

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITE DE MOSTAGANEM
Abd el Hamid Ibn Badis



Faculté des Sciences Exactes et d'Informatique
Département de Mathématiques-Informatique

Mémoire de Master en mathématiques
Option : Analyse Harmonique et EDP

Intitulé

INFORMATION QUANTIQUE ET SON
APPLICATION À LA TRANSFORMATION DE
FOURIER

Présenté par
Benhenni Hakima

Soutenu le : 22 /06/2013.

Devant les membres du jury :

Présidente : M. HAMANI, Maître de Conférence A, Université de Mostaganem.

Examineur : Monsieur LAID Maître Assistant A, Université de Mostaganem.

Encadreur : A. BENBERNOU, Professeur, Université de Mostaganem.

Année universitaire : 2012-2013

UNIVERSITÉ ABDELHAMID IBN BADIS-MOSTAGANEM
FACULTÉ DES SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES



MÉMOIRE
DE MASTER DE MATHÉMATIQUES

Information quantique et son application
à la transformation de Fourier.

Présenté par
Benhenni Hakima

Soutenu le 22 /06 / 2013 devant le Jury

M. HAMANI	Président	MCA	U. MOSTAGANEM
Amina LAHMAR-BENBERNOU	Encadreur	Prof	U. MOSTAGANEM
Monsieur LAID	Examineur	MAA	U. MOSTAGANEM

Dédicaces

Je dédie ce travail

A mes parents

A mes soeur, mes frère

A ma famille. A mes amis, en particulier à toute personne aide Hakima.

Remerciements

Je tiens à remercier

Amina LAHMAR-BENBERNOU professeur à l'université de Mostaganem, qui a accepté la direction de ce mémoire, et a mis à notre disposition tous les moyens nécessaires ainsi que ses conseils et sa présence pendant la réalisation de ce travail.

M^{me}. HAMANI Maître de conférence A à l'université de Mostaganem, qui me fait l'honneur de présider ce jury.

Monsieur LAID Maître assistant A à l'université de Mostaganem, qui a bien voulu s'intéresser à ce travail et me fait l'honneur de participer au jury.

Résumé :

Dans ce travail, nous avons s'intéressé à l'information quantique, plus précisément nous avons s'intéressé au qubit quantique, qui est plus puissant que bit classique, puis nous avons vu les postulats de la mécanique quantique, en fin nous avons étudié la transformation de Fourier quantique et son application à la recherche de la période d'une fonction.

Table des matières

Introduction	1
1 Information Quantique	2
1.1 Bit classique et qubit quantique	2
1.1.1 Bit classique [2]	2
1.1.2 Qubit quantique [3]	2
1.1.3 Propriétés d'un qubits	3
1.1.4 Représentation géométrique d'un qubit [3]	3
1.1.5 Réalisation physique d'un qubit	7
1.2 Les postulats de la mécanique quantique [1]	11
2 intrication quantique [4]	15
2.1 Etat à deux qubit	15
2.1.1 Définition d'état à deux qubit	15
2.1.2 Mesure d'un état à deux qubit	17
3 Transformation de Fourier quantique [9] et [10]	18
3.1 Algorithme de Shor :	18
3.2 Transformation de fourier quantique	18
3.3 Recherche à la période d'une fonction [11]	21

4	Annexe	23
4.1	Le photon [12]	23
4.2	Espace de Hilbert	23
4.3	Espace hermitien	23
4.4	Produit scalaire [13].	24
4.5	Produits Tensoriels	24
4.6	Définition de l'observable	25
4.7	Rappel de quelques définitions sur les opérateurs et les matrices	25
4.8	La biréfringence	25
4.9	Opérateur hermitien	26
4.10	Opérateur hamiltonien	26
4.11	Fonction trace [8]	26

Introduction

En 1982. L'information quantique a été constaté par Richard Feynman, qui était difficile de simuler des systèmes quantiques par ordinateur classique, cette difficulté provient de la propriété que possèdent ces systèmes de pouvoir se trouver simultanément dans une superposition d'états quantiques. Il propose alors de construire un ordinateur quantique qui exploiterait et permettrait ainsi de simuler efficacement le comportement de tout système quantique.

L'information Quantique consiste à exploiter les propriétés quantiques fondamentales de cette superposition, afin de communiquer de façon plus sécurisée (« communication quantique ») et traiter l'information efficacement (calcul quantique).

L'information Quantique a connu depuis 20 ans essor.

Ce mémoire contient trois chapitres, dans le premier chapitre on a le qubit (bit quantique), sa différence avec le bit classique sa représentation géométrique, sa réalisation physique, et les postulats de la mécanique quantique mis en place étudié.

Dans le deuxième chapitre, on a l'état à deux qubits, et sa mesure.

Dans le troisième chapitre on a la transformation de Fourier quantique, et son application à la recherche de la période d'une fonction.

Information Quantique

Pour stocker les informations le système utilise est le système binaire, appelé bit classique possèdent deux états "0" ou "1". Pour l'avancé technologie l'homme s'est développé, et utilise un système à deux niveaux, qui on appelle qubit (bit quantique), plus puissant que le premier, ce dernier peut stocker des informations dans plusieurs états, que nous définissons ci-dessous.

1.1 Bit classique et qubit quantique

1.1.1 Bit classique [2]

- À l'heure actuelle, la plupart des systèmes de communication ou de traitement de l'information sont basés sur une entité fondamentale que nous appelons le bit. Ce bit est un chiffre binaire qui peut prendre deux valeurs "0" ou "1".

1.1.2 Qubit quantique [3]

- Un qubit est un terme du domaine naissant de l'informatique quantique qui est une forme abrégée de l'expression (bit quantique).

Un mémoire à qubits diffère significativement d'un mémoire classique.

Un bit classique se trouve toujours soit dans l'état 0, soit dans 1. Un qubit peut quant à lui être soit dans l'état 0, soit dans l'état 1, soit dans une superposition de 0 et 1. Mais ce n'est pas un troisième état, c'est une infinité d'autres états. Tout qubit est de la forme :

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{1.1}$$

où les coefficients α, β sont des nombres complexes vérifiant la condition de normalisation :
 $|\alpha|^2 + |\beta|^2 = 1$.

L'état du qubit est un vecteur d'un espace vectoriel complexe de dimension 2 dans lequel les éléments $|0\rangle$ et $|1\rangle$ forment une base orthonormée dite base de calcul.

1.1.3 Propriétés d'un qubits

– Si on pose $\alpha = \cos \theta$ et $\beta = \sin \theta$, le qubit peut aussi s'écrire :

$$|\Psi\rangle = \cos \theta |0\rangle + \exp(i\varphi) \sin \theta |1\rangle$$

avec $\theta \in [0, \frac{\pi}{2}]$, et $\varphi \in [0, 2\pi]$.

Car

$$|\cos \theta|^2 + |\exp(i\varphi) \sin \theta|^2 = 1.$$

Donc la condition de normalisation est vérifiée.

