriquer un message chiffré $c = C(m, K_s)$. C'est ce message c qui est transmis à Bob. Au préalable, Bob a reçu par un moyen sûr la clé secrète K_s et peut donc utiliser le mécanisme de déchiffrement C^{-1} pour déchiffrer le message et obtenir $m = C^{-1}(c, K_s)$.

Un tel système de chiffrement est dit **symétrique** car Alice et Bob doivent tous les deux posséder la même clé K_s pour communiquer. La sécurité du système repose donc sur le secret de la clé, qui ne doit pas être divulguée.

C.3 Problématique de l'authentification

Dans la vie courante, le besoin d'authentification apparaît souvent. Il résolu par l'emploi de méthodes anciennes mais qui ont fait leurs preuves... et aussi montré leurs limites : signature, sceau, tampon, etc...). Les méthodes d'authentification classique reposent sur la difficulté à reproduire ou à falsifier un élément reconnaissable par tous. Lors d'une fraude, la détection est rendue possible par l'expertise physique de la preuve (expertise graphologique, vérification d'un sceau ou d'un tampon).

Le développement des transmissions électroniques a fait apparaître un nouveau problème : comment garantir qu'un message a été effectivement écrit une personne, et comment garantir que cette même personne ne puisse pas nier l'avoir écrit. Cette problématique est celle de la signature électronique.

Pour résoudre ce problème de la cryptographie symétrique est totalement impuissante, car elle suppose la possession par deux ou plusieurs entités d'une même clé secrète. Rien n'empêche donc l'une des parties de se faire passer pour une autre personne disposant de la même clé.

C.4 Principe du chiffrement asymétrique

Le principe de cryptographie asymétrique va au contraire permettre de résoudre ce problème. En effet, en cryptographie asymétrique, Alice qui souhaite s'authentifier va disposer d'un secret qu'elle est seule à connaître. Associée à cette clé privée, une clé publique va permettre à tout le monde, et en particulier à Bob, de vérifier la signature d'Alice. Toutefois, pour atteindre ces objectifs, le système doit absolument garantir l'intégrité de la clé publique. En effet, dans le cas contraire, il suffirait de se forger un couple de clé privée et publique et de faire passer

la fausse clé publique auprès de Bob pour celle d'Alice, pour lui faire croire que c'est Alice qui lui écrit des messages. Il est donc facile de voir que l'exigence de secret absolu observée dans un système symétrique est remplacée dans système asymétrique par l'exigence d'intégrité absolue.

ANNEXE D

CODE RSA

Créé en 1977 par Rivest, Shamir et Adelman, ce code de cryptographie, a bâti sa fiabilité sur la difficulté de factoriser des grands nombres. Cependant, en novembre 2005, au moyen de cinq mois de calculs complexes réalisés sur plus de 80 ordinateurs en réseau, des mathématiciens allemands réussissaient à factoriser un nombre de 193 chiffres, remportant ainsi un défi lancé par RSA. On pense qu'avec des ordinateurs quantiques effectuant des calculs parallèles, on peut relever le défi en quelques secondes.

L'algorithme de ce code est le suivant :

1. Bob choisit deux nombres premiers p et q suffisamment grands et calcule $N = pq$.
2. Bob choisit au hasard un nombre c n'ayant pas de diviseur commun avec le produit $(p-1)(q-1)$, c'est-à-dire $\gcd(c, (p-1)(q-1)) = 1$.
3. Bob calcule d qui est l'inverse de c pour la multiplication modulo $(p-1)(q-1)$

$$cd \equiv 1 \pmod{(p-1)(q-1)}. \quad (\text{D.0.1})$$

4. Bob publie la paire (d, N) . C'est la clé publique que n'importe qui peut utiliser pour envoyer un message à Bob.
5. La paire (c, N) est la clé privée que possède seule Bob. Ainsi, il est le seul à pouvoir déchiffrer un message chiffré au moyen de la clé publique.
6. Alice veut envoyer à Bob un message codé, qui doit être représenté par un nombre $a < N$. Si le message est trop long, Alice le segmente en plusieurs sous messages $a_i < N$. Elle chiffre ensuite chaque sous-message en calculant,

$$b \equiv a_i^d \pmod{N}, \quad (\text{D.0.2})$$

et envoie b à Bob.

7. Quand Bob reçoit le message qu'il déchiffre en calculant

$$b^c \pmod{N} = a_i(!) \quad (\text{D.0.3})$$

En effet, le fait que le résultat soit précisément a_i , c'est-à-dire le message original d'Alice, est un résultat de théorie des nombres.