- La mesure de la valeur du qubit, est obtenu ce forme 0 ou 1, Après mesure, le qubit se trouve dans l'état mesuré.
- La probabilité de mesurer l'état 0 vaut $|\alpha|^2$, tandis que celle de mesurer l'état 1 vaut $|\beta|^2$.
- Le qubit ne peut pas être dupliqué. En effet, pour le dupliquer, il faudrait pouvoir de mesurer α et β d'un qubit (tout en préservant l'état du qubit), de sorte à préparer un autre qubit dans le même état $\alpha |0\rangle + \beta |1\rangle$. ceci est doublement :
 1. il est impossible de lire un qubit sans détruire définitivement son état (puisque après mesure le qubit est dans l'état mesuré).
 2. une mesure de qubit ne donne (et ne peut donner) aucune information sur α et β puisque le résultat soit $|0\rangle$, soit $|1\rangle$ ce qui équivaut à $(\alpha, \beta) = (1, 0)$ ou $(0, 1)$, ce qui ne correspond pas aux valeurs initiales de α et β .

1.1.4 Représentation géométrique d'un qubit [3]

1. Sur une sphère de Bloch-Poincaré :

Définition 1.1 La sphère de Bloch-Poincaré est la représentation géométrique dans un espace \mathbb{R}^3 , de l'ensemble $D(2)$ des états quantiques à deux dimension 2.

Nous pouvons définir les qbits à l'aide de ces deux paramètres, et les représenter sur une sphère, dite sphère de Bloch-Poincaré, comme le montre la Fig. 1.2, où l'état quantique est de la forme :

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right) \exp\left(-i\frac{\varphi}{2}\right) |0\rangle + \exp\left(+i\frac{\varphi}{2}\right) \sin\left(\frac{\theta}{2}\right) |1\rangle, \quad \text{avec } 0 \leq \varphi < 2\pi \text{ et } 0 \leq \theta < \pi.$$

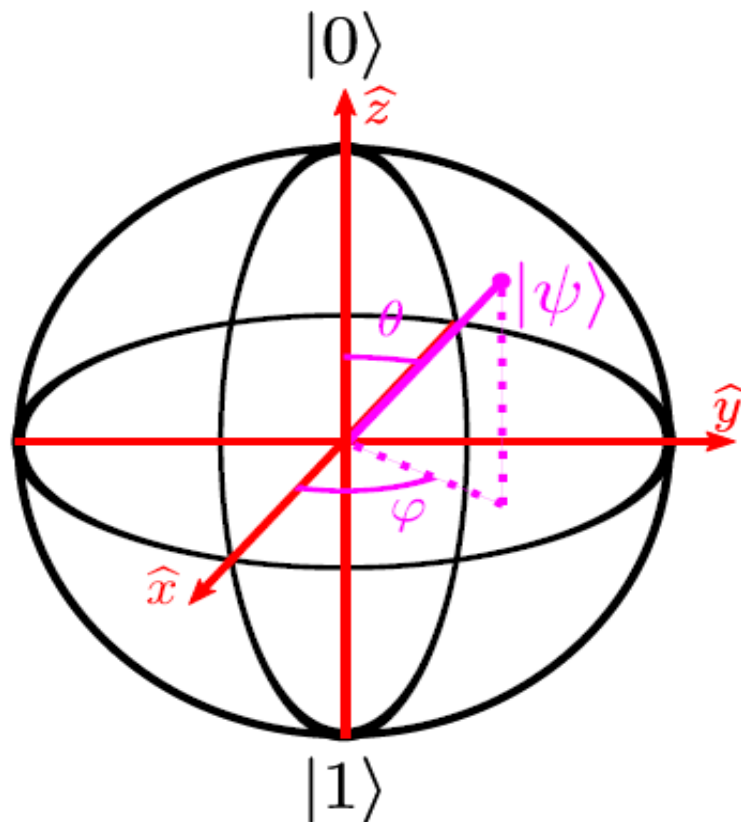


Fig 1.2- Representation d'un qubit sur une sphere de Bloch-poincare.

Où $|0\rangle$ correspond à l'angle θ , et $|1\rangle$ correspond à l'angle φ .

1. Représentation à l'aide de sa matrice de densité d'état :

Rappel :

$SU(E)$ est un sous groupe de $U(E)$, où $U(E)$ est un groupe des matrices unitaires à coefficients complexes de dimensions $n \times n$ et de déterminant 1, et E est un espace hermitien.

Exemple 1.1 $SU(2) = \left\{ \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}$.

Définition 1.2 (*Matrice de Pauli*)[8]

Les matrices de Pauli, développées par Wolfgang Pauli, forment une base de l'algèbre de Lie du groupe $SU(2)$. Elles sont définies comme l'ensemble des matrices de dimensions 2×2 suivantes :

$$\begin{aligned} X &\stackrel{\text{def}}{=} \sigma_0 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & X &\stackrel{\text{def}}{=} \sigma_1 \text{ (ou } \sigma_x) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ Y &\stackrel{\text{def}}{=} \sigma_2 \text{ (ou } \sigma_y) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, & Z &\stackrel{\text{def}}{=} \sigma_3 \text{ (ou } \sigma_z) \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

Ces matrices satisfont les égalités suivantes :

$$\text{et } \begin{aligned} \sigma_x^2 &= \sigma_y^2 = \sigma_z^2 = 1 \\ \sigma_x \sigma_y &= i \sigma_z \end{aligned} .$$

On rappelle définition de quelques états quantiques :

$$\begin{aligned} |0\rangle &= |\rightarrow\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & |1\rangle &= |\uparrow\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ |\nearrow\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|\rightarrow\rangle + |\uparrow\rangle) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & |\searrow\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|\rightarrow\rangle - |\uparrow\rangle) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ |\odot\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|\rightarrow\rangle + i|\uparrow\rangle) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, & |\ominus\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|\rightarrow\rangle - i|\uparrow\rangle) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \end{aligned} \quad (1.2)$$

Définition 1.3 (*Matrice densité d'état*)[7]

La matrice densité, ou opérateur densité est une entité mathématique introduite par le mathématicien et physicien John Von Neumann. Elle permet de résumer en une seule matrice tout l'ensemble possible des états quantiques d'un système physique donné à un instant donné, marquant ainsi mécanique quantique et physique statistique.

La matrice de densité p étant hermitienne, peut donc s'écrire sous la forme :

$$p = aI + bX + cY + dZ, \text{ avec } a, b, c, d \in \mathbb{R}.$$

Aussi, comme $\text{tr}(p) = 1$, il faut que

$$\begin{aligned} 1 &= \text{tr}(p) \\ &= \text{tr}(aI + bX + cY + dZ) \\ &= a \text{tr}(I) + b \text{tr}(X) + c \text{tr}(Y) + d \text{tr}(Z) \\ &= 2a \end{aligned}$$

puisque $\text{tr}(I) = 2$, tandis que $\text{tr}(X) = \text{tr}(Y) = \text{tr}(Z) = 0$,

on pose

$$r_1 = 2b, r_2 = 2c, r_3 = 2d$$

donc on obtient :

$$p = \frac{1}{2} (I + \vec{r} \cdot \vec{\sigma})$$

avec \vec{r} le vecteur de Bloch, défini par :

$$\vec{r} = \begin{pmatrix} r_x \\ r_y \\ r_z \end{pmatrix} = \begin{pmatrix} \sin 2\theta \cos \varphi \\ \sin 2\theta \sin \varphi \\ \cos 2\theta \end{pmatrix}$$

e $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ les matrices de Pauli qui ont été définies précédemment.

Ces trois matrices ne commutent pas, nous pouvons alors définir trois bases conjuguées à partir de leurs vecteurs propres.

Les bases sont définies d'après 1.2 par les vecteurs :

$$\begin{cases} |0_z\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1_z\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{cases}$$

qui est la base usuelle pour décrire les qubits :

$$\begin{cases} |0_y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0_z\rangle + |1_z\rangle}{\sqrt{2}} \\ |1_y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{|0_z\rangle - |1_z\rangle}{\sqrt{2}} \end{cases}$$

$$\begin{cases} |0_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{|0_z\rangle + i|1_z\rangle}{\sqrt{2}} \\ |1_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} = \frac{|0_z\rangle - i|1_z\rangle}{\sqrt{2}} \end{cases}$$

1.1.5 Réalisation physique d'un qubit

Etat interne d'un qubit

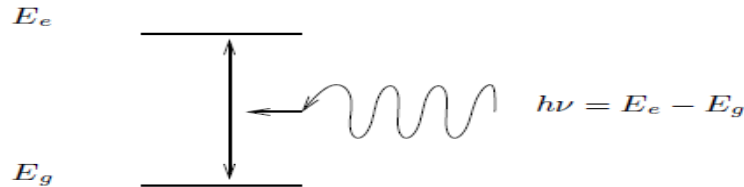


Fig 1.3- Atome a deux niveaux.

Par exemple dans le diagramme ci-contre on considère deux niveaux de l'atome :

- le niveau fondamentale : c'est ce lui le plus basse énergie, l'état quantique de l'atome est noté $|g\rangle$ et son énergie E_g .
- le premier niveau excité ; l'état atomique est noté $|e\rangle$ et son énergie E_e .

Si on envoi sur l'atome dans son état fondamental un photon d'énergie exactement $E_e - E_g$ le photon est absorbé (Absorbation, (fig 1.4)) par l'atome qui passe dans le niveau excité : $|g\rangle \rightarrow |e\rangle$. Les énergies mises en jeu atomique à l'échelle atomique sont de l'ordre de l'électron-volt ($1,6 * 10^{-19}j$), le rayonnement lumineux associé au photon à une longueur d'onde : $\lambda = \frac{c}{\nu} = \frac{hc}{E_e - E_g}$ où c la vitesse de la lumière (3.10^8ms^{-1}) et h la constante de Planck ($6,6 * 10^{-34}js$), l'ordre de grandeur des longueurs d'onde correspondant aux énergies atomiques de l'ordre eV est entre $0,4$ et $1\mu m$, c'est le domaine de la lumière visible.

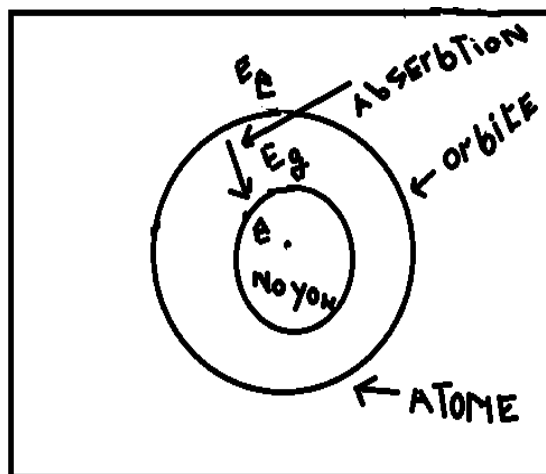


Fig 1.4- L'absorbation de l'Atome.

L'atome revient dans son état fondamentale au bout d'un temps moyen appelé durée de vie de niveau excité, en émettant un photon de même énergie $E_e - E_g$ (émission spontanée). La durée de vie d'un niveau atomique varie de quelques nanosecondes à la seconde.

Si on envoie un photon d'énergie $E_e - E_g$ sur l'atome quand il est encore dans l'état excité, l'atome va se désexciter en émettant un photon à la même énergie (émission induite (fig 1.5)).

Supposons qu'on éclaire continuellement l'atome avec cette radiation lumineuse composée de photons d'énergie $E_e - E_g$ (radiation résonante), l'atome va osciller entre l'état $|g\rangle$ à l'état $|e\rangle$. A l'instant t il sera dans un état de superposition

$$|\Psi\rangle = \cos\left(\frac{wt}{2}\right)|g\rangle + \sin\left(\frac{wt}{2}\right)|e\rangle \exp(i\varphi) \quad (1.3)$$

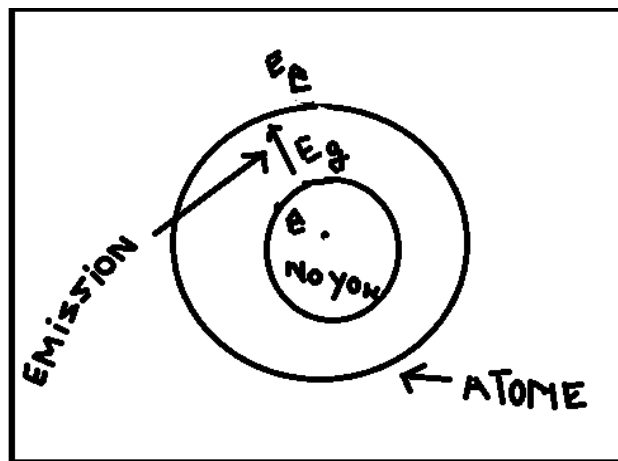


Fig 1.5- L'émission de l'Atome.

On voit que si on associe à l'état $|g\rangle$ le qubit est $|0\rangle$ et à l'état $|e\rangle$ le qubit est $|1\rangle$ on peut, en jouant sur le temps d'éclairement, mettre l'atome dans n'importe quel état de superposition $\alpha|0\rangle + \beta|1\rangle$.

Pour mesurer l'état de l'atome à un moment donné, on envoie sur celui-ci une impulsion laser "accordée" sur une transition $|g\rangle \rightarrow |a\rangle$ qui n'a pas d'équivalent à partir de l'état $|e\rangle$. Si le photon est absorbé c'est que le système est dans l'état $|g\rangle$ sinon il est dans l'état $|e\rangle$.

Polarisation d'un photon

Définition 1.4 *La polarisation est une propriété des ondes vectorielles telles que la lumière décrivant l'orientation de leurs oscillations, le fait que ces ondes soient caractérisées par*

des vecteurs les différences des autres types d'ondes comme les ondes sonores, et implique ce phénomène de polarisation. Sachant que n_0 est l'indice de réfraction de la polarisation perpendiculaire à l'axe d'anisotropie du matériel, tandis que n_e est l'indice de réfraction de la polarisation parallèle à l'axe d'anisotropie.

Une onde électromagnétique, la lumière par exemple, peut être représentée mathématiquement par un champs vectoriel transverse, i.e. orthogonal à la direction de propagation. Dans un référentiel $(O, \hat{e}_x, \hat{e}_y, \hat{e}_z)$, de coordonnées (x, y, z) , choisi tel que l'onde se propage selon l'axe des z , le champ électrique est décrit par :

$$\overline{E}(t, z) = \overline{E}_0 \exp i (wt - kz)$$

où $\overline{E}_0 = E_{0x}\hat{e}_x + E_{0y}\hat{e}_y$. Le vecteur E_0 , vu comme un nombre complexe, définit la polarisation de l'onde. L'intensité de l'onde est proportionnelle au module au carré de \overline{E}_0 : $\|\overline{E}_0\|^2$.