En résumé, sont envoyés sur voie publique, non sécurisée, les nombres N , d et b . Les avantages par rapport au code *one-time Pad* sont :

- Il n'est point besoin de distribuer une clé secrète par un canal supposé sécurisé. La clé publique peut être utilisée par quiconque veut communiquer avec Bob, lequel possède seul la clé secrète.
- La clé publique peut être re-utilisée autant de fois qu'on le désire.

Exemple D.0.1 $p = 3$, $q = 7$, $N = 21$, $(p - 1)(q - 1) = 12$.

$c = 5$ n'a aucun facteur commun avec 12, et son inverse par rapport à la multiplication modulo 12 est $d = 5$ car $5 \times 5 = 24 + 1$. Alice choisit pour message $a = 4$. Elle calcule

$$4^5 = 1024 = 21 \times 48 + 16, \quad 4^5 = 16 \pmod{21} \quad (\text{D.0.4})$$

Alice envoie donc à Bob le message 16. Bob calcule

$$16^5 = 16^5 = 49\,328 \times 21 + 4, \quad 16^5 = 4 \pmod{21} \quad (\text{D.0.5})$$

et Bob récupère donc le message original $a = 4$.

ANNEXE E

CORRECTION DES EXERCICES

E.1 Qubits et états quantiques

E.1.1 Chat de Shrödinger

Les états $|\psi_1\rangle$ et $|\psi_2\rangle$ sont donnés par :

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|m\rangle + |v\rangle) \\ |\psi_2\rangle &= \frac{1}{2}(\sqrt{3}|m\rangle + |v\rangle). \end{aligned} \tag{E.1.1}$$

Pour les représenter sur la sphère de Bloch, on procède comme suit :

```
#Chat de Shrodinger
```

```
from qutip import *
from pylab import *
```

```
#Definition des etats morts et vivants : ces etats representent les etats 0 et 1
mort = basis(2,0)
```

```
vivant = basis(2,1)
```

```
#Definition des etats Psi_1 et Psi_2
```

```
Psi_1 = (mort+vivant)/sqrt(2)
```

```
Psi_2 = (sqrt(3)*mort+vivant)/2
```

```
B=Bloch()
```

```
B.add_states([mort,vivant,Psi_1,Psi_2])
```

```
B.show()
```

E.2 Mesure et opérateurs linéaires

E.2.1 Représentation matricielle

En utilisant QuTiP, répondre aux questions de l'exercice 2.5.1.

En QuTiP, le programme est le suivant :

```
In [65]: from qutip import *

In [66]: from pylab import *

In [67]:

In [67]: Phi_1 = basis(3,0)

In [68]: Phi_2 = basis(3,1)

In [69]: Phi_3 = basis(3,2)

In [70]:

In [70]: Psi_0 = Phi_1/sqrt(2)+1j*Phi_2/2+Phi_3/2

In [71]: Psi_1 = (Phi_1+1j*Phi_3)/sqrt(3)

In [72]:

In [72]: # Verification de la norme

In [73]: Psi_0.norm()
Out[73]: 1.0

In [74]: Psi_1.norm()
Out[74]: 0.81649658092772615

In [75]:

In [75]: # Calcul de P0 et P1

In [76]: P0 = Psi_0*Psi_0.dag()

In [77]: P1 = Psi_1*Psi_1.dag()

In [78]:

In [78]: # Hermiticite

In [79]: P0.isherm
Out[79]: True
```

```
In [80]: P1.isherm
Out[80]: True

In [81]:

In [81]: # Définir Y

In [82]: Y = sigmay()

In [83]:

In [83]: #Est-elle hermitienne?

In [84]: Y.isherm
Out[84]: True

In [85]:

In [85]: #Valeurs propres et vecteurs propres

In [86]: Val, Vec = Y.eigenstates()

In [87]:

In [87]: Vec1 = Vec[0]

In [88]: Vec2 = Vec[1]

In [89]:

In [89]: # Calcul des projecteurs sur ces etats

In [90]: P_1 = Vec1*Vec1.dag()

In [91]: P_2 = Vec2*Vec2.dag()

In [92]:

In [92]: # Relation de fermeture et d'orthogonalite

In [93]: P_1+P_2 # Ce resultat doit etre Identite
Out[93]:
Quantum object: dims = [[2], [2]], shape = [2, 2], type = oper, isherm = True
Qobj data =
[[ 1.  0.]
 [ 0.  1.]]
```

```
In [94]: P_1*P_2 # Celui-ci doit etre une matrice nulle
Out[94]:
Quantum object: dims = [[2], [2]], shape = [2, 2], type = oper, isherm = True
Qobj data =
[[ 0.  0.]
 [ 0.  0.]]
```

E.2.2 ECOC avec QuTiP

Cet exercice est lié à l'exercice (??). Écrire un programme en utilisant QuTiP permettant de répondre aux questions suivantes.