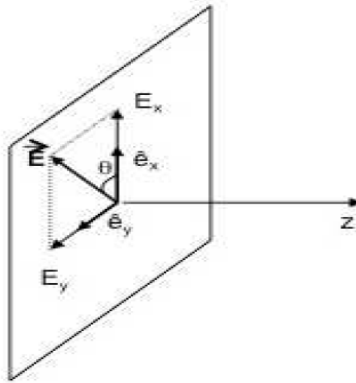


Fig 1.6- Onde polarise.

La polarisation peut être mise en évidence à l'aide de cristaux ayant une propriété optique particulière :

la biréfringence (voir Annexe 8). Si nous envoyons sur une lame biréfringente un faisceau d'intensité I , polarisé linéairement suivant une direction qui fait un angle θ avec l'axe ordinaire du cristal qu'on prend comme axe O_x : le faisceau est séparé en un faisceau polarisé suivant O_x d'intensité $I \cos 2\theta$ et un autre faisceau polarisé suivant O_y d'intensité $I \sin 2\theta$.

Planck et Einstein ont suggéré au début du XXème siècle que la lumière puisse aussi être décrite en termes de flot de photons. Les sources de lumière "classiques" émettent des grandes

quantités de photons même pour des faibles intensités (plusieurs milliards de milliards de photons à la seconde pour une lampe de 1w) ce qui fait que l'aspect "corpusculaire" de la lumière est difficile à mettre en évidence. L'avènement récent de l'optique quantique et des nanotechnologies a permis de développer des sources qui émettent des photons "un par un", c'est à dire séparés par des intervalles de temps mesurables avec la technologie actuelle (nanoseconde).

Comment interpréter l'expérience du dédoublement du faisceau lumineux dans une lame biréfringente si on considère le faisceau comme un flot discret de photons ? Quand un photon arrive à l'entrée de la lame, quel chemin va-t-il choisir ? Comment se fait-il qu'une fraction $\cos 2\theta$ va passer d'un côté et qu'une fraction $\sin 2\theta$ va passer de l'autre ?

La réponse est donnée par la mécanique quantique : le photon est un "objet quantique" ; on associe un état quantique à chaque vecteur de base de polarisation de l'onde : $|x\rangle$ pour l'état de polarisation suivant l'axe O_x et $|y\rangle$ pour l'état de polarisation suivant l'axe O_y . A l'orientation θ de la polarisation on associe l'état

$$|\Psi\rangle = \cos \theta |x\rangle + \sin \theta |y\rangle \quad (1.4)$$

En jouant sur l'orientation du polariseur et sur le type de polarisation (linéaire, circulaire, elliptique) on peut construire là aussi un état quelconque de superposition $\alpha |1\rangle + \beta |0\rangle$.

1.2 Les postulats de la mécanique quantique [1]

Postulat 1 : Définition de l'état quantique

A un instant $t = t_0$ donné, l'état d'un système est décrit par la donnée d'un ket $|\Psi(t = t_0)\rangle$ appartenant à l'espace des états ε .

Explication :

Dans notre espace de Hilbert H à deux dimensions, on peut utiliser la représentation matricielle

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in H, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in H. \quad (1.5)$$

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \rightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in H, \quad \langle \Psi | \stackrel{\text{def}}{=} |\Psi\rangle^\dagger = (\bar{\alpha}, \bar{\beta}) \quad (1.6)$$

Dans ce postulat les coefficients α et β sont des amplitudes de probabilité et qu'ils doivent satisfaire :

$$|\alpha|^2 + |\beta|^2 = 1. \quad (1.7)$$

Postulat 2 : Définition d'un observable

Toute grandeur physique mesurable A est décrite par un opérateur \hat{A} agissant sur ε .
Cet opérateur est une observable.

Les opérateurs associés aux propriétés observables sont définis par des règles de construction qui reposent sur un principe de correspondance :

Opérateur	la forme générale :
L'opérateur de position	$\hat{Q} = r$
L'opérateur d'énergie potentielle classique ou électromagnétique	$\hat{V}(r) = V_d(r)$
L'opérateur de quantité de mouvement	$\hat{P}(r) = -i\hbar\nabla$, où ∇ désigne le gradient des coordonnées r .
L'opérateur de moment angulaire	$\hat{L}(r) = \hat{Q} * \hat{P}$
L'opérateur d'énergie cinétique	$\hat{K}(r) = \frac{\hat{P} * \hat{P}}{2m} = -\frac{\hbar^2}{2m} \nabla^2$
L'opérateur d'énergie totale, appelé hamiltonien	$\hat{H} = \hat{K} + \hat{V} = \hat{K}(r) + V_d(r)$
L'opérateur action du système, appelé lagrangien	$\hat{L} = \hat{K} - \hat{V}$

Postulat 3 : Valeurs possibles d'une observable

La mesure d'une grandeur physique A ne peut donner comme résultat qu'une des valeurs propres a_n de l'observable A correspondante.

Explication :

Les vecteurs propres et les valeurs propres de cet opérateur ont une signification spéciale : les valeurs propres sont les valeurs pouvant résulter d'une mesure idéale de cette propriété, les vecteurs propres étant l'état quantique du système lors de cette mesure. En utilisant la notation bra-ket, ce postulat peut s'écrire ainsi :

$$\hat{A} |\alpha_n\rangle = a_n |\alpha_n\rangle$$

où \hat{A} , α_n et a_n désignent, respectivement, l'observable, le vecteur propre et la valeur propre correspondante.

Les états propres de tout observable \hat{A} sont complets et forment une base orthonormée dans l'espace de Hilbert.

Cela signifie que tout vecteur $|\Psi(t)\rangle$ peut se décomposer de manière unique sur la base de ces vecteurs propres ($|\phi_i\rangle$) :

$$\Psi = c_1 |\phi_1\rangle + c_2 |\phi_2\rangle + \dots + c_n |\phi_n\rangle$$

Postulat 4 : Probabilité d'obtention d'une valeur d'une observable

La mesure d'une grandeur physique représentée par l'observable A , effectuée sur l'état quantique (normalisé) $|\Psi(t)\rangle$, donne le résultat a_n , avec la probabilité p_n égale à $|c_n|^2$.

Explication

Le produit scalaire d'un état et d'un autre vecteur (qu'il appartienne ou non à H) fournit une amplitude de probabilité, dont le carré correspond à une probabilité ou une densité de probabilité de la façon suivante :

- Pour un système constitué d'une seule particule, la fonction d'onde $\Psi_\alpha(r) = \langle r|\alpha\rangle$ est l'amplitude de probabilité que la particule est à la position r . La probabilité $P_\alpha(r)$ de trouver la particule entre r et $r + dr$ est :+8

$$P_\alpha(r) = |\langle r|\alpha\rangle|^2 d^3r$$

Donc $P_\alpha(r) = |\langle r|\alpha\rangle|^2$ est une densité de probabilité.

- Si le système est dans un état $|\alpha\rangle$, alors l'amplitude de probabilité $C_{\beta\alpha}$ et la probabilité $P_{\beta\alpha}$ de le retrouver dans tout autre état sont :

Ni $|\alpha\rangle$, ni $|\beta\rangle$ ne doivent être nécessairement un état propre d'un opérateur quantique.

- Dans l'éventualité où un système peut évoluer vers un état $|\alpha, t\rangle$ au temps t par plusieurs trajets différents, alors, pour autant que l'on n'effectue pas de mesure pour déterminer quel trajet a été effectivement suivi $|\alpha, t\rangle$, est une combinaison linéaire des états $|\alpha_j, t\rangle$ où j spécifie le trajet :

$$|\alpha, t\rangle = \sum w_j |\alpha_j, t\rangle$$

où w_j sont les coefficients de la combinaison linéaire. L'amplitude $C_{\beta\alpha}(t) = |\langle\beta|\alpha, t\rangle|$ devient alors la somme des amplitudes $C_{\beta\alpha_j}(t)$ et la probabilité $P_{\beta\alpha}(t)$ contient des termes d'interférence :

$$C_{\beta\alpha}(t) = |\langle\beta|\alpha, t\rangle|^2 = \left| \sum w_j \langle\beta|\alpha_j, t\rangle \right|^2 = \left| \sum w_j C_{\beta\alpha_j}(t) \right|^2$$

Mais si une mesure a déterminé que le trajet k a été suivi, alors les coefficients deviennent $w_j \rightarrow \delta_{jk}$ et les sommes précédentes se réduisent à un seul terme.

- En supposant que le système se trouve dans un état $|\alpha\rangle$, alors la prédiction théorique de la valeur moyenne de la mesure de l'observable est donnée par :

$$\langle \hat{A} \rangle_\alpha = \langle \alpha | \hat{A} | \alpha \rangle$$

L'évolution de l'état quantique entre deux mesures est gouvernée par un nouveau postulat, appelé **postulat d'évolution**.

Postulat 5 : postulat d'évolution

L'évolution dans le temps de $|\Psi\rangle$ est régie par l'équation de Schrödinger

$$i\hbar \frac{d|\Psi(t)\rangle}{dt} = \hat{H}(t) |\Psi(t)\rangle \text{ ou } H \text{ est le hamiltonien.}$$

Entre deux mesures le système quantique évolue avec le temps. Soit $\Psi(t)$ la fonction d'onde normée décrivant l'état dynamique du système à l'instant t .

Cette évolution de l'état résulte de l'application d'un opérateur linéaire, appelé opérateur d'évolution qui est de la forme :

$$|\Psi(t_0)\rangle \rightarrow |\Psi(t)\rangle = T(t, t_0) |\Psi(t_0)\rangle.$$

L'opérateur possède une propriété particulière qui résulte de la conservation de la norme de

l'état quantique au cours du temps. En effet on doit avoir

$$\begin{aligned}\langle \Psi(t_0) | \Psi(t_0) \rangle &= 1 \\ &= \langle \Psi(t) | \Psi(t) \rangle \\ &= \langle \Psi(t_0) T^\dagger T | \Psi(t_0) \rangle \quad \text{où } U^\dagger = \overline{(U^t)} \\ \implies T^\dagger T &= T T^\dagger = I\end{aligned}$$

d'où l'opérateur est unitaire.

La question est de savoir quel est cet opérateur unitaire

En fait, l'évolution temporelle de l'état est gouvernée par la célèbre équation de Schrödinger

$$i\hbar \frac{d}{dt} |\Psi(t)\rangle = H |\Psi(t)\rangle$$

où H est l'opérateur hamiltonien, c'est-à-dire l'opérateur quantique associé à l'observable "énergie totale du système".

La solution formelle de cette équation est :

$$|\Psi(t)\rangle = \exp\left(-i\frac{t-t_0}{\hbar}H\right) |\Psi(t_0)\rangle$$

de laquelle on déduit

$$T(t, t_0) = \exp\left(-i\frac{t-t_0}{\hbar}H\right)$$

intrication quantique [4]

Définition 2.1 Soit $|\Psi\rangle \in H^{2n}$, cet état est dit intriqué s'il n'existe pas d'état : $|\Psi\rangle_1 \in H^{2p}$ et $|\Psi\rangle_2 \in H^{2q}$ tels que : $|\Psi\rangle = |\Psi\rangle_1 \otimes |\Psi\rangle_2$ et $n = p + q$.

2.1 Etat à deux qubit

2.1.1 Définition d'état à deux qubit

Nous avons étudié au premier chapitre l'état d'un seul qubit, sa forme est introduit par la formule 1.1 ,et dans ce chapitre nous avons intéressé à l'état a deux qubits, pour cela, on prend deux qubit A et B ,où le premier qubit, A , est dans un espace de Hilbert H_A , dont une base orthonormée est $\{|0_A\rangle, |1_A\rangle\}$, et le second qubit B , est dans un espace de Hilbert H_B , dont une base orthonormée est $\{|0_B\rangle, |1_B\rangle\}$. Il est naturel de représenter un état physique où le premier qubit est dans l'état $|0_A\rangle$ et le second dans l'état $|0_B\rangle$ par un vecteur que l'on écrit $|X_{00}\rangle = |0_A \otimes 0_B\rangle$, en prenant en compte les autres valeurs possibles de qubits on aura quatre possibilités

$$|X_{00}\rangle = |0_A \otimes 0_B\rangle, \quad |X_{01}\rangle = |0_A \otimes 1_B\rangle, \quad |X_{10}\rangle = |1_A \otimes 0_B\rangle, \quad |X_{11}\rangle = |1_A \otimes 1_B\rangle$$

Donc le qubit A est dans

$$|\varphi_A\rangle = \alpha |0_A\rangle + \beta |1_A\rangle, \quad \text{où } (\alpha, \beta) \in \mathbb{C}^2, \quad \text{et } |\alpha|^2 + |\beta|^2 = 1$$

et le qubit B dans

$$|\varphi_B\rangle = \gamma |0_B\rangle + \delta |1_B\rangle, \quad \text{où } (\gamma, \delta) \in \mathbb{C}^2, \quad \text{et } |\gamma|^2 + |\delta|^2 = 1.$$

Donc le système a deux qubits (A, B) , qui l'on note $|\varphi_A \otimes \varphi_B\rangle$ est décrit comme suit :

$$\begin{aligned} |\varphi_A \otimes \varphi_B\rangle &= \alpha\gamma|0_A \otimes 0_B\rangle + \alpha\delta|0_A \otimes 1_B\rangle + \beta\gamma|1_A \otimes 0_B\rangle + \beta\delta|1_A \otimes 1_B\rangle \\ &= \alpha\gamma|X_{00}\rangle + \alpha\delta|X_{01}\rangle + \beta\gamma|X_{10}\rangle + \beta\delta|X_{11}\rangle \end{aligned} \quad (2.1)$$

Les physiciens sont assez laxistes sur les notations, et on trouvera au lieu de $|\varphi_A \otimes \varphi_B\rangle$, soit $|\varphi_A\rangle \otimes |\varphi_B\rangle$, soit même $|\varphi_A\varphi_B\rangle$, en omettant le symbole du produit tensoriel.