1. Définir les états $|u1\rangle$, $|u2\rangle$, $|u3\rangle$ ainsi que le hamiltonien H .
2. Calculer les énergies $E1$, $E2$, $E3$ ainsi que les vecteurs propres $|E1\rangle$, $|E2\rangle$, $|E3\rangle$.
3. QuTiP permet de résoudre l'équation de Schrödinger et de calculer les états $|\psi(t)\rangle$ pour les valeurs de temps données. Il permet en même temps de calculer les valeurs moyennes voulues. Calculer pour $t \in [0, 10]$, les états les états $|\psi(t)\rangle$ lorsque l'état initial du système est $|u1\rangle$.
4. Calculer la déviation standard de H pour $t = 10s$.

E.2.3 ECOC Avec QuTiP

ECOC

```
from qutip import *
from pylab import *

#Definition des etats de base.
u1 = basis(3,0)
u2 = basis(3,1)
u3 = basis(3,2)

#Definition de l'operateur H.
H = [[2, -3*sqrt(2), 3*sqrt(2)], [-3*sqrt(2), -1, -3], [3*sqrt(2), -3, -1]]
H = Qobj(H) # Rendre H un objet Quantique

#Calcul des energies et vecteurs propres de H
[E1, E2,E3], [ketE1, ketE2, ketE3] = H.eigenstates()

#Resolution de l'equation de Schrodinger
T = linspace(0,10,11) #Partitionner l'intervall de temps
data = mesolve(H,u1,T,[],[H,H*H]) #Resolution de l'equation avec mesolve
Etat = data.states #Extraire les etats pour t dans [0,10]
MoyenH = data.expect[0] #Moyenne de H pour t dans [0,10]
MoyenHH = data.expect[1] # Moyenne de H*H pour t dans [0,10]
DeltaH = sqrt(MoyenHH[10]-MoyenH[10]**2)
```

E.3 Postulats et évolution

E.3.1 Évolution d'un état de spin 1/2

Le programme est le suivant :

```
from qutip import *
from pylab import *

#Hamiltonien H et ses etats propres
H = 0.25*sigmaz()
zp = basis(2,0)
zm = basis(2,1)
#Projecteurs sur les etats x+ et x-
xp = (zp+zm)/sqrt(2)
xm = (-zp+zm)/sqrt(2)
Pp = xp*xp.dag()
Pm = xm*xm.dag()
#Resolution de l' equation de schrodinger
T = linspace(0,30,100)
data = mesolve(H, xp, T, [], [Pp,Pm,H,H*H])
P1 = data.expect[0]
P2 = data.expect[1]
MoyH = data.expect[2]
MoyHH = data.expect[3]
#Representation
plot(T, P1, T, P2)
xlabel('Temps $t$')
ylabel('Probabilite')
legend(("P+", "P-"))
title(("Probabilite de transition"))
show()
#Calcul de la deviation standard
DeltaH = sqrt(MoyHH[99]-MoyH[99]**2)
```

E.4 Calculs quantiques

E.4.1 Circuit intraportation avec QuTiP

Un des programmes en QuTiP qui implémente le circuit intraportation est le suivant

```
# Teleportation d'une paire EPR sans bruit

from qutip import *
from pylab import *

# Definitions des operateurs intervenants dans le programme
X = sigmax()
Z = sigmaz()
```

```

Y = sigmay()
W = (X+Z)/sqrt(2)
I = qeye(2)

CX_12 = tensor(ket0*ket0.dag(), I, I) + tensor(ket1*ket1.dag(), X, I)
W_1 = tensor(W, I, I)
CX_23 = tensor(I, ket0*ket0.dag(), I) + tensor(I, ket1*ket1.dag(), X)
CZ_13 = tensor(ket0*ket0.dag(), I, I) + tensor(ket1*ket1.dag(), I, Z)

# Definition de B
W_2 = tensor(W, I)
CX_23_1 = tensor(ket0*ket0.dag(), I) + tensor(ket1*ket1.dag(), X)
B = CX_23_1*W_2
U = CZ_13*CX_23*W_1*CX_12 # Operateur d'evolution du circuit de la teleportation

#Generer l'etat EPR
ket00 = tensor(ket0, ket0)
EPR = B*ket00

# Definition de l'etat d'entree
ket0 = basis(2,0)
ket1 = basis(2,1)
Psi = (ket0+ket1)/sqrt(2)
Psi_in = tensor(Psi, EPR)

# Calcul de l'etat de sortie (Psi_out et Rho_out)
Psi_out = U*Psi_in
Rho_Bob = Psi_out.pttrace(2)
Prob = Psi.dag()*Rho_Bob*Psi