Le point crucial est que l'état le plus général de $H_A \otimes H_B$ n'est pas de la forme produit tensoriel $|\varphi_A \otimes \varphi_B\rangle$:

les états de la forme $|\varphi_A \otimes \varphi_B\rangle$ ne forment qu'un petit sous-ensemble des vecteurs de $H_A \otimes H_B$. L'état le plus général est de la forme

$$\begin{aligned} |\Psi\rangle &= \alpha_{00}|0_A \otimes 0_B\rangle + \alpha_{01}|0_A \otimes 1_B\rangle + \alpha_{10}|1_A \otimes 0_B\rangle + \alpha_{11}|1_A \otimes 1_B\rangle \\ &= \alpha_{00}|X_{00}\rangle + \alpha_{01}|X_{01}\rangle + \alpha_{10}|X_{10}\rangle + \alpha_{11}|X_{11}\rangle \end{aligned} \quad (2.2)$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \quad (2.3)$$

et pour que $|\Psi\rangle$ soit de la forme $|\varphi_A \otimes \varphi_B\rangle$, une condition nécessaire (et suffisante) est que

$$\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}$$

ce qui n'a aucune raison d'être valide a priori. Donnons un exemple très simple d'un état $|\Phi\rangle$ qui n'est pas de la forme $|\varphi_A \otimes \varphi_B\rangle$

$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|0_A \otimes 1_B\rangle - |1_A \otimes 0_B\rangle)$$

en effet

$$\alpha_{00} = 0, \quad \alpha_{01} = \frac{1}{\sqrt{2}}, \quad \alpha_{10} = -\frac{1}{\sqrt{2}}, \quad \alpha_{11} = 0$$

Donc, il est clair qu'il existe des états qui ne pouvant pas se factoriser en un produit d'états à un qubit, on appelle ces états, états intriqué.

Une exemple particulièrement utilisé d'état intriqué est le premier état de Bell défini par

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \quad (2.4)$$

Tant qu'aucune mesure n'est effectuée sur le système l'état de chaque qubit n'est pas défini. Supposons que nous mesurons le premier état et que nous trouvons l'état $|0\rangle$. Cela signifie que l'état $|\beta_{00}\rangle$ est projeté sur l'état $|00\rangle$ ce qui entraîne que le deuxième qubit est forcément lui aussi dans l'état $|0\rangle$ [5].

2.1.2 Mesure d'un état à deux qubit

La mesure d'état de deux qubits donne l'un des états de base $|00\rangle$, $|01\rangle$, $|10\rangle$ ou $|11\rangle$ avec une probabilité $|\alpha_{ij}|^2$ où α_{ij} sont les coefficients des états de base de décomposition de l'équation (2.2).

On peut effectuer une mesure partielle c'est-à-dire uniquement sur l'un des deux qubits. La mesure va fixer l'état de qubit mesuré ; l'état du système mesuré sera une superposition des états de base compatible avec l'état initiale et dans laquelle le qubit mesuré aura une valeur fixée.

Par exemple si on mesure le premier qubit pour un système dans l'état (2.2) et qu'on trouve $|0\rangle$ le système est projeté dans l'état

$$|\tilde{\Psi}\rangle = \frac{\alpha_{00}}{|\alpha_{00}|^2 + |\alpha_{01}|^2} |00\rangle + \frac{\alpha_{01}}{|\alpha_{00}|^2 + |\alpha_{01}|^2} |01\rangle.$$

Si maintenant l'état initiale du système est l'état de Bell $|\beta_{00}\rangle$ (équation 2.4) et que la mesure du premier bit donne $|0\rangle$ alors le système est projeté dans l'état $|00\rangle$ [5].

Transformation de Fourier quantique [9] et [10]

La transformé de Fourier quantique est une transformation introduite par Peter Shor. Cette opération unitaire est probablement la plus importante.

3.1 Algorithme de Shor :

Cet algorithme ainsi que plusieurs autres reposent sur la mise en oeuvre efficace de la transformation de Fourier sur un circuit quantique. En fait l'algorithme classique de transformée de Fourier rapide (FFT) nécessite $O(n2^n)$ opérations pour transformer un nombre de n bits. Nous allons voir que la TF quantique ne nécessite que $O(n^2)$ opérations : le gain est ici exponentiel.

3.2 Transformation de fourier quantique

On définit d'abord la transformation de Fourier classique :

Définition 3.1 (*Transformation de Fourier classique*) La transformée de Fourier classique d'un vecteur complexe X de N éléments (x_0, \dots, x_{N-1}) un autre vecteur complexe Y de N éléments (y_0, \dots, y_{N-1}) est définie par :

$$Y = F(X) \Leftrightarrow y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(\frac{2i\pi}{N}kj\right) x_j \quad (3.1)$$

Définition 3.2 (*Transformation de Fourier quantique*) Soit un espace de Hilbert H de dimension N , donc de la même manière, on définit la transformée de Fourier quantique (TFQ) par son action sur les vecteurs de la base orthonormée $|j_0\rangle, \dots, |j_{N-1}\rangle$

$$|j\rangle \xrightarrow{TFQ} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2i\pi}{N}kj\right) |k\rangle \quad (3.2)$$

L'équivalence avec la transformée de Fourier discrète est visible lorsqu'on applique la transformée de Fourier quantique à une superposition d'états :

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} \tilde{x}_k |k\rangle$$

Même si l'unitaristé d'une telle transformation n'est pas évidente au premier abord, on peut la décomposer en une série de transformations unitaires élémentaires. On suppose dans la suite que $N = 2^n$; cette hypothèse n'est à vrai dire pas très restrictive car elle est généralement faite aussi dans le cas de la transformée de Fourier discrète (l'algorithme de la transformée de Fourier rapide ne marche que pour N de la forme a^b). Le calcul s'effectue donc sur les vecteurs de base $|0\rangle \dots |2^n - 1\rangle$, et on note $j_1j_2\dots j_n$ la représentation binaire de j (où $j = j2^n - 1 + \dots + j_n2^0$), et $0j_lj_{l+1} + \dots + j_m$ la fraction binaire $\frac{j_l}{2} + \frac{j_{l+1}}{4} + \dots + \frac{j_m}{2^{m-l+1}}$.

On peut factoriser la transformation de Fourier quantique de la façon suivante :

$$\begin{aligned} |j\rangle &\rightarrow \frac{1}{2^{\frac{n}{2}}} \sum_{k=0}^{N-1} \exp\left(\frac{2i\pi}{2^n}kj\right) |k\rangle \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \exp\left(2i\pi j \left(\sum_{l=1}^n k_l 2^{-l}\right)\right) |k_1 \dots k_n\rangle \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \otimes_{l=1}^n \exp(2i\pi j k_l 2^{-l}) |k_l\rangle \\ &= \frac{1}{2^{\frac{n}{2}}} \otimes_{l=1}^n \left[\sum_{k_n=0}^1 \exp(2i\pi j k_l 2^{-l}) |k_l\rangle \right] \\ &= \frac{1}{2^{\frac{n}{2}}} \otimes_{l=1}^n (|0\rangle + \exp(2i\pi j 2^{-l}) |1\rangle) \\ &= \frac{1}{2^{\frac{n}{2}}} (|0\rangle + \exp(2i\pi 0 j_n) |1\rangle) \otimes (|0\rangle + \exp(2i\pi 0 j_{n-1} j_n) |1\rangle) \otimes \dots \otimes (|0\rangle + \exp(2i\pi 0 j_1 j_2 \dots j_n) |1\rangle) \end{aligned}$$

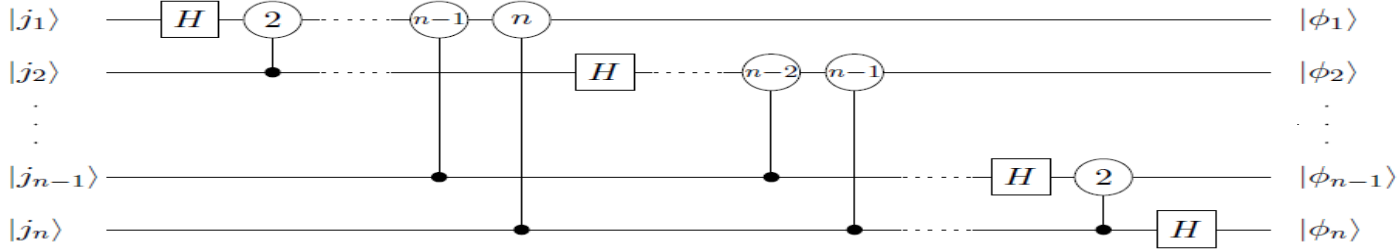


Fig 4.1-Circuit de la transformation de Fourier quantique.