```

E.4.2 Téléportation d'une paire EPR

Une façon d'écrire ce programme en QuTiP est le suivant

```

# Teleportation d'une paire EPR

from qutip import *
from pylab import *

#Definitions des etats
ket0 = basis(2,0)
ket1 = basis(2,1)
Psi = (ket0+ket1)/sqrt(2)

# Definition des operateurs
X = sigmax()
Y = sigmay()
Z = sigmaz()
W = (X+Z)/sqrt(2)

```

```

I = qeye(2)

W_2 = tensor(I,W,I,I,I)
W_3 = tensor(W,I,I)
W_4 = tensor(I,I,I,W,I)
W_5 = tensor(I,I,I,I,W)

CX_12_1 = tensor(ket0*ket0.dag(), I) + tensor(ket1*ket1.dag(), X)
CX_12_2 = tensor(ket0*ket0.dag(), I, I) + tensor(ket1*ket1.dag(), X, I)
CX_13 = tensor(ket0*ket0.dag(), I, I) + tensor(ket1*ket1.dag(), I, X)
CX_14 = tensor(ket0*ket0.dag(),I,I,I,I) + tensor(ket1*ket1.dag(),I,I,X,I)
CX_23 = tensor(I,ket0*ket0.dag(),I,I,I) + tensor(I,ket1*ket1.dag(),X,I,I)
CX_24 = tensor(I,ket0*ket0.dag(),I,I,I) + tensor(I,ket1*ket1.dag(),I,X,I)
CX_34 = tensor(I,I,ket0*ket0.dag(),I,I) + tensor(I,I,ket1*ket1.dag(),X,I)
CX_35 = tensor(I,I,ket0*ket0.dag(),I,I) + tensor(I,I,ket1*ket1.dag(),I,X)
CX_54 = tensor(I,I,I,I,ket0*ket0.dag()) + tensor(I,I,I,X,ket1*ket1.dag())
CX_53 = tensor(I,I,I,I,ket0*ket0.dag()) + tensor(I,I,X,I,ket1*ket1.dag())
CX_51 = tensor(I,I,I,I,ket0*ket0.dag()) + tensor(X,I,I,I,ket1*ket1.dag())

#Definitions des etats
ket0 = basis(2,0)
ket1 = basis(2,1)
Psi = (ket0+ket1)/sqrt(2)
# Generation des etats EPR et GHZ
EPR = CX_12_1*tensor(Psi, ket1)
GHZ = CX_13*CX_12_2*W_3*tensor(ket0, ket0, ket0)
#etat d'entree
Psi_in = tensor(EPR,GHZ)

# Operateur d'evolution du circuit
U = CX_51*W_5*CX_14*CX_54*CX_35*W_4*CX_24*W_4*CX_34*W_2*CX_23*W_2

# Calcul de l'etat de sortie du circuit
Psi_out = U*Psi_in
Rho_5 = Psi_out.ptrace(4)

# Comparaison : calcul de la probabilite
Proba = Psi.dag()*Rho_5*Psi

```

- [MLB2005] Michel Le Bellac, *Introduction à l'Information Quantique*, Belin, 2005.
- [VSC2004] Valerio Scarani, *Initiation à la Physique Quantique*, Vuibert, 2004.
- [BCS2004] Giuliano Benenti, Giulio Casati and Giuliano Strini, *Principles of Quantum Computation and Information, Vol.I*, World Scientific, 2004.
- [MLB2003] Michel Le Bellac, *Physique Quantique*, 2e Édition, CNRS ÉDITIONS, 2007.
- [MNIC2000] Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [JPresk1998] John Preskill, *Lecture note on quantum information and computation*, <http://theory.caltech.edu/people/preskill/>
- [SCHWWW] C. Schiller, *Motion Mountain*, www.motionmountain.org