Cette décomposition permet de concevoir aisément un circuit pour la transformée de Fourier quantique, comme celui de la figure 4.1, où

$$\boxed{k} \rightarrow \text{représente l'opérateur } \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}$$

Pour comprendre le fonctionnement de ce circuit, suivons son action sur $|j\rangle = |j_1 \dots j_n\rangle$. La première porte de Hadamard donne

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2i\pi 0 j_1) |1\rangle) |j_2 \dots j_n\rangle$$

Puis, la première rotation contrôlée ajoute un bit de phase supplémentaire suivant l'état de $|j_2\rangle$

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2i\pi 0 j_1 j_2) |1\rangle) |j_2 \dots j_n\rangle$$

Et ainsi de suite jusqu'à la rotation n

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2i\pi 0 j_1 j_2 \dots j_n) |1\rangle) |j_2 \dots j_n\rangle$$

De même, la deuxième série de porte de Hadamard et de rotations contrôlées conduisent à l'état

$$\frac{1}{\sqrt{2}} (|0\rangle + \exp(2i\pi 0 j_1 j_2 \dots j_n) |1\rangle) \cdot (|0\rangle + \exp(2i\pi 0 j_2 \dots j_n) |1\rangle) |j_3 \dots j_n\rangle$$

A la fin du circuit, nous obtenons donc l'état

$$\begin{aligned} & |\phi_1\rangle \otimes |\phi_2\rangle \otimes \dots \otimes |\phi_{n-1}\rangle \otimes |\phi_n\rangle \\ = & \frac{1}{\sqrt{2}} (|0\rangle + \exp(2i\pi 0 j_1 j_2 \dots j_n) |1\rangle) \cdot (|0\rangle + \exp(2i\pi 0 j_2 \dots j_n) |1\rangle) \dots (|0\rangle + \exp(2i\pi 0 j_n) |1\rangle) \end{aligned}$$

3.3 Recherche à la période d'une fonction [11]

L'algorithme de Shor repose sur la possibilité de trouver "rapidement" la période d'une fonction. Dans ce paragraphe nous allons voir comment l'algorithme de transformée de Fourier quantique permet de résoudre ce problème.

L'algorithme de Shor consiste en deux parties :

- I) Une réduction du problème de factorisation en un problème de recherche d'ordre, qui peut être effectué sur un ordinateur classique.
- II) Un algorithme quantique pour résoudre le problème de recherche d'ordre.

Partie classique

1. Prendre un nombre pseudo-aléatoire $a < N$.
2. Calculer le PGCD(a, N). Ceci peut être effectué par l'utilisation de l'algorithme d'Euclide.
3. Si $PGCD(a, N) \neq 1$, alors c'est un facteur non-trivial de N , donc effectué.
4. Autrement, utiliser le sous-programme de recherche de période (ci-dessous) pour trouver r , la période de la fonction suivante :

$$f(x) = a^x \bmod N$$

c.à.d. le plus petit entier r pour lequel $f(x+r) = f(x)$.

5. Si r est impair, retourner à l'étape 1.
6. Si $a^{\frac{r}{2}} = -1 \pmod{N}$, retourner à l'étape 1.
7. Les facteurs de N sont $PGCD(a^{\frac{r}{2}} \pm 1, N)$. Effectué.

Partie quantique : sous-programme de recherche de période

1. Commencer avec des registres d'entrée et de sortie de chacun $\log_2 N$ qubits, et les initialiser à :

$$N^{-\frac{1}{2}} \sum_x |x\rangle |0\rangle \text{ où } 0 \leq x \leq N-1.$$

2. Construire $f(x)$ comme une fonction quantique et l'appliquer à l'état précédent, pour obtenir

$$N^{-\frac{1}{2}} \sum_x |x\rangle |f(x)\rangle$$

3. Appliquer la transformée de Fourier quantique au registre d'entrée. La transformée de Fourier quantique sur N points est définie par :

$$U_{QFT} |x\rangle = N^{-\frac{1}{2}} \sum_y \exp\left(\frac{2\pi ixy}{N}\right) |y\rangle$$

Ce qui donne l'état suivant :

$$U_{QFT} |x\rangle = N^{-1} \sum_x \sum_y \exp\left(\frac{2\pi ixy}{N}\right) |y\rangle |f(x)\rangle.$$

4. Effectuer une mesure. On obtient ainsi une certaine valeur y dans le registre d'entrée et $f(x_0)$ dans le registre de sortie. Comme f est périodique, la probabilité de mesurer un certain y est donné par

$$\left| N^{-1} \sum_{x:f(x)=f(x_0)} \exp\left(\frac{2\pi ixy}{N}\right) \right|^2 = \left| N^{-1} \sum_b \exp\left(\frac{2\pi i(x_0 + rb)y}{N}\right) \right|^2$$

Le calcul montre que cette probabilité est plus haute quand $\frac{yr}{N}$ est proche d'un entier.

5. Mettre $\frac{y}{N}$ sous forme irréductible, et extraire le dénominateur r' , qui est un candidat pour r .
6. Vérifier si $f(x) = f(x + r')$. Si c'est le cas, c'est terminé.
7. Autrement, obtenir plus de candidats pour r en utilisant des valeurs proches de y , ou multiples de r' . Si un autre candidat marche, c'est terminé.
8. Sinon, retourner à l'étape 1 du sous-programme.

Annexe

4.1 Le photon [12]

Les photons ont originellement été appelés « quanta de lumière » (das Lichtquant) par Albert Einstein. Le nom moderne « photon » est dérivé du mot grec qui signifie soleil (translittéré phos, photos) et a été choisi en 1926 par le chimiste Gilbert N. Lewis, dans la publication d'une théorie spéculative dans laquelle les photons étaient « incroyables et indestructibles ». Bien que la théorie de Lewis ne fût jamais acceptée, étant contredite par plusieurs expérimentations, son nouveau nom, photon, fut adopté immédiatement par la communauté scientifique.

4.2 Espace de Hilbert

Un espace de Hilbert est un espace de Banach (donc complet) dont la norme découle d'un produit scalaire \langle, \rangle par la formule $\|x\| = \sqrt{\langle x, x \rangle}$. C'est la généralisation en dimension quelconque d'un espace euclidien ou hermitien [13].

4.3 Espace hermitien

Un espace hermitien est un espace vectoriel défini sur les nombres complexes, de dimension finie et disposant d'un produit hermitien, correspondant à une généralisation du cas réel [13].

4.4 Produit scalaire [13].

Soit H un espace vectoriel sur le corps des nombres complexes \mathbb{C} . On appelle "produit scalaire" sur H toute application de $H \times H$ dans \mathbb{C} , notée :

$$(u, v) \rightarrow (u|v)$$

qui vérifie les propriétés suivantes :

linéarité à droite : pour tous $u, v_1, v_2 \in H, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(u|\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (u|v_1) + \lambda_2 (u|v_2)$$

anti-linéarité à gauche : pour tous $u_1, u_2, v \in H, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(\lambda_1 u_1 + \lambda_2 u_2|v) = \bar{\lambda}_1 (u_1|v) + \bar{\lambda}_2 (u_2|v)$$

positivité : pour tout $u \in H$

$$(u|u) \geq 0$$

Définie : pour tout $u \in H$

$$(u|u) = 0 \Rightarrow u = 0.$$

Exemple 4.1 1. Dans l'espace \mathbb{R}^n , on définit le produit scalaire canonique :

$$((x_1, \dots, x_n) | (y_1, \dots, y_n)) = x_1 y_1 + x_2 y_2 + \dots + x_n y_n.$$

2. Dans l'espace \mathbb{C}^n , on définit le produit scalaire canonique :

$$((z_1, \dots, z_n) | (w_1, \dots, w_n)) = \bar{z}_1 w_1 + \dots + \bar{z}_n w_n.$$

4.5 Produits Tensoriels

Le produit tensoriel d'un tenseur p de $\otimes^p E$ et d'un tenseur q de $\otimes^q E$ est un tenseur de $\otimes^{p+q} E$ défini de la manière suivante (ici $p = 2, q = 3$) :

$$(p \otimes q)(u, v, x, y, z) = p(u, v) q(x, y, z) \quad \forall u, v, x, y, z \in E.$$

4.6 Définition de l'observable

Les observables sont des opérateurs définis sur l'espace d'Hilbert ou classiquement des fonctions réelles de $2N$ variables réelles.

4.7 Rappel de quelques définitions sur les opérateurs et les matrices

A est un opérateur agissant dans un espace ε ; $|i\rangle$, $i = 1 \dots \dim \varepsilon$ une base orthonormée dans ε , on appelle éléments de matrice de l'opérateur

$$A_{ij} = \langle i | A | j \rangle$$

- Opérateur adjoint ou conjugué hermitique, A^\dagger d'un opérateur A : $(A^\dagger)_{ij} = \overline{A_{ji}} \iff \langle i | A | j \rangle = \overline{\langle j | A^\dagger | i \rangle}$

L'action de l'opérateur adjoint se situe dans l'espace dual :

$$A |\phi\rangle = |\Psi\rangle \iff \langle \phi | A^\dagger = \langle \Psi |$$

- Opérateur hermitique : $A^\dagger = A$.
- Opérateur unitaire $A^\dagger A = A A^\dagger = I \implies A^\dagger = A^{-1}$. Un opérateur ayant cette propriété conserve la norme. En effet

$$\begin{aligned} A |\phi\rangle &= |\Psi\rangle \iff \langle \phi | A^\dagger = \langle \Psi | \\ \langle \Psi | \Psi \rangle &= \langle \Psi | A^\dagger A | \Psi \rangle = \langle \phi | \phi \rangle \end{aligned}$$

4.8 La biréfringence

La biréfringence est une propriété qu'ont certains matériaux transparents vis-à-vis de la lumière. Leur effet principal est de diviser en deux un rayon lumineux qui les pénètre. C'est pourquoi, sur la photographie ci-contre, certaines lettres apparaissent en double derrière un cristal biréfringent.

La biréfringence, encore appelée double réfraction, s'explique par l'existence de deux indices de réfraction différents selon la polarisation de la lumière. Ces deux indices sont appelés indice

ordinaire n_0 et indice extraordinaire noté n_e . La biréfringence est la valeur sans dimension :

$$\Delta n = n_e - n_0$$

sachant que n_0 est l'indice de réfraction de la polarisation perpendiculaire à l'axe d'anisotropie du matériel, tandis que n_e est l'indice de réfraction de la polarisation parallèle à l'axe d'anisotropie

4.9 Opérateur hermitien

Un opérateur u de l'espace hermitien E est dit hermitien si :

$$\forall x \in E, \forall y \in E, (u(x)|y) = (x|u(y))$$

Les opérateurs hermitiens jouent un rôle important en mécanique quantique, car ils représentent les grandeurs physiques. Les valeurs propres (réelles) représentent les valeurs possibles de la grandeur et les fonctions propres (ou vecteurs) les états associés [13].

4.10 Opérateur hamiltonien

L'opérateur hamiltonien H est défini par la forme :

$$\hat{H} = \frac{\widehat{P}^2}{2m} + V(\widehat{r} + t)$$

où

- \widehat{r} est l'observable position.
- \widehat{P} est l'observable impulsion.
- t le temps.
- m la masse.
- V est une fonction à valeurs réelles, appelée potentiel.

4.11 Fonction trace [8]

Définition 4.1 *La trace d'une matrice A est la somme de ses éléments diagonaux. On la définit comme suit :*

$$\text{tr}(A) \stackrel{\text{d\'ef}}{=} \sum_{i=0}^{d-1} \langle i | A | i \rangle,$$

où A est une matrice $d \times d$ et $\{|i\rangle\}$ est une base orthonormée de l'espace de Hilbert de dimension d (H^d). Voici quelques propriétés utiles de la trace :

$$\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B),$$

$$\text{tr}(\lambda A) = \lambda \text{tr}(A),$$

$$\text{tr}(AB) = \text{tr}(BA).$$

Bibliographie

- [1] **J.L. basdevant and J. Dalibar**; *Mecanique quantique*, Eddition de l'école polythec-nique 2011.
- [2] **Steven R. Givant et Paul Richard Halmos**, *Introduction to boolean algebras*. Sprin-ger New York (Undergraduate Texts in Mathematics), 2009.
- [3] **N. J. Cerf, G. Leuchs et E. S. Polzik**, *Quantum information with continuous va-riables of atoms and light*, Imperial College Press, 2007.
- [4] **D. M. Greenberger**, *Bell's theorem without inequalities*, Am. J. Phys., vol. 58, no. 12, page 1131, 1990.
- [5] **M. Le Bellac**; *Introduction à l'information quantique*. Belin, 2005.
- [6] **Lyons, D.W**, (2003) *An elementary introduction to the Hopf fibration*, Mathematics Magazine 76, 87 – 98.
- [7] **C. Cohen-Tannoudji, B. Diu et F. Laloë**, *Mécanique quantique*.
- [8] **Paolo Zanardi**, *A note on quantum cloning in d dimensions*.
- [9] **P. W. Shor**, *Algorithms for quantum computation : discrete logarithms and factoring*. Dans Proc. of the 35th Annual Symposium on Foundations of Computer Science, pages 124–134 (1994).
- [10] **D. Coppersmith**, *An approximate fourier transform useful in quantum factoring*, IBM Research Report RC 19642 (1994).
- [11] **Peter W. Shor**, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, Texte en accès libre sur arXiv : quant-ph/9508027.

-
- [12] **Richard Kidd, James Ardin et Anatol Anton**, *Evolution of the modern photon*, American Journal of Physics 57 (1) (Janvier 1989), pp. 27-35.
- [13] **H.G. Grassmann (1847)**, *Geometrische Analyse*, Leipzig.